**UNIVERSIDAD DE CHILE**
**FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS**
**DEPARTAMENTO DE INGENIERÍA ELÉCTRICA**

# ESTUDIO DE ARQUITECTURAS PARA LA CONVERGENCIA DE TELEFONÍA FIJA-MÓVIL

**MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL ELECTRICISTA**

**PAULINA NATALIA PEÑA ZAMUDIO**

PROFESOR GUÍA:
ALFONSO EHIJO BENBOW

MIEMBROS DE LA COMISIÓN:
HELMUTH THIEMER WILCKENS
NICOLÁS LEIVA DOMIC

SANTIAGO DE CHILE
ABRIL 2007

UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

# "ESTUDIO DE ARQUITECTURAS PARA LA CONVERGENCIA DE TELEFONÍA FIJA-MÓVIL"

PAULINA NATALIA PEÑA ZAMUDIO

| COMISIÓN EXAMINADORA | | NOTA (n°) | CALIFICACIONES (Letras) | FIRMA |
|---|---|---|---|---|
| PROFESOR GUÍA: | | | | |
| SR ALFONSO EHIJO BENBOW | : | _____ | _____ | _____ |
| PROFESOR CO-GUÍA: | | | | |
| SR HELMUTH THIEMER WILCKENS | : | _____ | _____ | _____ |
| PROFESOR INTEGRANTE: | | | | |
| SR NICOLÁS LEIVA DOMIC | : | _____ | _____ | _____ |
| | | | | |
| NOTA FINAL EXAMEN DE TÍTULO | : | _____ | _____ | _____ |

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL ELECTRICISTA

SANTIAGO DE CHILE
ABRIL 2007

RESUMEN DEL INFORME FINAL
PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL ELECTRICISTA.
POR: PAULINA PEÑA ZAMUDIO
PROF. GUÍA: SR ALFONSO EHIJO

# ESTUDIO DE ARQUITECTURAS PARA LA CONVERGENCIA DE TELEFONÍA FIJA-MÓVIL

El acelerado desarrollo de las tecnologías en telecomunicaciones tanto de telefonía fija y móvil como de las redes de datos, junto con el surgimiento de nuevas tecnologías de acceso para proveer distintos servicios han abierto las puertas a nuevos problemas y oportunidades a las empresas. Mientras por un lado, la amplia gama de tecnologías ha permitido un mayor número de servicios y de penetración en los distintos estratos y nichos de usuarios, por otro lado, la interoperabilidad entre distintas redes se ha vuelto un problema no menor.

Desde hace algún tiempo se están viviendo una serie de cambios dentro de las redes de los operadores de telecomunicaciones: ya no basta que una empresa de telefonía ofrezca sólo servicios de telefonía e Internet, o que las empresas distribuidoras de televisión por cable ofrezcan sólo servicios de televisión, sino que todas las redes de telecomunicaciones se están orientando y evolucionando a brindar un amplio espectro de servicios. Este fenómeno se conoce como convergencia de redes o FMC (Fixed Mobile Convergence). El concepto de convergencia fija-móvil se enfoca a la provisión de servicios desde cualquier tipo de terminal y sin importar la red de acceso utilizada. Para eso es necesario hacer que todos los tipos de redes de telecomunicaciones interactúen entre sí, de forma de orientarlas a los servicios y aplicaciones sin importar la naturaleza del acceso utilizado por el usuario. Surgen así conceptos como el de NGN (Next Generation Network) para lograr este objetivo y nuevas arquitecturas integradoras como lo son IMS (IP Multimedia Subsystem).

En este trabajo se presenta un estudio de las principales arquitecturas actuales de telefonía tanto fijas como móviles, donde se contempla la telefonía fija tradicional, celular e IP. Dentro de este estudio se examinan sus componentes funcionales, protocolos e interfaces con la finalidad de plantear y estudiar las arquitecturas y componentes necesarias para que estas redes sean interoperables, planteando una arquitectura convergente y orientada a servicios.

Se expone como resultado principalmente un estudio de la arquitectura IMS como una opción factible para lograr la convergencia, mostrando sus principales entidades y procedimientos de interoperación con otras redes. Además, como un aporte a las tecnologías de acceso inalámbricas emergentes en servicios de redes se plantea una arquitectura con WiMAX como tecnología de acceso y se comparan sus ventajas y desventajas en relación a otras tecnologías de acceso a las redes de telecomunicaciones.

La descripción detallada tanto de las componentes de IMS como paraguas de la convergencia como de los procedimientos de interoperación entre esta arquitectura y diferentes redes de acceso da pie para el desarrollo de nuevas memorias relativas a este tema, como por ejemplo la implementación de una arquitectura convergente a nivel docente basada en IMS utilizando tecnologías de acceso de interés en la actualidad, como lo son las tecnologías inalámbricas y en particular WiMAX. Las futuras investigaciones y trabajos de desarrollo basados en la convergencia de redes son de gran importancia en la formación de ingenieros útiles y valiosos para el mercado de hoy en día.

*"Dedico esta memoria*
*a mis queridísimos padres José y Mirta y*
*a mi amado Mauricio"*

# Agradecimientos

Quiero destacar el gran apoyo que me ha brindado en el trabajo en mi memoria dentro de un grupo con tan buena disposición como lo es el "Team ToIP", grupo de memoristas y ex-memoristas liderado por el señor Alfonso Ehijo, gerente de Ingeniería en Telmex y mi profesor guía. Es a él a quién le agradezco por permitirme realizar con él un trabajo de memoria de un tema tan actual y de mi interés como lo es el actual desarrollo de las redes y la movilidad. Además, le agradezco por su buena voluntad, claridad, consejos y tiempo aún cuando él mismo se encuentra agobiado en muchas oportunidades por un cargo con tantas responsabilidades como es el que tiene.

Le agradezco entonces a mis compañeros de trabajo y a todos los integrantes del Team, en particular a Nicolás Leiva, cuyo apoyo también fue muy importante para mí. Nicolás Leiva es parte del team ToIP y mi profesor integrante, que siempre estuvo dispuesto a ayudarme, aclararme dudas e invirtió mucho tiempo en correcciones y consejos de gran valor para mí.

Por otra parte, agradezco mucho a todas las personas que me han apoyado con su amor y cariño, gracias a mis queridos papás que me han entregado tanto sin exigirme nada, a mis hermanos que cuentan conmigo y a mis "amigas-hermanas" Carolina, Paulina y Marcela que han sido un maravilloso apoyo durante parte importante de mi vida y espero que lo sigan siendo mucho más. Finalmente, gracias a mi amor Mauricio por su apoyo, amor y por entregarme permanente confianza en que puedo lograr este trabajo.

# Índice de Contenidos

# Índice de Figuras

# Índice de Tablas

# Capítulo 1
# Introducción

## 1.1. Motivación

Desde hace algún tiempo hasta ahora, el servicio de telefonía fija ha mantenido constante su nivel de penetración en el mercado y, en algunos casos, ésta se ha visto incluso disminuida en cierto grado. Por otra parte, el surgimiento de la telefonía celular ha tenido un crecimiento explosivo y una alta penetración en el mercado en todo el mundo.

La telefonía celular abrió una nueva era de movilidad y de conectividad para las personas: ahora pueden comunicarse en cualquier momento con quien deseen a través de un teléfono móvil. Estudios internacionales han arrojado como resultado que un número considerable de personas prefieren hablar por celular desde sus casas aún cuando la cobertura celular indoor es deficiente e incluso teniendo la opción de utilizar un teléfono fijo para esa llamada lo que significaría un costo menor y mejor calidad de servicio (La empresa BT, en el lanzamiento de su producto BT Fusion reportó que el 30% de las llamadas celulares en el Reino Unido son originadas en el hogar). Así, el negocio de la telefonía celular ha logrado una penetración en el mercado mundial sumamente alta y, debido a esto, el mercado se ha vuelto altamente competitivo.

Por otra parte, el acceso a redes de Internet por parte de los usuarios ha ido evolucionando desde unos pocos usuarios iniciales a 220 millones de clientes estimados para el 2007 (Bilderbeek, Finger y Vestergaard, [13]). Junto con el crecimiento de los clientes de conexiones a Internet ha ido creciendo la capacidad de dichas conexiones permitiendo cada vez más el acceso de los usuarios a servicios que demandan mayor velocidad de datos. Con el pasar del tiempo, se han desarrollado tecnologías de acceso a Internet más eficientes tanto en capacidad de transmisión de datos como en costo para el usuario, de la misma forma se he mejorado la comodidad del enlace llegando, incluso, a las redes wireless (o inalámbricas), principalmente con tecnología Wi-Fi. Se han implementado muchas de estas redes en forma gratuitas (llamadas hotspots, que son espacios con una red de acceso a Internet a través de Wi-Fi) que se encuentran disponibles para los usuarios en aeropuertos, cafés y universidades (entre otros), las que constituyen una señal de modernidad de parte de las empresas operadoras.

Los usuarios pueden acceder a una serie de servicios que le permiten estar conectado dentro de su espacio tanto laboral como personal. Ya no se trata sólo de telefonía fija, también está la telefonía celular y todos los servicios de voz que pueden ofrecerse a través de Internet junto con un software adecuado partiendo desde una comunicación de voz básica, por ejemplo, a través de MSN

Messenger hasta aplicaciones más sofisticadas donde se puede montar videoconferencia, llamadas simultáneas, etc.

Es así, dada esta gran cantidad de recursos de comunicaciones y el surgimiento e implementación creciente de tecnologías de acceso wireless a Internet, que las personas han ido adquiriendo cada vez más movilidad en sus trabajos y en su vida en general. Sin embargo, la innovación en productos de telecomunicaciones ha creado mayor complejidad para los usuarios. El abanico de alternativas disponibles para la comunicación abre una problemática que tiene que ver con la interoperación que debiera existir entre dichos servicios de comunicaciones. Un ejemplo de este escenario es el siguiente: Juan está disponible solamente para comunicarse en línea a través de un programa como Messenger. Hasta hace poco tiempo, Juan no podría ser alcanzado por Ana, la que desea comunicarse con él, pero sólo cuenta con un teléfono móvil o celular. Sin embargo, ya es posible la interoperación entre algunos programas como Messenger y la telefonía celular de forma que Juan y Ana puedan comunicarse.

Así, si un cliente deseara cubrir todas las alternativas vigentes de telecomunicaciones debiera llevar consigo aproximadamente 6 tipos de terminales distintos y su tasa de éxito para comunicarse con un compañero de trabajo en el primer intento sería del 36% (Santarelli, [35]). Y no sólo la cantidad de formas de comunicación sería un problema sino que la cantidad de cuentas y alternativas tarifarias para cada uno de estos equipos hacen una situación bastante engorrosa para el usuario.

Surge entonces el concepto de Convergencia Fija-Móvil o FMC (Fixed-Mobile Convergence) como la solución para el complejo problema de interoperabilidad planteado en los párrafos anteriores. Esta solución implica que un usuario pueda acceder a todos los servicios que tenga contratados desde un terminal único y a través de cualquier red de acceso sin importar su naturaleza, es decir, desde la red xDSL del hogar, Wi-Fi, Bluetooth o desde una red celular, entre otros.

Que una arquitectura de red convergente sea independiente de la tecnología de acceso abre las puertas para que las empresas de telecomunicaciones que no cuentan con última milla instalada (empresas conocidas como CLEC, sigla en inglés que significa Competitive Local Exchange Carrier) puedan optar por brindar servicios al usuario final sin tener la necesidad de utilizar las redes de terceros para llegar a éstos (desagregación de redes) sino que por medio de la instalación de tecnologías de acceso inalámbrico de bajo costo de implementación como lo es, por ejemplo, la tecnología WiMAX, que es una tecnología que está en constante actualización de sus capacidades y que podría permitir en el futuro su implementación como tecnología de acceso móvil. De esta forma, comienza a derrumbarse una de las mayores barreras de entrada para nuevos operadores de telecomunicaciones: La inversión inicial en que deben incurrir para desplegar redes de acceso.

## 1.2. Objetivos Generales

Se busca establecer la arquitectura de red necesaria para migrar y finalmente ofrecer servicios convergentes de red y determinar las ventajas y desventajas de la utilización de WiMAX como tecnología de acceso a una red de telefonía convergente.

## 1.3. Objetivos Específicos

- Ordenar y especificar las principales arquitecturas necesarias y la evolución de las redes actuales hacia dichas arquitecturas para brindar servicios convergentes.
- Identificar y analizar dichas arquitecturas y sus principales características como protocolos, bloques funcionales e interfaces utilizadas para brindar servicios de redes convergentes.
- Caracterizar la tecnología WiMAX junto con sus avances como tecnología de acceso wireless y discutir la factibilidad de su utilización en servicios de convergencia.
- Plantear una solución de arquitectura convergente y los principales factores de factibilidad de su implementación.

## 1.4. Estructura de la Memoria

La consumación de esta memoria se basa en las siguientes labores a realizar:

- Estudio del desarrollo de las telecomunicaciones a nivel internacional.
- Estudio de los servicios de convergencia fija-móvil.
- Estudio de las principales arquitecturas de redes de telefonía.
- Estudio de arquitecturas convergentes.
- Descripción de interoperación de componentes entre las distintas redes.
- Descripción del funcionamiento de la red convergente.
- Estudio comparativo entre la arquitectura convergente y la PSTN.
- Análisis de WiMAX como tecnología de acceso.

# Capítulo 2
# Antecedentes

## 2.1. Evolución de las Telecomunicaciones en el Mundo

Los servicios de telecomunicaciones generalmente se engloban en el término TIC que quiere decir Tecnologías de la Información y la Comunicación y que incluye tanto servicios de telefonía de línea fija, móvil como servicios de acceso a Internet.

La industria de las telecomunicaciones se ha caracterizado siempre por un avance continuo tanto en los aspectos regulatorios como tecnológicos. El crecimiento de las TIC se ha visto beneficiado por dos hechos: la privatización y la apertura de los mercados a la competencia. Así, en América la privatización de los operadores tradicionales de telecomunicaciones ha alcanzado un 74% y los niveles de competencia en servicios de Internet alcanzan el 93%, en telefonía móvil es del 76% y en telefonía fija, 61% (datos obtenidos para el año 2005). Es la competitividad la que ha provocado un aumento en el flujo de inversiones en las telecomunicaciones y al mismo una serie de fusiones y adquisiciones (un ejemplo claro de esto es la fusión Metrópolis-VTR y Telefónica Móvil-BellSouth). Asimismo, las grandes empresas telefónicas han comenzado a incorporar nuevos productos y tecnologías como la IPTV a través de ADSL o ADSL2+.

Es importante destacar que, aunque el crecimiento de las TIC ha sido incesante, no se observa el mismo nivel de crecimiento en todo el mundo, observándose una brecha tecnológica entre países desarrollados y países en desarrollo además de diferencias entre las distintas clases sociales dentro de un mismo país. Con el pasar del tiempo, estas divergencias han tendido a sesgarse y se espera que siga así. Sin embargo, la brecha aún es considerable. Este fenómeno se observa en la Figura 1 y Figura 2 (ITU, [22]).

Cada una de estas figuras describe dos casos diferentes. En cuanto a la telefonía móvil el número de abonados se mantiene en aumento para todo el mundo aunque se observa una clara diferencia en los niveles de penetración para cada grupo.

En cambio, la telefonía fija pareciera haber estancado su crecimiento. Sin embargo, más que una condición estática se observa que los países desarrollados (naciones con mayor penetración de líneas fijas) han ido disminuyendo su porcentaje de líneas fijas mientras que los países en vías de

desarrollo (naciones con menor penetración) han experimentado un crecimiento del porcentaje de líneas fijas.

El aumento en la penetración de la telefonía móvil junto con el estancamiento o disminución de la telefonía fija abren el debate sobre si estos dos tipos de telefonía son sustitutivos. En estudios estadísticos realizados se ha encontrado que, aunque el número de líneas móviles superan a las fijas, la cantidad de minutos hablados a través de las fijas ha aumentado, principalmente debido a la diferencia de precios de ambos servicios, por lo que se deduce que son complementarias. Aún en países en que la telefonía móvil se encuentra en una etapa de baja de precios, el nivel sustitutivo es débil, encontrándose que ambas alternativas no son sustitutos cercanos.

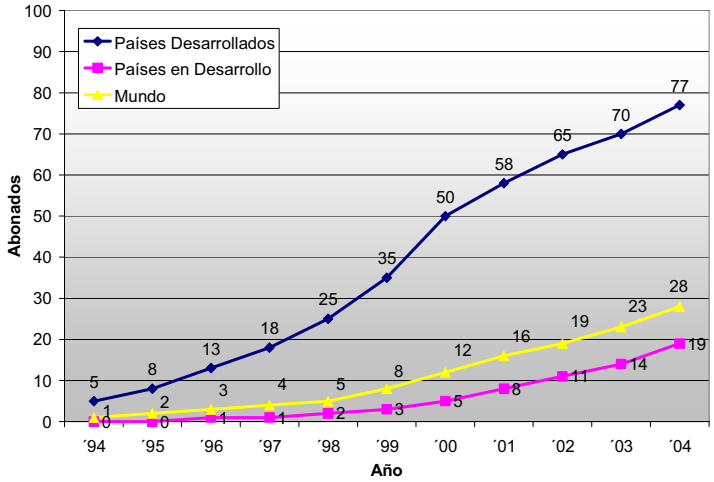



**Figura 1: Número de Abonados Móviles por cada 100 Habitantes.**

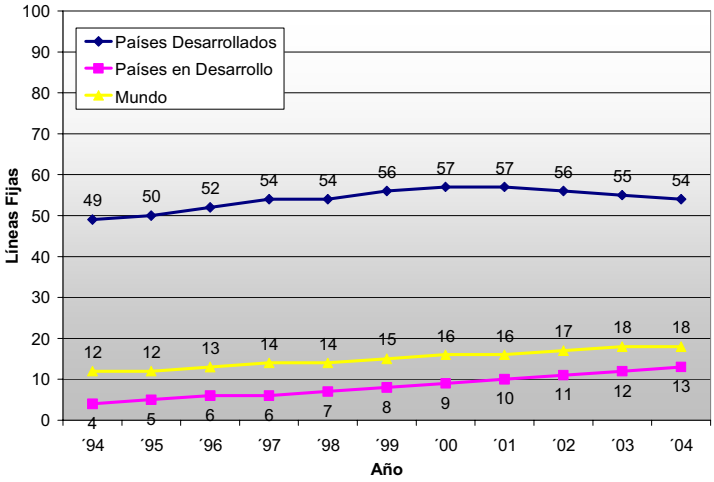



**Figura 2: Número de Líneas Fijas por cada 100 Habitantes**

Los servicios de línea fija corresponden a la tecnología de telecomunicaciones que menos cambios ha experimentado en el tiempo y, debido al ingreso de las empresas de televisión por cable al mercado de la telefonía fija, las ILECs (Incumbent Local Exchange Carrier) corren el riesgo de seguir disminuyendo su participación en el mercado. Por otra parte, el éxito mundial de la telefonía móvil se debe a varios factores tales como la introducción de las tarifas de prepago, la subvención de equipos en algunos países y la disponibilidad de servicios como la mensajería corta (SMS).

En cuanto a los servicios 3G GSM de telefonía móvil, dada la brecha tecnológica existente es muy poco probable que los operadores de países en desarrollo la ofrezcan en un futuro muy próximo. El mayor uso de esta tecnología no se ha visto, como se tendería a pensar, en Europa, sino que en América del Norte y en Asía Pacífico, zonas que concentran aproximadamente el 93% de los abonados a dicha tecnología. Ya en el año 2004, Estados Unidos, Corea y Japón concentraban por sí solos el 75% de los abonados a tecnologías 3G.

La Figura 3 (ITU, [22]) muestra la distribución de abonados a tecnologías 3G a nivel mundial para el año 2004. Es importante mencionar que el número total de abonados a estas tecnologías durante el 2004 alcanzaba los 160 millones de clientes.

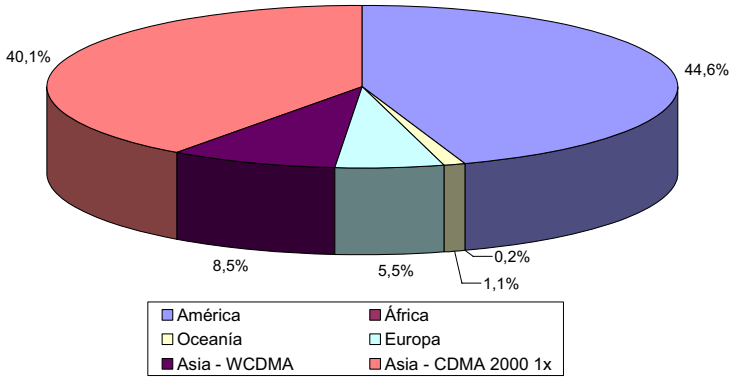



**Figura 3: Distribución Mundial de Abonados a Servicios 3G, Año 2004.**

Con respecto a la disponibilidad de acceso a Internet, la evolución de este servicio ha sido notable aunque aún falta mucho para disminuir la brecha tecnológica entre los distintos países y clases sociales. En el año 1988 había solamente 8 países con acceso a Internet, en el año 2003, el número de países con acceso a Internet alcanzaba los 209. Para el 2004, se estimó que el 13,2% de la población del mundo tendría acceso a Internet, como se muestra en la Figura 4 (ITU, [22]).

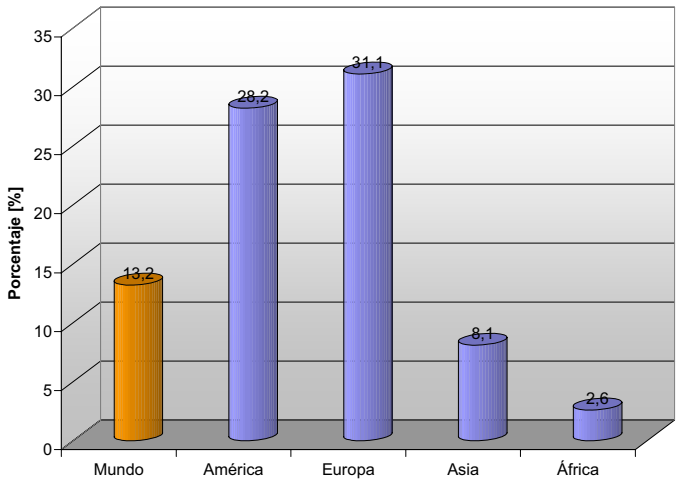



**Figura 4: Tasa de Penetración de Internet por Continente, Año 2004.**

Sin embargo, es importante notar que estas tasas de penetración no son uniformes en cada continente. En la zona de Asia Pacífico el acceso a Internet alcanza el 60% en países tales como la

República de Corea, Australia y Nueva Zelanda, mientras que no supera el 5% en países como Bangla Desh y Camboya. Por otra parte, hay países en África en que el acceso a Internet tiene una penetración del 50%.

Un factor importante dentro del desarrollo de las telecomunicaciones es el acceso a Internet a través de tecnologías de Banda Ancha. Las tecnologías de Banda Ancha, al contar con una mayor velocidad de datos permiten el desarrollo de nuevos servicios en Internet más exigentes en cuanto a tasa de transferencia. Estos servicios pueden ir desde aplicaciones recreativas, didácticas hasta la creación de nuevos negocios y servicios públicos. Para el 2004, se tenía que el 2,5% de la población mundial tenía acceso a estas tecnologías, lo que constituye el 38% del total de los usuarios a Internet.

La Banda Ancha sigue, por consiguiente, en aumento tanto que incluso en algunos países las conexiones de banda ancha han superado por mucho al número de conexiones por módem. Así, además de los sitios "HotSpots" (con tecnología Wi-Fi) que han tenido gran éxito en algunos países, se está comenzando a hacer pruebas pilotos con tecnología WiMAX.

## 2.2. Crecimiento de las Telecomunicaciones en Chile

Chile es un país que no se ha visto exento de la evolución en telecomunicaciones que ha experimentado el mundo. La competitividad del mercado de Telecomunicaciones ha permitido una serie de fusiones de empresas a partir del 2004, como por ejemplo entre Telefónica Móvil y Bellsouth (actual Movistar) y entre VTR y Metrópolis, lo que demandó la participación del Tribunal de Defensa de la Libre Competencia. Asimismo, se han producido una serie de adquisiciones, dentro de las que destaca la adquisición de Smartcom por Telmex.

En la Figura 5 se muestra la evolución de los servicios de telefonía fija, móvil y acceso a Internet entre los años 2000 a 2004.

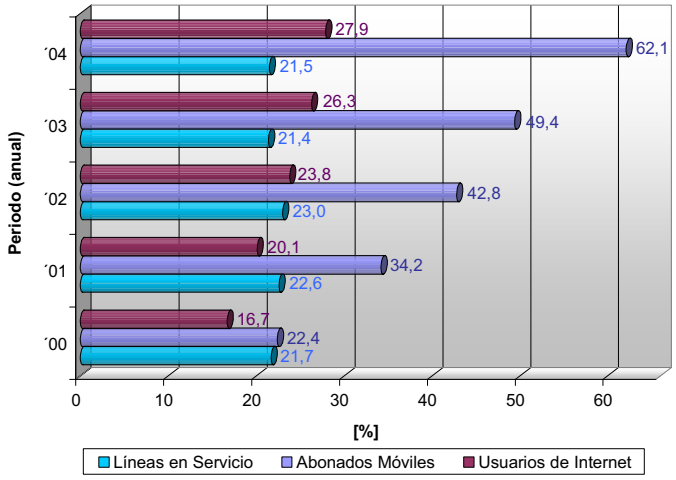



**Figura 5: Evolución de la Penetración de Servicios de Telecomunicaciones en Chile.**

Lo primero que se observa es que las líneas de telefonía fija en servicio comienzan a aumentar después de un periodo en que la tendencia de éstas era a disminuir. Así mismo, la cantidad de abonados móviles han aumentado vigorosamente en el tiempo alcanzando una penetración de 62,1

abonados por cada 100 habitantes. Al mismo tiempo que ha aumentado el número de abonados, también ha aumentado el uso que se hace de servicios de valor agregado en los servicios móviles como en el caso de la mensajería SMS además del servicio básico de voz. En relación al crecimiento de la penetración a Internet, la cantidad de conexiones alcanzó un total de 940'695 mostrando un aumento de conexiones dedicadas y disminución de las conmutadas.

En cuanto a la telefonía fija cabe destacar dos tecnologías diferentes para brindar este servicio y que son las líneas analógicas y digitales. Las líneas analógicas son las tradicionales de una red PSTN (Public Switched Telephone Network) mientras que las líneas digitales corresponden a las ofrecidas por empresas de Televisión por Cable e ISDNs (Integrated Services Digital Network) y corresponden a una tecnología de hace pocos años que le han entregado un nuevo impulso al mercado de la telefonía fija.

La Figura 6 muestra la evolución de las dos tecnologías de líneas fijas en los últimos años en el país. La telefonía digital ha tenido una tasa de aumento del 11% desde el periodo de diciembre del 2004 a junio del 2005, mientras que en ese mismo periodo la tasa de aumento de la telefonía analógica es del 2%. Sin embargo, es importante notar que estos porcentajes de crecimiento son relativos ya que la telefonía fija analógica posee alrededor de 3'120'000 líneas y la telefonía digital no alcanza las 220'000 líneas.

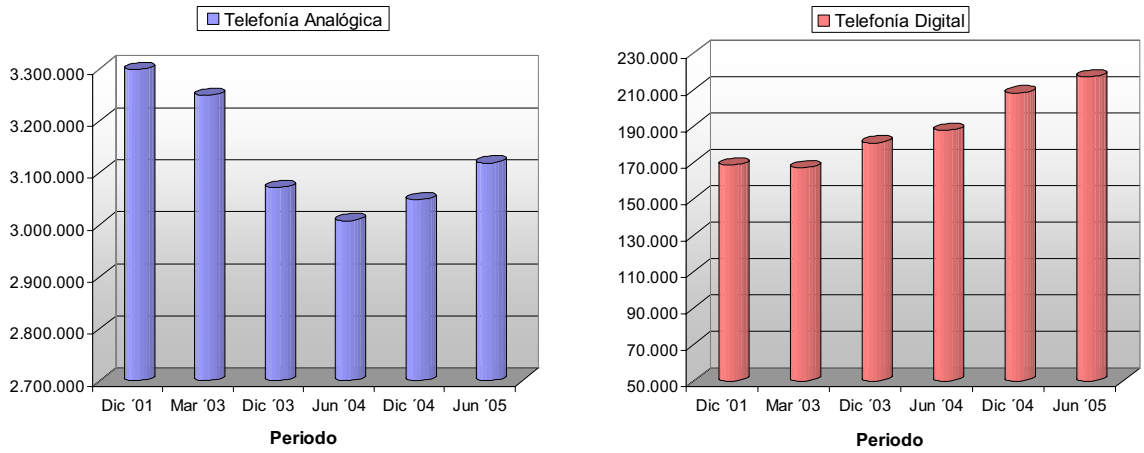



**Figura 6: Evolución de Telefonía Fija Analógica y Digital**

Con relación a las conexiones a Internet, éstas se pueden dividir en dos grandes grupos:

- Conexiones conmutadas: Una conexión de este tipo corresponde a un usuario que se conecta a Internet llamando desde su teléfono. Las tecnologías que se distinguen en Chile para este tipo de conexión son:
  - Telefónica Analógica.
  - ISDN (Integrated Services Digital Network).
- Conexiones dedicadas: Dentro de este tipo de conexión se distinguen las siguientes tecnologías:
  - ADSL (Asymmetric Digital Subscriber Line).
  - Cable Módem.
  - Otras tecnologías: En este conjunto se engloban tecnologías de acceso dedicado vía enlace satelital dedicado, Frame Relay, Wireless Local Loop, HDSL, Ethernet y ATM.

En la Figura 7 (SUBTEL, [38]) se muestra la distribución de tecnologías de acceso a Internet, tanto para conexiones conmutadas como dedicadas. Claramente se observa un rápido crecimiento en las conexiones dedicadas y que las conexiones conmutadas han disminuido, esto debido a las tasas de transferencia superiores que alcanzan las conexiones dedicadas en comparación con las conmutadas.

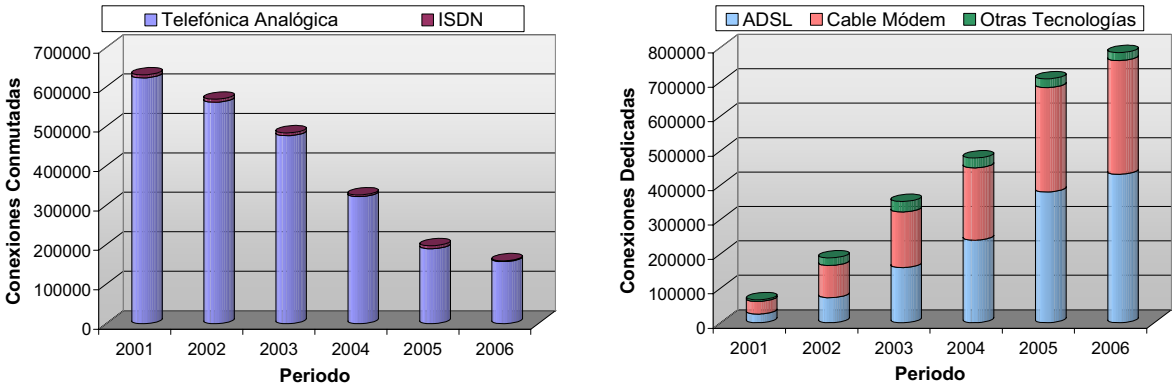



**Figura 7: Distribución de Tecnologías de Acceso a Internet en Chile.**

## 2.3. Fixed – Mobile Convergence (FMC)

Como se mencionó en la sección anterior, el número de tecnologías disponibles hoy en día hacen que las personas y empresas posean una elección sumamente amplia en cuanto al acceso en las telecomunicaciones. Por un lado, este fenómeno permite que sea más fácil contactar personas pero por otro lado se hace cada vez más difícil mantenerse en contacto con la parte deseada a través del medio apropiado y de forma eficiente.

La ETSI (European Telecommunications Standards Institute) define el concepto de FMC como el préstamo de capacidades de red independientes de la técnica de acceso. Es importante destacar que esta definición no implica la convergencia física de redes, sino que se involucra con el desarrollo de una arquitectura de red convergente y los estándares que la soporten; este conjunto de estándares debiera ser capaz de entregar servicios fijos, móviles o híbridos.

Así, el objetivo de la convergencia fija-móvil es entregar servicios de comunicaciones centrados en el cliente en vez de una tecnología de acceso a la red. Esto implica un cambio fundamental en la forma en que las comunicaciones mundiales funcionan actualmente. FMC busca combinar la conveniencia, libertad de movimiento y servicios personalizados del mundo inalámbrico con la calidad de servicio de las comunicaciones fijas. De esta forma, los usuarios estarán siempre conectados mientras el servicio de comunicaciones de la red optimiza el enrutamiento a través de balanceo de calidad, cobertura y ancho de banda eficiente.

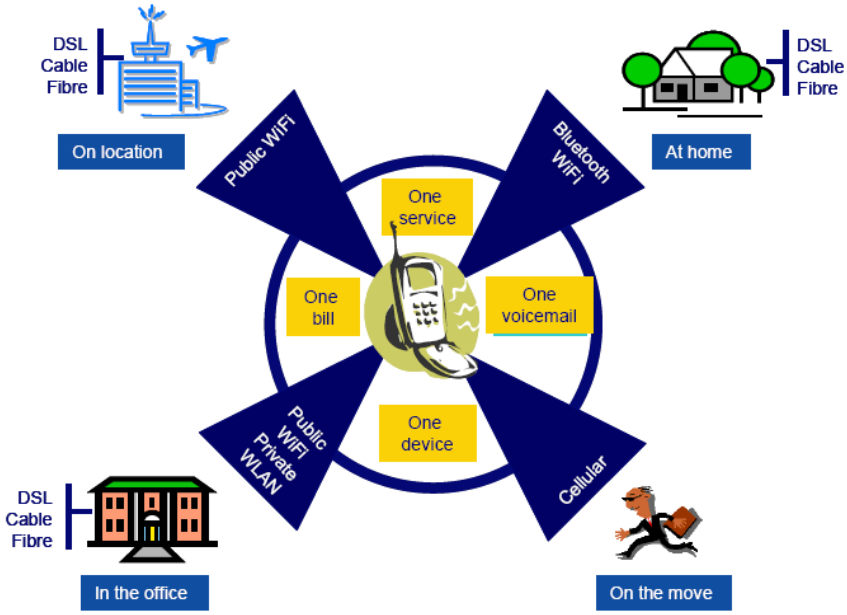



**Figura 8: Concepto básico de FMC.**

## 2.3.1. Características de un Servicio FMC

Como se mencionó anteriormente, un servicio FMC debe permitir al usuario el acceso a un amplio rango de comunicaciones, información y servicios de entretenimiento, con calidad de servicio permanente sin importar el terminal utilizado, la ubicación de usuario o la red sobre la cual corren las aplicaciones. Así, un servicio FMC debiera tener una o más de las siguientes características:

- Uniformidad: Puede estar en el terminal, arquitectura y/o nivel de servicio. A nivel de terminal y de red, esto se presenta en el llamado handoff: Las llamados originadas en la red móvil pueden moverse a una red fija y viceversa, o entre diferentes redes wireless como Wi-Fi y 2G, sin interrupción o cambio en la calidad de servicio. A nivel de arquitectura, esto es transferir aplicaciones de una plataforma de red a otra, sin necesitar codificación complicada o traducción.
- Flexibilidad en métodos de acceso: Los servicios de convergencia y terminales permitirán a los clientes usar la tecnología de acceso más apropiada, como celular o Wi-Fi, basados en criterios tales como ubicación actual, aplicación requerida, calidad de servicio y tarifa de llamadas.
- CPE Convergente (Converged Customer Premise Equipment): O equipamiento local para el cliente convergente. La disponibilidad de CPE permitirá a los clientes moverse entre tipos de acceso más fácilmente. Los usuarios actuales poseen generalmente un teléfono de línea fija para voz a bajo costo y acceso a Internet y un teléfono móvil para voz inalámbrica y quizás aplicaciones básicas de datos como SMS. Los usuarios de empresas, comúnmente tienen más terminales como un PDA o un laptop para datos móviles. Sin embargo, la entrada de CPEs como teléfonos Wi-Fi permitirán a los usuarios usar un terminal para acceder a las aplicaciones a las que actualmente accede con algunos dispositivos.
- Personalización: Los servicios FMC permiten al usuario final decidir el conjunto de servicios a recibir tan bien como la apariencia y ambiente de la interfaz de usuario del terminal. La disponibilidad del CPE dará a los usuarios una identidad unificada. Por ejemplo, en vez de que los usuarios deban configurar un dispositivo móvil y luego uno fijo,

cada uno con el mismo conjunto de servicios como libreta de direcciones personalizada, sólo deberán hacerlo una vez para un dispositivo. Hoy, la personalización está asociada principalmente con el mundo móvil, como los dispositivos móviles incluyen una mayor variedad de opciones de personalización que los dispositivos fijos. FMC llevará la personalización al ámbito de la línea fija.

- Lo mejor del mundo celular, fijo e inalámbrico: Un servicio FMC debe unir la libertad de la movilidad con la seguridad, calidad de servicio, mayor ancho de banda y menores costos de los servicios de línea fija. Esto es posible a través del uso de varias redes, ya sean celular, fija o inalámbrica.

### 2.3.2. Etapas de la Convergencia

La adopción y migración de la convergencia fijo-móvil ocurrirá en una serie de etapas, en las cuales están trabajando una amplia variedad de industrias. Sin embargo, la adopción de FMC está condicionada por el panorama existente en cada país en términos de niveles de competencia, regulación, infraestructura y requerimientos de usuario lo que ha permitido la existencia de variados modelos del desarrollo de la convergencia adaptados a la realidad de cada país.

La evolución común considerada para FMC considera tres etapas donde las dos primeras se definen como de pre-convergencia y se basan en la forma en cómo el servicio es vendido y lanzado al mercado en vez de cambios de infraestructura de la red o de la interfaz de usuario. La tercera etapa se define como de convergencia ya que implica cambios fundamentales en la infraestructura de red como en los terminales de usuario. Las etapas son:

- Convergencia Comercial: Lanzamiento de "bundles" (lotes, referido a un conjunto) con múltiples servicios con un precio.
- Convergencia a Nivel de Producto: Como por ejemplo un buzón de mensajes único para teléfono fijo y móvil.
- Convergencia de Terminales y de Red: Existencia de un único dispositivo para múltiples tipos de acceso y aplicaciones junto con la existencia de continuidad en cuanto al handoff entre redes.

En la Figura 9 se muestra una tabla con las etapas propuestas por la IDC para la convergencia.

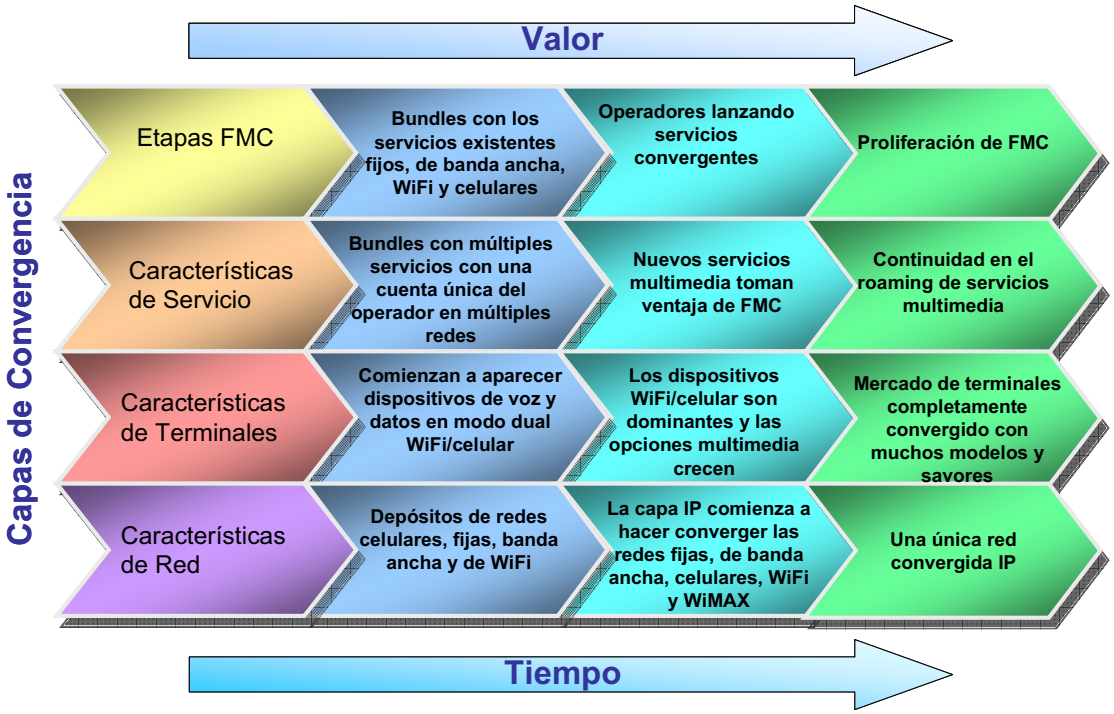



**Figura 9: Etapas de adopción de FMC.**

## 2.3.3. Proposición de valor al Cliente de FMC

FMC propone cambios en las arquitecturas y servicios de red que no son igualmente vistos por los usuarios finales como por las empresas. Así, se describirán brevemente las proposiciones de valor para cada uno de estos clientes.

### 2.3.3.1. Proposición de valor al Consumidor

FMC se enfoca a presentar a los consumidores una experiencia de comunicación uniforme tanto dentro como fuera del hogar. En su forma más extrema, esta experiencia de consumidor uniforme puede entregar un terminal, un servicio y un precio. Los clientes estarán siempre conectados, mientras el servicio de comunicaciones balanceará la calidad, cobertura y ancho de banda eficientes, presentando al cliente con la mejor experiencia posible donde sea que esté. Los beneficios del consumidor serán por su conveniencia y simplicidad, activando nuevos servicios al mismo tiempo. Estos beneficios pueden incluir:

- Un terminal y número de teléfono por miembro de la familia.
- Una cuenta combinando servicios sobre redes fijas y móviles (celular y wireless).
- Una guía de teléfonos y un buzón de voz.
- Mejor calidad para las llamadas móviles indoor.
- Menor costo para las llamadas móviles en el hogar.
- La disponibilidad de música, e-mail, juegos, videos y otros servicios en el hogar o mientras se está a través de otras casas con FMC activado o hotspots Wi-Fi para menores costos y mayores velocidades.

- La disponibilidad de ambientes wireless con altas velocidades y con múltiples sesiones posibles desde la misma casa a menor costo y mayor calidad.
- Balanceo de calidad de servicio, cobertura y eficiencias de ancho de banda.

Es importante destacar que no todos los consumidores pueden beneficiarse de esta experiencia. El principal pre-requisito para el concepto actual de terminal único de FMC es la existencia de una conexión de banda ancha a Internet, tal como xDSL o cable junto con una instalación Wi-Fi o Bluetooth.

### 2.3.3.2.Proposición de valor a la Empresa

Actualmente, muchas compañías están experimentando la creciente movilidad de su fuerza de trabajo, tales como ejecutivos viajando a través del mundo, vendedores en campo y telefonistas operando desde el hogar ciertas horas del día. Se observa entonces que la línea entre el hogar y lugar de trabajo y entre ocupación y recreación se hace cada vez más difusa.

La mayoría de las empresas están de acuerdo que la eficiencia de los empleados y la satisfacción del cliente aumentarían si los servicios de voz y datos de la empresa se movilizaran más; sin embargo, el costo de la movilidad es un gran problema de las empresas actualmente. La realidad actual es que muchos empleados tienen un teléfono de línea fija en su escritorio y un teléfono móvil adicional para ser contactados fuera de la oficina.

FMC combinado con la telefonía IP y el uso de tecnologías inalámbricas puede lograr que una empresa evite costos en infraestructura y en llamadas móviles en la oficina, es decir, los empleados pueden ser ubicados más eficientemente. Sin embargo, en la actualidad, el costo de implementar un servicio convergente es prohibitivo para la gran mayoría de las empresas fuera de los servicios de voz.

Los beneficios de FMC para las empresas incluyen:

- Los funcionarios estarán siempre conectados por telefonía, mail y las aplicaciones de la empresa, lo que aumentará la eficiencia y satisfacción del cliente.
- Los funcionarios utilizarán un terminal, una suscripción y un número, lo que disminuye los costos, aumenta la manejabilidad y simplifica las cuentas a través de los registros de llamadas.
- Las mejoras en los costos totales de la empresa pueden ser logradas a través de PBX, servicios móviles e infraestructura de red.
- Nuevos servicios de comunicación para la empresa tales como presencia, mensajería y conferencia instantánea y otros servicios multimedia disponibles.
- Balanceo de calidad de servicio, cobertura y eficiencia del ancho de banda.

Esto no implica un camino fácil para las empresas, ya que el cambio debe ir acompañado de seguridad móvil punto-a-punto y la integración con las redes ya existentes.

## 2.4. Conceptos Básicos de Comunicaciones Móviles

### 2.4.1. Celda

El concepto de celda, surge para solucionar el problema dado por el limitado número de usuarios que brinda la telefonía inalámbrica con una única antena por zona y la alta potencia que debía ser emitida por la antena tanto como por los propios terminales para establecer un enlace de comunicación. De esta forma, se divide la zona a que se le quiere brindar cobertura en varias sub-zonas o celdas, cada una con una antena que puede establecer cierto número de llamadas.

Dado que cada antena cubre una zona de radio reducido, la emisión de potencia es elegida de forma de minimizar la interferencia causada por el reuso de frecuencias en las celdas posteriores. Además, las celdas por lo general se configuran en grupos de de 7 llamados "clúster" cada uno con diferente frecuencia, de forma que se vayan repitiendo en la zona como un patrón, como se observa en la Figura 10.

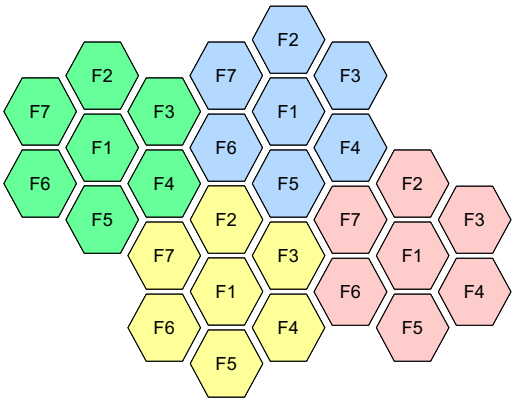



**Figura 10: Clústers de 7 Celdas.**

Como se observa en la Figura 10, las celdas son representadas como figuras hexagonales; sin embargo, esta representación es sólo explicativa y la verdadera forma de una celda depende de las características del terreno y de la propagación de radio.

***(a) Tres Sectores*** ***(b) Seis Sectores***

**Figura 11: Tipos de Sectorización de Celdas.**

Si se produce que, a pesar de las celdas configuradas, comienza a producirse congestión de tráfico en cada una de ellas, entonces las celdas pueden subdividirse en celdas más pequeñas de manera de entregar servicios a más clientes. La antena dentro de una celda puede ser omnidireccional

o direccional. Si es omnidireccional, entonces la antena estará ubicada en el centro de la celda. Si la antena es direccional, lo más común es que tenga una cobertura de 120º (antena de tres sectores) o de 60º (antena de seis sectores). En la Figura 11 se muestra la sectorización con estos dos tipos de antenas.

### 2.4.2. Handoff

Se conoce como handoff al procedimiento de traspasar una llamada en una canal de voz dentro de cierta celda hacia otro canal en otra celda o dentro de la misma. Existen dos tipos principales de handoff:

- Hard handoff: Consiste en el cambio de frecuencia cuando se pasa de un canal de comunicación a otro (FDMA - TDMA).
- Soft handoff: Consiste en el cambio de código (CDMA) al pasar de un canal de comunicación a otro.

Además, es muy importante saber administrar el handoff dentro de una red desde una celda hacia otra debido a que pueden ofrecerse inestabilidades entre celdas lo que produce un efecto de ping-pong y que, dado el caso, obliga a que se produzca un handoff forzado.

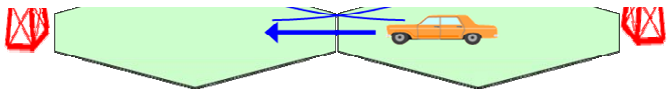


**Figura 12: Administración del Handoff.**

El handoff puede producirse gracias a la superposición de las celdas. El terminal necesita una potencia mínima recibida desde la antena para que se produzca la comunicación; así puede cambiar su enlace desde una celda a otra cuando la potencia recibida desde la antena de la primera celda resulta ser inferior a la potencia mínima de recepción tolerada por el terminal o a la potencia recibida desde la antena de la otra celda.

### 2.4.3. Roaming

El concepto de roaming se basa en la capacidad de que un terminal funcione en una zona de cobertura que no corresponde a su red de procedencia (más conocida como red Home). En esa red visitada, el usuario puede hacer y recibir llamadas (o iniciar sesiones en el caso de un servicio no celular) como si fuera la red local en un proceso que le es transparente.

La implementación del roaming se hace posible gracias a la interconectividad que existen entre las bases de datos y redes de distintos proveedores d servicio.

### 2.4.4. Enlaces Uplink y Downlink

Dentro de las telecomunicaciones, se producen dos tipos de enlace:

- Enlace Uplink: Es la información transmitida desde el terminal hacia la estación base.
- Enlace Downlink: Es la información transmitida desde la estación base al terminal.

### 2.4.5. Comunicaciones Dúplex

Se le denomina comunicación dúplex a aquellas en que el flujo de información (voz y/o datos) puede ser transmitido por todos los participantes de dicha comunicación. Se destacan dos tipos de comunicaciones dúplex:

- Half-dúplex: En que el flujo de datos fluye ya sea en un sentido o el otro, es decir, no hay transmisión simultánea de las dos partes.
- Full-dúplex: En que los flujos de datos de cada una de las partes pueden ser enviados simultáneamente.

Ahora, cuando se tiene un acceso punto-a-multipunto y las comunicaciones uplink y downlink utilizan el mismo medio físico, como es el caso celular, suelen utilizarse métodos de duplexación, tales como:

- TDD (Time Division Duplex): Consiste en la aplicación de TDMA para separar los flujos de uplink y downlink. Su ventaja es que las velocidades de transmisión de estos flujos pueden ser asimétricas.
- FDD (Frequency Division Duplex): Consiste en la aplicación de FDMA para separar los flujos de uplink y downlink. Este método es mucho más eficiente para enlaces con tráfico simétrico.

### 2.4.6. Tipos de Acceso en la Interfaz Radioeléctrica

Los tipos de acceso utilizados en la telefonía celular son básicamente tres, y son los que se explicarán a continuación.

#### 2.4.6.1.FDMA: Frequency Division Multiple Access

Corresponde simplemente a la modulación en frecuencia de la voz, este tipo de acceso a la red se utilizaba en los sistemas celulares analógicos, por lo que fue el primer método de acceso de telefonía celular. En la Figura 13 se muestra un tipo de acceso FDMA que era el utilizado en AMPS.

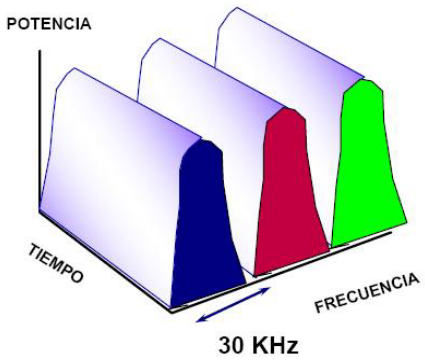
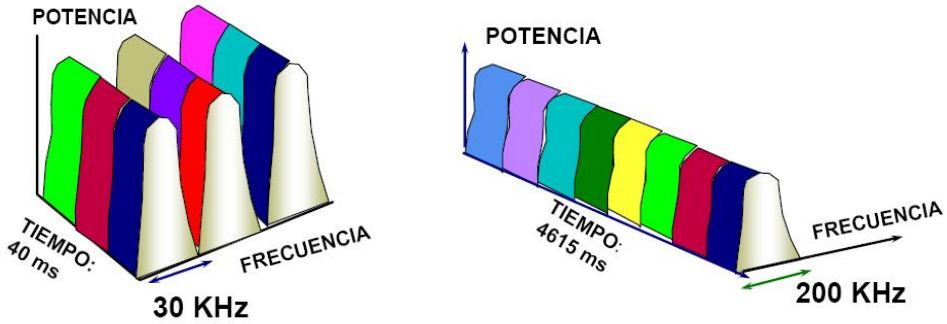



**Figura 13: Frequency Division Multiple Access (FDMA).**

### 2.4.6.2.TDMA: Time Division Multiple Access

Corresponde propiamente a los sistemas digitales ya que discretiza el tiempo en unidades de largo fijo llamadas time-slots. TDMA por lo general es utilizada en conjugación con FDMA para brindar más canales de acceso en cada célula.

En la Figura 14 se muestran dos aplicaciones de TDMA para dos tecnologías distintas. La imagen de la izquierda muestra la configuración de TDMA y FDMA que era utilizada en la tecnología D-AMPS (Digital AMPS), aquí se observan tres canales de tiempo por frecuencia donde cada time-slot tiene una duración de 40 ms. Por otra parte, en la figura de la izquierda se muestra una aplicación TDMA de la tecnología GSM, en este caso se tienen ocho time-slots por frecuencia en que cada time-slot tiene una duración de 4615 ms.




***(a) Utilización en D-AMPS*** ***(b) Utilización en GSM***

**Figura 14: Time Division Multiple Access.**

### 2.4.6.3.CDMA: Code Division Multiple Access

CDMA es una tecnología que aumenta la capacidad de la telefonía celular mediante una transmisión en una amplia porción del espectro. Así, cada señal de voz es enviada en todo el ancho del espectro pero está multiplicada por un código seudo-aleatorio único con una tasa de bits mucho más alta que el mensaje de voz, por lo que se crea un efecto de ensanchamiento de la banda de frecuencia.

La idea es que la cantidad de códigos que son multiplicados por la señal de voz son ortogonales entre sí de forma que un mensaje debe ser decodificado por el receptor con el mismo código de forma que no se pierda la información original. De esta manera, toda la información que

no corresponda a la que se desea recibir es eliminada debido a la ortogonalidad de los códigos, apareciendo como un ruido aleatorio que es ignorado.

CDMA es considerada superior a los otros métodos de acceso por varias empresas y organizaciones. Sin embargo, CDMA sólo funciona si todas las señales de radio recibidas poseen la misma potencia ya que si una señal es mucho más potente que las otras, esta señal dominante hará que el resto no se pueda recuperar. La Figura 15 muestra la relación que tiene CDMA con los dominios del tiempo y la frecuencia.

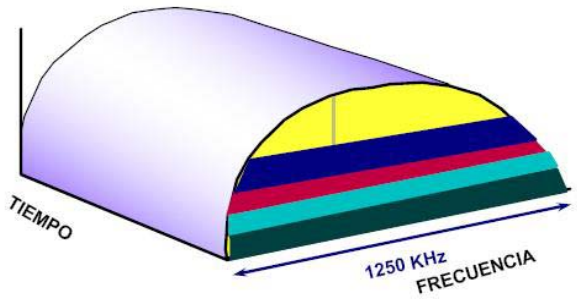



**Figura 15: Code Division Multiple Access.**

## 2.5. Next Generation Network (NGN)

Una red NGN (en castellano, Red de Próxima Generación) responde a la visión final de una red que cumpla con todos los requerimientos de una red convergente universal (Figura 16).

Al pasar el tiempo, se han introducido al concepto de red nuevas atribuciones y necesidades para las cuales originalmente no estaba diseñada. Así, la recomendación de la ITU-T (International Telecommunication Union – Telecommunication Standardization Sector) Y.2001 identifica cierto número de características necesarias de una red NGN y en su recomendación Y.2011 entrega una marco general de la arquitectura necesaria para cumplir con los requerimientos deseados.

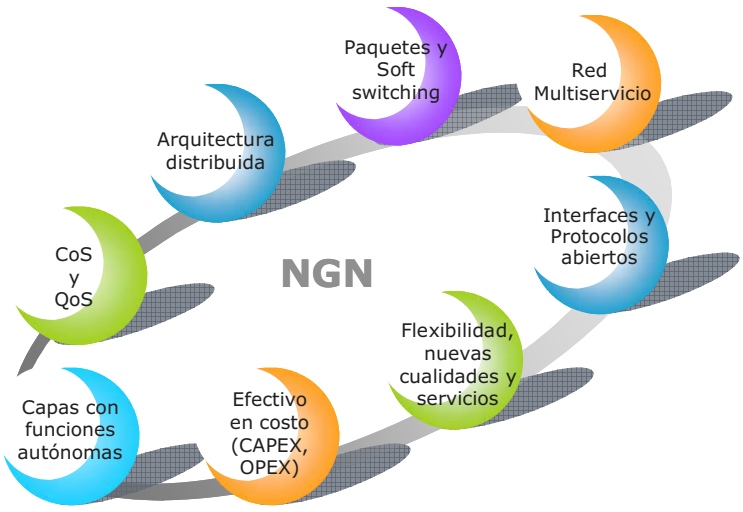



**Figura 16: Principios de NGN.**

En la Recomendación Y.2001, NGN se define como una red de paquetes capaz de entregar servicios de telecomunicaciones y de hacer uso de múltiples tecnologías de transporte de banda ancha con QoS y en la cual las funciones relativas al servicio son independientes de las tecnologías de transporte utilizadas, es decir, el acceso de los usuarios a la red puede realizarse a través de cualquier tecnología de acceso. Además, la red debe ser capaz de soportar movilidad generalizada pero que permita el acceso de los usuarios a los servicios sin depender de la ubicación.

En la Recomendación Y.2011 se entregan las bases para el desarrollo de los modelos funcionales de una red NGN. Así, se separa la arquitectura que pueda tener una red NGN con la del modelo básico de referencia OSI, entre las situaciones que se pueden encontrar se tienen:

- El número de capas de una red NGN puede no ser 7.
- Las funciones de las capas individuales pueden no corresponder a las del modelo OSI.
- Ciertas condiciones o definiciones descritas para el modelo OSI pueden no ser aplicables.
- Los protocolos involucrados pueden no ser protocolos OSI.
- Los requerimientos de red para el modelo OSI pueden no ser aplicables.

## 2.5.1. Arquitectura NGN

En la Figura 17 se muestra un diagrama de la arquitectura NGN, se observa en esta figura que las funciones NGN se dividen en estratos de servicio y transporte como lo especifica la recomendación Y.2011.

Las funciones del usuario final se conectan a la NGN a través de la interfaz UNI (User-to-Network Interface), mientras que las otras redes se encuentran interconectadas a través de la interfaz NNI (Network-to-Network Interface). Por último, la interfaz ANI (Application-to-Network Interface) demarca la frontera con los proveedores de aplicaciones.

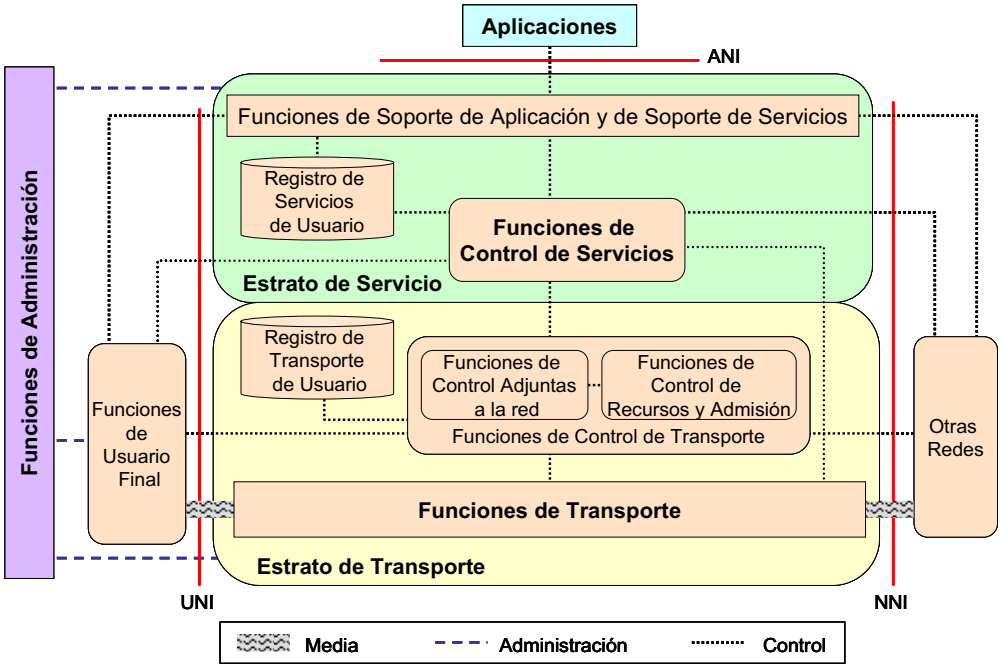



**Figura 17: Diagrama de la Arquitectura NGN.**

### 2.5.1.1. Funciones del Estrato de Transporte

Las funciones del estrato de transporte permiten la conectividad entre todas las componentes y funcionalidades separadas físicamente. El estrato de transporte es responsable de proveer QoS punto a punto, lo que constituye una muy importante característica. El estrato de transporte se divide en las redes de acceso y el Core de la red con una función de enlace entre las dos entidades.

#### 2.5.1.1.1. Funciones de Transporte

Esta entidad se puede dividir en las siguientes funciones:

- Funciones de Acceso: Administra el acceso de los usuarios finales a la red. Las funciones de acceso dependen de la tecnología utilizada para esto, tales como W-CDMA, xDSL, acceso por cable, tecnologías inalámbricas, Ethernet, acceso óptico, etc.
- Funciones de Transporte de Acceso: Estas funciones son responsables de transportar información a través de la red de acceso. También proveen mecanismos de control de QoS interactuando directamente con el tráfico de usuario, incluyendo administración del buffer, encolamiento y programación, filtrado de paquetes y clasificación de tráfico entre otros.
- Funciones de Borde: Son las funciones utilizadas para el procesamiento de tráfico cuando el tráfico de acceso es fusionado en el Core de la red.
- Funciones de Transporte del Core: Funciones responsables de asegurar el transporte de la información a través del core de la red. Entregan los medios que permiten diferenciar la calidad de transporte en la red, de acuerdo a las interacciones con las Funciones de Control de Transporte. También proveen mecanismos de QoS interactuando directamente con el tráfico de usuario, encolamiento y programación, filtrado de paquetes, clasificación de tráfico, control de entrada y Firewalls entre otros.

#### 2.5.1.1.2. Funciones de Control de Transporte

Estas funciones se dividen en dos entidades más:

- Funciones de Control Adjuntas a la red: Funciones que proveen registro a nivel de acceso y la inicialización de las funciones del usuario final para acceder a los servicios NGN. Éstas proveen identificación y autentificación a nivel de red, administran el espacio de direcciones IP de la red de acceso y autentifican las sesiones de acceso. También anuncian el punto de contacto del servicio NGN y las funciones de aplicación al usuario final.
- Funciones de Control de Recursos y Admisión o RAFCs (Resource and Admission Control Functions): Proveen el control de admisión y funcionalidades de entrada, incluyendo el control de la dirección de red y traducción de puertos (NAPT) y puntos de campos de código de servicios diferenciados (DSCP). El control de admisión envuelve chequeo de autentificación basado en los registros de usuario a través de las Funciones de Control Adjuntas a la red. Las RAFCs interactúan con las funciones de transporte para controlar una o más de las siguientes funcionalidades en la capa de transporte: filtrado de paquetes, clasificación de tráfico, marcación y políticas, reservación de ancho de banda y ubicación.

#### 2.5.1.1.3. Registro de Transporte de Usuario

Este bloque representa la compilación del usuario y otros datos de control dentro de una función única de "Registro de Usuario" en el estrato de transporte. Esta función puede ser

especificada e implementada como un conjunto de bases de datos cooperándose con funcionalidades dentro de cualquier parte de la NGN.

### 2.5.1.2.Funciones del Estrato de Servicio

Estas funciones proveen servicios basados en la sesión y no basados en sesión, incluyendo suscripción o notificación de información de presencia y un método de mensajes para intercambio de mensajería instantánea. Las funciones del estrato de servicio también entregan todas las funcionalidades de red asociadas a los servicios existentes de la PSTN o ISDN y las capacidades e interfaces para los equipos legacy de clientes.

#### 2.5.1.2.1. Funciones de Control de Servicios

Se incluyen aquí funciones de control de sesión, de registro, autentificación y autorización en este nivel. También pueden incluir funciones como recursos de control de media.

#### 2.5.1.2.2. Funciones de Registro de Servicios de Usuario

Estas funciones representan la compilación de datos de usuario y otros datos de control dentro de una única función de registro de usuario en el estrato de servicio. Esta función puede ser especificada e implementada como un conjunto de bases de datos cooperativas con funcionalidades que residen en cualquier parte de la red NGN.

#### 2.5.1.2.3. Funciones de Soporte de Aplicación y de Soporte de Servicio

NGN soporta APIs (Application Programming Interfaces) abiertas que permiten aplicar capacidades NGN a los proveedores externos de servicios para crear servicios mejorados para los usuarios NGN. Todas las funciones de aplicación y los proveedores externos de servicios acceden a las capacidades y recursos del estrato de servicio de NGN a través de servidores o gateways en este estrato.

### 2.5.1.3.Funciones de Administración

Las funciones de administración permiten a los operadores de una NGN administrar la red y entregar servicios que cumplan con la calidad, seguridad y fiabilidad esperadas. Estas funciones se localizan de forma distribuida a cada entidad funcional e interactúan con la administración de elementos de red, administración de red y entidades funcionales administradoras de servicios.

Las funciones de administración incluyen funciones de precios y facturas. Estas funciones interactúan entre ellas dentro de la NGN para recolectar la información de cobranza y para permitir que los operadores de la red NGN cuenten con los recursos necesarios para cobrar apropiadamente a los clientes. Los cargos pueden realizarse tanto en aplicaciones fuera de línea como servicios en línea.

#### 2.5.1.4. Funciones de Usuario Final

Las interfaces hacia el usuario final son tanto físicas como funcionales (control). En una red NGN se deben soportar todas las categorías de equipos de clientes, desde los teléfonos utilizados en una red PSTN a complejas redes corporativas. Además, el terminal de usuario puede ser fijo o móvil.

## 2.6. IP Multimedia Subsystem (IMS)

IMS es una arquitectura basada en los conceptos de NGN capaz de proveer sesiones multimedia en tiempo real (como sesiones de voz, video y conferencia) y sesiones que no requieren de tiempo real (como Push-to-Talk, presencia o mensajería instantánea) sobre redes all-IP. IMS apunta a la entrega de servicios indiferentemente de la red utilizada: fija, móvil o Internet y se basa en interfaces y protocolos abiertos.

IMS fue diseñado por la 3GPP (Third Generation Partnership Project), que corresponde al grupo que crea las especificaciones de telecomunicaciones de tercera generación, y fue inicialmente diseñado como parte de la arquitectura de UMTS. Además, existe la 3GPP2 que corresponde a un proyecto entre organizaciones de América del Norte y Asia para adaptar IMS a la versión 3G de CDMA, CDMA2000. Así como muchas organizaciones tratando de adaptar sus modelos (CableLabs, ETSI, etc.)

### 2.6.1. Capas de la Arquitectura IMS

La arquitectura IMS crea un ambiente de acceso agnóstico para entregar un amplio rango de servicios multimedia a los que un usuario puede acceder usando cualquier dispositivo o conexión de red. IMS soporta sesiones IP-a-IP sobre cualquier protocolo de conexión alámbrica o inalámbrica.

Además, IMS permite la interoperación entre redes TDM e IP para brindar una experiencia de servicio continuo. Las capas definidas en IMS son:

- Capa de Acceso: IMS es agnóstico al acceso. Puede ser GPRS, EDGE, UMTS, Wi-Fi, WiMAX, redes tradicionales análogas (como xDSL), etc. 3GPP2 asume accesos CDMA2000.
- Capa de Transporte: Es una red all-IP conformada por routers IP (Edge y core IP).
- Capa de Control de Sesión: Comprende los servidores de Control de la Red para administrar llamadas o establecer sesiones y modificaciones.
- Capa de Aplicación: Utiliza servidores de aplicación y contenido para proveer servicios de valor agregado. Los elementos principales de esta capa son el AS (Application Server), MRFC (Multimedia Resource Function Controller) y MRFP (Multimedia Resource Function Processor).

En la Figura 18 se muestra un diagrama con las capas definidas en IMS y sus principales componentes:

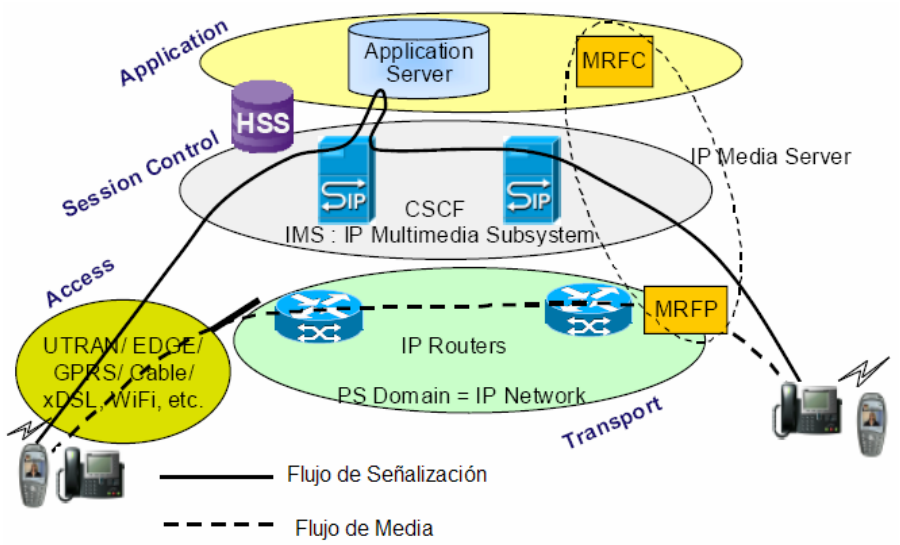



**Figura 18: Capas de la Arquitectura IMS.**

Con este modelo de capas, IMS define una arquitectura horizontal donde los servicios y funciones comunes pueden ser reutilizadas en múltiples aplicaciones y además se pueden especificar características como interoperabilidad y roaming. También se observa que existen dos flujos de datos, uno de señalización (plano de control) y otro con el flujo de media (plano de usuario.)

Esta arquitectura horizontal permite que los operadores puedan moverse fuera de las implementaciones verticales tradicionales, como se muestra en la Figura 19. La arquitectura de red tradicional (con funcionalidades de servicio único para cobros, presencia y enrutamiento entre otras) es muy costosa y compleja para construir y mantener. Por otra parte, IMS brinda un número de funciones genéricas en estructura e implementación que puedan ser reutilizadas por todos los servicios en la red. Así se pueden observar funciones comunes como administración de grupos o listas, presencia, operación y administración, directorios y cobranza.

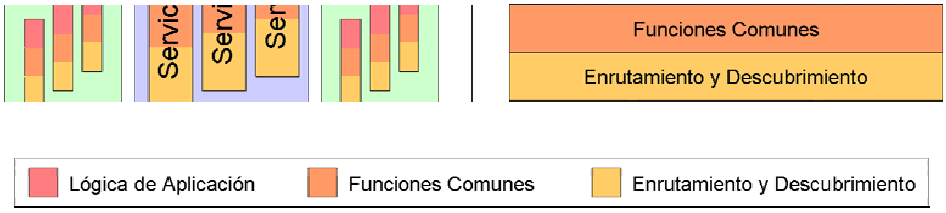



**Figura 19: Cambio de Integración vertical a horizontal dado por IMS.**

## 2.6.2. Arquitectura de IMS

En la Figura 20 se presenta la configuración de las entidades del IM CN (Core Network) Subsystem. Aquí, todas las configuraciones se consideran implementadas en distintos puntos lógicos.

Si se instalan dos puntos lógicos en el mismo equipamiento físico, las interfaces relevantes estarán dentro de ese equipo.

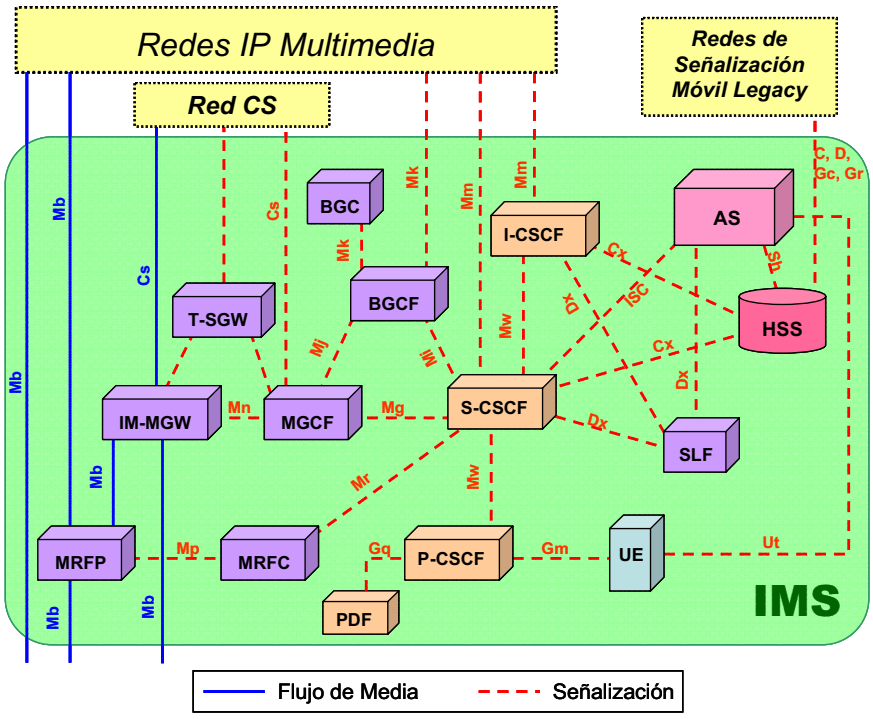



**Figura 20: Arquitectura del Core de IMS.**

### 2.6.2.1. User Equipment (UE)

Corresponde al terminal utilizado por el usuario para acceder a los servicios de la red IMS, puede ser un teléfono celular, un computador portátil o cualquier equipo que permita acceder a servicios de comunicaciones multimedia.

### 2.6.2.2. Home Subscriber Server (HSS)

El HSS corresponde a la base de datos principal de un usuario. Esta entidad contiene la información de suscripción necesaria para brindar soporte a las entidades de red que manipulan llamadas o sesiones.

Una red local (también llamada red Home) puede contener uno o más HSSs. Esto depende del número de suscriptores móviles, capacidad del equipo y organización de la red. El HSS es responsable de la participación de la siguiente información relacionada con el usuario:

- Identificación de usuario, numeración e información de direccionamiento.
- Información de Seguridad del usuario: Información de control de acceso a la red para autentificación y autorización.
- Información de Ubicación del usuario a nivel inter-sistema: El HSS soporta el registro del usuario y guarda información de ubicación inter-sistema.
- Información de profile (registro) del usuario.

El HSS también genera la información de Seguridad del usuario para autentificación mutua, comunicación de verificación de integridad y cifrado. Basado en toda esta información, el HSS también es responsable de soportar las entidades de control de llamadas y administración de sesión de los diferentes dominios y subsistemas del operador, como se muestra en la Figura 21.

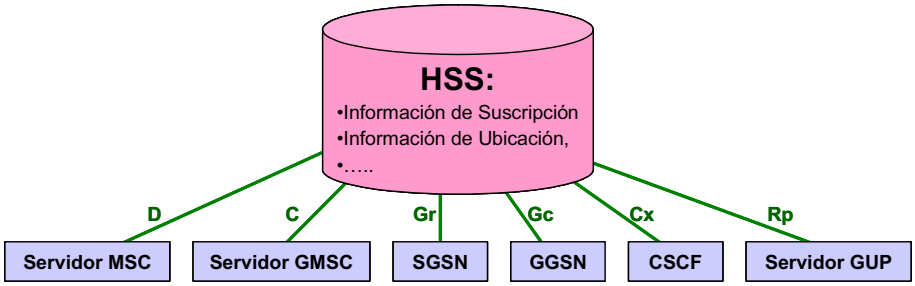



**Figura 21: Entidades soportadas por el HSS.**

El HSS consta de las siguientes funcionalidades:

- Funcionalidad IP multimedia para brindar soporte a las funciones de control de IMS como el CSCF.
- El subconjunto de funcionalidades HLR/AuC requerido por el dominio PS (Packet Switched) y CS (Circuit Switched) (si es que se desea permitir el acceso de los suscriptores al dominio CS o soportar roaming a las redes GSM/UMTS legacy del dominio CS).
- El HSS se considera como un depósito de datos GUP (Generic User Profile) para los datos del usuario en IMS.

Las funcionalidades de HLR y AuC, se explican a continuación:

- HLR (Home Locator Register): Representa una parte del HSS con la funcionalidad de brindar soporte para las entidades del dominio PS y CS.
- AuC (Authentification Center): Es una parte del HSS que se asocia con el HLR y guarda una clave de identidad para cada suscriptor móvil registrado con el HLR asociado, esta clave se usa para generar datos de seguridad para cada suscriptor móvil. Además, el AuC se comunica sólo con su HLR asociado, el que solicita los datos necesarios para autentificación y cifrado al AuC, los guarda y entrega al VLR y SGSN que los necesita para realizar las funciones de seguridad para una estación móvil.

### 2.6.2.3.Call Session Control Function (CSCF)

Corresponde a un servidor SIP; existen tres "sabores" de CSCFs.

#### 2.6.2.3.1. Proxy-CSCF

El Proxy-CSCF (P-CSCF) es el primer punto de contacto dentro de IMS. El P-CSCF se comporta como un proxy, es decir, acepta requerimientos y los sirve internamente o los reenvía. En condiciones anómalas, el P-CSCF puede terminar e independientemente generar transacciones SIP.

El PDF (Policy Decision Function) puede ser una entidad lógica del P-CSCF o un nodo físico separado. Si el PDF se implementa en un nodo físico separado, las funciones desempeñadas por el P-CSCF son:

- Reenviar el requerimiento de registro SIP recibido desde el UE a un punto de entrada determinado usando el nombre del dominio Home, como se entregó por el UE.
- Reenviar mensajes SIP recibidos desde el UE hacia algún Servidor SIP (por ejemplo un S-CSCF) cuyo nombre haya sido recibido por el P-CSCF como resultado de un procedimiento de registro.
- Reenviar el requerimiento SIP o respuesta al UE.
- Mantener una Asociación de Seguridad entre él mismo y cada UE.
- Debiera realizar la compresión y/o descompresión de mensajes SIP.
- Autorización de portadores de recursos y administración de QoS.

#### 2.6.2.3.2. Interrogating-CSCF

El Interrogating-CSCF (I-CSCF) es el punto de contacto dentro de la red de un operador para todas las conexiones destinadas a un usuario de ese operador de red, o un usuario con roaming actualmente localizado dentro del área de servicio de ese operador de red.

Puede haber múltiples I-CSCFs dentro de un operador de red. Las funciones realizadas por el I-CSCF son:

- Registro: Asignación de un S-CSCF a un usuario realizando registros SIP.
- Flujos relacionados y no relacionados con la sesión:
  - Enrutamiento de un requerimiento SIP recibido desde otra red hacia el S-CSCF.
  - Obtener la dirección del S-CSCF del HSS.
  - Reenviar el requerimiento SIP o respuesta al S-CSCF determinado anteriormente.

Basado en la configuración local, el I-CSCF puede realizar funciones de enrutamiento de tránsito. Si el I-CSCF determina, basado en una consulta al HSS, que el destino de la sesión no está dentro del IMS, este debe reenviar el requerimiento o retornarlo con una respuesta de falla hacia el punto de origen.

#### 2.6.2.3.3. Serving-CSCF

El Serving-CSCF (S-CSCF) realiza los servicios de control de sesión para el UE. Éste mantiene un estado de sesión como lo necesite el operador de red para el soporte de los servicios. Dentro de un operador de red, diferentes S-CSCFs pueden tener diferentes funcionalidades. Las funciones realizadas por el S-CSCF durante una sesión son:

- Registro: Puede comportarse como un Registrador, es decir, acepta requerimientos de registro y hace que su información esté disponible a través del Servidor de Localización (por ejemplo, el HSS).
- Flujos relacionados y no relacionados con la sesión
  - Control de Sesión para las sesiones de los extremos registrados.
  - Se puede comportar como un servidor Proxy, es decir, acepta requerimientos y los sirve internamente o los reenvía, posiblemente luego de una traducción.
  - Puede terminar e independientemente generar transacciones SIP.
  - Interacciona con las Plataformas de Servicios para el soporte de Servicios.

- Entrega a los extremos información relacionada con eventos de servicios (Por ejemplo, notificación de tonos o de cuenta).
- Para un punto de origen (es decir, el UE de origen, o AS de origen):
  - Obtener desde una base de datos, la dirección del punto de entrada para el operador de red que sirve al usuario de destino desde el nombre de destino (por ejemplo, número de teléfono discado o SIP URI), cuando el usuario de destino es un cliente de un operador de red diferente, reenvía el requerimiento SIP o responde a un I-CSCF dentro del operador de red.
  - Cuando el nombre de destino del usuario de destino y el usuario de origen es un cliente del mismo operador de red, reenvía el requerimiento SIP o lo responde a un I-CSCF dentro de la red del operador.
  - Reenvía el requerimiento SIP o responde a un BGCF para el enrutamiento de llamadas a la PSTN o dominio CS.
- Para un extremo de destino (es decir, para un UE final):
  - Reenviar el requerimiento SIP o respuesta a un P-CSCF.
  - Modificar el requerimiento SIP para enrutar una sesión entrante al dominio CS de acuerdo al HSS y a las interacciones de control de servicio, en caso de que el usuario reciba la sesión entrante a través del dominio CS.
  - Reenviar el requerimiento SIP o responder a un BGCF para el enrutamiento de llamadas a la PSTN o dominio CS.

Además todos los tipos de CSCF son capaces de crear CDRs (Charging Data Records), lo que corresponde a un registro que contiene los eventos necesarios para las operaciones de cobro en la red (por ejemplo, el horario de la llamada, duración, cantidad de datos transferidos, etc.).

#### 2.6.2.4.Subscription Locator Function (SLF)

El SLF es necesario en la red sólo en el caso en que exista más de un HSS en dicha red. Tampoco se necesita si el AS está configurado para usar un HSS predefinido. El SLF cumple con las siguientes funciones:

- Es solicitado por el I-CSCF durante el levantamiento de Registro y Sesión para obtener el nombre del HSS que contenga los datos específicos del suscriptor requerido. Además, el SLF es solicitado también por el S-CSCF durante el Registro.
- Es solicitado por el AS para obtener el nombre del HSS que contiene los datos específicos del suscriptor requerido.

#### 2.6.2.5.Policy Decision Function (PDF)

El PDF actúa como un punto de decisión de políticas para el control de política basado en servicios de los recursos portadores IP.

#### 2.6.2.6.Media Gateway Control Function (MGCF)

El MGCF se encarga de:

- Controlar las partes del estado de llamada que pertenecen al control de conexión para canales media en un IMS-MGW.
- Se comunica con las entidades CSCF, BGCF y PSTN.
- Determina el next hop ("paso siguiente" se refiere a la próxima entidad a la cual se enviará el requerimiento) dependiendo del número de enrutamiento para las llamadas entrantes desde redes legacy.
- Realiza la conversión de protocolos entre ISUP/TCAP y los protocolos de control de llamadas IMS.
- La información fuera de banda recibida en el MGCF puede ser reenviada al CSCF/IMS-MGW.

### 2.6.2.7.IP Multimedia Subsystem – Media Gateway Function (IMS-MGW)

Un IMS-MGW puede crear terminaciones de canales portadores desde una red CS y flujos de media desde una red PS (por ejemplo, flujo RTP en una red IP). El IMS-MGW puede soportar conversión de media, control de portadores y procesamiento de carga útil. El IMS-MGW:

- Interactúa con el MGCF para el control de recursos.
- Posee y maneja recursos como echo cancellers, etc.
- Puede necesitar tener codecs.

El IMS-MGW será equipado con los recursos necesarios para el soporte del transporte de media UMTS/GSM. Además, se puede requerir la adaptación de H.248 para soportar codecs adicionales y protocolos de framing, etc.

### 2.6.2.8.Multimedia Resource Function Controller (MRFC)

El MRFC se encarga de:

- Controlar los recursos de flujos de media en el MRFP.
- Interpretar información entrante desde el AS y S-CSCF (por ejemplo, identificador de sesión) y controla de forma acorde el MRFP.
- Generar CDRs.

### 2.6.2.9.Multimedia Resource Function Processor (MRFP)

El MRFP se encarga de:

- Controlar los portadores en el punto de referencia Mb.
- Entregar recursos a ser controlados por el MRFC.
- Mezclar los stream media entrantes (por ejemplo, para múltiples partes).
- Originar flujos de media (para anuncios multimedia).
- Procesar los flujos de media (por ejemplo, transcodificación de audio, análisis de media).
- Control de Piso (es decir, administra los derechos de acceso para recursos compartidos en un ambiente de conferencia).

#### 2.6.2.10. Breakout Gateway Control Function (BGCF)

El BGCF selecciona la red en la cual ocurrirá el paso a la PSTN y, dentro de la red donde ocurrirá el paso, selecciona el MGCF.

#### 2.6.2.11. Application Server (AS)

Un Servidor de Aplicación (AS) ofrece servicios IM de valor agregado y se ubica ya sea en la red Home del usuario o en una ubicación de tercera parte. La ubicación de tercera parte puede ser una red o simplemente un AS autónomo.

La interfaz S-CSCF al AS es usada para entregar servicios que se ubican en el AS. Se identifican dos casos:

- S-CSCF a un AS en la red Home.
- S-CSCF a un AS en una red externa confiable (por ejemplo, de tercera parte o visitada). El S-CSCF no entrega funcionalidades de autentificación y seguridad para asegurar el acceso directo de la tercera parte al Subsistema IM.

La interfaz del I-CSCF al AS se utiliza para reenviar requerimientos SIP destinados a una Identidad de Servicio Público alojado por el AS directamente a ese AS. Un AS puede influenciar e impactar la sesión SIP en nombre de los servicios soportados por la red del operador y puede alojar y ejecutar servicios.

#### 2.6.2.12. Trunking Signaling Gateway (T-SGW)

El T-SGW es el encargado de la conversión de señalización a nivel de transporte entre el transporte de señalización SS7 y el transporte de señalización basado en IP.

### 2.6.3. Interfaces entre Entidades Funcionales

La Tabla 1, a continuación, presenta las principales interfaces (también llamadas puntos de referencia) presentes en la arquitectura IMS junto con una breve descripción de éstas.

**Tabla 1: Interfaces en IMS.**

| Interfaz | Une las entidades | Breve Descripción | Protocolo |
|---|---|---|---|
| Gm | UE, P-CSCF | Usada para intercambiar mensajes entre el UE y los CSCFs. | SIP |
| Mw | P-CSCF, I-CSCF, S-CSCF | Usada para intercambiar mensajes entre CSCFs | SIP |
| ISC | S-CSCF, I-CSCF, AS | Usada para intercambiar mensajes entre el CSCF y el AS | SIP |
| Cx | I-CSCF, S-CSCF, HSS | Usada para comunicarse entre el I-CSCF o S-CSCF y el HSS | Diameter |
| Dx | I-CSCF, S-CSCF, SLF | Usada por el I-CSCF o S-CSCF para encontrar el HSS correcto en caso de que exista más de uno. | Diameter |
| Sh | AS, HSS | Usada para intercambiar información entre el AS y el HSS. | Diameter |
| Dh | AS, SLF, HSS | Usada por el AS para encontrar el HSS correcto en caso de que exista más de uno. | Diameter |
| Mm | I-CSCF, S-CSCF, red IP externa | Usada para intercambiar mensajes entre IMS y redes IP externas. | No especificada |
| Mg | MGCF a I-CSCF | El MGCF convierte la señalización ISUP a SIP y la reenvía al I-CSCF. | SIP |
| Mi | S-CSCF a BGCF | Usada para intercambiar mensajes entre S-CSCF y BGCF. | SIP |
| Mj | BGCF a MGCF | Usada para intercambiar mensajes entre BGCF y MGCF en la misma red IMS. | SIP |
| Mk | BGCF a BGCF | Usada para intercambiar mensajes entre BGCFs en redes IMS diferentes | SIP |
| Mr | S-CSCF, MRFC | Usada intercambiar mensajes entre el S-CSCF y MRFC. | SIP |
| Mp | MRFC, MRFP | Usada para intercambiar mensajes entre MRFC y MRFP | H.248/ MEGACO |
| Mn | MGCF, IM-MGW | Permite el control de recursos del plano de usuario. | H.248/ MEGACO |
| Ut | UE, AS | Permite administrar al UE información relacionada con sus servicios. | HTTP/ HTTPS |
| Mb | Hacia servicios de redes IPv6 | Permite acceder a los servicios de la red IPv6 para transportar datos de usuario. | |
| Gq | P-CSCF, PDF | Usada para intercambiar decisiones de políticas con información relacionada entre el P-CSCF y PDF | Diameter |

En la sección 9.3 de Anexos se muestra un diagrama de resumen de las principales entidades de IMS con sus respectivas interfaces, protocolos utilizados y funciones principales.

## 2.6.4. Protocolos en IMS

A continuación se presentan los principales protocolos utilizados en IMS.

#### 2.6.4.1.SIP (Session Initiation Protocol)

IMS utiliza el protocolo de iniciación de sesión de la IETF para control y señalización de sesiones. Así, cualquier terminal con un software compatible con SIP y una dirección SIP, la cual es un tipo de identificador fuente, puede participar en sesiones IMS. En la sección 2.7.3.2 se explica este protocolo más en detalle.

#### 2.6.4.2.COPS (Common Open Policy Server)

IMS utiliza COPS, de la IETF, para asegurar calidad de servicio, lo cual es importante para telefonía y otros tipos de tráfico que no toleran latencia. COPS permite la comunicación de QoS y otra información de políticas de tráfico entre un servidor de políticas (que para efectos de IMS, corresponde al PDF) y los clientes.

#### 2.6.4.3.Diameter

IMS usa el protocolo Diameter, del IETF, para permitir a los terminales acceder al HSS, y después entrega la necesaria autentificación, autorización y, para comunicaciones con cobro, servicios de accounting.

#### 2.6.4.4.Megaco

El protocolo Megaco (H.248), del IETF y la ITU, es el protocolo que define las operaciones necesarias para que un Media Gateway Controller sea capaz de soportar llamadas entre redes RTC-IP o IP-IP. En la sección 2.7.3.4 se describe más en detalle este protocolo.

## 2.7. Arquitecturas de Redes de Telefonía

En esta sección se pretende estudiar las arquitecturas más conocidas para brindar servicios de telefonía, tanto fija como móvil. Se comenzará entonces por la arquitectura inicial de telefonía correspondiente a la PSTN, luego se estudiarán algunas tecnologías de telefonía móvil (con especial énfasis en la familia GSM) entendiéndose por telefonía móvil a la telefonía celular y no a los nuevos tipos de telefonía IP wireless. Posteriormente se estudiará la telefonía a través de Internet o ToIP y finalmente se incluirán arquitecturas actuales como IMS y PacketCable.

### 2.7.1. Public Switched Telephone Network (PSTN)

#### 2.7.1.1.Breve Descripción

La red PSTN corresponde a la red de telefonía conmutada tradicional, y corresponde a la red de mayor cobertura geográfica. Esta arquitectura ha evolucionado a su forma actual en sus 100 años de existencia. Inicialmente, la red PSTN se adaptó para manipular manualmente canales de ancho de

banda bajo (4 KHz). Posteriormente, la red se digitalizó para brindar servicios de datos de alta velocidad. Sin embargo, esta digitalización fue desarrollada solamente entre centrales, la señal de llegada a los terminales telefónicos sigue siendo analógica. Los avances en las tecnologías de conmutación de paquetes permitieron que la transformación de la señalización de la red soporte un amplio rango de mejoras al servicio básico.

Aún así, una red PSTN se caracteriza principalmente por las siguientes características:

- Es capaz de manipular varios canales dedicados de bajo ancho de banda (64 Kbps o 4 KHz).
- Una vez que se ha asignado un canal, éste permanece asignado se esté utilizando o no. El número de canales existentes en la red es muy inferior a las líneas suscritas (teoría de Erlang), estos canales se van asignando a medida que se requiere establecer una llamada.
- Posee retardos inferiores a 100 ms y bajos tiempos de establecimiento de la llamada.
- Está optimizada para el transporte de voz. Sin embargo, se ha utilizado el mismo medio para proveer enlaces xDSL.
- Posee ancho de banda para la voz garantizado.
- Los terminales de esta red (por ejemplo, teléfonos) son baratos debido a su funcionalidad limitada y especializada.

### 2.7.1.2.Arquitectura

La red PSTN posee una arquitectura jerárquica, como se puede apreciar en la Figura 22.

En la arquitectura de una red PSTN se cuenta con cinco clases de switches o conmutadores:

- Clase 5: Corresponde al primer conmutador de contacto para el usuario y también recibe el nombre de switch local o End Office.
- Clase 4: Corresponden a los switches regionales y también son llamados Tándem de acceso.
- Clase 3: Corresponden a los Tándem de acceso inter-regional.
- Clase 2: Corresponde al switch IXC (IntereXchange Carrier) o compañía de larga distancia.
- Clase 1: Corresponde a un Gateway entre distintos IXC.

En Chile, se cuenta con switches Clase 4 y 5 solamente.

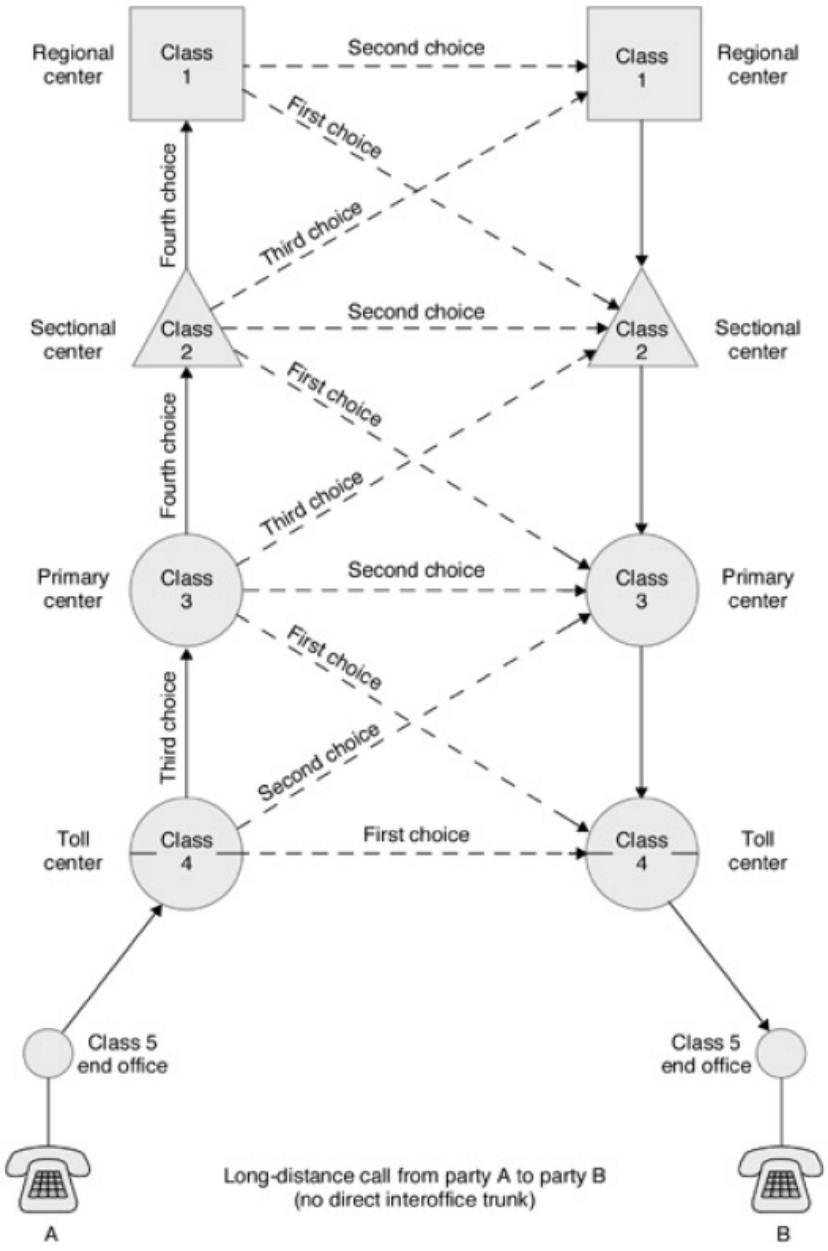



**Figura 22: Ejemplo de Llamada de Larga Distancia de A hasta B.**

### 2.7.1.3. Señalización SS7 en la PSTN

Al igual que la arquitectura PSTN, la señalización dentro de esta red ha evolucionado en el tiempo. Luego de la conmutación manual hasta principios del siglo XX, en 1910 se implementó la conmutación electromecánica que duró hasta los años 60 y en que la señalización se transportaba "en banda" y era interpretada por elementos electromecánicos y electrónicos dentro de la red. A mediados de los 60, se introdujeron las centrales digitales y el control de conmutación por CPU (control por programa almacenado). Los primeros protocolos de señalización eran bastante limitados, pero con la llegada de las redes de computadores, las señales comenzaron a ser

intercambiadas a través de una red de conmutación de paquetes fuera de banda y dedicada solo para señalización. Aún así, la red de acceso del abonado se mantiene generalmente analógica y la señalización de la red se mantiene transparente para éste. Actualmente, el sistema de señalización utilizado es SS7 (Signaling System 7), el cual provee una estructura universal para la señalización, mensajería, interfaces y mantención de red para redes telefónicas. Éste lleva los establecimientos de llamadas, intercambiar la información de usuario, enrutamiento de llamadas, diferentes estructuras de cuentas (de precio) y soporte de servicios de red inteligente.

SS7 es un sistema de señalización bien estructurado que define una arquitectura de señalización conformado por 2 conjuntos principales de elementos:

- Puntos de señalización, que se explicaron anteriormente y que son:
  - SSP (Serving Switching Point): Originan, terminan o transportan llamadas. Se comunica con otros SSPs para iniciar, administrar o alcanzar circuitos de voz para terminar llamadas. Además, envía mensajes de consulta a una base de datos centralizada (SCP) para determinar cómo enrutar una llamada.
  - STP (Signal Transfer Point): Consiste en un conmutador de paquetes para transportar el tráfico de red entre los puntos de señalización. Para esto se basa en la información de enrutamiento contenida en el mensaje SS7. Además, un STP puede realizar traducción global de título, un procedimiento en el cual el punto de señalización de destino se determina de los dígitos presentes en el mensaje de señalización y puede actuar como Firewall.
  - SCP (Service Control Point): Envía respuestas a los SSPs que originan consultas conteniendo el número de enrutamiento asociado con el número discado.
- Enlaces de Señalización: Los mensajes SS7 son intercambiados entre elementos de red sobre canales bidireccionales de 56 o 64 Kbps llamados enlaces de señalización. Estos enlaces están dedicados exclusivamente a la señalización fuera de banda, por lo que ofrece que las llamadas se creen más rápidamente que la señalización en banda. Éstos están organizados lógicamente por tipo de enlace de acuerdo a su uso en la red. En la Tabla 2 se muestra una breve descripción de estos enlaces.

**Tabla 2: Descripción de los Enlaces SS7.**

| Enlace | Descripción |
|---|---|
| A (Access) | Conecta un SCP o SSP con un STP. Sólo transmite mensajes desde los puntos finales de origen o hacia los de destino. |
| B (Bridge) | Conecta un STP con otro STP. Su distinción con el enlace D es arbitraria por lo que también se llama enlace B/D. |
| C (Cross) | Conecta un par de STPs que realizan funciones idénticas. Es usado sólo cuando un STP no tiene acceso a alguna ruta disponible por alguna falla de enlace(s). |
| D (Diagonal) | Conecta un STP secundario (local o regional) a un STP primario (gateway de inter-red). Su distinción con el enlace B es arbitraria por lo que también se llama enlace B/D. |
| E (Extended) | Conecta un SSP con un STP. Provee un mapa de señalización alternativo si un SSP no puede ser alcanzado por el STP mediante el enlace A. Se implementa sólo para mayor robustez de la red y no siempre es necesario. |
| F (Fully associated) | Conecta dos puntos finales de señalización (SSPs y SCPs). Usualmente no se usa en redes con STPs. |

En la Figura 23 se muestran tanto los puntos de señalización como los enlaces de la arquitectura SS7.

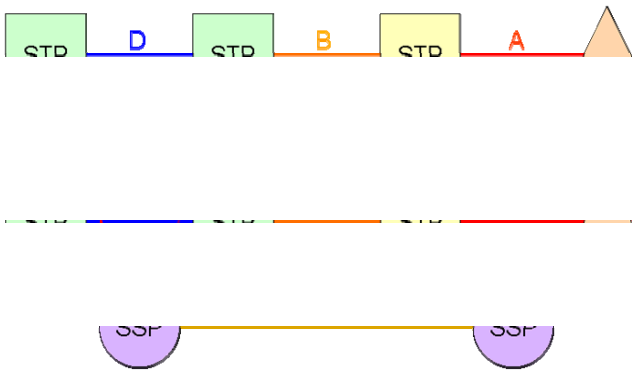



**Figura 23: Tipos de Puntos y Enlaces de Señalización en SS7.**

Cada nodo se identifica en la red por un número o código. Los enlaces entre nodos son full-dúplex de 56 Kbps o 64 Kbps. La Figura 24 muestra una red PSTN actual con señalización SS7.

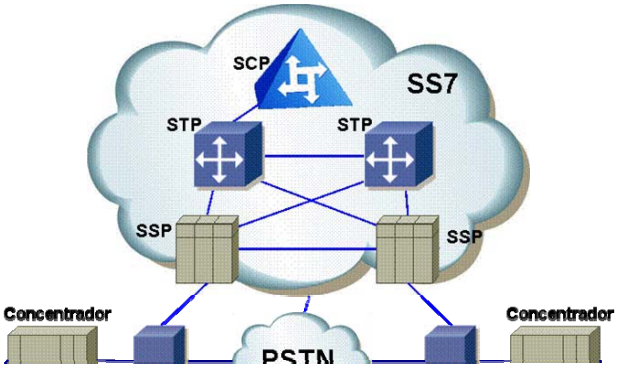



**Figura 24: Arquitectura PSTN con SS7.**

El protocolo SS7 se divide en estratos de sub-protocolos, de forma muy similar al modelo de capas OSI, la Figura 25 muestra un paralelo entre las capas del modelo OSI y del protocolo SS7.

**Figura 25: Comparación entre el modelo OSI y protocolo SS7.**

- MTP (Message Transfer Part): El protocolo MTP se divide en tres niveles:
  - MTP Nivel 1: Es equivalente a la capa física del modelo OSI. Define las características físicas, eléctricas y funcionales del enlace de señalización digital. Las interfaces físicas definidas incluyen E-1 (32 canales de 64 Kbps), DS-1 (24 canales de 64 Kbps), V.35 (64 Kbps), DS-0 (64 Kbps) y DS-0A (56 Kbps).
  - MTP Nivel 2: Es equivalente a la capa de enlace del modelo OSI. Asegura las transmisiones precisas End-to-End de un mensaje a través de un enlace de señalización. Este protocolo implementa control de flujo, validación de secuencia de mensajes, y verificación de error.
  - MTP Nivel 3: Es equivalente a la capa de red del modelo OSI. Permite el enrutamiento de mensajes entre puntos de señalización en la red SS7, se encarga de re-enrutar el tráfico desde enlaces fallidos y puntos de señalización y controla el tráfico en casos de Congestión.
- ISUP (ISDN User Part): Define el protocolo usado para iniciar, administrar y actualizar circuitos troncales que llevan voz y datos entre las líneas de origen y destino. ISUP se usa para llamadas ISDN y no-ISDN. Sin embargo, las llamadas que se originan y terminan en el mismo switch no usan señalización ISUP.
- TUP (Telephone User Part): En algunas partes del mundo, TUP se usa para soportar y terminar llamadas básicas. TUP maneja sólo circuitos analógicos.
- SCCP (Signaling Connection Control Part): Provee servicios orientados y no orientados a la conexión y capacidades de Traducción Global de Título (GTT: Global Title Translation) sobre MTP Nivel 3. Un título global es una dirección (número 800, número de tarjeta de llamadas o número de identificación de suscriptores móviles) que es traducido por SCCP a un código de punto de destino y número de subsistema (identifica una aplicación en el punto de señalización de destino). SCCP se utiliza en la capa de transporte para servicios basados en TCAP.
- TCAP (Transaction Capabilities Applications Part): Soporta el intercambio de datos no relacionados con circuitos entre aplicaciones a través de la red SS7 usando servicios SCCP no orientados a la conexión. Las consultas y respuestas enviadas entre SSPs y SCPs son llevadas en mensajes TCAP.

El tipo de mensaje ISUP que se está transmitiendo se define en un octeto de bits que puede contener alguna de las opciones que se presentan en la Tabla 3.

**Tabla 3: Mensajes de Señalización en ISUP.**

| Mensaje ISUP | Asunto |
|---|---|
| IAM (Initial Address Message) | Primer mensaje enviado para informar al switch partner que se debe establecer una llamada en el CIC contenido en el mensaje. Contiene la llamada y número de llamada, tipo de servicio (voz o datos) y otros parámetros opcionales. |
| ACM (Address Complete Message) | Mensaje retornado desde el switch terminante cuando el suscriptor es alcanzado y el teléfono empieza a sonar. |
| ANM (Answer Message) | Se envía cuando el suscriptor levanta el teléfono. Normalmente el cobro de la llamada comienza en ese momento. |
| REL (Release) | Es enviado para limpiar la llamada cuando un suscriptor cuelga. |
| RLC (Release Complete) | Es un acuse de recibo del Release. |

## 2.7.2. Telefonía Móvil

### 2.7.2.1. Breve Historia de la Telefonía Móvil

El primer servicio de telefonía móvil fue introducido por AT&T en Estados Unidos el año 1946 y estaba destinado a usuarios que viajaban en auto. Este sistema no era propiamente celular ya que no operaba con un sistema de celdas sino que con una única antena que brindaba todo el servicio a la zona que por lo general era de un radio de 80 Km, por lo cual dicha antena debía ser muy potente. El servicio de voz ofrecido durante este periodo era analógico con transmisión en frecuencia modulada (FM). El sistema utilizado para hablar era muy similar al de Push-to-Talk ya que el usuario debía presionar un botón en el teléfono para hablar de forma de cortar la recepción del teléfono. Sin embargo, a medida que aumentó la demanda de este servicio, el sistema no pudo soportar la capacidad necesaria por lo que la calidad de éste era muy deficiente con probabilidades de bloqueo superiores al 65%.

Luego, a mediados de los años 60', la Bell System implementó el sistema IMTS (Improved Mobile Telephone System), el que correspondía a una mejora al sistema anterior. Éste también poseía una antena transmisora de alta potencia pero que utilizaba dos frecuencias: una para enviar y otra para recibir. IMTS soportaba 23 canales en el rango de los 150 a 450 MHz con un ancho de banda reducido de 25 a 30 KHz. Es a finales de los 60's y principios de los 70's cuando surge la idea de la utilización de células y por tanto una telefonía propiamente celular. Por otra parte, la invención del microprocesador a principios de los años 70's y el uso de un enlace de control digital entre el teléfono móvil y la estación base dieron un impulso al desarrollo de la telefonía celular.

El primer sistema de telefonía móvil completamente celular fue AMPS (Advanced Mobile Phone Service), este sistema aún seguía siendo analógico y cada usuario utilizaba completamente un canal de radio. Las células en AMPS poseían un tamaño de aproximadamente 10 Km y la principal innovación fue que se introdujo el concepto de handoff. En AMPS, el ancho de banda destinado a una comunicación era de 30 KHz, y la separación entre las frecuencias de transmisión y de recepción era de 45 MHz. Desde el punto del espectro radioeléctrico, AMPS utilizaba 25 MHz. En Chile, el espectro de 25 MHz se dividió entre las compañías Telefónica móvil y Bellsouth, por lo que cada célula de cada compañía podía tener 416 canales, de los cuales 21 eran de control.

Durante 1990, la voz de la telefonía celular se convirtió en digital en EE.UU. Ya en el año 1989, se creó en Europa la agrupación GSM (Groupe Spéciale Mobile) para crear un estándar de telefonía digital, el que culminó en el año 1992 con la aparición de la telefonía GSM (Global System for Mobile communications). En 1994, Qualcomm, Inc. Propuso una nueva tecnología celular que funcionaba en un escenario de espectro esparcido llamado CDMA (Code Division Multiple Access) que prometía mayor cantidad de usuarios por célula.

La evolución de los sistemas celulares se divide en generaciones, la Tabla 4 muestra las principales características de cada generación.

**Tabla 4: Características Principales de las Generaciones de Telefonía Móvil.**

| Características | Generaciones Móviles | | |
|---|---|---|---|
| | 1G | 2G | 3G |
| Transmisión | Analógica | Digital | Digital |
| Acceso | FDMA | TDMA, CDMA | TDMA, W-CDMA |
| Ejemplos de Tecnología | AMPS, JTACS | GSM, IS-95 | UMTS, CDMA-2000, ARIB-W-CDMA. |
| Funcionalidades | Voz | Voz y Mensajería corta | Voz<br>Datos a alta velocidad |
| Velocidad de Transmisión de datos | Máximo a 9600 bps utilizando módems de banda vocal. | * 9600-14400 bps<br>* Hasta 115200 bps (GSM-GPRS) | * Doméstico: 2 Mbps<br>* Exterior a interior peatonal: 348 Kbps<br>* En vehículos: 144 Kbps |
| Espectro | 800 – 900 MHz | * 800 – 900 MHz<br>* 1800 – 1900 MHz (PCS) | * 1885 – 2025 MHz<br>* 2110 – 2200 MHz |

### 2.7.2.2.GSM

GSM (Global System for Mobile communications) corresponde a un estándar europeo para telefonía móvil de de segunda generación y que fue diseñado para la transmisión de voz y servicios de manejo de mensajes.

La arquitectura y protocolos de GSM se basan en el modelo de referencia OSI de siete capas. Su método de acceso corresponde a FDMA con 124 canales y TDMA con 8 intervalos de tiempo por trama donde una trama comprende 8 canales físicos que transportan lo canales lógicos de tráfico y señalización (control). El canal de tráfico hace uso de un codificador vocal que proporciona una señal digital de 13Kbps; mientras que el canal de señalización se sustenta sobre el canal de tráfico a velocidades de 2.4, 4.8 y 9.6 Kbps con diferentes procedimientos de adaptación de la velocidad, codificación de canal y entrelazado.

La arquitectura de una red GSM está compuesta por numerosas entidades funcionales. En la Figura 26 se muestra una red GSM típica. La red GSM puede dividirse en cuatro partes:

- Equipo móvil (ME), que corresponde al terminal de usuario.
- Subsistema de Estaciones Base (BSS), que controla el enlace de radio con el ME.
- Subsistema de Conmutación y Red, cuya parte principal es el Centro de Conmutación para Móviles (MSC). Ofrece el servicio de conmutación de llamadas entre los móviles y la red fija y el manejo de la movilidad.
- Subsistema de Soporte y Operación (OSS), que controla la operación del sistema y la inicialización de la red.

Además, en la sección 9.2.1 de Anexos, se explican algunas características técnicas de esta arquitectura como protocolos, canales físicos y lógicos e interfaces entre entidades funcionales.

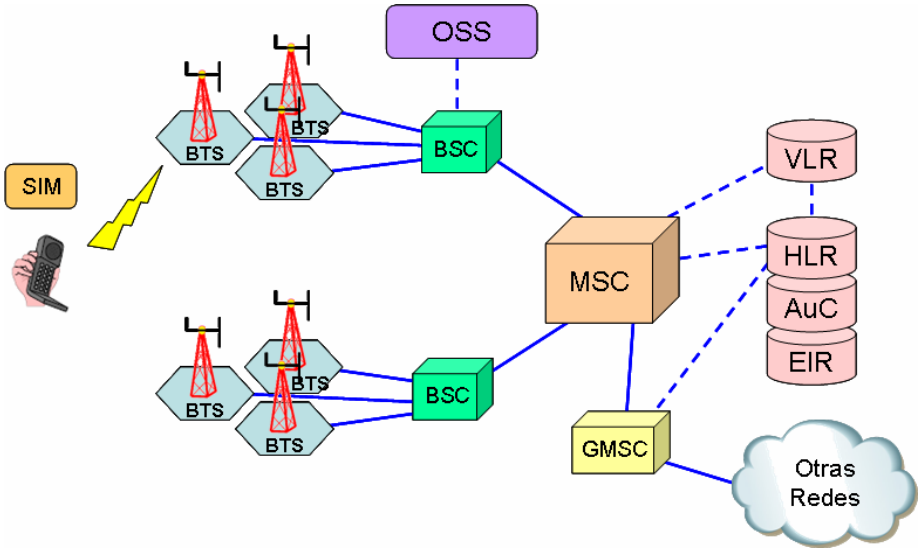



**Figura 26: Arquitectura GSM.**

#### 2.7.2.2.1. Equipo Móvil

El equipo móvil o MS (Mobile Station) está compuesto por el terminal y una tarjeta inteligente llamada SIM (Subscriber Identity Module).

El SIM es el que permite la movilidad de forma que el usuario pueda acceder a la red con esta tarjeta desde cualquier terminal. La tarjeta SIM puede ser protegida contra uso no autorizado mediante el uso de un password o número de identificación personal de 4 dígitos conocido como PIN (Personal Identification Number). Además, dentro del SIM se encuentra almacenado el IMSI que corresponde a un número personal del usuario, de ámbito internacional.

El terminal se identifica de forma inequívoca mediante el IMEI (International Mobile Equipment Identity), que corresponde a un número de identificación grabado internamente por el fabricante. Este número puede ser solicitado por la red para comprobar si no se encuentra en una lista de equipos robados o con mal funcionamiento. El IMEI y el IMSI son independientes.

#### 2.7.2.2.2. Subsistema de Estaciones Base

El BSS (Base Station Subsystem) está compuesto por dos partes: el BTS (Base Transceiver Station) y el BSC (Base Station Controller). Estas se comunican mediante la llamada Interfaz Abis.

- BTS: Esta componente consta de las antenas y transmisores de radio que define la célula y maneja el protocolo de radio con la Estación Móvil.
- BSC: Maneja los recursos de radio de una o más BTS junto con la inicialización de los canales de radio, el salto en frecuencia y los handoff. Es la conexión entre la Estación Móvil y el MSC.

#### 2.7.2.2.3. Subsistema de Conmutación y Red

El Subsistema de Conmutación y Red o NSS (Network and Switching Subsystem) se encarga de administrar las comunicaciones que se realizan entre los diferentes usuarios de la red. El componente principal de este sistema es el MSC (Mobile services Switching Center). Actúa como un

nodo de conmutación normal de una red PSTN o ISDN añadiendo todas las funciones necesarias para manejar un usuario móvil, como su registro, autenticación, localización handoffs, etc.

El MSC facilita la conexión con las redes fijas utilizando SS7. Cada MSC tiene su propio VLR, que puede cubrir varias áreas. Cada área se identifica por una identidad de área (LAI) compuesta por tres dígitos de país, dos de red GSM y dos octetos de identidad de área. Cada celda se identifica por una identidad de área, más un campo variable de identidad de celda que siempre es menor de 16 bits.

Por otro lado, cada estación base tiene un código de 6 bits denominado BSIC con el que se distingue de los adyacentes para el envío de las medidas hacia el MSC. Este BSIC puede repetirse en el mismo país para dos BTS que no estén próximas.

El MSC se sustenta en 4 registros o bases de datos:

- HLR (Home Location Register): Contiene toda la información administrativa de cada cliente registrado en la red GSM con la actual localización del móvil. Entre la información que almacena el HLR tenemos fundamentalmente la localización del usuario y los servicios a los que tiene acceso. Hay un HLR por cada red GSM, aunque puede estar implementado en una base de datos distribuida. El HLR y el VLR junto con el MSC proporcionan la ruta o camino de la llamada (routing) y la capacidad de roaming de GSM.
- VLR (Visitor Location Register): Contiene la información del HLR necesaria para el control y ejecución de los servicios contratados para cada móvil situado en el área geográfica controlada por el VLR. Aunque el VLR puede ser configurado como una entidad independiente todos los fabricantes lo sitúan junto en el MSC, de forma que el área geográfica controlada por el MSC corresponde a la controlada por el VLR. De esta forma se simplifica la señalización.
- EIR (Equipmenent Identity Register): Es una base de datos que se utiliza para proporcionar seguridad en las redes GSM pero a nivel de equipos válidos. La EIR contiene una base de datos con todos los terminales que son válidos para ser usados en la red. Esta base de datos contiene los IMEI de cada terminal, de manera que si un determinado móvil trata de hacer uso de la red y su IMEI no se encuentra localizado en la base de datos del EIR no puede hacer uso de la red.
- AuC (Authentication Center): Es una base de datos protegida que almacena una copia de la clave secreta almacenada en cada tarjeta SIM y que se utiliza para la autenticación y encriptado de la señal en el canal de radio. El AuC almacena una copia del PIN almacenado en la tarjeta SIM de cada usuario. Cuando un móvil se mueve por un área controlada por un VLR, en éste se le asigna un número temporal (TMSI). En el HLR y en el VLR se memorizan para usuario unas claves Ki y Kc que sirven para autenticar y cifrar. En la tarjeta también se graba la identidad de la última área de localización visitada. En el centro de autenticación (AuC) que puede estar en el mismo lugar que el HLR se generan y almacenan por cada IMSI cinco tripletas de autenticación compuestas por cinco conjuntos de serie pregunta, serie respuesta y llave de cifrado.

Además de las componentes antes mencionadas, el NSS cuenta con el GMSC (Gateway Mobile Services Switching Center) que consiste en un gateway que se encarga intermediar entre las redes de telefonía fijas y la red GSM.

#### 2.7.2.2.4. Subsistema de Soporte y Operación

Los subsistemas de Soporte y Operación u OSS (Operation and Support Subsystem) se conectan a diferentes NSS y MSC para controlar y monitorizar toda la red GSM. La tendencia actual en estos sistemas es que, dado que el número de BSS se está incrementando se pretende delegar funciones que actualmente se encarga de hacerlas el subsistema OSS en los BTS de modo que se reduzcan los costes de mantenimiento del sistema.

#### 2.7.2.2.5. Acceso al Medio Físico

Como se mencionó anteriormente, GSM utiliza una combinación de TDMA y FDMA para acceder a la interfaz física. En cuanto a técnicas de duplexación, GSM utiliza FDD con dos canales físicos de 25 MHz cada uno, el uplink está implementado entre los 890 y 915 MHz y el downlink se ubica entre los 935 y 960 MHz. Además, cada banda posee canales portadores de 200 KHz de ancho.

A su vez, cada canal portador utiliza TDMA siendo dividido en 8 time-slots donde en cada uno de ellos se transmite información. La modulación utilizada para la información es GMSK (Gaussian Minimum Shift Keying), lo que permite alcanzar una velocidad de 270 Kbps.

### 2.7.2.3. GPRS

GPRS (General Packet Radio Services) corresponde a una evolución de la tecnología GSM que se ubica entre la segunda y tercera generación de telefonía celular, por lo que se identifica como una tecnología 2.5G a modo de transición entre ambas generaciones. GPRS surge para dar solución a ciertos problemas y limitaciones de GSM, entre los que se encuentran:

- Velocidad de transferencia de 9,6 Kbps.
- Tiempo de establecimiento de conexión, de 15 a 30 segundos. Además, en cada sesión se deben reiniciar las aplicaciones.
- Pago por tiempo de conexión.
- Problemas para mantener la conectividad casos de Roaming.

Al sistema GPRS se le conoce también como GSM-IP ya que usa la tecnología IP para acceder directamente a los proveedores de contenidos de Internet. Es una tecnología que comparte el rango de frecuencias de la red GSM utilizando una transmisión de datos por medio de 'paquetes' y fue diseñado para ser utilizada en conjunto con GSM.

GPRS cuenta con dos características principales:

- Canales compartidos entre diferentes usuarios: A diferencia de GSM, que durante una llamada el canal de comunicación de usuario permanece asignado aunque no se envíen datos; en GPRS los canales de comunicación se comparten entre los distintos usuarios en forma dinámica, de modo que un usuario sólo tiene asignado un canal cuando se está realmente transmitiendo datos.
- Mayor velocidad y eficiencia de la red: la velocidad se ve aumentada hasta un mínimo de 40 Kbps y un máximo de 115 Kbps por comunicación en comparación con GSM cuya velocidad es de 9,6 Kbps, y la tecnología utilizada permite la comparación de cada canal con varios usuarios, mejorando de esta manera su eficiencia en la utilización de los recursos de la red.

En la tecnología GPRS, se pueden encontrar tres tipos de terminales, los que se nombran a continuación:

- Clase A: Permite el uso simultáneo de GSM y GPRS asignando 1 time-slot para GSM y 1 o más para GPRS sin que se produzca degradación de ninguno de los dos servicios.
- Clase B: Permite el uso de GPRS y GSM alternadamente, pero dándole prioridad al acceso GSM, produciéndose degradación de QoS sólo para GPRS.
- Clase C: Permite una elección manual de GPRS o GSM sin uso simultáneo.

En cuanto a la arquitectura de red de GPRS está basada fundamentalmente en GSM pero con algunos elementos adicionales. En la Figura 27 se muestra la arquitectura lógica de GPRS con GSM. Además, en la sección 9.2.2 de Anexos, se explican algunas características técnicas de esta arquitectura como protocolos, canales físicos y lógicos e interfaces entre entidades funcionales.

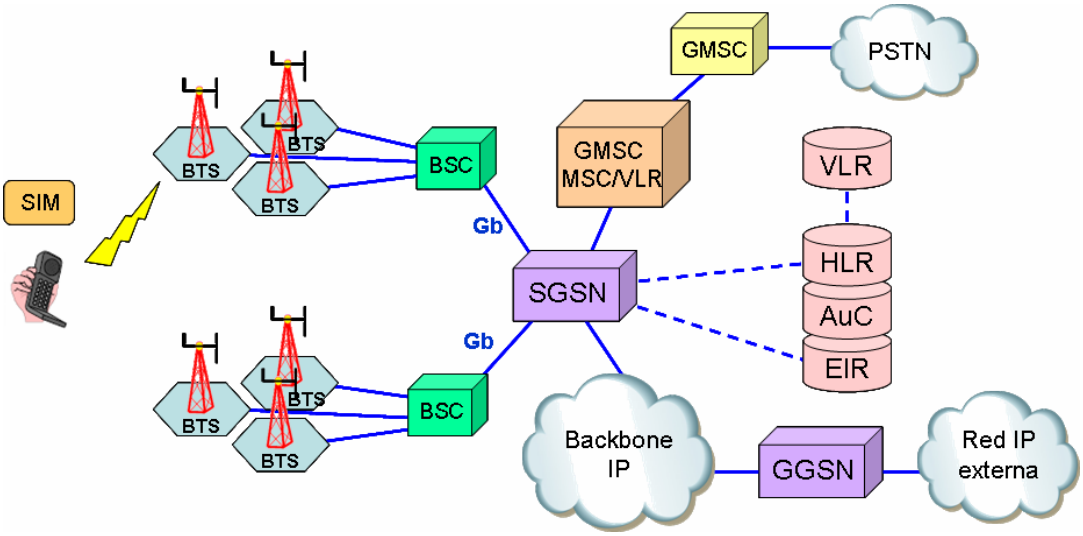



**Figura 27: Arquitectura GPRS.**

Los elementos principales introducidos en GPRS son:

- Nodos de soporte GPRS (GSN): Se encargan de integrar las redes GPRS sobre las GSM. Además, son los responsables de enrutar los paquetes de datos entre estaciones móviles y redes de paquetes de datos externas (PDN).
- Servicio de soporte de nodos de GPRS (SGSN): El SGSN almacena información de localización y perfiles de usuario de todos los usuarios registrados a dicho SGSN. Elige los datos desde y hacia las estaciones móviles sin su servicio de área. Además realiza las operaciones de un servidor AAA.
- Nodo soporte GPRS pasarela (GGSN): actúa como interfaz entre la red troncal GPRS y las redes de paquetes de datos externos. Además convierte los paquetes al protocolo de paquetes de datos correspondiente y viceversa.
- Interfaz Gb: Es la encargada de conectar la estación base de control (BSC) con el SGSN. Todas las GSN se interconectan utilizando una red troncal IP-based GPRS (Inter PLMN GPRS). Con esta troncal las GSN encapsulan los paquetes PDN y los transmiten usando GTP (GPRS tunneling protocol). Existen dos tipos de troncal GPRS:
  - Redes troncales Intra-PLMN conectan GSN a la misma PLMN y son por tanto redes IP-Based del proveedor de GPRS.

- Redes troncales Inter-PLMN conectan GSN a diferentes PLMN. Un acuerdo de roaming entre dos proveedores de red GPRS es necesario para instalar este tipo de redes.

#### 2.7.2.3.1. Acceso al Medio Físico

A diferencia de GSM, que asignaba a cada usuario ranuras de tiempo de forma indefinida, GPRS permite que los recursos de radio y time-slots sean utilizados por múltiples usuarios, asignando así un time-slot a cierto usuario en un intervalo de tiempo dado. Así, para que GPRS permita el acceso múltiple de usuarios a través de TDMA, éste coordina un número específico de tramas y time-slots en un tiempo limitado.

### 2.7.2.4.EDGE

La tecnología EDGE (Enhanced Data Rates for Global Evolution), también conocida como EGPRS (Enhanced General Packet Radio Service) corresponde al paso siguiente en la evolución de GSM hacia 3G. El objetivo de esta nueva tecnología es incrementar la tasa de transmisión de datos y la eficiencia del espectro, así como el de facilitar nuevas aplicaciones e incrementar la capacidad para usos móviles.

EDGE es introducido dentro de especificaciones y descripciones existentes en GPRS, sólo que se varía la capa física con una nueva técnica de modulación y métodos de tolerancia de errores de transmisión, combinados con mecanismos mejorados de adaptación de acoplamiento. Así, se mejora la eficiencia del espectro y de las aplicaciones. GPRS y EGPRS tienen diferentes protocolos y diferentes comportamientos en el lado del sistema de la estación base. Sin embargo, en el lado de la red, GPRS y EGPRS comparten los mismos protocolos de dirección de paquetes y por lo tanto se comportan de la misma manera. Así se aprecia en la Figura 28.

Además de aumentar el rendimiento de procesamiento de datos para cada usuario, EDGE también aumenta la capacidad. Con EDGE, durante el mismo time-slot puede atenderse a más usuarios. Esto disminuye el número de los recursos de radio requeridos para atender el mismo tráfico, y tener mayor capacidad de datos o servicios de voz. EDGE hace más fácil la coexistencia de la conmutación de circuitos y la conmutación de paquetes logrando un uso más eficiente de los recursos de radio.

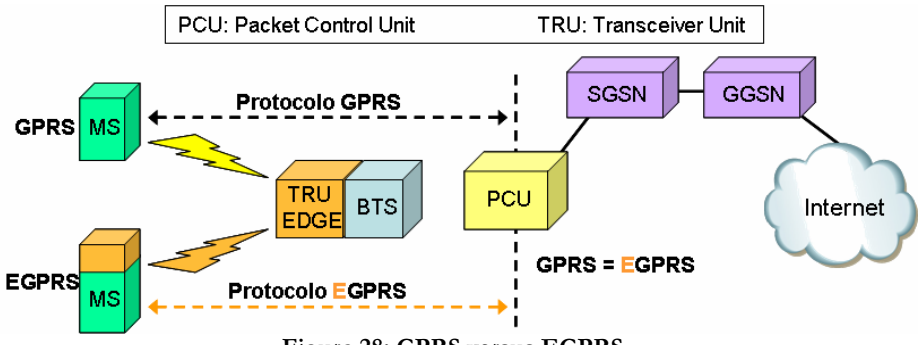



**Figura 28: GPRS versus EGPRS.**

### 2.7.2.5.UMTS

UMTS (Universal Mobile Telecommunications System) corresponde a un estándar de telefonía móvil de tercera generación que posee una red núcleo basada en la evolución de GSM y cuya red de acceso se basa en la tecnología de acceso W-CDMA (Wideband CDMA). UMTS pretende ser el paso final en la convergencia de Internet y las redes móviles, en ella, los usuarios tendrán la posibilidad de acceder a contenidos y servicios multimedia de banda ancha independientemente del lugar donde se encuentren.

El desarrollo de la arquitectura UMTS se dividió en varias fases hasta alcanzar la arquitectura final de una red integrada de servicios multimedia independientes de la posición del usuario:

- Release 1999 (R99) o primera fase o propone una evolución más o menos lógica desde las arquitecturas de segunda generación. Esta versión introduce el concepto de UTRAN (UMTS Terrestrial Radio Access Network).
- Release 4 (R4, también conocida como Release 2000) o segunda fase propone reemplazar la componente de conmutación de circuitos, que seguía vigente en la versión 99, por una red completamente basada en tráfico IP (All-IP UMTS network architecture) con una arquitectura estratificada y la implementación de calidad de servicio a nivel de transporte.
- Release 5: Implementa transporte IP sobre UTRAN, calidad de servicio punto-a-punto y se agrega IMS y HSDPA (High Speed Downlink Packet Access).
- Release 6: Realiza ampliaciones sobre IMS.

UMTS pretende entregar servicios de voz y datos con diferentes clases de servicios y con diferente calidad de servicio (QoS). Se han definido clases de calidad de servicio para responder a cuatro tipos de tráfico cuyas características se muestran en la Tabla 11, en la sección 9.2.3.1 de Anexos.

En cuanto a la arquitectura de UMTS de la especificación R99 se consideran tres categorías de elementos:

- Elementos de la red núcleo de GSM: Entre ellos están el MSC, los registros EIR, VLR y HLR y el AuC.
- Elementos de la red GPRS: Entre ellos, el SGSN y el GGSN.
- Elementos específicos de UMTS: El equipo del usuario UE (User Equipment) y la Red de Radio Acceso Terrestre UMTS (UMTS Terrestrial Radio Access Network-UTRAN).

En la Figura 29 se muestra el esquema general de la arquitectura UMTS R99 que se compone de tres grandes bloques:

- Terminales móviles UE (User Equipment) (Figura 29.a.): Consta de dos partes, el equipo móvil (ME) y el USIM (Universal Subscriber Identity Module).
- Red de acceso a radio (UTRAN) (Figura 29.b): Sus límites son la interfaz Iu hacia el Core y la interfaz Uu (interfaz de radio) hacia el UE. Considera la incorporación de dos nuevos elementos: el RNC y el Nodo B cuyas funciones equivalen a la función de la BSC y la BTS en las redes GSM/GPRS, ambas entidades juntas forman un RNS (Radio Network System).
    - Controlador de Radio de la Red RNC (Radio Network Controller): Controla uno o más nodos B. Entre sus funciones se encuentra la administración de recursos de transporte,

de control de los nodos, información del sistema, handoff y control de potencia del enlace downlink y del ciclo de control de potencia uplink, entre otros.

- Nodo B: Cada uno de estos puede proveer servicio a múltiples celdas y corresponde básicamente a una entidad lógica, entre sus funciones se encuentra la implementación lógica de los nodos, mapeo de los recursos lógicos a recursos de hardware, control del ciclo interno de control de potencia uplink, detección de errores y multiplexación en los canales de transporte, modulación y desmodulación de los canales físicos, sincronización de tiempo y frecuencia, entre otros.

- Red troncal o núcleo CN (Core Network) (Figura 29.c): Está basada en la topología de la red GSM/GPRS, provee funciones de conmutación, enrutamiento, transporte y bases de datos para el tráfico de la red, contiene elementos de conmutación de circuitos, tales como el MSC, el VLR y el GMSC, elementos de conmutación de paquetes, tales como el SGSN y el GGSN, y elementos que soportan ambos tipos de conmutación, tales como el EIR, el HLR y el AuC.

Para mayor información, en la sección 9.2.3 de Anexos, se explican algunas características técnicas de esta arquitectura como protocolos, canales físicos y lógicos e interfaces entre entidades funcionales.

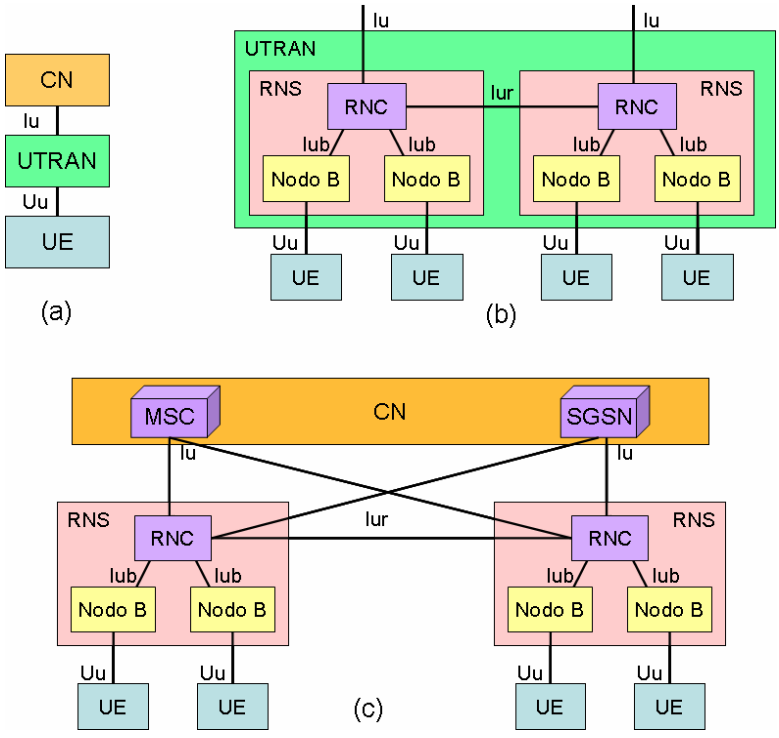



**Figura 29: Arquitectura UMTS.**

### 2.7.2.5.1. Acceso al Medio Físico

UMTS utiliza como tecnología de acceso a CDMA pero con una expansión del ancho de banda del espectro a 5 MHz, lo que se conoce como WCDMA (Wideband-CDMA).

La modulación utilizada por UMTS corresponde a QPSK (Quadrature Phase Shift Keying) y posee tanto duplexación FDD como TDD. En FDD, el enlace downlink se encuentra entre los 2110

y 2170 MHz y el enlace uplink se encuentra entre los 1920 y 1980 MHz, cada uno de estos enlaces cuenta con 12 canales portadores. En cambio, si se utiliza TDD las frecuencias utilizadas están entre los 2010 y 2025 MHz y entre los 1900 y 1920 MHz, lo que permite obtener 7 canales portadores.

Se debe tener en cuenta que todos los datos de UMTS hasta aquí mencionados corresponden a la versión 99 de esta arquitectura. La evolución de UMTS es clave para comprender el fenómeno de la convergencia de redes, por lo que procederá a mencionarlos principales cambios en las versiones siguientes de esta arquitectura.

El segundo paso en la evolución de la arquitectura UMTS corresponde a la versión 4, los principales cambio experimentados corresponden a una completa migración del tráfico de voz a tráfico IP; además, la entidad lógica MSC se divide en dos entidades funcionales:

- MGW (Media Gateway): Responsable de proveer conectividad y señalización de control (en caso de un servidor de control).
- MGC (Media Gateway Controller): Entrega servicios al MGW de forma de que este último permita acceder a redes tradicionales.

La versión 5 de UMTS, corresponde a un importante avance en la arquitectura. En este caso, los principales cambios realizados son:

- El tráfico dentro de toda la red es IP (red all-IP), incluyendo en la UTRAN.
- Como mejora al acceso de radio de la red, se implementa HSDPA (High Speed Downlink Packet Access).
- Se produce una separación entre los planos de transporte y control de la red debido a la implementación de IMS (IP Multimedia Subsystem), el que (en esta versión) posee las siguientes entidades funcionales:
  - HSS (Home Subscriber Server).
  - CSCF (Call Session Control Function), el cual puede ser de uno de estos tres tipos: Serving-CSCF, Interrogating-CSCF o Proxy-CSCF.
  - MRF (Media Resource Function) y MGCF (Media gateway Control Function), entidades que permiten que UMTS interactué con las redes tradicionales y celulares.

En la Figura 30 se muestra un esquema sobre el papel que juega IMS en la versión 5 de UMTS.

La versión 6 de UMTS realiza ampliaciones a la arquitectura de IMS de forma de implementar mensajería e imposición de los precios o cargos basado en los flujos de datos y permitiendo a UMTS operar con redes LAN inalámbricas.

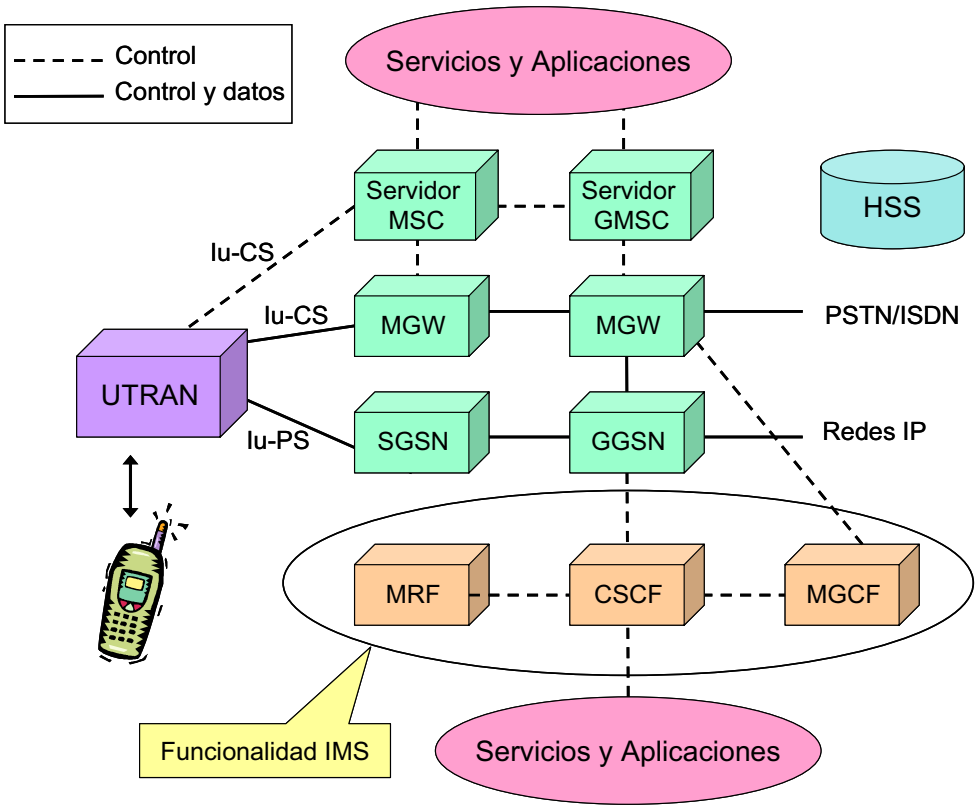



**Figura 30: Core de la Arquitectura UMTS Release 5.**

### 2.7.2.6. Resumen de Características

A continuación se presenta una tabla comparativa que muestra la evolución de las tecnologías GSM desde 1G hasta 3G junto con sus características básicas.

**Tabla 5: Comparación de Características de la familia GSM.**

| Tecnología | Generación | Acceso | Modulación | Ancho de banda | Velocidad |
|---|---|---|---|---|---|
| GSM | 2G | TDMA | GMSK | 200 KHz | 9,6 Kbps |
| GPRS | 2,5G | TDMA | GMSK | 200 KHz | 160 Kbps |
| EDGE | 2,75G | TDMA | 8-PSK | 200 KHz | 384 Kbps |
| UMTS | 3G | WCDMA | Q-PSK | 5 MHz | 2 Mbps |

## 2.7.3. VoIP

El término genérico de Voz sobre IP (VoIP) consiste en la transmisión de voz a través de la red IP por medio de protocolos IP para aplicaciones multimedia, de forma de aprovechar el ancho de banda más eficientemente que en una red telefónica tradicional o PSTN y utilizando técnicas de compresión vocal.

El estándar de VoIP fue definido por la ITU en 1996; sin embargo, VoIP no define un protocolo como estándar sino que define una serie de normas y elementos con los que debe cumplir toda red de VoIP. La IETF (Internet Engineering Task Force) definió una pila de protocolos que en su conjunto se denominó "Internet Multimedia Conferencing Architecture" (Arquitectura para aplicaciones de Conferencia Multimedia en Internet), la que se puede observar en la Figura 31.

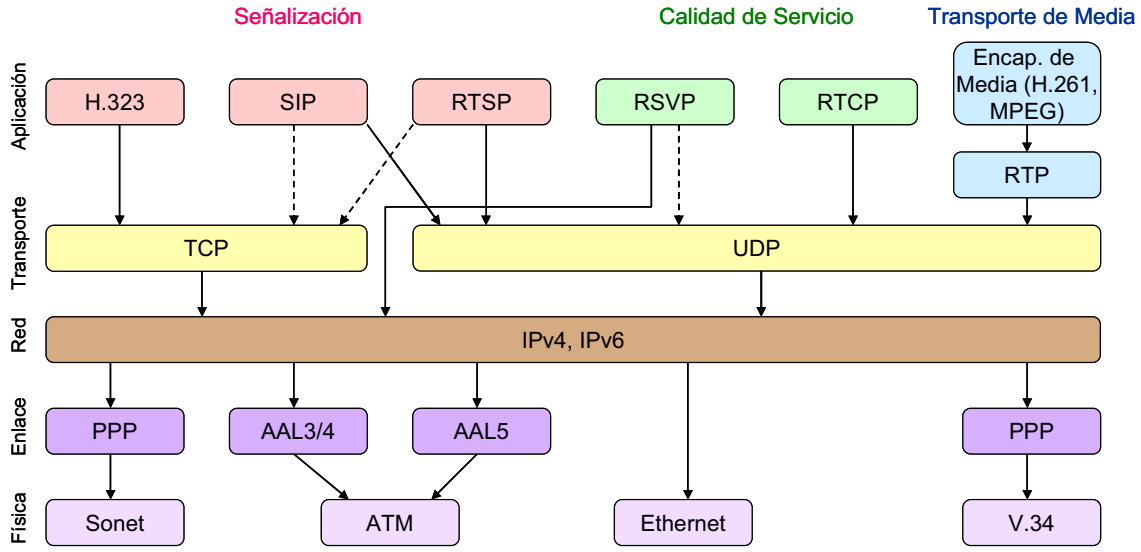



**Figura 31: Pila de Protocolos para servicios Multimedia en Internet.**

Dentro de los protocolos más importantes, se encuentran los protocolos de señalización, donde se destacan H.323 y SIP, los cuales se describirán brevemente a continuación.

### 2.7.3.1.H.323

H.323 corresponde a un protocolo creado por la ITU-T estandarizado en 1996, este protocolo recibió el nombre de "Sistemas y terminales de telefonía visual sobre redes de área local sin garantías de calidad de servicio" y fue el primer protocolo en cumplir con la normativa de VoIP.

Los terminales y dispositivos de H.323 pueden soportar aplicaciones en tiempo real (voz, video) como aplicaciones de datos y combinaciones de éstas.

La arquitectura de H.323 contiene las siguientes entidades funcionales:

- Terminal: Corresponde a un dispositivo de usuario que permite la comunicación en tiempo real con otro terminal, gateway o MCU. Puede entregar soporte de audio, video y datos y debe contener un sistema de control, el codec de audio e interfaz de la red, mientras que los codec de video y aplicaciones de datos del usuario son optativas.
- Gateway: Es el encargado de proveer la conexión entre los terminales H.323 y otros terminales de otras redes, como por ejemplo la PSTN.
- Gatekeeper: También llamado Controlador de Acceso, representa al elemento inteligente de la red H.323 y provee servicios de control de llamadas a los puntos finales. Dentro de sus funciones se encuentra la conversión de dirección IP a E.164 o viceversa, control del

establecimiento de llamadas, de ancho de banda, administración de equipos en una misma zona, enrutamiento de llamadas, tarificación, etc.

- MCU (MultiControl Unit): También llamada Unidad de Multi-Control, es la encargada de soportar conferencias entre tres o más terminales y gateways en una conferencia multipunto. Puede negociar las capacidades de los terminales y revisar capacidades durante la conferencia.

### 2.7.3.2.SIP

SIP (Session Initiation Protocol) es un protocolo de la IETF que define una arquitectura de señalización y control y cuya finalidad es la inicialización, modificación y término de sesiones multimedia (por ejemplo video, voz, mensajería, etc). SIP implementa un conjunto de funciones de procesamiento de llamadas y características similares a las de una red PSTN, es un protocolo punto a punto, escalable y con inteligencia distribuida.

SIP realiza la comunicación entre dispositivos a través de los protocolos RTP, RTCP y SDP. Una característica importante de SIP es que es un protocolo basado en texto lo que permite que sea de implementación simple, flexible y ampliable, está basado en mensajes de requerimiento y respuesta y toma muchos conceptos utilizados en protocolos como HTTP.

Dentro de las entidades funcionales necesarias para la arquitectura SIP se encuentran:

- UA (User Agent o Agente de Usuario): Son entidades que se comunican entre ellas para permitir la comunicación entre los clientes, estas comunicaciones son del tipo cliente-servidor. Éste se divide en dos componentes lógicas:
  - UAC (User Agent Client): Genera requerimientos SIP y recibe las respuestas a estos requerimientos.
  - UAS (User Agent Server): Genera respuestas a los requerimientos SIP.
- Servidores SIP: Estos pueden ser de tres tipos:
  - Proxy Server: Reenvían requerimientos y resuelven a qué servidores reenviar y, en caso que se necesite, modificando algunos campos. Dentro de los Proxy Server se contemplan dos tipos:
    - Statefull Proxy: Mantiene el estado de las sesiones mientras se procesan los requerimientos y permite la opción de forking en el envío de los requerimientos de forma de encontrar la mejor respuesta y enviarla al usuario.
    - Stateless Proxy: No mantiene el estado de las sesiones durante el procesamiento de los requerimientos sino que solamente reenvía los mensajes.
  - Registrar Server: Acepta los requerimientos de registro de los usuarios y guarda su información para brindar servicios de localización y traducción de direcciones del dominio que controla.
  - Redirect Server: Genera respuestas para el redireccionamiento de los requerimientos que recibe hacia el próximo servidor.

Los mensajes SIP pueden dividirse en requerimientos y respuestas SIP. En la Tabla 6 se muestran los distintos tipos de requerimientos SIP.

Las respuestas SIP se caracterizan por el Código de Estatus, que consiste en un número de tres dígitos que identifica la naturaleza de la respuesta. Los Códigos de Estatus se clasifican en seis clases, las que se observan en la Tabla 7.

**Tabla 6: Tipos de Requerimientos SIP.**

| Requerimiento | Descripción |
|---|---|
| INVITE | Inicia una sesión. |
| Re-INVITE | Se utiliza para cambiar el estado de la sesión. |
| ACK | Confirma el establecimiento de sesión y sólo puede ser usado con un INVITE. |
| BYE | Termina una sesión. |
| CANCEL | Cancela una invitación pendiente. |
| REGISTER | Vincula una dirección permanente a una ubicación actual y puede incluir datos de usuario. |
| OPTIONS | Investigación de capacidad, que determina características soportadas por el otro lado de la sesión. |

**Tabla 7: Tipos de Códigos de Estatus en una Respuesta SIP.**

| Códigos de Estatus | Descripción |
|---|---|
| 1xx | Respuesta Provisional/Informacional. Indica que el requerimiento fue recibido y que el recipiente va a procesarlo. |
| 2xx | Respuesta de Éxito. El requerimiento fue exitosamente recibido, entendido y aceptado. |
| 3xx | Respuesta de Redirección. Es necesario que se tomen más acciones por el requeriente para completar el requerimiento. |
| 4xx | Respuesta de Error del Cliente. El requerimiento contiene un error de sintaxis o el servidor no puede satisfacer el requerimiento. |
| 5xx | Error del Servidor. El servidor falló en satisfacer un requerimiento válido. Corresponde a una falta del servidor. |
| 6xx | Respuesta de Falla Global. El requerimiento no puede ser satisfecho por ningún servidor. Para que el servidor responda esta clase de respuesta necesita tener información definitiva del usuario. |

### 2.7.3.3.Diferencias entre H.323 y SIP

H323 y SIP poseen dos enfoques bastante distintos. Mientras que el diseño de H.323 proviene de ingenieros vinculados cercanamente con las redes PSTN, SIP fue pensado aprovechando las características de Internet. Así mismo, H.323 posee un mayor nivel de complejidad y SIP es esencialmente flexible.

En la Tabla 8, a continuación se presentan las principales diferencias entre H.323 y SIP.

**Tabla 8: Principales Diferencias entre H.323 y SIP.**

| Característica | SIP | H.323 |
|---|---|---|
| Código | Texto | Binario |
| Complejidad | Estilo HTTP | Complejo |
| Arquitectura | Modular: sólo señalización | Monolítica: señalización, control de conferencia, registro, negociación |
| Mensajería instantánea | Si | No |
| Soporte de direcciones | Cualquier URL, direcciones e-mail, H.323, http, E.164 | Host, E.164, gatekeeper aliases |
| Protocolo de Transporte | Principalmente UDP, TCP | Principalmente TCP, UDP |
| Estandarización de servicios | Estandarizar protocolos, no servicios | Estandarizar todo |
| Servicios suplementarios | Pobremente definidos | Rigurosamente definidos |
| Ajuste a Internet | Alto | Bajo (impone arquitectura ISDN a redes IP) |
| Escalabilidad | Excelente | Pobre |
| Tipos de servicios | Sin limitaciones obvias | Sólo streams media, incluyendo voz |
| Interoperabilidad | Amplia | Limitada |

### 2.7.3.4. Otros Protocolos: MGCP y MEGACO

Hasta ahora, los protocolos SIP y H.323 no describen una clara separación entre el tráfico de media y de señalización. Sin embargo, la separación entre señalización y media es deseable para la red ya sea para centralizar la inteligencia de la red y diseñar redes costo-eficientes (así se aprecia desde las arquitectura PSTN a la IMS). Luego, si existe una separación entre las entidades de control de llamadas y de manejo del stream media (como un gateway de voz), se necesita un protocolo entre estos dos tipos de entidades de forma que la entidad de control pueda administrar la entidad de stream media.

El protocolo de control más utilizado actualmente en redes de VoIP es MGCP (Media Gateway Control Protocol) desarrollado por la IETF. Sin embargo, este protocolo ha sido desplazado por MEGACO/H.248 desarrollado en conjunto por la IETF y la ITU.

MGCP es utilizado por elementos externos de control de llamadas llamados MGCs (Media Gateway Controller) para controlar los MGs (Media Gateways). Los gateways VoIP son vistos desde afuera como un único gateway VoIP. Un ejemplo de esto son los Trunking gateways que unen las redes PSTN y VoIP.

MEGACO (H.248) es un protocolo con la función de interfaz entre los Call Agents externos (MGCs) y los MGs. Este estándar es el resultado de un esfuerzo colaborativo entre las organizaciones IETF y ITU. H.248 se basa fuertemente en MGCP, pero con algunas mejoras:

- Soporta servicios multimedia y de conferencia multipunto mejorados.
- Cuenta con una mejor sintaxis para un procesamiento de mensajes más eficiente.

- Opciones de transporte TCP y UDP.
- Permite codificación binaria o de texto.
- Formaliza procesos de extensión para funcionalidades mejoradas.

A pesar de que MGCP fue utilizado primero, H.248 ha ganado terreno y una amplia aceptación en la industria como el estándar oficial para las arquitecturas de gateways descompuestos. Hoy, no hay planes para mejorar el estándar MGCP por ningún cuerpo internacional.

## 2.7.4. PacketCable

PacketCable define especificaciones para una arquitectura que permita soportar la convergencia de voz, video, datos y tecnologías móviles aprovechando las redes de banda ancha por cable. PacketCable utiliza una arquitectura y un conjunto de interfaces abiertas para soportar la rápida introducción de nuevos servicios IP sobre las redes de cable. Esta arquitectura posee múltiples versiones, las que fueron desarrolladas para brindar inicialmente servicios de voz y multimedia. La versión PacketCable 2.0 está basada la arquitectura IMS Release 6 de la 3GPP, pero adaptada a las redes de cable.

PacketCable pretende ser una arquitectura flexible de forma que sea una plataforma que entregue las capacidades básicas necesarias para entregar servicios tales como:

- VoIP residencial y comunicaciones IP de video; Capacidades como videotelefonía, tratamiento de llamadas basado en presencia, capacidad de terminales e identidad entre otros.
- Características de integración de plataformas, como el nombre de la persona que llama e identificación del número en la TV y manejo de la llamada desde la TV.
- Servicios de Movilidad e integración con celulares y redes inalámbricas; capacidades como handoff de llamada y roaming entre VoIP de PacketCable sobre Wi-Fi y redes celulares inalámbricas, integración de buzón de voz, y un único número E.164 (por ejemplo, un número telefónico).
- Aplicaciones multimedia, como audio con QoS y video streaming.
- Extensiones de servicios comerciales, como extensiones de PBX, servicios IP Centrex para negocios pequeños y medianos, etc.
- Extensiones de telefonía SIP residencial, como características de la telefonía tradicional (por ejemplo, llamada en espera), servicios de operadora y de emergencia.

Para un conocimiento más acabado, en la sección 9.2.4 de Anexos, se explican algunas características técnicas de esta arquitectura como sistemas de soporte operacional, interfaces entre componentes funcionales, y principales protocolos.

### 2.7.4.1. Evolución de PacketCable

A grandes rasgos, cada versión abarca las siguientes implementaciones:

- Release 1.0: Brinda soporte para aplicaciones de telefonía usando E-MTAs.
- Release 1.5: Entrega nuevas capacidades y agrega SIP para la administración de sesión dentro y entre redes PacketCable.

- Multimedia: Separa capacidades de QoS y define una arquitectura genérica de QoS.
- Release 2: Agrega soporte para endpoints basados en SIP y una plataforma de servicio basada en SIP que puede ser utilizada para soportar variados servicios.

La Figura 32 ilustra las versiones de PacketCable. PacketCable 2.0 utiliza a PacketCable Multimedia para QoS. PacketCable Multimedia, sin embargo, está separada y puede ser usada por otras aplicaciones también. Las aplicaciones que hacen uso de la plataforma de servicio SIP están definidas en versiones separadas autónomas y no se muestran en la Figura 32.

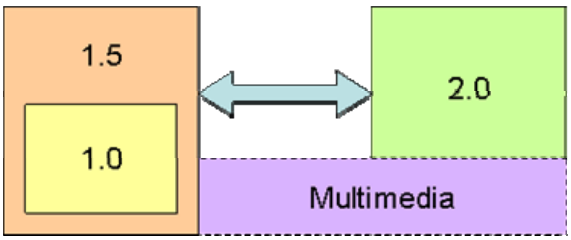



**Figura 32: Relación entre las distintas versiones de PacketCable.**

## 2.7.4.2.Arquitectura

En la Figura 33 se muestra un diagrama básico de la arquitectura PacketCable correspondiente a la Release 2.0.

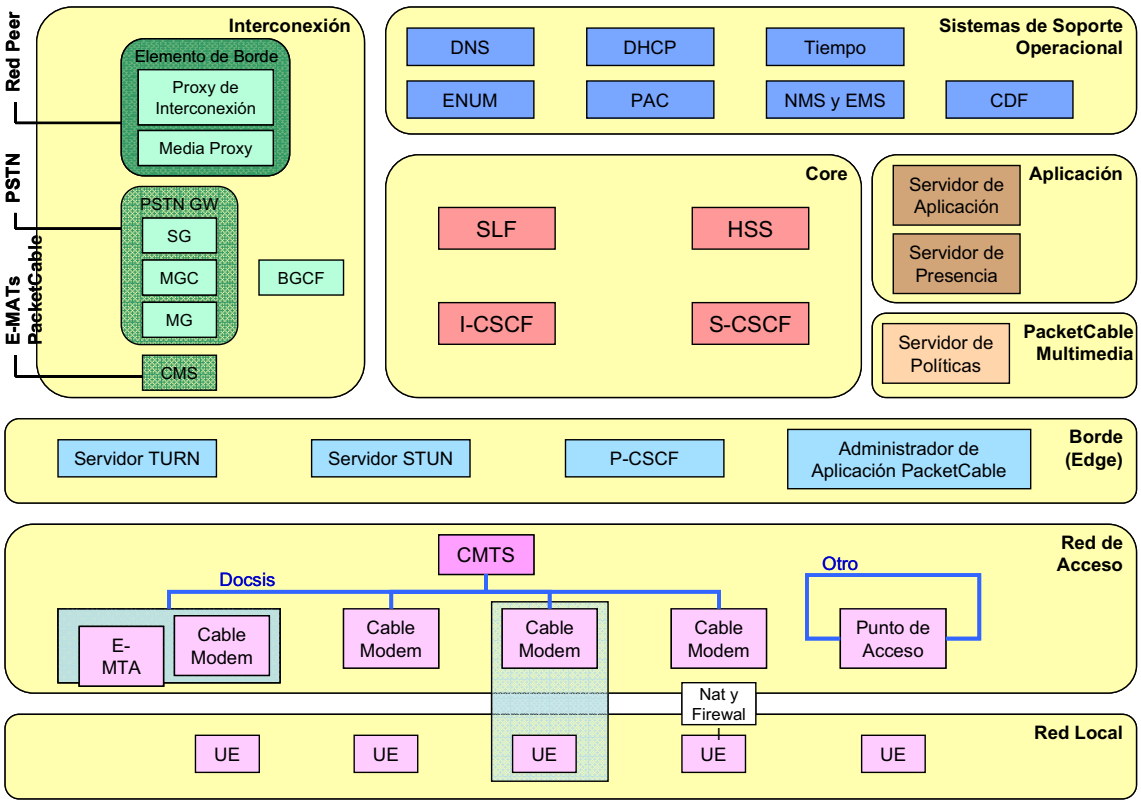



**Figura 33: Arquitectura PacketCable Release 2.0.**

A continuación se explicará brevemente cada bloque funcional de esta arquitectura:

#### 2.7.4.2.1. Red Local

En la red local se encuentran dos entidades principales:

- UE (User Equipment): PacketCable soporta clientes para servicios de telefonía. PacketCable Multimedia provee un marco de QoS y contabilidad. PacketCable agrega soporte para clientes basados en SIP con una variedad de capacidades, por ejemplo: soft y hard phones, teléfonos inteligentes, teléfonos inalámbricos o alámbrico, UEs de mensajería instantánea, terminales de video, etc. Los UE pueden ser dispositivos fijos o móviles tales como notebooks o teléfonos Wi-Fi. Pueden estar en la red de acceso cable, o pueden obtener servicios de otras redes de acceso.
- NAT y Firewall: Entre la red local y la red de acceso pueden estar presentes un NA(P)T (Network Address and Port Translation) y un Firewall. Como un NAT puede modificar direcciones IP y puertos y un Firewall restringe el acceso, la señalización y planos portadores necesitan comportarse en forma diferente cuando se insertan entre el UE y P-CSCF.

#### 2.7.4.2.2. Red de Acceso

El UE se conecta al Borde (Edge) a través de la red de acceso de cable existente o a través de otras redes de acceso (por ejemplo, puntos de acceso Wi-Fi públicos, redes celulares 3G de datos). Los elementos de la red de acceso entregan conectividad IP y los recursos de QoS necesarios por el UE para desplegar los servicios PacketCable.

En la red de acceso se pueden encontrar las siguientes entidades funcionales:

- CM (Cable Modem): El CM corresponde al CPE (Customer Premise Equipment) usado en conjunto con el CMTS para entregar servicios de transporte de datos en banda ancha sobre la red de acceso de cable HFC. Un E-MTA corresponde a un cliente basado en señalización de llamadas de red con un cable módem embebido. Es importante notar que, mientras el E-MTA no se comunica directamente con la red, un servicio de telefonía basado en señalización de red y un servicio basado en señalización SIP pueden entregarse a través del mismo CM. Además, los UE PacketCable 2.0 también pueden estar embebidos con un CM.
- CMTS (Cable Modem Termination System): El CMTS se encuentra en el headend del operador de red y, en conjunto con el CM, es utilizado para entregar transporte de datos de banda ancha sobre la red de acceso de cable HFC.
- Punto de Acceso: PacketCable puede ser utilizado para entregar servicios a los UEs que reciben conectividad IP a través de distintos tipos de redes de acceso.

El resto de la arquitectura se basa en IMS y se describe en la sección 9.2.4.1 de Anexos.

## 2.8. Tecnologías de Acceso

### 2.8.1. HFC

La red HFC (Hibrid Fibre Coaxial) es una red que corresponde a la evolución de las redes CATV coaxial para poder soportar otros tipos de servicios además de la televisión y tráfico

ascendente. La tecnología CATV surgió a partir de los años 60 y se caracterizaba por la transmisión de señal analógica sobre cable coaxial, ser unidireccional (sistemas broadcasting), con una topología de distribución en árbol y tecnología FDM (6 MHz por canal). El desarrollo de Ethernet permitió que se viera la oportunidad de utilizar el acceso de cable coaxial a los hogares para extender LANs; la hibridación de la red se produjo simultáneamente con el desarrollo del mundo Internet y la demanda de los usuarios de banda ancha.

La idea de una red HFC es llegar con fibra hasta un nodo y luego los usuarios de cada nodo se unen con un bus de cable coaxial. Sobre estas redes se pueden brindar servicios de televisión (tanto señal analógica como digital), de datos (principalmente basados en DOCSIS) y de Voz (basado principalmente en PacketCable). El espectro de radiofrecuencia en HFC se divide en dos regiones:

- Tráfico ascendente: Frecuencias entre 5 MHz y 40 MHz.
- Tráfico descendente y CATV: Frecuencias mayores a 50 MHz.

La estructura básica de una red HFC se compone de una cabecera (o headend) que funciona como un centro de control y emisión, la red troncal de fibra óptica que distribuye las señales hacia los nodos primarios (o hubs), la red secundaria que une los hubs con los nodos finales, los cuales distribuyen la señal a los clientes ya sea a través de un cable módem (CM) o MTA (Multimedia Terminal Adapter).

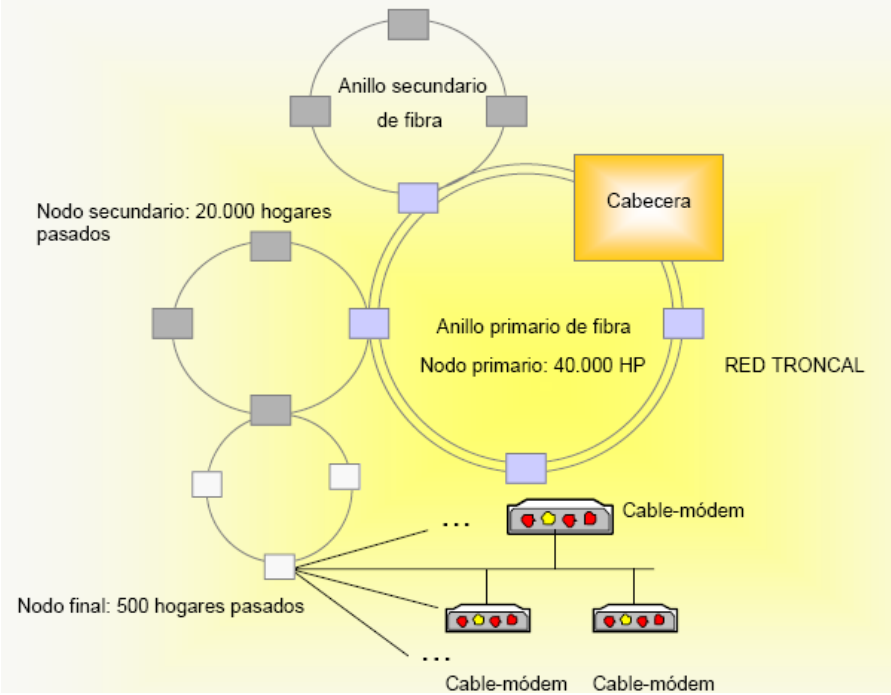



**Figura 34: Arquitectura de Acceso HFC.**

Para contar con una mayor robustez de la red, la red troncal de fibra óptica se construye en un doble anillo; los nodos ópticos principales reparten la señal hacia los anillos secundarios, donde otros nodos realizan la conversión opto-eléctrica de la señal u electro-óptica dependiendo si es tráfico descendente o ascendente respectivamente. En la Figura 34 se observa que cada nodo soporta cerca de 500 hogares y la red final posee una topología de anillo.

Para lograr una conexión a Internet o realizar una llamada telefónica a través de la red HFC se debe contar con un canal extra para transportar la señal de telefonía y datos ascendentes y descendentes. En la Figura 35 se muestra un diagrama de la red HFC para proveer televisión, telefonía e Internet.

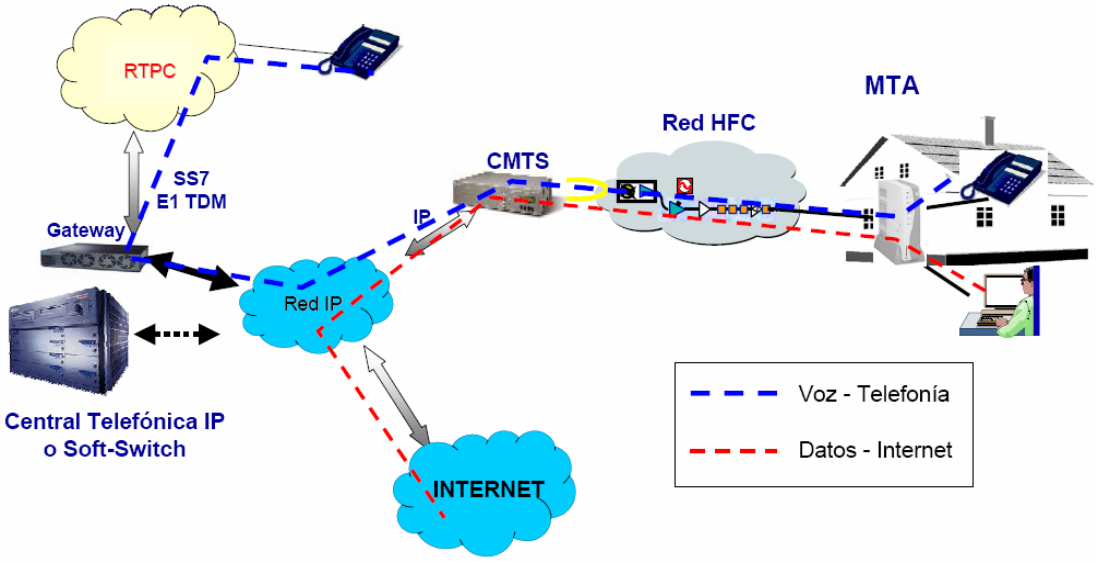



**Figura 35: Red HFC Actual.**

La entidad clave en esta arquitectura es el CMTS (Cable Modem Termination System), que corresponde a la función que permite el acceso de los CMs a la red telefónica tradicional (PSTN), red telefónica IP o a Internet.

## 2.8.2. xDSL

xDSL (x – Digital Subscriber Line) corresponde a una tecnología de acceso que reutiliza las redes de pares de cobre de telefonía tradicional para brindar acceso a Internet de banda ancha y, por tanto, permitiendo utilizar la red telefónica ya existente para transmitir datos.

xDSL está compuesto por un conjunto de "sabores" de tecnologías (cada una de las cuales se diferencia de las demás en el nombre por su primera letra, la que se generaliza con una "x") que transforman las líneas analógicas en digitales. xDSL corresponde a una tecnología punto a punto que funciona con un módem tanto en el lado del cliente como en el de la central telefónica (cada módem adaptado a las distintas necesidades de cada extremo) y sin amplificadores o repetidores entre ambos extremos.

La tecnología xDSL más masificada corresponde a ADSL, pero existen muchas otras variantes.

### 2.8.2.1.Asymmetrical DSL (ADSL)

Más que una nueva tecnología de acceso, ADSL es una tecnología de módem que es capaz de transmitir velocidades entre 1.5 Mbps y 6 Mbps bajo la tecnología actual. El módem ADSL además provee el proceso de multiplexación por división de frecuencia para separar los tráficos de voz y

datos para el transporte a través del bucle, tarea que actualmente es realizada por el splitter. Los tipos de multiplexación utilizados en ADSL son CAP (Carrierless Amplitude/Phase) o DMT (Discrete Multitone).

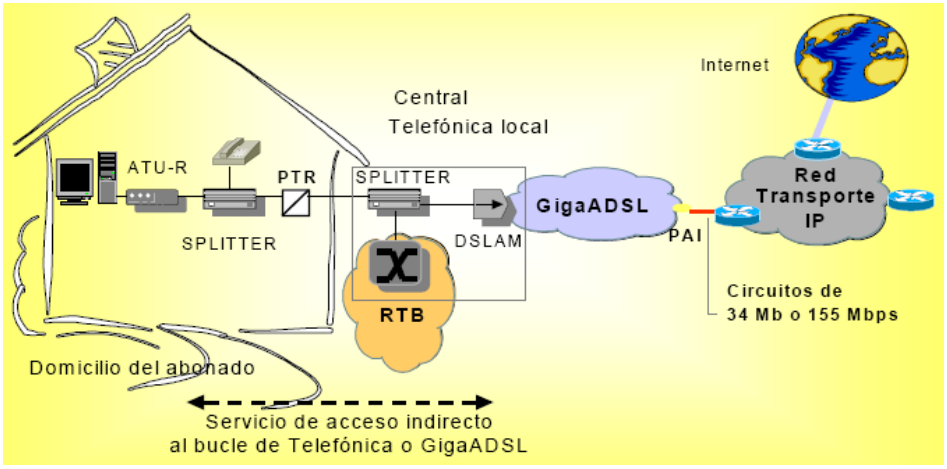



**Figura 36: Arquitectura de una red de acceso ADSL.**

ADSL recibe ese nombre por la asimetría existente entre su velocidad de datos ascendente y descendente. En la Figura 36 se observa la arquitectura de una conexión a Internet a través de ADSL, en la central se reciben distintas señales ADSL de un conjunto de clientes donde cada señal pasa por su filtro o splitter y luego se concentra en un único punto para su transporte a través de una red ATM. El multiplexor que une las líneas ADSL que llegan a la central recibe el nombre de DSLAM (Digital Subscriber Line Access Multiplexer).

### 2.8.2.2.Otros "sabores" xDSL

En la tabla a continuación se presentan las principales variantes de xDSL con sus principales características.

**Tabla 9: Resumen de las principales características de algunas tecnologías xDSL.**

| Nombre | Significado | Download | Upload | Modo de Operación |
|---|---|---|---|---|
| ADSL | Asymmetric DSL | 1.5 a 8.192 Mbps | 16 a 640 Kbps | Diferentes velocidades download y upload, un par de cables. |
| RADSL | Rate Adaptive DSL | 64 Kbps a 8.192 Mbps | 16 a 768 Kbps | Diferentes velocidades download y upload, diferentes operaciones comunes usan 768 Kbps. Un par de cables. |
| CDSL | Consumer DSL | 1 Mbps | 16 a 160 Kbps | Actualmente ratificado como DSL-lite (G.lite). No usa splitters. Un par de cables. |
| HDSL | High-data rate DSL | 1.544 Mbps (Norteamérica) | 1.544 Mbps | Servicios simétricos. Dos pares de cable. |
| | | 2.048 Mbps (resto del mundo) | 2.048 Mbps | |
| IDSL | ISDN DSL | 144 Kbps (64+64+16) como BRI | 144 Kbps (64+64+16) como BRI | Operación simétrica. Un par de cables. ISDN BRI. |
| SDSL | Single DSL | 1.544 Mbps, 2.048 Mbps | 1.544 Mbps, 2.048 Mbps | Usa sólo un par de cables, pero típicamente entrega 768 Kbps |
| VDSL | Very High data rate DSL | 13 a ~52 Mbps | 1.5 a 6 Mbps | Se necesita fibra y probablemente ATM |
| SHDSL | Single High-speed DSL | 192 Kbps a 2.36 Mbps | 192 Kbps a 2.36 Mbps | Usa un par de cables |
| | | 384 Kbps a 4.72 Mbps | 384 Kbps a 4.72 Mbps | Usa dos pares de cables |

### 2.8.3. WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) nace del estándar 802.16 Wireless MAN (Metropolitan Area Network) de Interfaz aérea de la IEEE y es una especificación que posee una arquitectura Punto-a-Multipunto (PMP). WiMAX ha evolucionado en sus características a través de las distintas versiones desarrolladas, las que se nombran a continuación:

- 802.16: Su rango de frecuencia está entre los 10 y 600 GHz y requiere de línea de vista (LOS: Line of Sight).
- 802.16a: Su rango de frecuencia está entre los 2 y 11 GHz y no requiere de línea de vista (NLOS: Non Line of Sight).

- 802.16d (o 802.16-2004): Se basa en 802.16 y 802.16a con algunas mejoras haciendo obsoletos los estándares anteriores. También soporta espectro bajo los 11 GHz y dispone de transmisión TDD y FDD.
- 802.16e: Posee la capacidad de entregar características de movilidad y portabilidad implementándolas en las capas MAC (de enlace) y PHY (física).
- 802.16g: Es capaz de soportar movilidad en capas superiores a las capas 1 y 2 y a través del backhaul (Backhaul es un término referido al transporte de tráfico entre sitios distribuidos, por ejemplo puntos de acceso, y puntos de presencia más centralizados). Esta estandarización no se ha determinado y es muy pronto para estimar los cambios requeridos cuando esta fase del estándar esté disponible.

Los estándares actuales especifican el uso de OFDM (Orthogonal Frequency Division Multiplexing) u OFDMA (Orthogonal Frequency Division Multiple Access). OFDMA se basa en OFDM y combina técnicas de división de tiempo de y frecuencia para una utilización más eficiente del espectro. En la Tabla 10 se muestra una comparación entre las dos versiones de WiMAX más recientes.

**Tabla 10: 802.16d versus 802.16e.**

| **Características** | **802.16d** | **802.16e** |
|---|---|---|
| Frecuencia | 2-11 GHz licenciado y no licenciado | 2-6 GHz licenciado y no licenciado |
| Línea de vista | NLOS | NLOS |
| Movilidad | Fijo y Nómada | Nómada (máxima velocidad ~70 Km/hr) |
| Rango | Radio promedio de celda 6,4 – 9,6 Kms | Radio promedio de celda 1,6 – 4,8 Kms |
| Canalización | Escalable1,5 - 20 MHz | Escalable1,5 - 5 MHz con sub-canales |
| Eficiencia Espectral | < 3,75 bps/Hz | < 3 bps/Hz |
| Tasa de bits | < 75 Mbps(20 MHz BW*) | < 15 Mbps(5 MHz BW) |
| Duplexación | TDD / FDD | TDD / FDD |
| Encriptación | Mandatoria -3DES Opcional-AES | Mandatoria-3DES Opcional-AES |
| Familia de Tecnología y Modulación | OFDM/OFDMA QPSK, 16QAM & 64QAM | Scalable OFDMA QPSK, 16 QAM & 64 QAM |

* BW: Bandwidth; ancho de banda.

Una MAN wireless basada en el estándar WiMAX se configura de forma muy similar a una red celular tradicional con estaciones base estratégicamente ubicadas utilizando una arquitectura punto-a-multipunto para entregar servicios a un área de algunos kilómetros de radio dependiendo de la frecuencia, potencia de transmisión y sensibilidad del receptor. Normalmente, las estaciones base son conectadas con un retorno al centro de la red mediante fibra o enlaces microondas punto-a-multipunto hacia nodos de fibra disponibles o a través de líneas arrendadas de algún operador de líneas cableadas. En la Figura 37 se muestra un diagrama básico de la arquitectura de WiMAX.

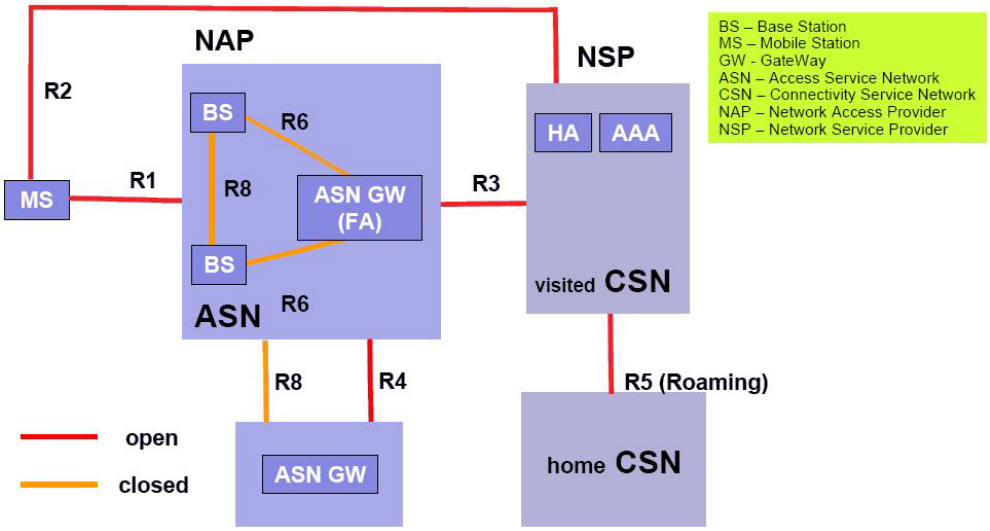



**Figura 37: Arquitectura de Referencia de WiMAX.**

El rango y la capacidad NLOS de WiMAX hacen atractiva a la tecnología y efectiva en costos en un amplio conjunto de ambientes. Esta tecnología fue ideada desde el principio como una forma de entregar acceso de banda ancha inalámbrico a la "última milla" en redes MAN con un desempeño y servicios comparables a las tecnologías de acceso tradicionales como DSL, Cable o líneas T1/E1.

# Capítulo 3
# Metodología

En este capítulo se describe la metodología utilizada en el presente documento para alcanzar los objetivos del trabajo de memoria y sus correspondientes resultados. En el capítulo anterior ya se entregó un marco de las arquitecturas de telefonía existentes, ahora se pretende ilustrar cómo es que estas arquitecturas interaccionan entre ellas para comunicarse y finalmente poder llegar a una arquitectura convergente como resultado del documento.

Así, primero se realizarán las siguientes tareas:

- Cómo es que funciona la arquitectura IMS mencionada en el capítulo anterior y algunos de sus procesos más importantes.
- Se analizarán las similitudes entre IMS y la arquitectura PSTN y entre IMS y PacketCable.
- Se establecerán los procesos de interoperación entre IMS y otras arquitecturas de redes de modo de obtener como resultado una arquitectura convergente.
- Se estudiará el funcionamiento de WiMAX como tecnología de acceso.

## 3.1. Conceptos y Funcionamiento de IMS

IMS corresponde a una arquitectura de red agnóstica del acceso, ya sea a través de las redes tradicionales o legacy (PSTN o GSM) o a través de tecnologías de acceso IP tales como xDSL, cable o tecnologías inalámbricas.

Como se vio anteriormente, IMS corresponde a una arquitectura orientada a los servicios, por lo que puede representar la clave para la interacción entre redes de distinto tipo y lograr así la convergencia de servicios y de redes.

### 3.1.1. Identificación de Usuarios

Existen dos tipos de identidades de usuario en IMS, una pública y una privada, las que se explicarán a continuación.

### 3.1.1.1. Identidad Privada de Usuario

La identidad privada de usuario es una identidad global única definida por el operador de la red Home y todo usuario de la red debe tener por lo menos una, la que puede utilizarse sólo para identificar al usuario desde una perspectiva de red y ser utilizada para propósitos de registro, autorización, administración y accounting. Ésta no identifica al usuario como persona sino que identifica la suscripción del usuario y será válida mientras exista dicha suscripción. Esta identidad tiene la forma de un NAI (Network Access Identifier) y debe ser almacenada en forma segura por una aplicación ISIM (IMS Identity Module) sin que el usuario pueda modificarla.

### 3.1.1.2. Identidad Pública de Usuario

Estas identidades son utilizadas para requerimientos de comunicación con otros usuarios y pueden ser publicadas (por ejemplo, en directorios telefónicos, tarjetas de presentación o páginas Web). Un usuario puede tener una o más identidades públicas y es necesario que sea capaz de utilizarse tanto en la numeración de la telefonía tradicional o para el enrutamiento en Internet. La identidad pública puede tener la forma de una SIP URI (Uniform Resource Identifier) o de URL (Uniform Resource Locator) de teléfono y por lo menos una identidad pública se debe almacenar en una aplicación ISIM. Es importante destacar que la identidad pública de usuario no es utilizada para fines de autentificación de usuario.

### 3.1.1.3. Relación entre la Identidad Privada y pública de Usuario

En la Figura 38 se muestra un ejemplo de un usuario con dos identidades privadas, la segunda es para su entorno laboral y la primera para su entorno familiar y amigos. Es posible que cada identidad privada tenga una colección de datos e identidades públicas diferentes pero en este ejemplo ambas identidades privadas comparten una identidad pública. Los dos profiles de servicio pueden estar programados y administrados de forma distinta, por ejemplo, las sesiones SIP realizadas desde el trabajo pueden desviarse a un buzón de mensajes durante los fines de semana.

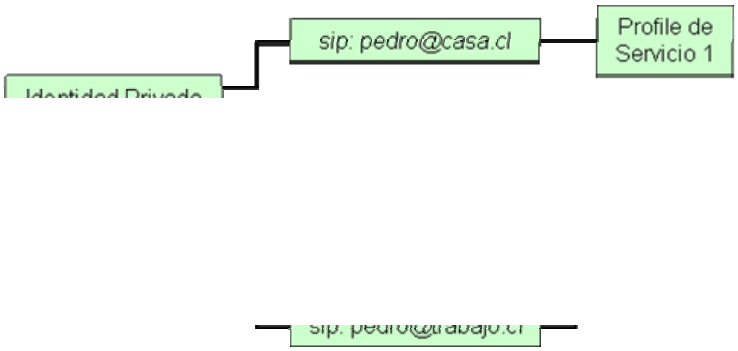



**Figura 38: Ejemplo de la Relación entre Identidades de Usuario.**

El Profile de Servicios de IMS es una colección de datos de servicios del usuario con un conjunto de características de registro independientes. El Profile de servicios es definido y mantenido en el HSS (Home Subscriber Server, la base de datos relacionada con los clientes de una red) y su alcance se limita al dominio del IMS. El S-CSCF tiene los datos de un solo Profile de Servicio de usuario en un momento.

### 3.1.2. Descubrimiento al Punto de Entrada de IMS

Para que el UE o terminal de usuario sea capaz de comunicarse con la arquitectura IMS de la red, éste debe saber al menos una dirección del P-CSCF (recordar que el Proxy-CSCF es el primer servidor SIP con el que se contacta el UE). Para esto, la 3GPP cuenta con dos procedimientos, uno para el acceso a través de la red GPRS y otro para el acceso a través de una red genérica utilizando un procedimiento DNS del protocolo DHCP.

En la Figura 39 se muestra el procedimiento realizado a través de una red GPRS. El UE envía un requerimiento de activación en un contexto PDP, en el cual agrega un flag para solicitar la dirección IP del P-CSCF y recibe una respuesta con la o las direcciones de P-CSCFs. Esta información es transportada a través de los elementos de red de GPRS, el SGSN y el GGSN.

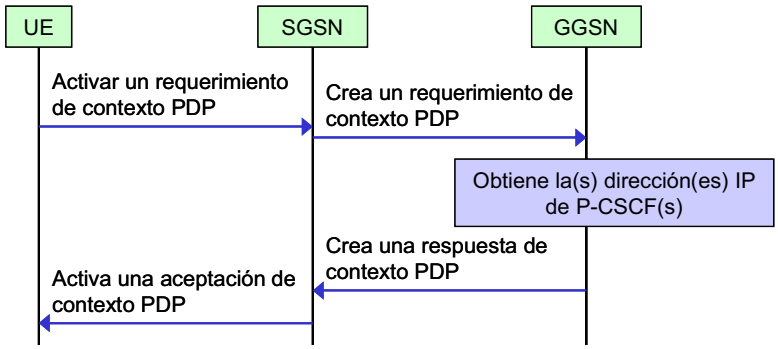



**Figura 39: Mecanismo para el descubrimiento del P-CSCF a través de GPRS.**

En la Figura 40 se muestra el procedimiento genérico para el descubrimiento del P-CSCF. En este proceso el UE envía una consulta DHCP a la red de acceso de conectividad IP (IP-CAN: IP Connectivity Access Network), la cual reenvía el requerimiento a un servidor DHCP. La respuesta al UE es una lista que puede que contenga los dominios de P-CSCFs o de direcciones IPv6 de P-CSCFs. Luego de obtener la lista, el UE realiza una consulta a un servidor DNS para encontrar la dirección IP del P-CSCF.

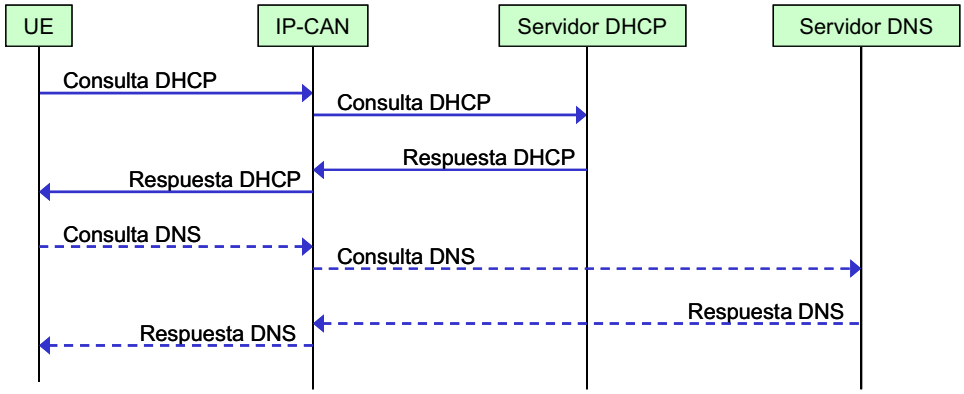



**Figura 40: Mecanismo Genérico para el descubrimiento del P-CSCF.**

### 3.1.3. Aspectos de Seguridad en IMS

La arquitectura de seguridad en IMS consta de tres bloques funcionales, los que se explican a continuación:

- Seguridad de Dominio de Red (NDS: Network Domain Security).
- Seguridad de Acceso a IMS.
- Autentificación y Acuerdos de Clave (AKA: Authentication and Key Agreement).

#### 3.1.3.1. Autentificación y Acuerdos de Clave (AKA)

La seguridad en IMS se basa en una clave secreta de varios términos, la que se comparte entre el ISIM y el AuC de la red. El módulo ISIM se desempeña como un bloque de almacenamiento para la clave secreta compartida (K) y está embebido en la tarjeta UICC (Universal Integrated Circuit Card). Para proteger a la tarjeta ISIM de acceso no autorizado se utiliza seguridad combinada de posesión (es decir, el acceso al dispositivo físico) y conocimiento (el usuario debe conocer el código PIN de la tarjeta).

AKA provee autentificación mutua del ISIM y el AuC y establece un par de claves de cifrado e integridad. Para el proceso de autentificación se utiliza un requerimiento de autentificación que contiene un reto o desafío aleatorio (RAND) y un token de autentificación de red (AUTN). El ISIM verifica el token y tanto éste como la red mantienen una secuencia de números para cada proceso de autentificación. El ISIM responde al requerimiento de la red aplicando la clave secreta al desafío aleatorio para producir una respuesta de autentificación (RES) la que sirve para autentificar el ISIM en la red.

#### 3.1.3.2. Seguridad de Domino de Red (NDS)

El sistema IMS también protege el tráfico en el core de la red de forma de proveer confidencialidad, integridad de datos, autentificación y protección de tráfico mediante el uso de mecanismos criptográficos de seguridad y protocolos de seguridad aplicados en seguridad IP (IPSec).

La parte central de NDS son los dominios de seguridad, usualmente un dominio de seguridad es una red operada por una única autoridad administrativa (en muchos casos referido al core de la red) que mantiene políticas uniformes de seguridad en el dominio. En NDS se definen dos tipos de interfaces:

- Interfaz Za: Utilizada entre diferentes dominios de seguridad y su uso es mandatorio.
- Interfaz Zb: Utilizada entre nodos dentro de un mismo dominio de seguridad. Su uso es opcional.

Cuando se tiene un flujo de tráfico entre dos dominios de seguridad, estos pasan a través de un gateway de seguridad (SEG), el que se ubica en el borde del dominio de seguridad y tuneliza tráfico a otros dominios. El SEG es responsable de aplicar las políticas de seguridad entre los dominios, lo que incluye filtrado de paquetes o funcionalidad de Firewall. Además es responsable de levantar y mantener las Asociaciones de Seguridad (SAs) IPSec con los otros SEGs. Las SAs son negociadas usando el protocolo IKE (Internet Key Exchange) y sólo dos SAs pueden establecerse en un SEG: para tráfico entrante y para tráfico saliente. En general, el tráfico se encuentra encriptado, con

protección de integridad de datos y autentificación mediante el protocolo ESP (IPSec Encapsulating Security Payload).

En la Figura 41 se muestra el uso de dominios y gateways de seguridad para dos usuarios que se encuentran en su red Home.

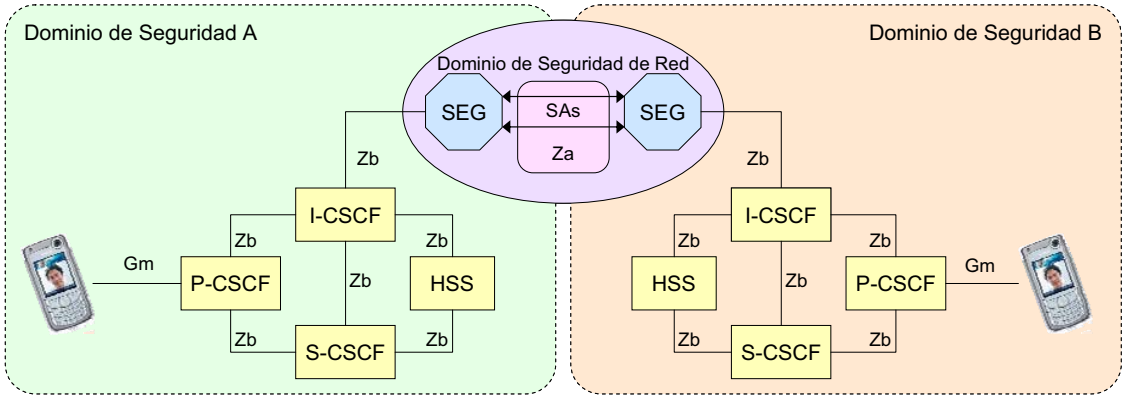



**Figura 41: Uso de Dominios de Seguridad de Red y Gateways de Seguridad.**

### 3.1.3.3. Seguridad de Acceso a Servicios de IMS

En seguridad, existen dos tipos de seguridad para acceder a servicios, uno de ellos es para servicios basados en SIP, el segundo es para servicios basados en HTTP. Dado que SIP es una parte muy importante de IMS, una clave de seguridad es proteger la señalización SIP en IMS de forma que se debe proteger de forma especial la interfaz entre el terminal de usuario y el P-CSCF (denominada Gm).

De esta forma, IMS define un "dominio de confianza" que incluye los elementos P/I/S-CSCF, BGCF (Breakout Gateway Control Function), MGCF/MRFC (Media Gateway Control Function / Multimedia Resource Function Controller) y todos los AS que no estén controlados por una tercera parte. La principal componente de confianza es la identidad de la entidad, que debe ser conocida y verificada por los otros nodos dentro de la red para establecer alguna relación. El nivel de confianza dependerá del rol que tiene la entidad en la red por lo que la confianza está condicionada por la función que cumple la entidad. Además, la confianza entre entidades es transitiva a otras entidades, es decir, si el nodo A tiene cierto nivel de confianza en B y B en C, luego A también tendrá cierto nivel de confianza en C.

Los términos que definen el comportamiento esperado para una entidad en el dominio de confianza (por ejemplo, el dominio F) y las garantías del cumplimiento de comportamiento en dicho dominio necesitan ser especificados en el llamado "Spec(F)".

En IMS, el usuario puede requerir que su identidad no sea revelada a las entidades fuera del dominio de confianza, esto lo realiza insertando sus preferencias de privacidad en un header de privacidad que es inspeccionado por la red. La autentificación para acceder a IMS se basa en el protocolo AKA, cuyos mensajes se transmiten tunelizados a través de SIP. Además de la autentificación, el UE necesita negociar los mecanismos de seguridad que serán utilizados en la interfaz Gm con la red IMS. La integridad de datos y la autentificación son mandatorios y son proveídos a través del protocolo ESP IPSec.

Además del tráfico basado en SIP, es necesario para el UE que se administren datos asociados con ciertas aplicaciones de IMS. De esta forma se necesita implementar confidencialidad y protección de integridad de datos basados en tráfico HTTP en la interfaz Ut (entre el UE y el AS).

## 3.1.4. Control de los Portadores de Tráfico

Para que el operador pueda brindar servicios, el sistema IMS debe ser capaz de controlar la QoS de las sesiones de usuario junto con el término/inicio de ellas. Para esto, el plano de control y el plano de usuario deben se capaces de interactuar entre ellos. Se pueden distinguir dos tipos de arquitecturas para el control de portadores. En el primer modelo el usuario accede a la red a través de GSM o UMTS, en el segundo modelo, la red de acceso corresponde a una red IP, generalmente inalámbrica.

### 3.1.4.1. Control para Acceso a través de UMTS o GPRS

Para este caso, existe un sistema para autorizar y controlar el uso de los portadores de tráfico llamado Control SBLP (Service-Based Local Policy Control). En la Figura 42 se muestran las entidades funcionales de este sistema.

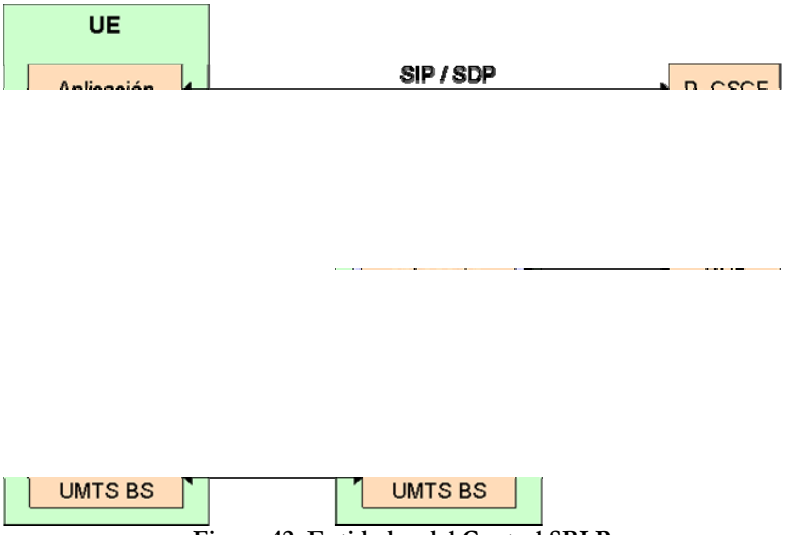



**Figura 42: Entidades del Control SBLP.**

Las entidades mostradas incluyen un PDF (Policy Decision Function) y un P-CSCF (Proxy-CSCF, el servidor SIP de contacto entre el UE y la arquitectura IMS). El resto de las componentes son:

- Administrador IP BS (Bearer Service: Portador de Servicio): administra y controla el IP BS externo usando un mecanismo IP estándar. Esta entidad se encuentra en el GGSN, pero puede encontrarse también en el UE y puede soportar funciones de diferenciación de servicio (DiffServ) y de RSVP (Resource ReSerVation Protocol, RFC 2205).
- Función Traducción/Mapeo: Permite la interoperación entre los parámetros y mecanismos usados dentro del Administrador UMTS BS y el Administrador IP BS. Esta función se encuentra en el GGSN pero también puede estar dentro del UE.

- Administrador UMTS BS: Se encarga de los requerimientos de reservación de recursos desde el UE y se encuentra tanto en el UE como GGSN.
- Punto de aplicación de Políticas: Aplica las decisiones de políticas realizadas por el PDF y se encuentra en el Administrador IP BS del GGSN.
- PDF: Elemento lógico de decisión de políticas que usa mecanismos IP estándar para implementar SBLP en la capa de portadores IP.
- Función de Aplicación (AF: Application Function): Ofrece servicios que requieren el control de portadores de recursos IP compartidos. El AF mapea parámetros a nivel de aplicación de QoS dentro de información de establecimiento y envía la información al PDF a través de la interfaz Gq. Un ejemplo de AF es el P-CSCF mostrado en la Figura 42.

En el contexto PDP, el usuario debe tener acceso a una de las siguientes alternativas:

- Servicio básico GPRS de conectividad IP: Los portadores se establecen de acuerdo a la suscripción de usuario, políticas de portadores de recursos del operador local, funciones de control del operador local y acuerdos de roaming GPRS.
- Servicios basados en mejoras GPRS: El portador es usado para soportar un servicio mejorado de la capa de aplicación.

Como se deduce del párrafo anterior, el GGSN es responsable de la autorización de QoS basado en las políticas del operador local, así, saca la información de QoS del contexto PDP y debe realizar el mapeo entre la información de QoS de los dominios IP y UMTS. Así, asigna las clases de QoS de acuerdo a la Tabla 11.

**Tabla 11: Asignación de QoS de acuerdo al Tráfico UMTS.**

| Clase de QoS | Clase de Tráfico UMTS | Prioridad de manejo de Tráfico |
|---|---|---|
| A | Conversacional | N/A |
| B | Streaming | N/A |
| C | Interactiva | 1 |
| D | | 2 |
| E | | 3 |
| F | Background | N/A |

Dentro de las funciones del control SBLP están la autorización de portadores, aprobación y eliminación de QoS, indicación de liberación, pérdida o recuperación de portadores, revocación de autorización e intercambio de identificadores de cobro.

En la sección 9.4.1.1 de Anexos se ilustra, a modo de ejemplo, el proceso de reservación de recursos para un servicio basado en una política local.

### 3.1.4.2. Control para Acceso a través de una WLAN

Algunos servicios 3GPP basados en conmutación de paquetes (como VoIP sobre IMS, streaming, etc.) requieren una disposición estricta de QoS. Así, para soportar estos servicios sobre redes WLAN se requiere una interoperación 3GPP-WLAN. Esto es muy importante ya que en la actualidad algunas tecnologías wireless (como Wi-Fi) no cuentan con QoS. De esta forma, la

arquitectura 3GPP I-WLAN (Interworking WLAN) utilizada debe ser independiente de la tecnología WLAN implementada y la QoS debe ser definida de forma general.

En la Figura 43 se muestra la arquitectura de QoS considerada para un acceso IP a través de una WLAN. Donde las entidades son: WLAN AN, que quiere decir WLAN Access Network, WAG es WLAN Access Gateway, PDG es Packet Data Gateway y TE es Terminal Equipment.

El Servicio End-to-End permite el transporte de la señalización y datos de usuario entre el WLAN UE y otro TE (o nodo correspondiente) y para el caso de acceso 3GPP consiste en un servicio de portadores WLAN y externos (los que pueden ser, por ejemplo, de tipo UMTS). El servicio de portadores de acceso IP provee el transporte de señalización y datos de usuario entre el WLAN UE y el PDG y soporta QoS I-WLAN. Mientras que el Servicio WLAN de Portadores soporta las capacidades de portadores específicas de la WLAN AN entre ésta y el WLAN UE.

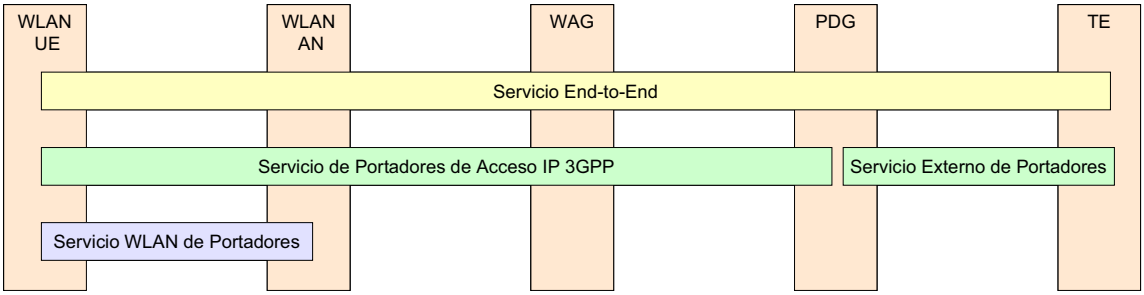



**Figura 43: Arquitectura de QoS para acceso 3GPP IP a través de una WLAN.**

Cuando se utiliza acceso 3GPP IP, se crea un túnel desde el UE al PDG para llevar el tráfico de servicios el cual puede cruzar backbones de operadores móviles en caso de roaming. Estos túneles pueden llevar tráfico a la red Home de más de un usuario sin importar que haya distintos tipos de servicios ni su QoS individual ya que normalmente los datos y headers interiores irán encriptados. Una forma de implementar QoS en estos casos es el uso de DiffServ por parte del UE y PDG para determinar los bits de DiffServ en los headers IP exteriores de forma de implementar diferentes clases de tráfico y, por tanto, diferentes niveles de QoS.

Una vez obtenida la QoS durante la fase de autentificación, los distintos tipos de QoS de tráfico se pueden mapear desde la red Home hacia la WLAN. De la misma forma, el UE puede marcar el tráfico en la dirección inversa. El profile de QoS debe incluir datos como la información de ancho de banda permitido y los máximos tipos de tráfico de servicio del usuario. El punto de aplicación de políticas de ancho de banda en un sistema 3GPP aún no está definido.

En la sección 9.4.1.2 de Anexos se muestra un proceso de asignación de QoS a través de una WLAN.

### 3.1.4.3.Factores para la Implementar QoS en Redes de Acceso WLAN

Como se mencionó anteriormente, las redes WLAN actuales implementan pocos mecanismos o ninguno de QoS. Por ejemplo, la tecnología IEEE 802.11 (o Wi-Fi) no considera QoS en sus enlaces. Sin embargo, nuevas tecnologías inalámbricas como la tecnología IEEE 802.16 consideran algunos mecanismos de QoS.

En redes, la QoS se encuentra definida por una serie de parámetros o problemas que se desean evitar o reducir tales como:

- Pérdida de Paquetes: En casos en que los buffers de los routers en una red se encuentren saturados, éstos se verán obligados a perder o "botar" paquetes.
- Retardo: Se refiere al tiempo que tarda un paquete para llegar a su destino a través de la red. El retardo se puede deber al encolamiento que puede sufrir el paquete en los buffers de algunos routers o al camino tomado para llegar a la dirección de destino, por ejemplo.
- Jitter: Este parámetro corresponde a la variación del tiempo de retardo que sufren los paquetes para llegar a su destino.
- Llegada fuera de orden: Al enviar una colección de paquetes a una dirección de destino en Internet, estos paquetes pueden tomar distintos caminos y, por lo tanto, pueden llegar a destino en un orden distinto al que fueron enviados por lo que se requieren protocolos adicionales para ordenar la información. Este tipo de parámetro es importante para transmisión de video, en que la sincronización es una característica deseada.
- Error: Muchos paquetes llegan a destino combinados con otros, corruptos o simplemente se pierden debido a problemas en la ruta.

Además de estos parámetros que son los más típicos, también pueden sumarse parámetros como ancho de banda del enlace, número de intentos para lograr la conexión o tiempo empleado en la conexión (en horas de más alto tráfico o en horario normal) juntos con muchos más parámetros diferentes dependiendo del tipo de servicio que se quiere entregar.

Sin embargo, en redes inalámbricas se suman otros parámetros característicos de este tipo de red de acceso. Dentro de estos parámetros se pueden distinguir los siguientes:

- Atenuaciones en el aire, causada por el entorno físico como edificios o clima, por ejemplo. Estas atenuaciones pueden cambiar en forma aleatoria.
- Degradación de la señal que puede deberse a la misma modulación utilizada por la tecnología y al uso de una frecuencia limitada.
- Muchas tecnologías inalámbricas están definidas en bandas de frecuencia de uso libre, por lo que las transmisiones pueden verse afectadas por transmisiones en la misma frecuencia de otras fuentes.
- Las técnicas de modulación también influyen en el ancho de banda logrado. Las técnicas con mayor ancho de banda no son muy robustas y requieren condiciones óptimas para poder implementarse, mientras que las conexiones más flexibles y robustas cuentan con un ancho de banda menor.
- La movilidad es una de las ideas objetivo principales en la utilización de tecnologías de acceso inalámbricas, por lo que debieran mantenerse parámetros de QoS en movimiento.

Se debe recordar que estos parámetros de QoS no son igualmente importantes para todos los tipos de servicios, sino que darán origen a variadas clasificaciones de QoS dependiendo de los requerimientos de cada sesión, por ejemplo, para un servicio SMS es más importante evitar la pérdida de paquetes que el retardo de éstos, al contrario que en un servicio de video-conferencia.

Para la implementación de QoS en redes inalámbricas probablemente se utilizarán protocolos ya existentes. Un protocolo de gran utilidad para la implementación de QoS puede ser el protocolo de la IEEE 802.1D. Esto se explica en la sección 9.4.1.3 de Anexos.

### 3.1.5. Proceso de Registro

Se llama proceso de registro al proceso que se produce entre el UE y la red de acceso cuando el UE requiere conectividad con la red.

Durante el proceso de registro se asigna un S-CSCF (Serving CSCF) que corresponde al servidor SIP que responderá a los requerimientos del UE, sin embargo, este S-CSCF asignado puede ser cambiado en un periodo posterior. Además existe un I-CSCF (Interrogating CSCF) que corresponde a un servidor SIP cuya función es determinar la dirección del S-CSCF a utilizar basado en las capacidades requeridas. El I-CSCF obtiene el nombre del S-CSCF de su rol de Seleccionador de S-CSCF para determinar y ubicar al S-CSCF durante el registro. Así, en el proceso de registro, el I-CSCF es el encargado de tomar la decisión de seleccionar el S-CSCF para el usuario en la red es tomada.

Para la realización del registro, se debe considerar una serie de requerimientos, entre los que destacan los siguientes:

- El S-CSCF debe tener diferentes capacidades o, en su defecto, poder acceder a diferentes capacidades.
- El operador de red debe tener la opción de ocultar su estructura de red interna a las otras redes y no debe ser necesario para la red exponer las direcciones IP explícitas dentro de la red.
- Es deseable que el UE utilice los mismos procesos de registro tanto en su red Home como red visitada.
- El HSS (Home Subscriber Server) debe ser capaz de restringir el acceso a usuarios del IMS desde redes visitadas no autorizadas.
- Debe ser posible registrar múltiples identidades públicas en el HSS con un sólo proceso de registro.

El proceso de registro distingue dos casos principales distintos, el primero en que un usuario se registra por primera vez en la red y el otro en que el usuario se registra nuevamente en una red en la que ya estaba registrado.

#### 3.1.5.1. Flujo de Información de Registro – Usuario no Registrado

El la Figura 44 se observa la cantidad de flujos entre entidades funcionales en IMS para el proceso de registro. En este caso se observa que el usuario está en "roaming", es decir, accede a través de una red visitada a su red Home; si el usuario iniciara el registro desde su propia red Home todas las entidades pertenecerían a la misma red.

Los procesos realizados, se resumen a continuación:

1. Después de que el UE obtuvo conectividad IP, éste puede realizar el registro enviando el flujo de información de registro al proxy (que contiene la Identidad de Usuario Público, Identidad de Usuario Privada, nombre del dominio de la red Home, dirección IP del UE).
2. El P-CSCF examina el "Home domain name" para descubrir el punto de entrada a la red Home (es decir, el I-CSCF). El proxy envía el flujo de información de registro al I-CSCF (nombre/dirección del P-CSCF, Identidad de Usuario Público, Identidad de Usuario

Privada, identificador de red P-CSCF, dirección IP del UE). Para determinar la dirección de la red Home en función del nombre de dominio de esta red, se utiliza un mecanismo de resolución nombre-dirección. El identificador de red P-CSCF es un string que identifica a la red Home, la red donde el P-CSCF está ubicado.

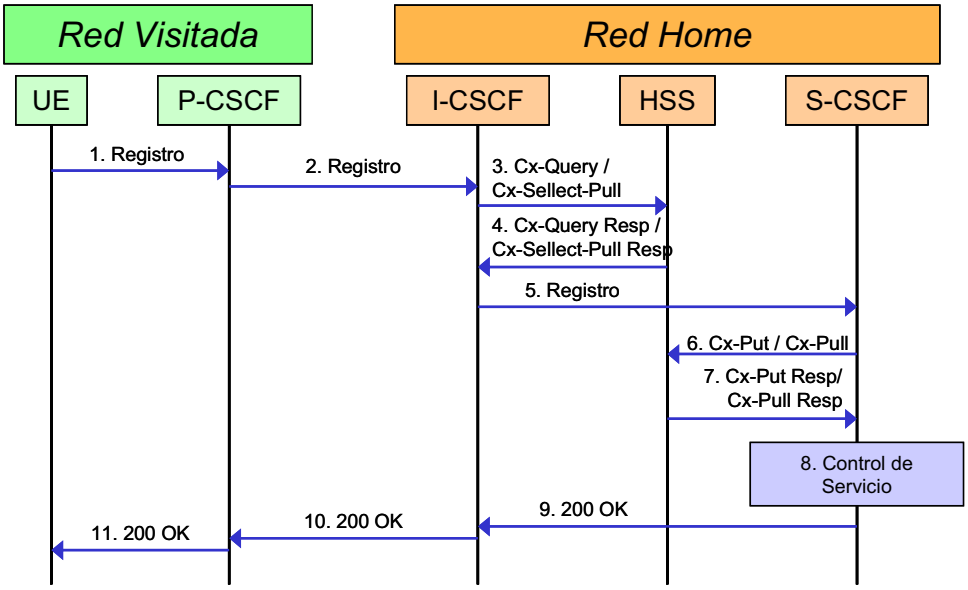



**Figura 44: Flujo de mensajes en IMS para el proceso de Registro - Usuario no Registrado.**

3. El I-CSCF envía el flujo de información "Cx-Query/Cx-Sellect-Pull" al HSS (Identidad de Usuario Público, Identidad de Usuario Privada, identificador de red P-CSCF a través del protocolo SIP).

   El HSS verifica si el usuario ya está registrado e indica si al usuario le está permitido registrarse en esa red (identificada por el identificador de red P-CSCF) de acuerdo a la suscripción de usuario y las restricciones/limitaciones del operador si las tuviera.

4. El HSS envía el mensaje SIP "Cx-Query Resp/CX-Sellect-Pull Resp" al I-CSCF. Éste contiene el nombre del S-CSCF, si es conocido por el HSS, o las capacidades del S-CSCF, si es que es necesario seleccionar un nuevo S-CSCF. Luego de que se retornan las capacidades, el I-CSCF realiza la función de selección del nuevo S-CSCF basado en las capacidades retornadas.

   Si la verificación en el HSS no fue exitosa, el Cx-Query Resp rechaza el intento de registro.

5. El I-CSCF, usando el nombre del S-CSCF, determina la dirección del S-CSCF a través de un mecanismo de resolución nombre-dirección. El I-CSCF también determina el nombre de una red Home de contacto conveniente, basado en la información recibida desde el HSS. Entonces, el I-CSCF envía el flujo de información de registro (nombre, dirección del P-CSCF, Identidad de Usuario Público, Identidad de Usuario Privada, identificador de red P-CSCF, dirección IP del UE) al S-CSCF seleccionado. La red Home de contacto es usada por el P-CSCF para reenviar la señalización de iniciación de sesión a la red Home.

   El S-CSCF guarda el nombre/dirección del P-CSCF proporcionado por la red visitada. Esto representa el nombre/dirección a la que la red Home reenvía la subsiguiente señalización se sesión al UE. El S-CSCF guarda la información de ID de red del P-CSCF.

6. El S-CSCF envía el Cx-Put/Cx-Pull (Identidad de Usuario Público, Identidad de Usuario Privada, nombre del S-CSCF) al HSS.

7. El HSS guarda el nombre del S-CSCF para el usuario y retorna el flujo de información Cx-Put Resp/Cx-Pull Resp (información de usuario) al S-CSCF. La información de usuario entregada por el HSS al S-CSCF incluye información de nombre(s)/dirección(es) que se pueden usar para acceder a las plataformas usadas por el control de servicio mientras el usuario esté registrado en ese S-CSCF. El S-CSCF guarda la información del usuario indicado. Además de la información de nombre(s)/dirección(es), también se puede usar información de seguridad para usarla dentro del S-CSCF.
8. Basado en un criterio de filtro, el S-CSCF envía información de registro a la plataforma de control de servicio y realiza los procedimientos de control de servicio apropiados.

9-11. Se retorna el flujo de información 200 OK (información de la red Home de contacto para el caso en que el registro sea exitoso) desde el S-CSCF hacia el UE.

#### 3.1.5.2. Flujo de Información de Re-registro – Usuario actualmente Registrado

El UE debe iniciar niveles de aplicación de re-registro periódico ya sea para refrescar un registro existente o en respuesta a un cambio en el estatus de registro del UE. Un procedimiento de re-registro también puede ser iniciado cuando las capacidades del UE hayan cambiado.

Cuando es iniciado por el UE, basado en el tiempo de registro establecido durante los registros previos, el UE debe mantener un timer más corto que el timer de registro de la red. Si el UE no se re-registra, cualquier sesión activa puede ser desactivada.

El procedimiento de re-registro es muy similar al proceso de registro explicado anteriormente, el requerimiento de re-registro iniciado por el usuario es tratado por el P-CSCF e I-CSCF como un registro nuevo. Sin embargo, al llegar al HSS, éste verifica si el usuario ya está registrado y retorna una indicación que revela que ya existe un S-CSCF asignado (paso 4 del proceso de registro). Luego de esto, todos los flujos de datos son iguales a los de un registro nuevo.

#### 3.1.5.3. Resumen de la Información Almacenada

En la Tabla 12 se muestra parte de la información almacenada en las entidades funcionales antes, durante y después de los procesos de registro explicados anteriormente.

**Tabla 12: Información almacenada antes, durante y después del Registro.**

| Entidad | Antes del Registro | Durante el Registro | Después del Registro |
|---|---|---|---|
| UE (red local) | Credenciales.<br>Dominio Home.<br>Nombre/Dirección del Proxy. | La misma que antes del registro | Credenciales.<br>Dominio Home.<br>Nombre/Dirección del Proxy. |
| P-CSCF (red Home o Visitada) | Función de Enrutamiento | Punto de entrada Inicial de la Red.<br>Dirección del UE.<br>IDs de Usuario Públicas y Privada. | Punto de entrada a la red Final.<br>Dirección del UE.<br>IDs de Usuario Pública y Privada. |
| I-CSCF (red Home) | Dirección del HSS o SLF | Nombre/Dirección del S-CSCF.<br>ID de red del P-CSCF.<br>Información de contacto de la red Home. | No declara información |
| HSS | Profile de Servicio de Usuario | ID de red del P-CSCF | Nombre/Dirección del S-CSCF |
| S-CSCF (red Home) | No declara información | Nombre/Dirección del HSS.<br>Profile de Usuario.<br>Nombre/Dirección de la ID de red del P-CSCF.<br>ID de Usuario Pública/Privada.<br>Dirección IP del UE. | Puede tener información del estado de sesión.<br>Lo mismo que durante el registro. |

### 3.1.6. Procedimientos de Sesión End-to-End

A continuación se presentarán brevemente los principales procesos utilizados para comunicar a dos terminales de usuario a través de IMS.

Los procedimientos para establecer una sesión se dividen en tres procesos dependiendo del nivel de red en el que se está y los que se distinguen en la Figura 45. Las principales secciones de procesos son:

- Procedimientos de origen, entre el UE que origina la sesión y el S-CSCF de su red Home.
- Procedimientos S-CSCF/MGCF a S-CSCF/MGCF, en que se pasa del S-CSCF/MGCF de la red del usuario de origen a la red del usuario final. Se tienen las opciones S-CSCF o MGCF, dependiendo si la red es IMS o la PSTN.
- Procedimientos de término, entre el S-CSCF de la red de término de sesión y el UE de término.

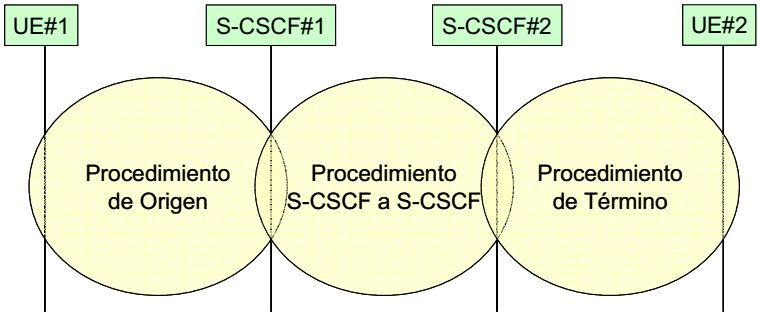



**Figura 45: Secciones de Procedimientos de Sesión.**

En la Tabla 13 se detallan cada una de las posibilidades de procedimientos para cada sección. Cuando se establece una sesión, esta se pueden realizar con cualquier opción de de los tres procedimientos explicados anteriormente.

**Tabla 13: Combinaciones de los Procedimientos de Sesión.**

| Procedimiento de Origen | Procedimiento S-CSCF a S-CSCF | Procedimiento de Término |
|---|---|---|
| ➢ Origen Móvil desde una red visitada (Roaming).<br>➢ Origen Móvil desde la red Home.<br>➢ Origen desde la PSTN.<br>➢ Origen desde el Servidor de Aplicación (AS).<br>➢ Origen desde una red NO-IMS. | Diferentes Operadores de Red como puntos de origen y término. | ➢ Término Móvil en una red visitada (Roaming).<br>➢ Término Móvil en su red Home.<br>➢ Término Móvil, en el dominio CS (Circuit Switched) en Roaming.<br>➢ Término en el Servidor de Aplicación (AS).<br>➢ Término desde una red NO-IMS. |
| ➢ Origen Móvil desde una red visitada (Roaming).<br>➢ Origen Móvil desde la red Home.<br>➢ Origen desde el Servidor de Aplicación (AS). | Un único Operador de Red como punto de origen y término. | ➢ Término Móvil en una red visitada (Roaming).<br>➢ Término Móvil en su red Home.<br>➢ Término Móvil, en el dominio CS (Circuit Switched) en Roaming.<br>➢ Término en el Servidor de Aplicación (AS). |
| ➢ Origen Móvil desde una red visitada (Roaming).<br>➢ Origen Móvil desde la red Home.<br>➢ Origen desde el Servidor de Aplicación (AS). | Terminación PSTN en la misma red que la del S-CSCF. | Término en una red PSTN. |
| ➢ Origen Móvil desde una red visitada (Roaming).<br>➢ Origen Móvil desde la red Home.<br>➢ Origen desde el Servidor de Aplicación (AS). | Terminación PSTN en una red diferente a la del S-CSCF. | Término en una red PSTN. |

## 3.1.7. Procedimientos de Inicio de Sesión

Los procedimientos de inicio de sesión especifican el mapa de señalización entre el UE realizando un intento de establecimiento de sesión y el S-CSCF asignado para realizar el servicio de origen de sesión. Este mapa de señalización se determina durante el registro del UE, y se mantiene fijo por la vida del registro. Por otra parte, el UE siempre tiene un P-CSCF asignado (el que se determina en el proceso de descubrimiento).

Como se tiene en la Tabla 13, existen varios procedimientos de inicio de sesión. En este trabajo se explican tres de estos procedimientos. El mostrado a continuación corresponde al caso de origen móvil en una red visitada, es decir, en caso de roaming, los casos restantes se encuentran en la sección 9.4.2 de Anexos.

### 3.1.7.1. Origen Móvil desde una red Visitada: Roaming

A continuación se considera un UE en una red visitada, éste determina el P-CSCF a través del procedimiento de descubrimiento de CSCF. La red Home publica el S-CSCF como punto de entrada desde la red visitada. La secuencia de mensajes se observa en la Figura 46 y el procedimiento es como sigue:

1. El UE envía un requerimiento SIP INVITE al P-CSCF, este mensaje puede representar uno o más tráficos de media para sesiones multimedia.
2. Se genera un Authorization-Token y se almacena en el P-CSCF. El P-CSCF recuerda S-CSCF y envía el requerimiento del UE.

3-4. El S-CSCF valida el perfil de servicio y realiza la lógica de servicio requerida para el usuario. Esto incluye autorización basada en la suscripción del usuario. Luego, el S-CSCF reenvía el requerimiento como se explica en los procedimientos S-CSCF a S-CSCF.

5-6. Se retornan las capacidades del flujo media de destino a través del mapa de señalización y el S-CSCF reenvía el mensaje al P-CSCF.

7. El P-CSCF autoriza los recursos necesarios para la sesión.
8. El Authorization-Token se incluye en el mensaje y el P-CSCF lo reenvía al punto de origen.

9-10. El UE decide el conjunto de flujos de media ofrecidos para esa sesión, confirma la recepción del mensaje y envía una confirmación al P-CSCF. Después de determinar los recursos necesarios, el UE comienza la reservación de dichos recursos para la sesión.

11-15. El P-CSCF reenvía la confirmación al S-CSCF y éste reenvía el mensaje al punto de término. El punto de término responde al punto de origen con un reconocimiento.

16-21. Cuando la reservación de recursos está completa, el UE envía un mensaje de reservación de recursos exitoso al punto de término a través del mapa de señalización establecido. El mensaje se envía primero al P-CSCF. Luego, el punto de término responde con una confirmación al de origen.

22-25. El punto de término puede generar un "ringing", el que es reenviado al UE. Y, en este caso, el UE indica al usuario de origen que el destino está "ringing".

26-27. Cuando la parte de destino contesta, el punto de término envía una respuesta final 200 OK al S-CSCF, la que es reenviada al P-CSCF.

28-29. El P-CSCF indica que los recursos reservados para esta sesión deben ser aprobados para su uso y luego envía una respuesta final 200 OK al origen de sesión.

30-33. El UE inicia el flujo(s) de media para esta sesión y responde al 200 OK con un mensaje SIP ACK enviado a través del mapa de señalización.

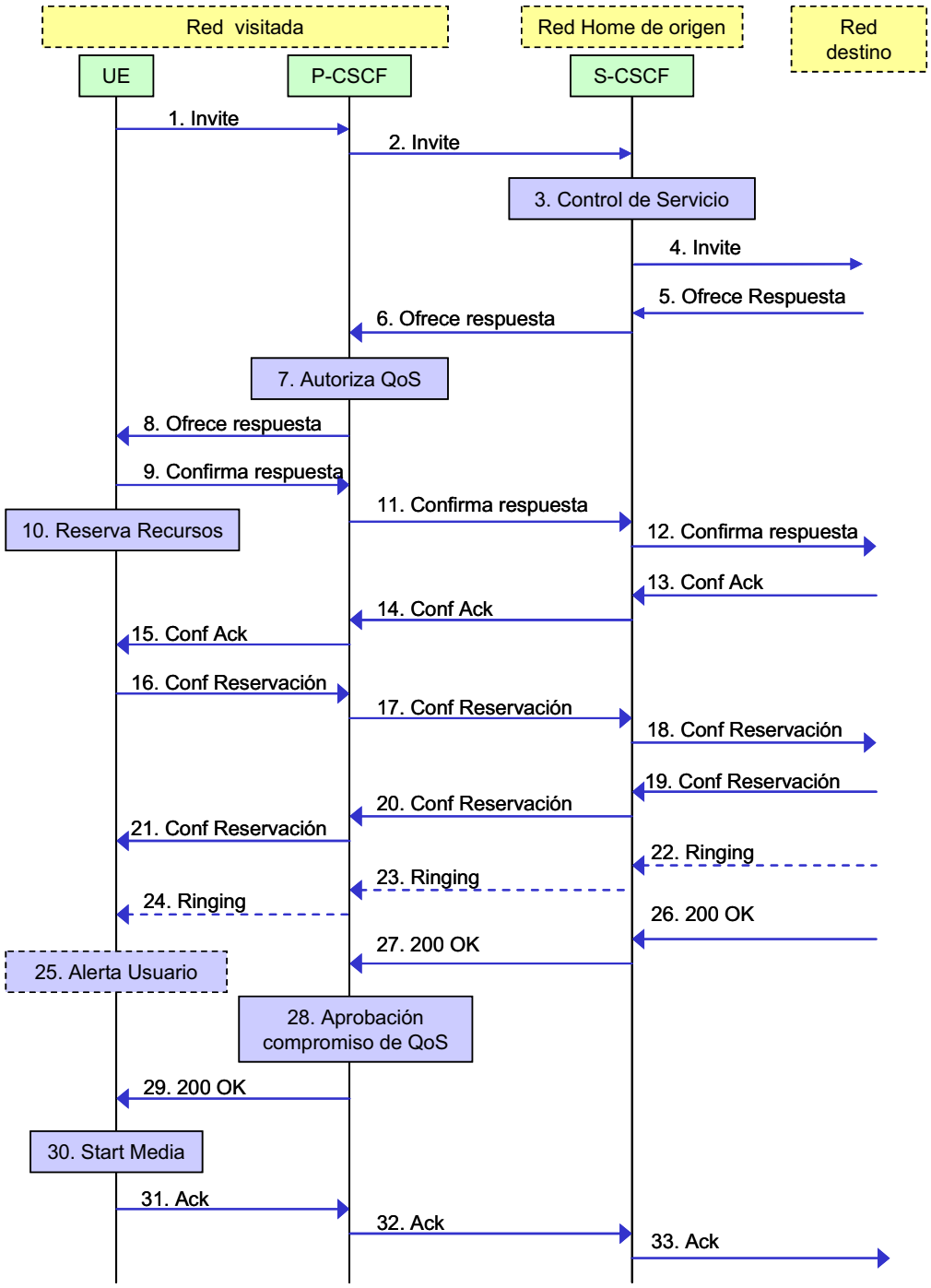



**Figura 46: Origen Móvil; Roaming.**

## 3.1.8. Procedimientos S-CSCF/MGCF ↔ S-CSCF/MGCF

En la arquitectura IMS, el MGCF se considera un punto final SIP, el que permite la interoperación entre la PSTN e IMS. Éste traduce mensajes ISUP/BICC del lado de la PSTN a señalización SIP en IMS y viceversa.

El S-CSCF que manipula el origen de sesión realiza un análisis de la dirección de destino y determina si es un suscriptor de la red del mismo operador o es de otro operador. Si el análisis de la dirección de destino determina que pertenece a un suscriptor de un operador diferente, el requerimiento es enviado dentro de la red del operador de origen a un punto de entrada conocido dentro de la red del operador de destino, el I-CSCF. Si el análisis de la dirección de destino determina que el suscriptor es de una red del mismo operador, el S-CSCF para el requerimiento a un I-CSCF local.

Como se mostró en la Tabla 13, en IMS se definen cuatro procedimientos dentro de esta sección:

1. Diferentes Operadores de Origen y Término.
2. Un único operador de origen y término.
3. Sesión con la parte de término en una red PSTN en la misma red del S-CSCF.
4. Sesión con la parte de término en una red PSTN en una red diferente a la del S-CSCF.

Los puntos 1 y 2 junto con los puntos 3 y 4 son bastante similares entre sí, por lo que sólo se explicarán dos casos correspondientes a los puntos 1 y 4 (el caso 4 se muestra en la sección 9.4.3 de Anexos).

### 3.1.8.1. Diferentes Operadores de Origen y Término

El flujo de mensajes para este caso es bastante extenso y se muestra en la Figura 47. Se considera que el S-CSCF de la red de origen conoce un punto de entrada a la red del otro operador, este punto será utilizado como el I-CSCF de entrada a la red de término. A continuación se presenta un resumen del procedimiento.

1-3. El requerimiento SIP INVITE se envía desde el UE al S-CSCF de origen mediante algún procedimiento de origen. El S-CSCF de origen invoca la lógica de servicio necesaria para el intento de sesión, analiza la dirección de destino y determina el operador de red al cual pertenece el suscriptor final. Así, reenvía el mensaje al I-CSCF de entrada a la red de término para el usuario de destino.

4-6. El I-CSCF de entrada consulta al HSS por la información de ubicación actual del usuario de término. El HSS responde con la dirección del actual S-CSCF para este usuario. El I-CSCF de entrada reenvía el requerimiento al S-CSCF de término que se encargará del término de sesión.

7. El S-CSCF de la red de término utiliza las lógicas de servicio apropiadas para intentar establecer la sesión.

8. La secuencia continua con los flujos de mensajes determinados por el procedimiento de término.

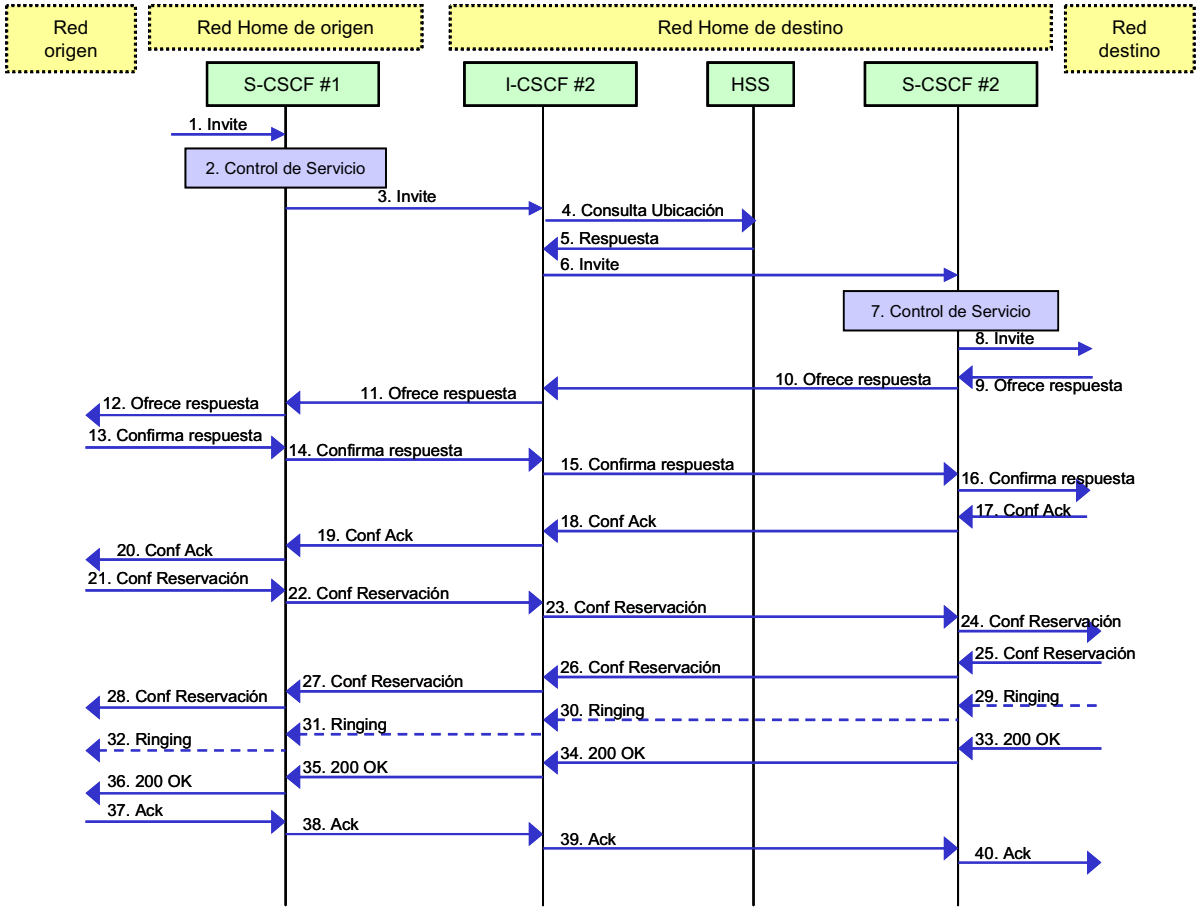



**Figura 47: Flujo de mensajes en IMS para Redes de distintos Operadores.**

9-12. Las capacidades de flujo de media del término son retornados a través del mapa de señalización y se reenvían desde el S-CSCF de la red de término hasta el S-CSCF de la red de origen y hasta el UE de origen a través de algún procedimiento de origen.

13-16. El punto de origen decide los flujos de media a usar de los ofrecidos y confirma la recepción del mensaje con una confirmación. Esta información es reenviada al S-CSCF de la red de origen, hacia el S-CSCF de la red de término y llega hasta el punto final de término.

17-20. El punto de término envía un reconocimiento (Acknowledgement) de la confirmación y pasa a través del mapa de sesión al punto de origen.

21-28. El punto de origen reconoce la reserva de recursos exitosa y el mensaje es reenviado al punto de término. Luego, el punto de término reconoce la respuesta y envía un mensaje al punto de origen a través del mapa de sesión establecido.

29-32. El punto de término puede generar un "ringing" y se reenvía un mensaje al punto de origen a través del mapa de sesión establecido.

33-40. El punto de término envía un mensaje 200 OK al punto de origen a través del mapa de sesión establecido. El punto de origen reconoce el establecimiento de sesión y envía al punto de término otro mensaje 200 OK a través del mapa de sesión establecido.

## 3.1.9. Procedimientos de Término de Sesión

Los procedimientos de término especifican el mapa de señalización entre el S-CSCF asignado para implementar el servicio y el UE de término. El mapa de señalización utilizado se define en el momento de registro del UE y permanece fijo durante la vida del registro. Además, se debe recordar que el UE tiene asignado un P-CSCF, el que se determina en el procedimiento de descubrimiento y, el cual conoce la dirección del UE por el proceso de registro. A continuación se presentan los procedimientos de los principales escenarios de término (La continuación de estos procedimientos se muestra en la sección 9.4.4 de Anexos).

### 3.1.9.1. Término Móvil en una red Visitada: Roaming

En este caso se considera que el UE no se encuentra en su red Home. En la Figura 48 se muestra la secuencia de mensajes necesarios para establecer la sesión en la parte de término, si el usuario estuviera en su propia red Home, la única diferencia sería que el P-CSCF al que esté conectado estaría también dentro de la red Home.

A continuación se resume el flujo de mensajes para establecer el término de sesión:

1. El origen envía un requerimiento SIP INVITE mediante algún procedimiento de inicio de sesión y de S-CSCF/MGCF a S-CSCF/MGCF.
2. El S-CSCF valida el profile y realiza la lógica de servicio necesaria para levantar la sesión como autorización basado en la suscripción del usuario
3. El S-CSCF recuerda que el UE se encuentra en una red visitada y reenvía el requerimiento al P-CSCF en esa red.
4. Se genera un Token de autorización y se incluye en el mensaje. Como el P-CSCF sabe la dirección del UE, le reenvía el mensaje de invitación.

5-8. El UE determina los tipos de stream media propuestos por la parte de origen que puede soportar y responde con un mensaje de oferta a la parte de origen. El P-CSCF autoriza los recursos necesarios y el mensaje de oferta es reenviado al origen.

9-15. El punto origen responde al mensaje con una confirmación a través del mapa de señalización. Cuando el UE de término recibe la confirmación, éste envía un mensaje de reconocimiento al origen mediante el mapa establecido y comienza los procedimientos de reservación de recursos.

16-18. Cuando la parte de origen completa su reservación de recursos, ésta envía al usuario final un mensaje de reservación exitosa de recursos.

19. Opcionalmente, el UE puede alertar al usuario de que se está intenta iniciar una sesión.

20-22. El UE responde a la reservación exitosa de recursos con un mensaje hacia el punto de origen.

23-25. En el caso que el UE alerte al usuario del intento de sesión y el usuario acepte, se envía hacia la parte de origen un mensaje de "ringing".

26-28. Cuando el UE responde, se envía un mensaje 200 OK al P-CSCF, el que luego indica que los recursos de QoS aprobados anteriormente deben ser ejecutados y el UE comienza el envío de stream media.

29-33. El P-CSCF envía un mensaje final 200 OK al S-CSCF y éste lo reenvía a la parte de origen, la que responderá con un mensaje de reconocimiento.

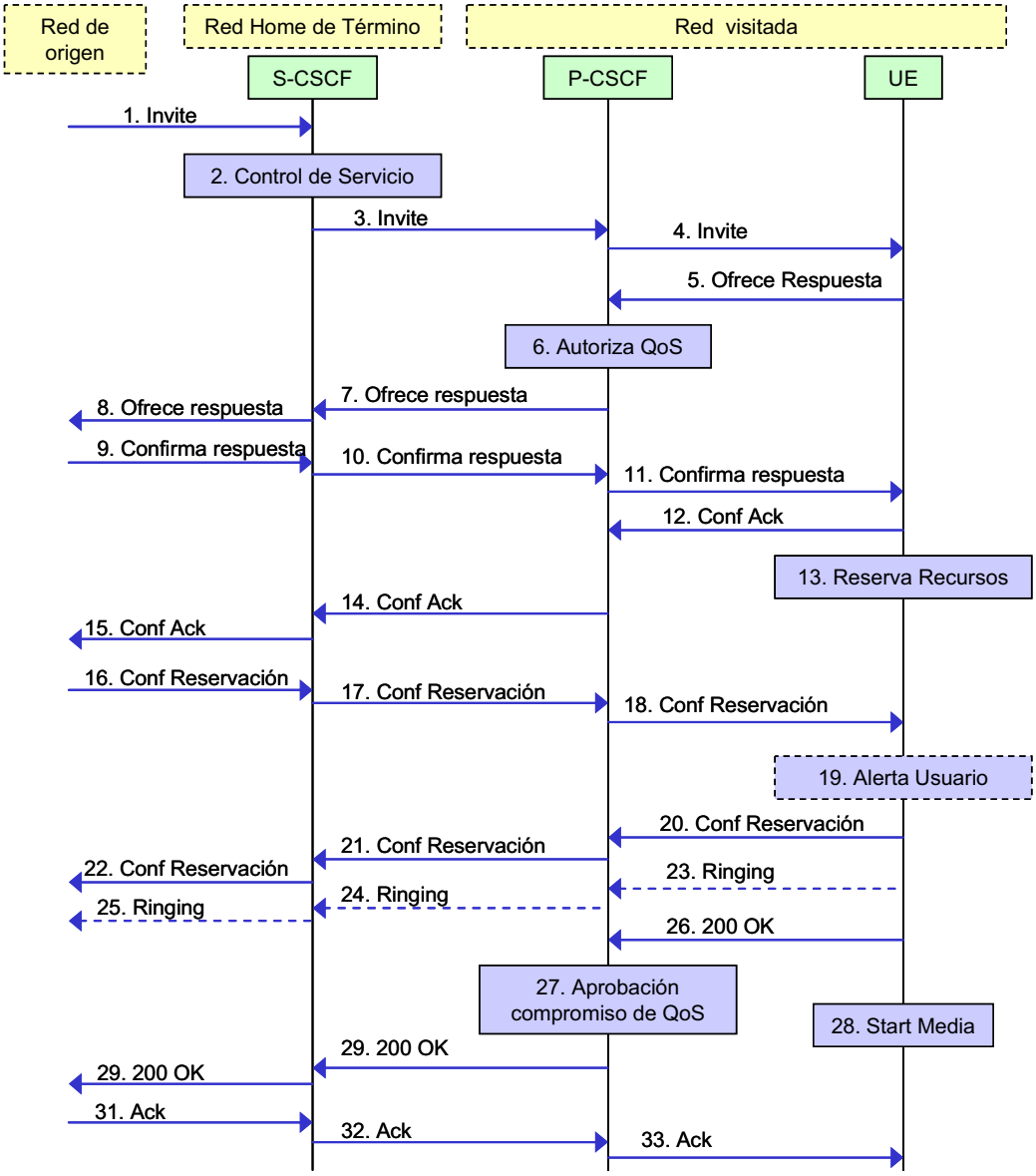



**Figura 48: Flujo de Mensajes para Término Móvil en una Red Visitada.**

## 3.1.10. Funciones de Control de Borde

En el caso real de muchos operadores IMS con sus redes interconectadas, se hace necesario un sistema de control de tráfico y administración en los "bordes" de las redes, o mejor dicho, en los puntos de interconexión.

En la Figura 49 se muestra un esquema de la arquitectura necesaria para la implementación del Control de Borde. Se debe recordar que la red de acceso (IP-CAN: IP Connectivity Access Network) puede ser o no UMTS.

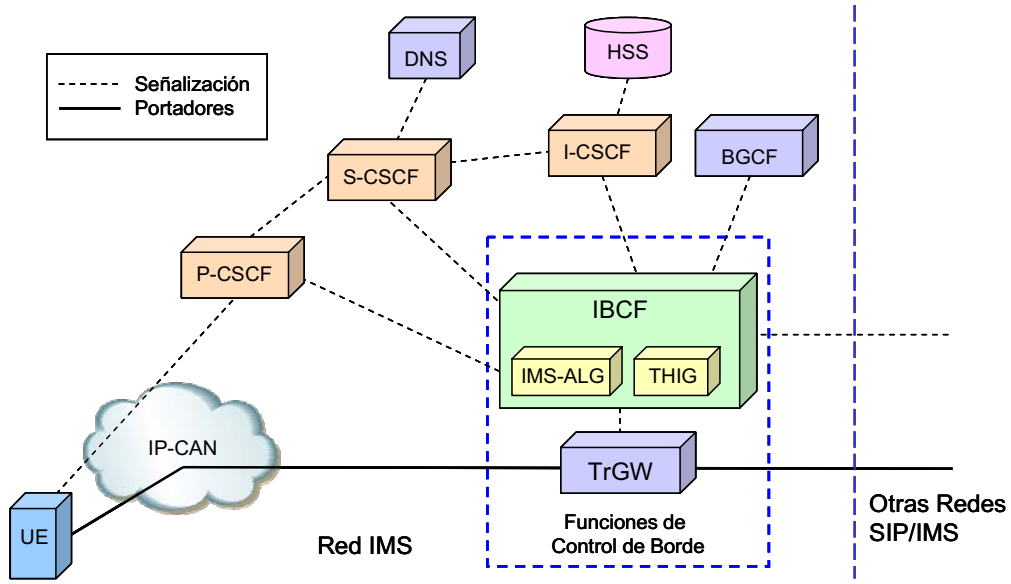



**Figura 49: Funciones de Control de Borde.**

Las entidades que componen el conjunto de Funciones de Borde son:

- IBCF (Interconnection Border Control Function): Provee funciones de aplicación específica en la capa de los protocolos SIP/SDP para realizar la interconexión entre dominios de dos operadores. Esta entidad permite el ocultamiento de la topología de red, funciones de control en el plano de transporte, exploración de la información de señalización SIP, generación de los CDRs apropiados. El IBCF contiene dos entidades funcionales más:
  - ✓ IMS-ALG (IMS – Application Level Gateway): Es una entidad funcional de aplicación que permite la comunicación entre nodos IPv6 e IPv4 y viceversa para el stack de protocolos SIP/SDP. Esta entidad recibe un mensaje SIP desde algún nodo CSCF o desde una red externa IPv4 y cambia los parámetros SIP/SDP apropiados para la traducción de direcciones entre IPv6 e IPv4. Para esto, el IMS-ALG necesita modificar los cuerpos y headers del mensaje SIP que tienen una asociación de dirección IP indicada.
  - ✓ THIG (Topology Hiding Inter-network Gateway): Como los indica su nombre, es la entidad encargada de ocultar en parte o por completo la topología de red del operador. También restringe la información de la red, como aspectos de seguridad, escalabilidad y administración de red.
- TrGW (Transition Gateway): Se ubica entre el mapa de información media y está controlado por el IBCF. Provee funciones como NA(P)T y traducción de protocolos IPv6/IPv4.

En la Figura 50 se muestra un ejemplo de interoperación entre redes con distintas versiones IP. En este escenario hay un cliente (A) en su red Home que es IPv6 y que desea iniciar una sesión con otro cliente (B) que se encuentra en la red de otro operador cuya versión de IP es IPv4.

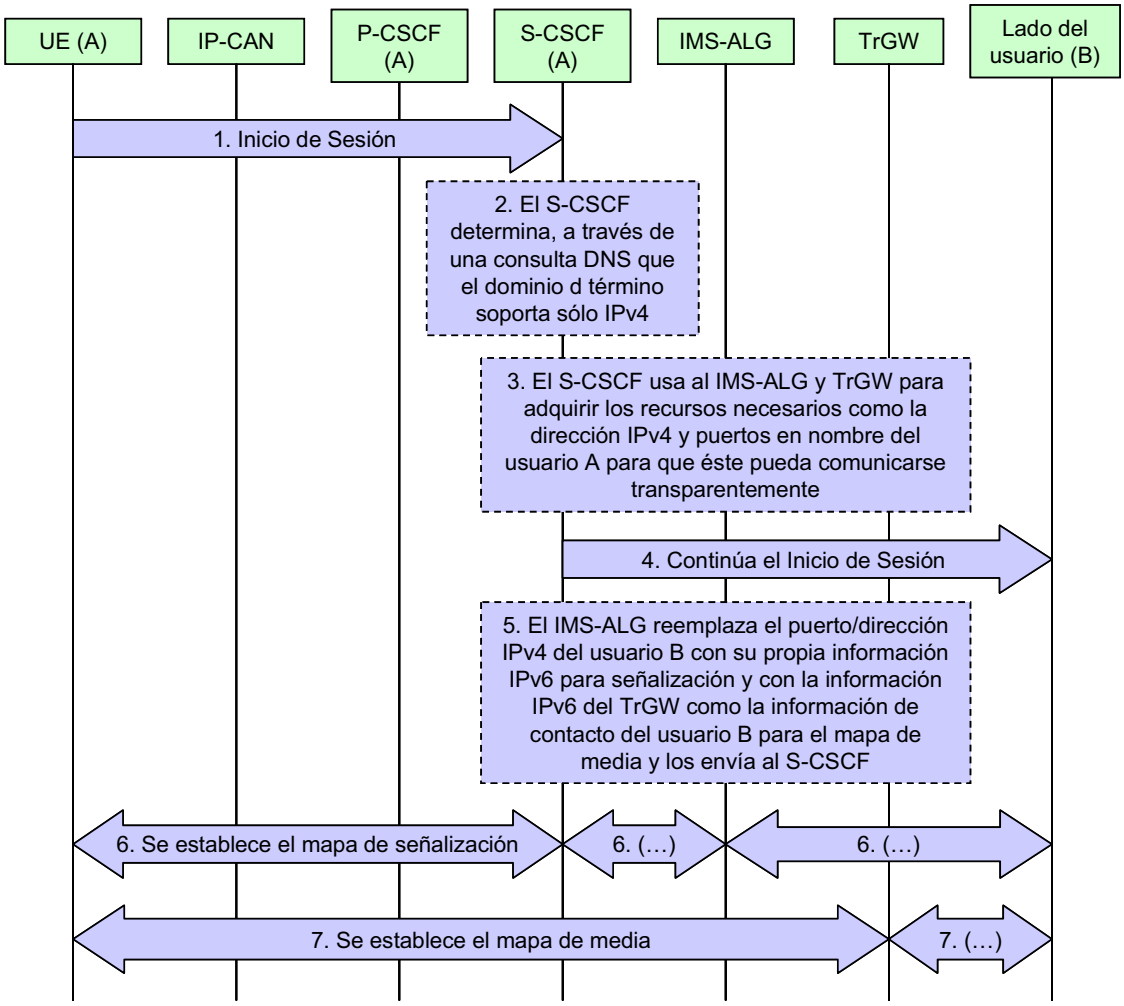



**Figura 50: Origen de sesión IMS hacia una red IPv4.**

Para una comprensión a mayor profundidad del transporte de datos en el plano de usuario entre redes IPv4 e IPv6, la sección 9.4.5 de Anexos describe este método. Además, en la sección 9.3.5 se describen los escenarios de Interoperación entre redes IMS IPv4 e IPv6.

## 3.1.11. Interoperación entre IMS y Redes de Acceso WLAN

En la actualidad se observa un fuerte crecimiento y desarrollo de las tecnologías inalámbricas de acceso. IMS define una arquitectura de interoperación entre la red IMS y una red WLAN (Wireless Local Area Network) para que un usuario pueda iniciar o recibir sesiones desde IMS.

### 3.1.11.1. Identidad de Usuario

Una característica importante que debiera tener una red de acceso WLAN para interoperar con IMS es el control de acceso por parte de los usuarios, por lo que se hace esencial un método de autentificación. El procedimiento de autentificación se basa en el método EAP (Extensible

Authentication Protocol), donde la identificación de usuario se sustenta en el Identificador de Acceso a la red (NAI: Network Access Identifier).

El NAI se compone de dos partes, una de nombre de usuario (NAI username) y otra de nombre de dominio (realm).

#### 3.1.11.1.1. NAI Username

Existen tres tipos de nombre de usuario:

1. Permanente: Usado para una autentificación completa y se deriva del IMSI.
2. Pseudónimo: Usada en identidades temporales y para autentificación completa, se usa para la protección de identidad de usuario para reemplazar la identidad permanente derivada del IMSI en transmisiones de radio de forma de proteger al usuario de rastreo de redes de acceso no autorizadas. Estas identidades son asignadas por el Servidor AAA 3GPP.
3. De re-autentificación rápida: Usada en identidades temporales y sólo en caso de re-autentificación. También provee protección de la identidad de usuario y son asignadas por el Servidor AAA 3GPP.

#### 3.1.11.1.2. NAI Realm Name

El nombre de dominio NAI debe estar en la forma de un nombre de dominio IP y debe identificar la red móvil Home del usuario.

### 3.1.11.2. Escenarios de Descubrimiento y Selección de Red

Cuando un terminal de usuario se encuentra en un ambiente con múltiples redes de acceso WLAN (WLAN AN), debe elegir como red de acceso a una de ellas basándose en sus características, por ejemplo, el WLAN UE puede necesitar seleccionar una red pública móvil visitada para autentificarse, o una red móvil que soporte sus llamadas de emergencia.

En la Figura 51 se muestra un escenario cubierto por algunas de acceso WLAN (WLAN AN #1, #2,..., #n) que tienen un conjunto de acuerdos de roaming con diferentes redes 3G (Redes 3GPP Visitadas #1, #2,..., #n). El UE puede conectarse a su red Home mediante la WLAN AN #1 a través de las redes visitadas #1 o #2 y a través la WLAN #2 está directamente enlazada con la red Home del usuario.

El descubrimiento de red depende de la tecnología de la red de acceso, la 3GPP especifica el escenario de descubrimiento para la tecnología Wi-FI (IEEE 802.11), pero no se descartan nuevas tecnologías a ser utilizadas.


**Figura 51: Escenario de Anunciación y Selección de Red.**

## 3.1.11.3. Arquitectura de Interoperación

### 3.1.11.3.1. Entidades Funcionales

En la Figura 52 se muestra la arquitectura necesaria para la interoperación entre una red de acceso WLAN y una red IMS. En este escenario, el UE se comunica a través de la WLAN AN con su propia red Home.

Los elementos necesarios para este modelo son:

- WLAN UE: Corresponde al equipo de usuario con una tarjeta o chip de seguridad que utiliza el suscriptor para acceder a la WLAN AN. Este terminal puede servir sólo para acceso a través de una WLAN o a través de múltiples métodos de acceso. Dentro de sus principales funciones está la asociación con una WLAN de interoperación, autentificación basada en métodos EAP, selección de una red visitada adecuada en casos de roaming, etc.
- Servidor 3GPP AAA: El servidor AAA (Autentificación, Autorización y Accounting) Se localiza dentro de la red 3GPP y entre sus funciones está recuperar la información de autentificación y profile del suscriptor desde el HSS/HLR de la red Home del Suscriptor, autentificar al suscriptor basado en la información obtenida, actualizar la información de autorización de acceso si la suscripción de usuario se modifica, comunicar información de autorización a la WLAN AN, registrar su nombre en el HSS para cada suscriptor autentificado y autorizado, puede actuar como Proxy, mantener el estatus del WLAN UE en la WLAN, generar información de accounting y cobro.
- WAG (WLAN Access Gateway): Corresponde a un gateway en el cual los datos hacia y desde la red de acceso WLAN puede ser enrutada a través de la red móvil pública para proveer servicios al WLAN UE. EL WAG permite a la red pública móvil visitada generar información de cobros para los usuarios que acceden a través de la WLAN AN en caso de roaming, mejorar el enrutamiento de paquetes a través del PDG, filtrar paquetes basado en la información no encriptada en los paquetes, soportar mecanismos DiffServ para paquetes IP downlink/uplink (en caso que se aplique QoS) y puede implementar políticas después de establecer el túnel.

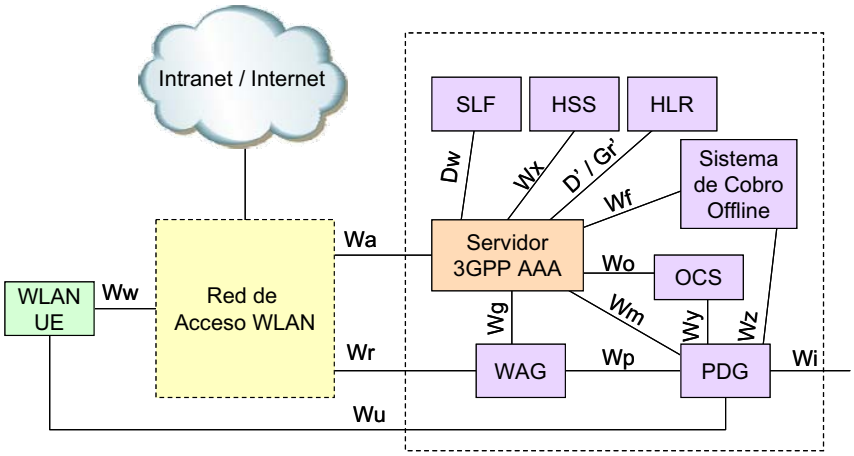



**Figura 52: Modelo de Interoperación con WLAN AN entre UE y su red Home.**

- PDG (Packet Data Gateway): A través del PDG se accede a los servicios PS (Packet Switched), el PDG puede estar en la red Home o visitada dependiendo de los procesos de autentificación, selección de servicio y verificación de suscripción. EL PDG contiene la información de enrutamiento de los usuarios conectados a la red WLAN, enruta los paquetes de datos recibidos desde el PDN hacia el usuario conectado a la WLAN AN y viceversa, realiza mapeo y traducción de dirección, encapsula y desencapsula, acepta o rechaza la red WLAN requerida de acuerdo a la decisión hecha por el Servidor 3GPP AAA, etc.
- Sistema de Cobro Offline: Se encuentra dentro de la red 3GPP e incluye mecanismos para la recolección y reenvío de información sobre el uso de recursos en la WLAN de acceso.
- OCS (Online Charging System): El OCS o Sistema de Cobro Online incluye mecanismos para adquirir permisos en línea para permitir al suscriptor acceder a la WLAN.

En la Figura 53 se muestra un escenario en que un cliente accede a los servicios de su red Home a través de una red visitada. La red Home es responsable del control de acceso y los registros de cobro pueden ser generados tanto en la red visitada como en la red Home.

En el modelo que muestra la Figura 53 se muestra una nueva entidad funcional además de las anteriormente nombradas:

- Proxy 3GPP AAA: Representa una función de aproximación y filtro que reside en la red visitada. Entre sus funciones está traspasar la información entre la WLAN y el Servidor 3GPP AAA, cumplir las políticas derivadas de los acuerdos de Roaming entre operadores de servicios y operadores de WLANs, limitar la información de acceso a la WLAN basado en información de autorización de la red Home, reportar información de cobro y accounting por usuario al Sistema de Cobro Offline de la red visitada para los usuarios en Roaming, terminación del servicio y conversión de protocolos cuando lo puntos de referencia Wa y Wd no usan el mismo protocolo.

En la sección 9.4.6 de Anexos se muestra una breve descripción de los puntos de referencia en la arquitectura de interoperación entre IMS y redes de acceso WLAN.

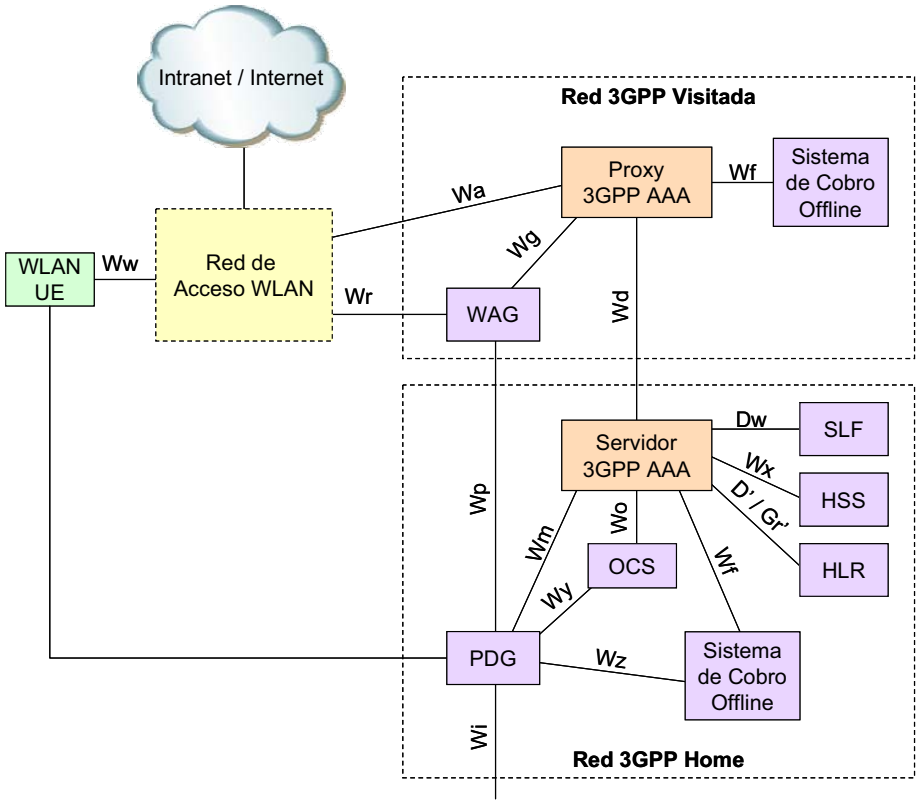



**Figura 53: Modelo de Interoperación con una red WLAN en caso de Roaming.**

## 3.1.11.4. Algunos Procedimientos

A continuación se ilustran algunos procedimientos básicos para mostrar de mejor forma el funcionamiento de la arquitectura de interoperación de la red IMS con una red de acceso WLAN.

### 3.1.11.4.1. Selección Inicial de Red

En la Figura 54 se muestran los pasos a seguir para que se realice la selección de red. Estos pasos son:

1. El WLAN UE selecciona una WLAN AN y establece la conexión con el procedimiento específico para esa WLAN.
2. Se inicia el procedimiento de autentificación propio de la tecnología WLAN. Así, el WLAN UE envía el NAI a la WLAN AN.
3. Si la WLAN AN no es capaz de enrutar el requerimiento de autentificación, ésta envía una respuesta al WLAN UE que contiene información de las redes a las que la WLAN AN puede enrutar requerimientos de autentificación. Luego, el puede WLAN UE continua la autentificación de acceso con un NAI diferente o iniciar la autentificación de acceso con otra WLAN UE o puede detenerse. Si el WLAN UE continúa el acceso a través de la WLAN AN seleccionada, debe elegir una red visitada de las propuestas por la WLAN AN y construir el nuevo NAI indicando roaming.
4. La WLAN AN enruta el mensaje 3GPP AAA al Servidor/Proxy 3GPP AAA basado en el NAI para realizar la autentificación de acceso.

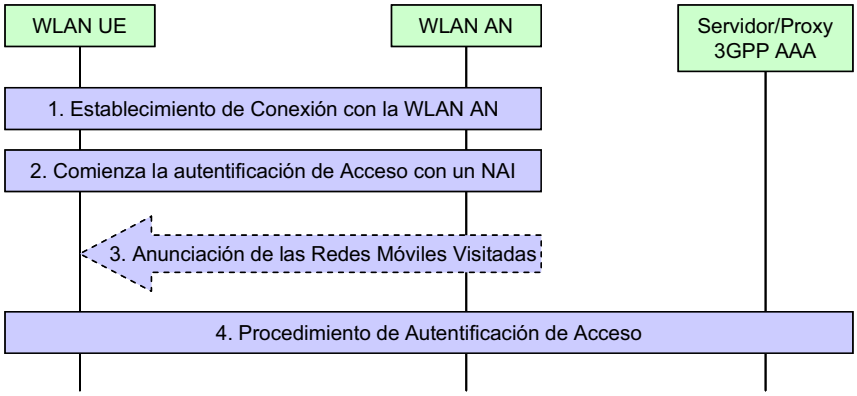



**Figura 54: Selección de WLAN de Interoperación y red Visitada.**

#### 3.1.11.4.2. Autentificación y Autorización de Acceso a la WLAN

En la Figura 55 se muestra el proceso de autentificación y autorización de acceso a la WLAN. Los pasos seguidos se explican a continuación:

1. Se establece la conexión WLAN con el procedimiento específico de la tecnología de la WLAN.
2. Se inicia el procedimiento de autentificación EAP en la forma específica de la tecnología de la WLAN, los paquetes EAP son transportados en forma encapsulada por la interfaz Wa y se intercambian mensajes EAP entre el Servidor 3GPP AAA y el WLAN UE (la cantidad depende del tipo de EAP utilizado). La WLAN AN puede enviar sus capacidades o políticas de QoS al Servidor AAA en los procedimientos de señalización.
3. Si no está disponible en el Servidor 3GPP AAA, se recupera información del HSS para ejecutar la autentificación del usuario que accede. Para identificar al usuario se utiliza el username del NAI. Durante la recuperación de información el HSS verifica si existe otro servidor AAA que esté sirviendo al usuario, si es así, el HSS envía la dirección del Servidor donde el usuario está registrado al servidor actual para que la información sea enrutada al servidor previamente utilizado.
4. Si no está disponible en el Servidor 3GPP AAA, se recuperan del HSS los profiles relacionados con la WLAN de suscriptores. El profile incluye información de autorización e identidad permanente del usuario.
5. Opcionalmente, el Servidor/Proxy 3GPP AAA puede enviar información de aplicación de políticas al WAG de la red móvil pública visitada por el WLAN UE.
6. Si la autentificación y autorización EAP fueron exitosas, el Servidor 3GPP AAA envía un mensaje "Acceso Aceptado" a la WLAN. Mensaje que incluye información de autentificación EAP, autorización de conexión, y profile de QoS (si se aplica).
7. La WLAN informa al WLAN UE sobre el éxito en la autentificación y autorización con un mensaje EAP de éxito.
8. El Servidor 3GPP AAA recibe de la WLAN un mensaje para iniciar el Accounting.
9. El Servidor 3GPP AAA considera que se inicia una nueva sesión autentificada y verifica su validez. Si es de un usuario que ya tiene una sesión previamente establecida, el servidor cierra las sesiones previas para evitar múltiples sesiones WLAN.
10. El Servidor 3GPP AAA registra los usuarios de la WLAN en el HSS, los que son identificados por su identidad permanente.

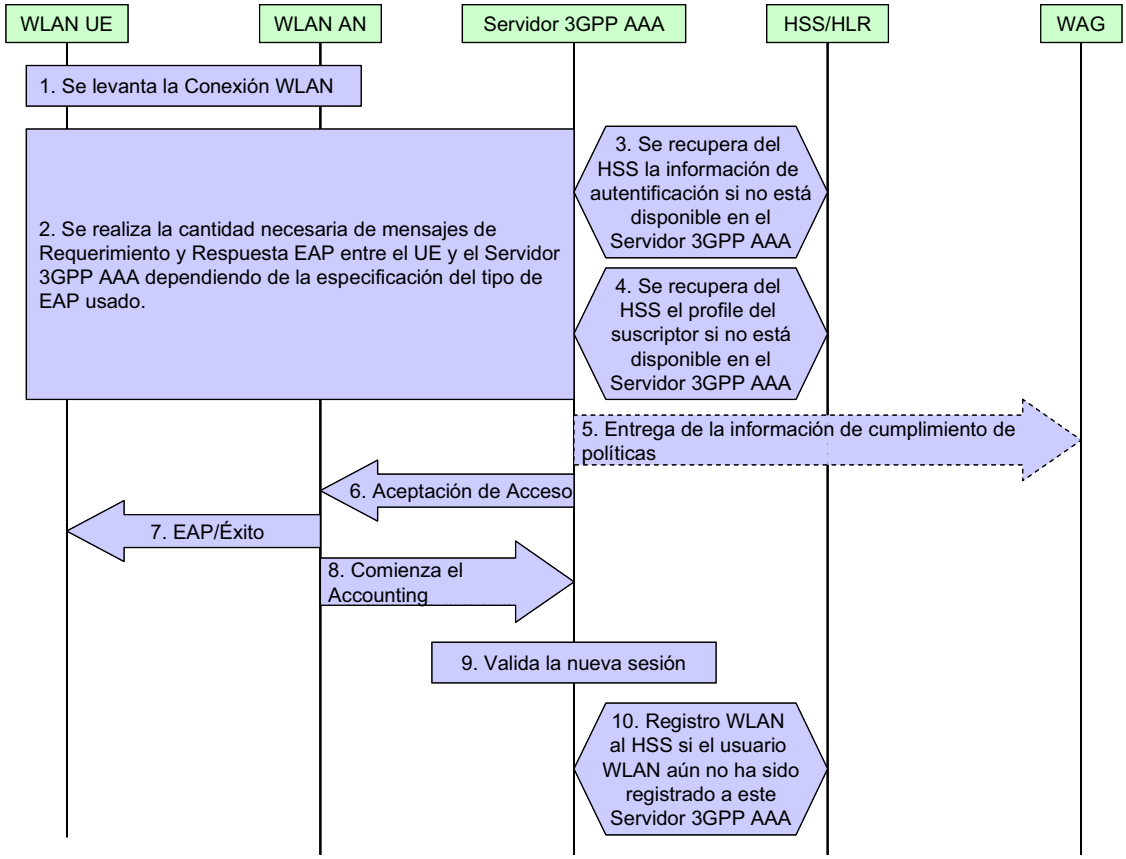



**Figura 55: Procedimiento de Autentificación y Autorización para una WLAN.**

## 3.1.12. Generic Access Network (GAN)

A pesar de que IMS se ha planteado como agnóstica al acceso, es importante mencionar la Red de Acceso Genérico (GAN) que corresponde a una alternativa de acceso a la red IMS. El modelo GAN también es conocido como UMA (Unlicensed Mobile Access) y, a grandes rasgos, define un sistema de telecomunicaciones que permite acceder tanto a redes locales (como tecnologías de acceso Bluetooth o 802.11) como a redes de áreas más amplias (como lo serían redes GSM/GPRS o UMTS) a través de un único terminal conocido como teléfono móvil de modo dual.

La arquitectura funcional de la Red de Acceso Genérico se muestra en la Figura 56. Dentro de las entidades funcionales de esta arquitectura se incluyen:

- Estación Móvil (MS: Mobile Station), que contiene un nuevo bloque funcional para acceder a la GAN.
- Red de Acceso Genérica IP: Es la red que provee conectividad entre el MS y el GANC. La conexión de transporte IP se extiende desde el GAN al MS definiéndose la interfaz Up entre estas entidades.
- Controlador de Acceso Genérico a la Red (GANC: Generic Access Network Controller), que aparece como un Subsistema de Estación Base (BSS) GERAN (Red de Acceso de Radio GSM EDGE) desde el punto de vista del Core de la red. Esta entidad incluye un Gateway de Seguridad (SEGW: Security Gateway) que termina los túneles de acceso

remoto desde el MS, entregando autentificación mutua, encriptación e integridad de datos para el tráfico de señalización, voz y datos.

- SMLC (Serving Mobile Location Center): el GANC puede entregar la información de ubicación requerida al SMLC a través de la interfaz Lb y el SMLC es responsable de la determinación final de localización.
- CBC (Cell Broadcast Centre) que permite servicios de broadcasting a las celdas.

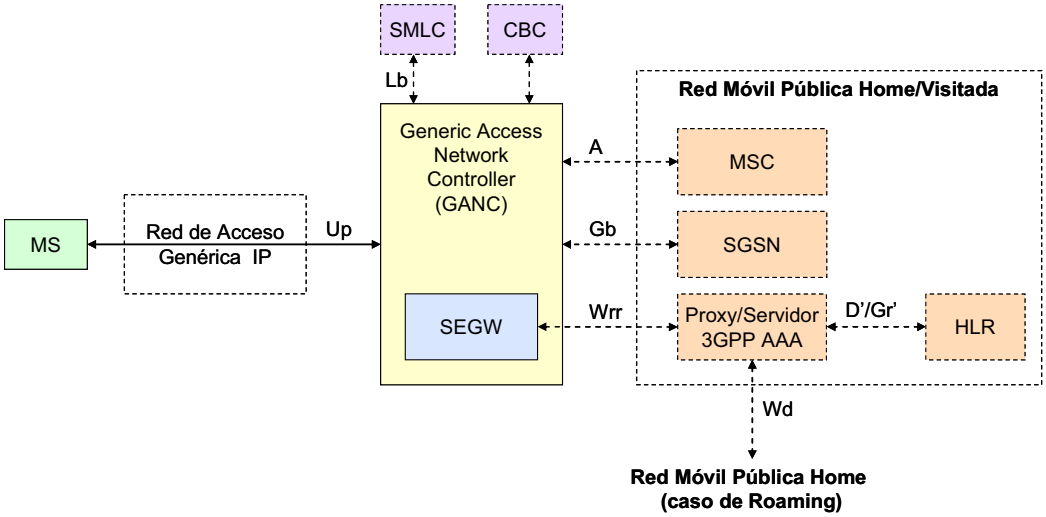



**Figura 56: Arquitectura funcional de GAN.**

Además, GAN cuenta con las siguientes interfaces:

- Interfaz A, para servicios de conmutación de circuitos.
- Interfaz Gb, para servicios de conmutación de paquetes.
- Interfaz CBC-BSC, para soportar servicios de broadcasting en las celdas.

### 3.1.12.1. Selección de Modo en Terminales Multimodales

Un terminal que soporte acceso genérico debe soportar cualquier tipo de tecnología IP además de las interfaces de radio de GERAN (recordar que GERAN consiste al acceso a través de una red GSM EDGE) y, posiblemente, UTRAN (red de acceso UMTS) por lo que el terminal puede estar en cualquiera de estos tipos de operación.

De esta forma, el terminal debe ser configurado para operar en uno de los modos (GERAN/UTRAN o GAN) en un tiempo dado. Cuando el MS se enciende, siempre comienza en modo GERAN/UTRAN, de forma que pueda conmutar al modo GAN basado en preferencias del usuario o en la configuración del operador. Dentro de las preferencias posibles se encuentran:

- Sólo GERAN/UTRAN: El MS nunca conmuta al modo GAN.
- Preferencia GERAN/UTRAN: El MS se encontrará en este modo siempre que detecte una celda adecuada de este tipo de acceso. Si no se encuentra una celda adecuada, entonces el MS conmuta a modo GAN. Sin embargo, si el MS detecta una celda GERAN o UTRAN adecuada se de-registra de la GAN e inicia un registro con la red GERAN/UTRAN.

- Preferencia GAN: Luego de que el MS se ha registrado exitosamente en la GAN con la red de acceso genérica IP, el MS conmuta al modo GAN todo el tiempo que la GAN esté disponible. Si el MS se de-registra o se pierde la conectividad con la GAN, entonces el MS conmuta al modo GERAN/UTRAN.
- Sólo GAN: Luego de que el MS se enciende en modo GERAN/UTRAN para obtener información de la red, éste conmuta al modo GAN y no vuelve a conmutar al modo GERAN/UTRAN.

### 3.1.12.2. Procedimientos de Descubrimiento y Registro en la GAN

Cuando un MS realiza procedimientos de descubrimiento y registro con una GAN, es porque se encuentra en los modos de sólo GAN, preferencia GAN o, si no existe alguna celda GERAN/UTRAN, en el modo preferencia GERAN/UTRAN.

Una vez que el MS establece la conexión con la red IP de acceso genérico, determina un GANC-SEGW apropiado al cual conectarse. Primero, el MS se conecta a una red GANC provisional en su red Home (la dirección de esta entidad se encuentra almacenada en la tarjeta SIM del MS), la que le entrega la dirección del GANC por defecto de la red Home, en el cual el móvil se puede registrar para completar el proceso de registro. El GANC por defecto puede aceptar el registro, redireccionar el MS a otro GANC o rechazar el registro.

Cuando el MS complete exitosamente un registro, éste puede guardar la información del GANC que le está sirviendo que es el GANC con el que pudo realizar el registro. Así mismo, si es rechazado por un GANC o si el registro falla por otra razón, el MS borrará de su lista la información de ese GANC.

En la Figura 57 se presenta un caso normal del proceso de descubrimiento. En resumen, los pasos seguidos son:

1-2. Si al MS se le ha entregado o derivado el nombre de un dominio calificado para obtener el SEGW, éste realiza una consulta DNS a través de la red IP de acceso genérico para obtener la dirección IP del SEGW. Luego, el servidor DNS retorna la dirección IP del SEGW entregado.

3. El MS establece un túnel seguro entre él y el SEGW entregado.

4-5. Si al MS se le ha entregado un nombre de dominio calificado para el GANC, éste realiza una consulta DNS a través del túnel seguro para obtener la dirección IP del GANC. Luego, el servidor DNS retorna una respuesta con la dirección IP del GANC.

6-8. El MS establece una sesión TCP con un puerto del GANC provisional y le consulta a éste la dirección del GANC por defecto usando un mensaje de requerimiento de descubrimiento GA-RC. Luego, el GANC provisional responde con un mensaje de aceptación y usa la información entregada por el MS para entregar la dirección IP o nombre del dominio del GANC por defecto y su SEGW asociado. En caso de que el GANC no pueda aceptar el requerimiento de descubrimiento, éste retorna un mensaje de rechazo al MS indicando la causa de éste rechazo.

9. Se actualiza el túnel seguro IPSec hacia el SEGW. Este mismo túnel puede ser reutilizado para los procedimientos de registro en la GAN.

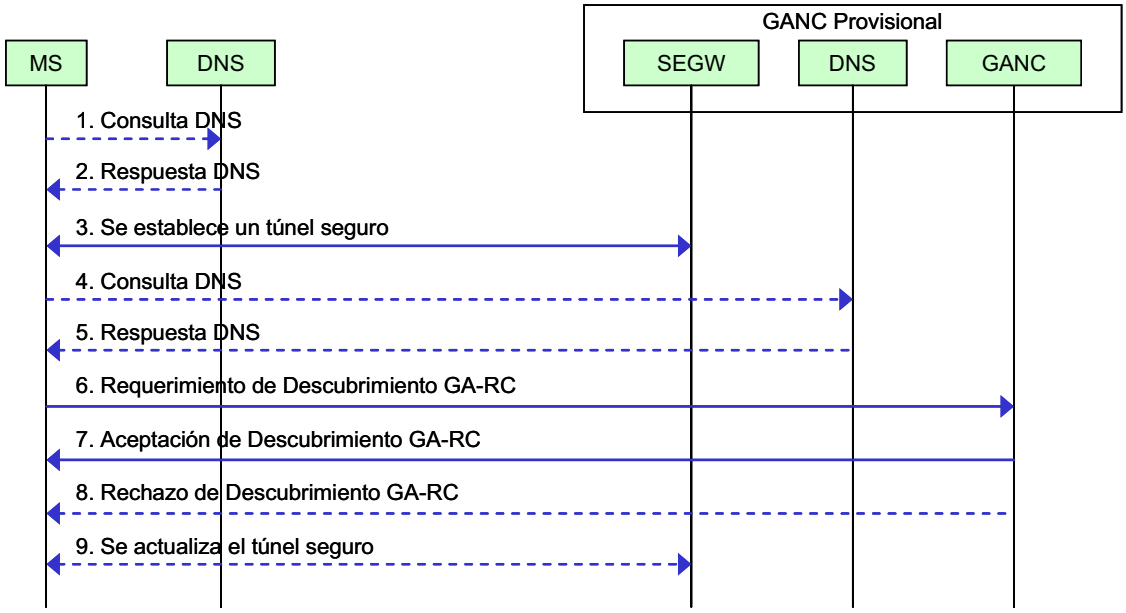



**Figura 57: Procedimiento de Descubrimiento en una GAN.**

Luego del proceso de descubrimiento, el MS establece un túnel seguro con el SEGW del GANC por defecto e intenta registrarse con éste. Si éste GANC acepta el registro entonces se convierte en el GANC Servidor, o el GANC provisional puede redireccionar el registro a un GANC Servidor diferente. El redireccionamiento de GANC puede deberse a la información entregada por el MS, políticas del operador o balanceo de carga de la red.

En la Figura 58 se muestra el proceso normal para un caso de registro. Los pasos seguidos para este proceso son:

1-2. Si el MS sólo cuenta con el nombre de dominio del SEGW por defecto o servidor, debe realizar una consulta DNS para obtener su dirección IP. Luego, el DNS retorna una respuesta.

3. El MS establece un túnel seguro IPSec con el SEGW si es que no se reutiliza el túnel establecido en el proceso de descubrimiento.

4-5. Si el MS tiene el nombre del dominio del GANC por defecto o servidor, éste debe realizar una consulta DNS para obtener su dirección IP. Luego, el servidor DNS entrega una respuesta.

6-9. El MS levanta una conexión TCP con un puerto TCP en el GANC e intenta registrarse en éste transmitiendo un requerimiento de registro GA-RC. Si el GANC acepta el intento de registro, responde con un mensaje de aceptación de registro GA-RC. En el caso de que el GANC rechace el registro, responde con un mensaje de rechazo de registro con las razones del rechazo. Alternativamente, si el GANC desea redireccionar el MS a otro GANC Servidor, le envía un mensaje de Redirección de registro GA-RC entregando el nombre del dominio o dirección IP del GANC objetivo junto con su SEGW asociado.

10. Si la conexión TCP es actualizada, el túnel IPSec puede ser actualizado dependiendo si la red indica que el mismo túnel puede ser reutilizado para el próximo registro.

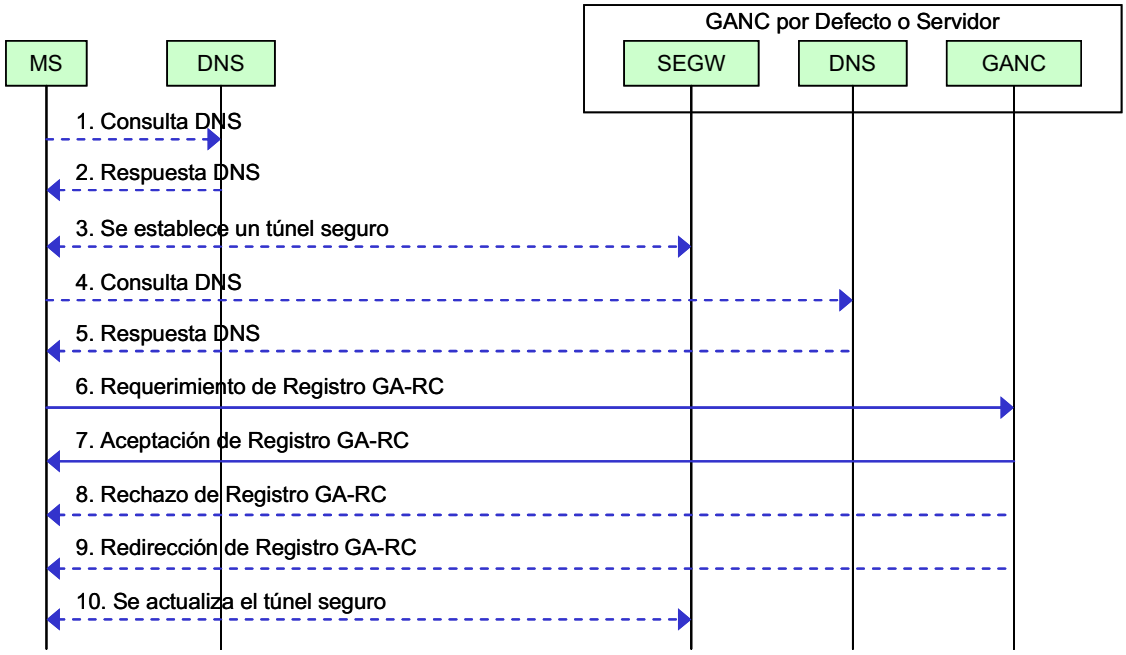



**Figura 58: Procedimiento de Registro en una GAN.**

### 3.1.12.3. Manejo de Handoff

Dado que en los terminales multimodales existentes para el acceso GAN definen perfiles de preferencias de acceso a la red GERAN/UTRAN o GAN que no necesariamente excluye a una de estas tecnologías se tienen dos tipos de handoff:

- Handoff GERAN/UTRAN a GAN: El que se produce asumiendo que el MS se encuentra con una llamada activa en la GERAN/UTRAN y que su modo seleccionado es Preferencia GAN o es Preferencia GERAN/UTRAN pero se pierde el acceso a una celda con estas características. Así, el MS se ha registrado exitosamente con una GANC obteniendo la información necesaria del sistema GAN.
- Handoff GAN a GERAN/UTRAN: Se produce asumiendo que el MS está con una llamada activa en la GAN cuando un acceso GERAN/UTRAN se vuelve disponible y que el modo seleccionado del MS es Preferencia GERAN/UTRAN o es de Preferencia GAN pero el MS comienza a perder cobertura de la GAN basándose en sus medidas locales, reportes RTCP recibidos o indicaciones de calidad del enlace uplink recibidas de la GANC.

En la Figura 59, a modo de ejemplo, se muestra el proceso de handoff desde una red UTRAN a GAN. El procedimiento realizado es:

1. El MS comienza a incluir información sobre una celda GAN en los mensajes de Reporte de Medidas enviados al RNC (Radio Network Controller, en UMTS controla uno o más nodos B). Así, el MS reporta el nivel de señal más alto de la celda GAN, este valor no es el valor real medido, sino que un valor artificial que le permite al UE indicar preferencia por la GAN.

2-4. Basado en las medidas del MS el RNC decide iniciar el handoff a la celda GAN y comienza la fase de preparación del proceso de reubicación enviando un mensaje de Reubicación Requerida al CN identificando la celda objetivo (GAN). Luego, el CN envía un requerimiento al GANC objetivo para la asignación de recursos del handoff y el GANC objetivo envía un reconocimiento del requerimiento de handoff enviado

indicando que puede soportar el handoff y el canal de radio al que se debe dirigir la estación.

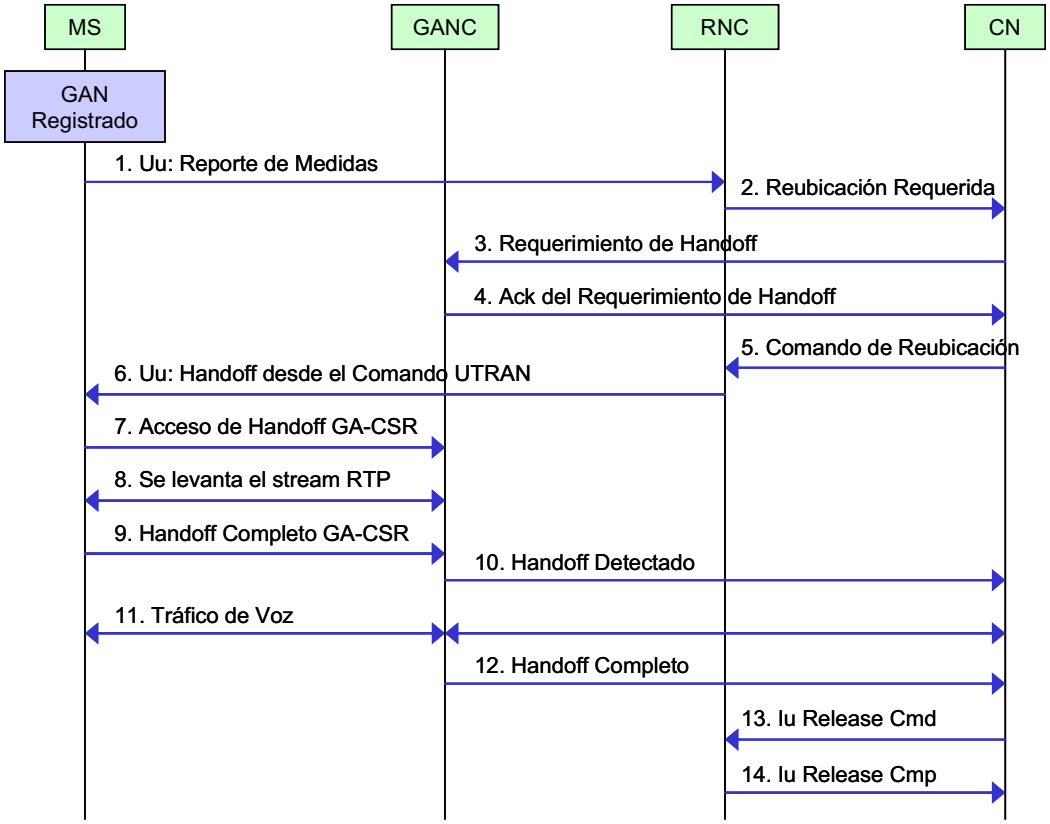



**Figura 59: Procedimiento de Handoff desde una celda UTRAN a una GAN.**

5-6. El CN envía un comando de Reubicación al RNC y éste envía al MS un mensaje de Handoff desde la UTRAN para iniciar el handoff a la GAN. El MS no conmuta su mapa de audio desde la UTRAN a la GAN hasta que se complete el handoff para reducir el tiempo de corte de la señal de voz.

7-9. El MS accede al GANC con el mensaje de acceso recibido y el comando de handoff desde la UTRAN recibido desde el RNC, con este mensaje el GANC correlaciona el handoff con el reconocimiento que le había enviado al CN e identifica el éxito del handoff. Luego el GANC activa el mapa de portadores con el MS y el MS transmite un mensaje de handoff completo para indicar el término del procedimiento desde su perspectiva.

10-12. El GANC indica al CN que ha detectado al MS y el CN tiene la opción de conmutar el plano de usuario desde el RNC hacia el GANC. Se establece el tráfico de voz bidireccional entre el MS y CN a través del GANC y el GANC indica que el handoff está completo. Si aún no se ha conmutado el plano de usuario, se conmuta en este momento.

13-14. Finalmente, el CN derriba la conexión hacia el RNC con el Comando Release Iu y el RNC confirma la actualización de los recursos UTRAN asignados para la llamada.

## 3.2. Diferencias entre IMS y PSTN

Hasta ahora ya se han definido las entidades funcionales necesarias para la interoperación entre una red IMS y una red PSTN. Estas entidades son:

- MGCF (Media Gateway Control Function), que es el encargado del control del estado de llamadas y el control de conexión en el IMS-MGW. Además se comunica con las entidades CSCF, BGCF y PSTN y realiza la conversión de protocolos entre ISUP/TCAP y protocolos de control de llamadas de IMS.
- IMS-MGW (IMS – Media Gateway), que puede levantar terminaciones de canales de portadores desde una red CS y stream media desde una red PS (por ejemplo transmisiones RTP). Además interactúa con el MGCF para el control de recursos y administra ciertos recursos.
- BGCF (Border Gateway Control Function), que selecciona la red en la cual ocurrirá el paso a la PSTN y, dentro de esta red, selecciona el MGCF.
- T-SGW (Trunking Signaling Gateway) que se encarga de la conversión de señalización a nivel de transporte entre SS7 y señalización IP.

Para una mayor comprensión en las diferencias que deben soslayar estas entidades para la interoperación entre ambas redes se analizan las principales diferencias entre las redes IMS y PSTN.

### 3.2.1. Numeración e Identidades

#### 3.2.1.1. Identidad de Usuario

Como se mencionó anteriormente, un suscriptor en IMS cuenta con dos tipos de identidades: privadas y públicas. Una identidad privada puede componerse de una o más identidades públicas y un usuario puede tener, a su vez, una o más identidades privadas. De la misma forma, un suscriptor puede contar con uno o más Perfiles (Profiles) de Servicio que corresponden a un conjunto de datos relacionados con el usuario y servicio (ver Figura 38).

Por otra parte, en la red PSTN no existe una relación así para los suscriptores. Un suscriptor está asignado a una conexión telefónica mediante una base de datos con la finalidad básica de cobranza. De la misma forma, los planes de servicio están asignados a la conexión más que al suscriptor. Sin embargo, últimamente se han implementado servicios que ofrecen más control a un cliente mediante el uso de claves. Un ejemplo de este control se observa en planes de telefonía con bloqueo a ciertas llamadas excepto si se ingresa una clave en el teléfono, la que autentificaría al cliente dueño de la suscripción.

#### 3.2.1.2. Identidad en el Terminal

En IMS no sólo se identifica al usuario desde la red sino que existe un sistema de identificación del usuario dentro del propio terminal. Este sistema consiste en un módulo de identificación conocido como ISIM (IP Multimedia Services Identity Module) que reside en un dispositivo físico removible dentro del terminal llamado UICC (Universal Integrated Circuit Card). El ISIM almacena

datos específicos del suscriptor IMS, estos datos se pueden dividir en ser grupos, como se muestra en la Figura 60, estos grupos o bloques son:

- Claves de Seguridad, que se dividen en:
  - Claves de Integridad: usadas para proveer integridad a los datos de señalización SIP.
  - Claves de Cifrado: usadas para proveer confidencialidad a la señalización SIP.
  - Claves Identificadores: usadas para servicios de seguridad IMS.
- Identidad Privada de Usuario, utilizada en los requerimientos de registro para identificar la suscripción de usuario.
- Identidad Pública de Usuario, que contiene una o más identidades públicas y es usado en los requerimientos de registro y de comunicación con otros usuarios.
- Nombre de Dominio de la Red Home, consiste en el nombre del punto de entrada de la red Home y se usa para enrutar los requerimientos de registro del usuario a su red Home.
- Referencia de Reglas de Acceso, usado para guardar información sobre los números personales de identificación que necesitan ser verificados para tener acceso a la aplicación.
- Datos Administrativos, incluyen datos que pueden ser usados por los suscriptores IMS para ciertas operaciones o por manufactureras para ejecutar pruebas.

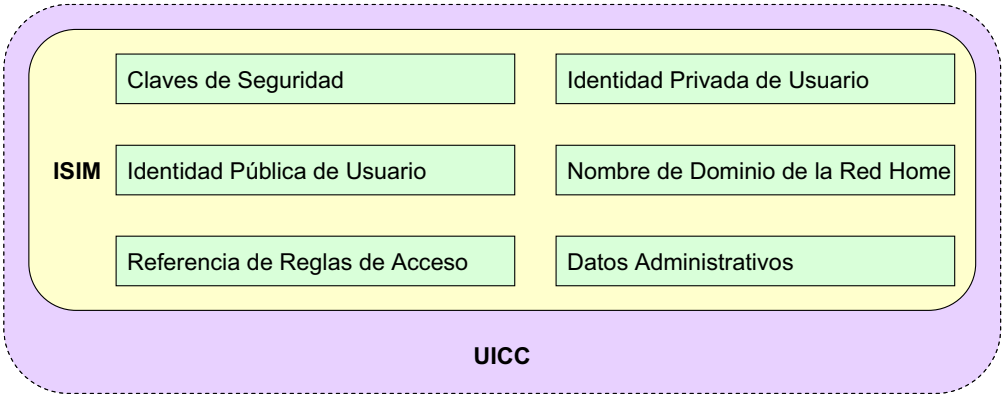



**Figura 60: Módulo de Identidad de Servicios IP Multimedia (ISIM).**

Además del módulo ISIM que identifica al usuario, el terminal puede contar con un identificador propio del terminal llamado IMEI (International Mobile station Equipment Identity) que, al igual que en GSM, define en forma única al terminal para mayor seguridad.

En cuanto a la arquitectura PSTN, estos módulos de identidad no son aplicables ya que el terminal no almacena ninguna información que haga que el Core de la red reconozca la suscripción. Los datos de la suscripción junto con la identidad de ésta se encuentran asociados exclusivamente a la "línea" que brinda el servicio siendo el terminal un dispositivo anónimo que puede ser conectado a cualquier línea.

### 3.2.1.3. Identidad para el Enrutamiento de Llamadas

Aquí se pretende comparar las identidades necesarias para poder enrutar una llamada hasta cierta dirección. En la red PSTN estas identidades tienen la forma de un plan de numeración. Este plan de numeración consiste en un sistema que identifica puntos de comunicación dentro de una red

mediante el uso estructurado de números. Dado que la telefonía tradicional es fija, la estructura de los números se divide para indicar regiones específicas o grupos de suscripciones.

No existe un único sistema de numeración telefónica en el mundo, sino que varía de país en país. Para identificar en forma única cada línea o conexión en la PSTN, la CCITT (Comite Consultatif Internationale de Telegraphique et Telephonique) diseñó un plan de numeración mundial que cuenta con códigos de acceso a cada país y llamados códigos nacionales. De la misma forma, la ITU-T administra y diseña el estándar de Plan de Numeración Mundial. La recomendación E.164 de la ITU-T describe la estructura de este plan y sus requerimientos. Esta recomendación provee la estructura de números y funcionalidades para tres categorías de numeración de telecomunicaciones públicas internacionales:

- Estructura de Numeración para Áreas Geográficas: Identifica una suscripción dentro de un área geográfica a nivel local, nacional e internacional. Su estructura tiene un número máximo de 15 dígitos y cuenta con las siguientes partes:
  - Código de país, que va de 1 a 3 dígitos.
  - Número Significativo Nacional (NSN: National Significant Number) que está conformado por el Código de Destino Nacional (NCD: National Destination Code) que es opcional y por el número de suscripción (SN: Subscriber Number). Su largo máximo está condicionado por el largo del código de país (ambos deben sumar a lo más 15 dígitos).
- Estructura de Numeración para Servicios Globales: Identifica suscripciones en forma única sólo a nivel internacional. Consiste en un código de país de tres dígitos y un número de suscripción global. El código de país se encuentra siempre en el rango de los 8xx o 9xx y se utiliza para servicios como números de teléfonos gratuitos internacionales entre otros.
- Estructura de Numeración para Redes: Identifica una suscripción únicamente dentro de una red e internacionalmente. Su estructura es básicamente para direccionar redes como sistemas satelitales globales o proveedores de servicios de red. Esta estructura cuenta con los siguientes bloques:
  - Código de país, que tiene tres dígitos y se encuentra siempre en el rango de los 8xx.
  - Código de Identificación de Red, que va de 1 a 4 dígitos.
  - Número de la suscripción.

En la Figura 61 se muestran los formatos para cada tipo de numeración establecidos por la recomendación E.164 de la ITU-T.

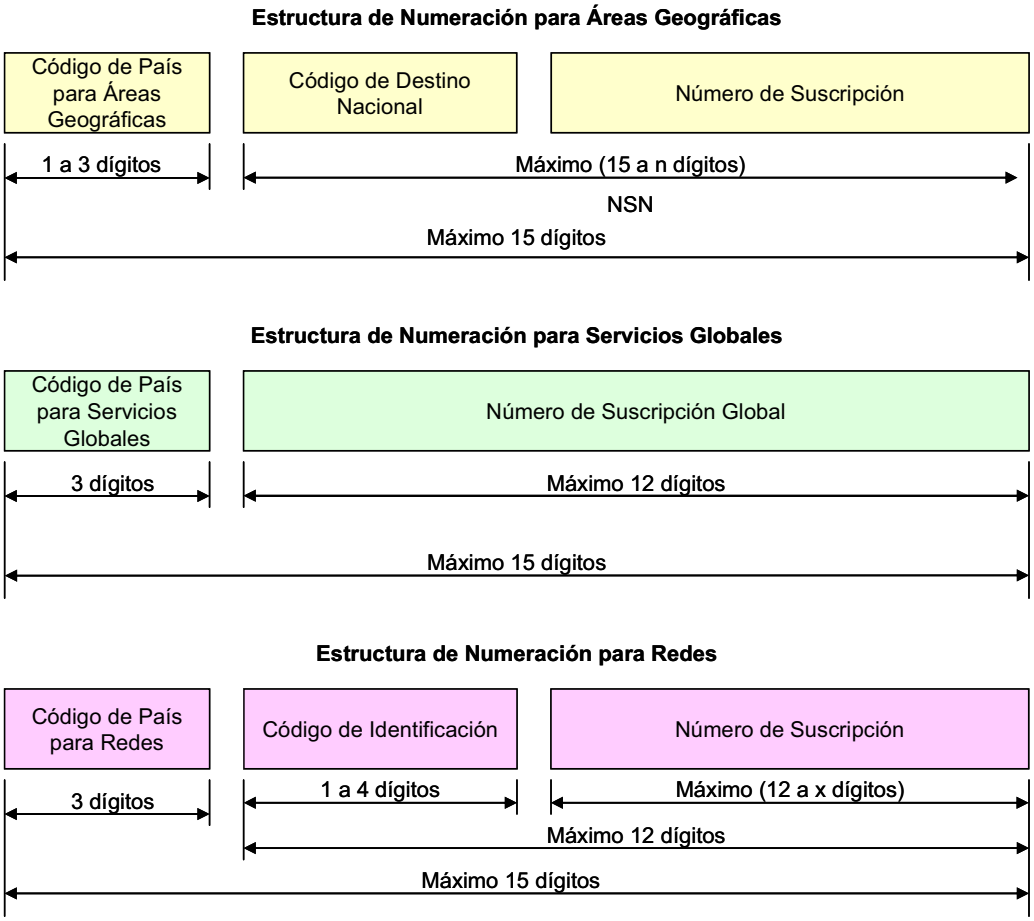



**Figura 61: Formatos de Numeración de la Recomendación ITU-T E.164.**

En el sistema IMS se utilizan las entidades privadas y públicas de usuario para lograr enrutar la llamada. Cada vez que un cliente IMS se registra en la red, el HSS (Home Subscriber Server) guarda la ubicación del suscriptor junto con el P-CSCF que le permite el acceso a la red IMS, ya sea si el cliente se encuentra en su red Home o en una red Visitada (caso de Roaming).

Un ejemplo de identidad privada de usuario sería "usuario_ejemplo@realm". Por otra parte, la identidad de usuario pública en IMS está definida por las identidades que provee el protocolo SIP. Estas identidades pueden ser de dos tipos:

- SIP URI (Uniform Resource Identifier): Este tipo de identidad tiene la misma forma que una dirección e-mail: "usuario@dominio". Existen dos esquemas de SIP URIs:
  - sip:pedro.perez@nokia.com es un SIP URI, que corresponde a la forma más común.
  - sips:pedro.perez@nokia.com es un SIP URI Seguro (Secure SIP URI).

  Además, existen dos tipos de SIP y SIP URIs:
  - Dirección de Registro (AOR: Address of Record), que es una dirección IP que identifica al usuario y que puede ser manejado por la gente como un número telefónico.
  - Nombre de Dominio Completamente Cualificado (FQDN: Fully Qualified Domain Name) o dirección IP (identifica un dispositivo) del dominio. Un ejemplo de ésta es sip:pedro.perez@127.233.4.16 o sip:pedro.perez@pc2.nmp.nokia.com.

- tel (telephone) URI: Se usa para identificar recursos usando un número de teléfono. SIP permite que los requerimientos sean enviados a un teléfono URI. El tel URI puede contener un número global o local. Si es un número global sigue la regla de la recomendación E.164 y comienza con un "+" (por ejemplo, tel:+358-9-123-45678), si es un número local sigue los planes privados de numeración.

Las entidades de red también cuentan con un sistema de identificación mediante SIP URIs. Sin embargo, no es necesario que estos identificadores sean globalmente publicados en servidores DNS. Un ejemplo de identificador de CSCF puede ser sip:chile.cscf3@ims.ejemplo.com.

Los distintos tipos de numeración para la PSTN e IMS pueden interactuar mediante un sistema de resolución de dirección E.164 a SIP-URI. El S-CSCF puede soportar la habilidad de traducir direcciones E.164 contenidos en un requerimiento URI a un tel URI no SIP utilizando traducción de un servidor ENUM DNS, donde ENUM es un protocolo que permite el mapeo de direcciones E.164 a planes de dirección IP DNS, utilizando un sistema jerárquico muy similar al del sistema DNS. La operación realizada por ENUM consiste en un mapeo de los dígitos E.164 a zonas separadas DNS concatenadas con el dominio "e164.arpa". El mapeo de los números es simple: Cada dígito del número de teléfono se invierte en orden de significancia y se inserta un punto (.) entre cada dígito. Luego se agrega el dominio "e164.arpa" a la secuencia de números invertida. El proceso puede resumirse en cinco pasos:

Se verifica que el número de teléfono esté escrito en su forma completa incluyendo el código de país. Por ejemplo, + 1-703-610-2000.

- Se remueve todos los caracteres que no sean dígitos, con la excepción del "+", que se mantiene como un flag para identificar que el número está completamente cualificado. Por ejemplo, 17036102000.
- Se insertan puntos entre cada dígito. Por ejemplo, 1.7.0.3.6.1.0.2.0.0.0.
- Se invierte el orden de los dígitos. Por ejemplo, 0.0.0.2.0.1.6.3.0.7.1.
- Se agrega el string "e164.arpa" al final del número. Por ejemplo, 0.0.0.2.0.1.6.3.0.7.1.e164.arpa.

Luego de mapear el número al nombre del dominio, se consulta un DNS para obtener la ubicación URI correspondiente. Un ejemplo de la traducción de E.164 a SIP URI se muestra en la Figura 62.

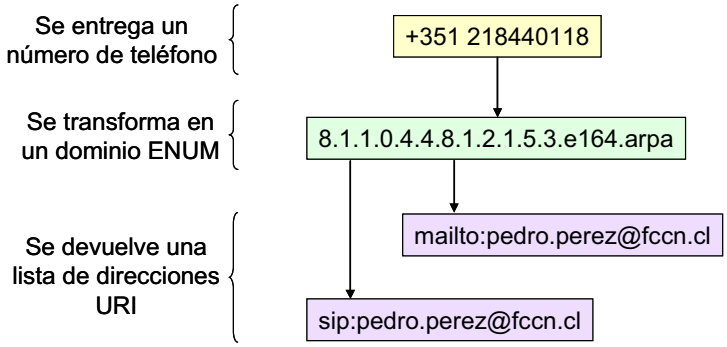



**Figura 62: Ejemplo de Traducción de E.164 a SIP URI.**

### 3.2.2. Movilidad

La telefonía fija no soporta movilidad ya que cada suscripción está asociada a una línea o conexión telefónica. Al contrario, la movilidad es una de las características más valiosas de IMS como arquitectura paraguas de la convergencia. La arquitectura IMS y los "sabores" de CSCFs (Proxy-CSCF, Interrogating-CSCF y Serving-CSCF) permiten que un cliente pueda acceder a sus servicios contratados dentro de su propia red Home. En la Figura 63 se muestra un usuario en caso de "Roaming" registrándose en su red, esto es un claro ejemplo del sistema de movilidad y de roaming en la arquitectura IMS.

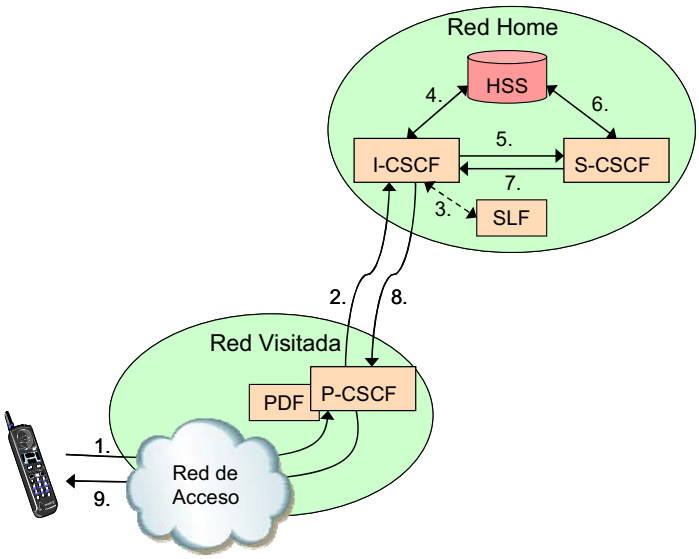



**Figura 63: Resumen de un Proceso de Registro en IMS.**

En resumen, el proceso es:

1-2. El UE descubre un P-CSCF en la red visitada y envía un requerimiento de registro. El P-CSCF determina que la red Home del usuario no es la propia y envía el requerimiento a un CSCF conocido de esa red, el I-CSCF.

3-5. El I-CSCF consulta al SLF la dirección del HSS al cual dirigirse para verificar la suscripción de usuario (si es que existe más de un HSS). Luego de verificar los datos de la suscripción con el HSS, envía el requerimiento a un S-CSCF asignado basado en los servicios requeridos.

6-9. El S-CSCF pide el Profile de Servicio al HSS y guarda en éste las direcciones necesarias para contactar al UE, luego se envía la respuesta al terminal de usuario a través del I-CSCF y P-CSCF.

### 3.2.3. Calidad de Servicio (QoS)

La arquitectura PSTN se conoce como una arquitectura CS o de Conmutación de Circuitos. Esto quiere decir que un usuario tiene cierta cantidad fija de recursos asignada durante la duración de la llamada (la que se asigna al inicio de ésta) por lo que esta arquitectura ofrece servicios de llamadas con calidad de servicio garantizada.

En el sistema IMS, en cambio, se tiene que la transmisión es PS o de conmutación de paquetes. Al ser la transmisión de naturaleza IP, los canales y recursos de transmisión son compartidos por todos los usuario dentro de la celda y se hace necesario un sistema de administración de recursos o de portadores de red. Como se expuso anteriormente, el sistema encargado de la administración de portadores de tráfico en IMS es el Control SBLP (Service-Based Local Policy Control), el que se encargará de la autorización de portadores (acción que realiza el PDF y que ejecuta el SGSN). La autorización de QoS es realizado por el PDF basándose en los siguientes datos:

- Identificador de flujo, que identifica los flujos IP descritos en las componentes de media asociados a una sesión SIP. Un ejemplo de identificador es: "m=video 50230 RTP/AVP 31".
- Tasa de datos, información que se deriva de los parámetros de ancho de banda SDP.
- Clase de QoS: Representa la clase más alta que puede ser usada por la componente media que requiere el UE.

### 3.2.4. Señalización de Llamadas

La arquitectura PSTN utiliza señalización SS7 (Signaling System #7), este estándar se encarga de enrutar los mensajes de control a través de la red para realizar la administración de llamadas (creación, mantención y terminación) y funciones de administración de red. A pesar de que la PSTN es una red de conmutación de circuitos, el sistema de señalización es de conmutación de paquetes y está sobrepuesto sobre la red de conmutación de circuitos. La red y protocolo SS7 se utilizan para lo siguiente:

- Levantar, administrar y eliminar llamadas.
- Servicios inalámbricos.
- Servicios de telecomunicaciones gratuitos (800/888) e inalámbricos (900).
- Características de llamadas mejoradas como reenvío de llamadas o conferencia.
- Telecomunicaciones eficientes y seguras.

SS7 se explica en forma más detallada en la sección 2.7.1.3 de Antecedentes. En la Figura 64 se observa el mapa de señalización que se establece con el protocolo ISUP en una llamada local. El significado de los mensajes de señalización puede encontrarse en la Tabla 3. En resumen, el procedimiento es como sigue:

- El teléfono de origen levanta el teléfono y marca el número del teléfono de destino
- El SSP más cercano genera un mensaje ISUP IAM para reservar un circuito, este requerimiento es enrutado desde el SSP de origen (SSP 1) hasta el de destino (SSP 2).
- El SSP de destino verifica que la suscripción de destino se encuentre en su entorno, en ese caso, envía al SSP de origen un mensaje ISUP ACM y genera un tono de llamada en el teléfono de destino.
- El SSP de origen recibe el ACM y genera un tono de marcado en el teléfono de origen.
- Cuando el teléfono de destino contesta, el SSP de destino deja de transmitir el tono de llamado y envía un mensaje ISUP ANM al SSP de origen.
- El SSP de origen conecta al usuario del teléfono de origen y se inicia el cobro de la llamada (proceso de facturación).

- Cuando un usuario cuelga (en este caso, el de origen) el SSP de origen envía al de destino un mensaje ISUP REL para limpiar la llamada y liberar recursos.
- El SSP de destino deja sin tono la línea o envía un tono al teléfono de destino, luego reconoce el mensaje ISUP REL con un mensaje ISUP RLC. El usuario de destino puede colgar en cualquier momento desde que el usuario de origen colgó.

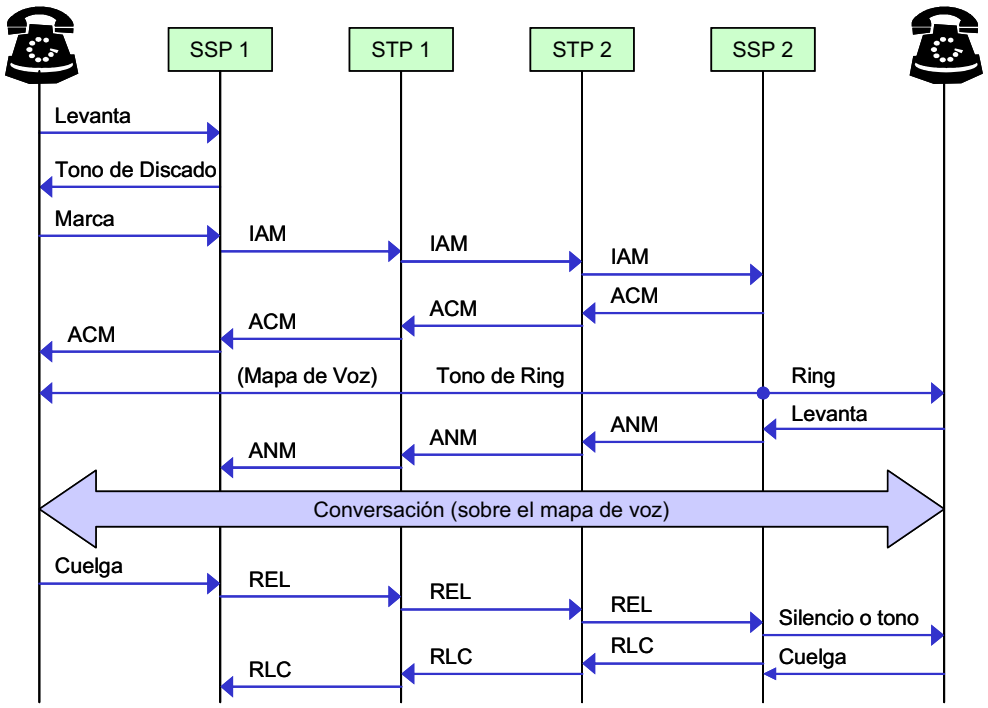



**Figura 64: Tráfico de Señalización ISUP generado en una llamada Local.**

En cuanto a IMS, el protocolo principal de señalización de llamadas es SIP (Session Initiation Protocol) de la IETF. El protocolo SIP tiene la finalidad de establecer, modificar y terminar sesiones multimedia y fue creado con los siguientes objetivos:

- Neutralidad del Protocolo de Transporte, que sea capaz de correr sobre protocolos confiables (TCP, SCTP) y no confiables (UDP).
- Requerimientos de Enrutamiento, que puede ser directo (desempeño) o enrutado por un proxy (control).
- Separación de la descripción de señalización y media.
- Extensibilidad.
- Movilidad Personal.

En todos los procesos mostrados para IMS está presente la señalización SIP en el enrutamiento de llamadas. A continuación se presente un ejemplo simple de la función que realiza un Servidor Proxy en una sesión SIP entre dos terminales.

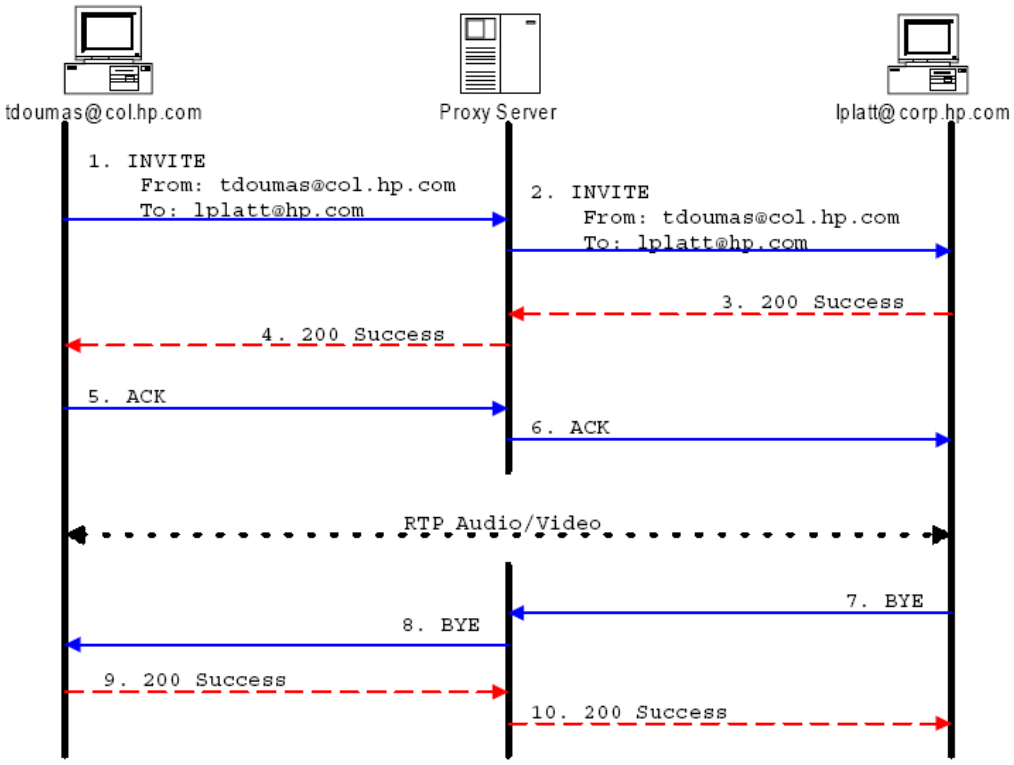



**Figura 65: Operación de un Servidor Proxy.**

## 3.3. Diferencias entre IMS y Packetcable

A diferencia de la relación entre la arquitectura PSTN e IMS, la arquitectura PacketCable (de CableLabs) corresponde a una adaptación de la arquitectura IMS a las redes de los operadores de cable. Esta adaptación se realiza con la finalidad de que los operadores de redes de cable agreguen servicios móviles a sus paquetes de servicios para atraer la atención del cliente mediante servicios multimedia. De esta forma, los operadores de cable saltarán de sus servicios "triple play" (datos, voz y televisión) a un "cuadruple play" con la adición de servicios inalámbricos. Dentro de los nuevos servicios multimedia que estos operadores podrían ofrecer ya se están viendo en el mercado, como por ejemplo VoD (Video on Demand) y otros están por venir como teléfonos celulares duales (tecnología celular más Wi-Fi).

PacketCable adapta sus entidades funcionales e interfaces junto con agregar otras nuevas para implementar una red tipo IMS. Aquí se pretende mencionar los principales cambios y aportes realizados por PacketCable a IMS de forma de ilustrar aplicaciones reales de IMS a redes actuales para implementar servicios convergentes.

### 3.3.1. Origen de las Arquitecturas

Ya se ha explicado que IMS proviene de la evolución de la tecnología celular UMTS, tecnología de acceso que define en el Core de su red a la arquitectura IMS. A pesar de que IMS fue ampliándose gradualmente a distintas arquitecturas de telecomunicaciones y a distintos métodos de acceso, el acceso a través de la tecnología GPRS o UMTS corresponden a su punto fuerte.

Por otra parte, la orientación de PacketCable responde a los intereses de los operadores de Cable. Las primeras versiones de PacketCable no estaban basadas en IMS sino que simplemente se orientaban a brindar servicios de voz y, posteriormente, algunos servicios multimedia. Sin embargo, en la versión 2.0, PacketCable se basa casi completamente en IMS (ver Figura 33).

### 3.3.2. Aplicación de QoS

Un ejemplo bastante ilustrativo de la adaptación que realiza PacketCable corresponde al sistema encargado de la aplicación de QoS en la red. En la Figura 66 se muestra un esquemático de las entidades necesarias para esta finalidad.

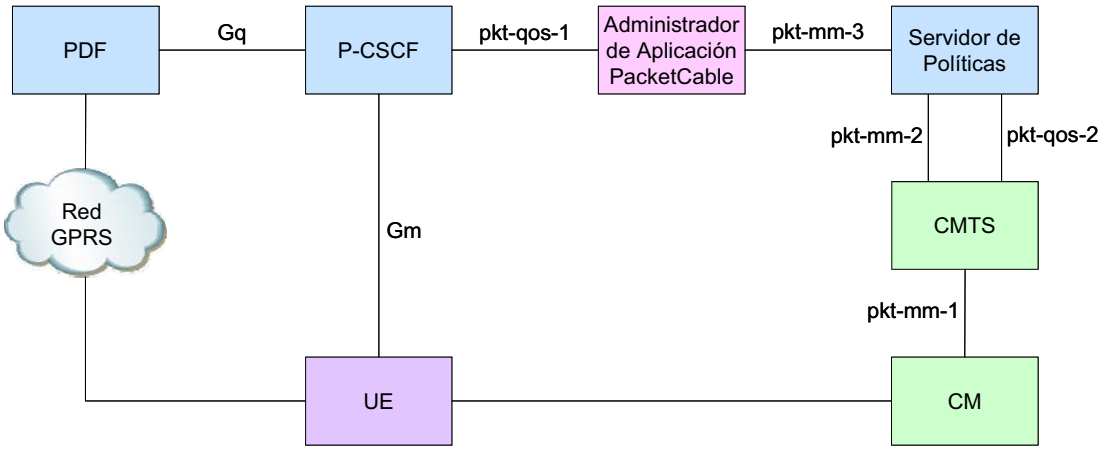



**Figura 66: Puntos de Referencia de QoS en PacketCable.**

Se observa que esta arquitectura es bastante similar a la de IMS, pero con la salvedad de que existe una entidad funcional, el Administrador de Aplicación PacketCable, y varias interfaces exclusivas de PacketCable (para más información, ver la ).

La función del Administrador de Aplicación (AM, Application Manager) es ser una interfaz entre la arquitectura SIP de PacketCable y la arquitectura PacketCable Multimedia (primera arquitectura desarrollada para brindar servicios Multimedia). De esta forma, recibe los mensajes de QoS desde el P-CSCF y los formula adecuadamente para que sean interpretados por el Servidor de políticas de la arquitectura PacketCable Multimedia. Es importante notar que, si el UE accede desde una red GPRS se utiliza la interfaz Gb, de IMS, para la administración de QoS desde el PDF hasta el P-CSCF. Por otra parte, si accede a través de una red de cable, los requerimientos de QoS son recibidos por el Servidor de Políticas, el que los envía al AM.

### 3.3.3. Adaptaciones a la Identidad de Usuario

Además de las identidades públicas y privadas de usuario definidas por IMS, PacketCable agrega la identidad GRUU (Globally Routable User Agent URI), en que cada GRUU se asocia con una identidad pública de usuario y un UE. Esta adaptación se explica en la sección 9.2.4.5 de Anexos.

### 3.3.4. Elementos de Interconexión

PacketCable posee elementos de borde de red para comunicarse con otras redes del tipo IMS y con la red PSTN. Además, esta arquitectura incluye la entidad funcional CMS (Call Management Server) que provee soporte a servicios de telefonía para clientes de señalización de llamadas (por ejemplo, E-MTAs). El CMS provee la mayoría de las características de telefonía e interactúa con los servidores de aplicación para proveer aplicaciones adicionales.

## 3.4. Management Information Base (MIB)

Una parte muy importante en el funcionamiento de redes es su nivel de administrabilidad. Una Base de Información de Administración o MIB consiste en una base de datos virtual utilizada para administrar las entidades en una red de telecomunicaciones (como por ejemplo routers o switches).

La base de datos es jerárquica con una estructura en forma de árbol y sus entradas son direccionadas mediante identificadores de objetos implementados mediante ASN.1. ASN.1 (Abstract Syntax Notation One) es un estándar de notación flexible que describe estructuras de datos para representar, codificar, transmitir y decodificar datos. Éste provee un conjunto de normas formales para describir estructuras de objetos independientes de las técnicas de comunicación de una máquina específica y permite remover ambigüedades. Las identidades objeto que son raíces en la jerarquía MIB pertenecen a diferentes organizaciones de estándares mientras que las identidades de niveles inferiores son asignados por organizaciones asociadas.

Una herramienta importante en la base de información de administración es SNMP (Simple Network Management Protocol) que consiste en un protocolo de comunicación entre estaciones de administración (como por ejemplo, consolas) y los objetos administrados (como routers, switches y gateways). Las componentes controladas por la consola de administración necesita un Agente SNMP que es un software que se puede comunicar con el administrador SNMP.

Un objeto administrado es uno de cierto número de características específicas del dispositivo administrado. Existen dos tipos de objetos administrados: los escalares (que definen una única instancia del objeto) y los tabulares (que definen múltiples instancias relacionadas a un objeto y que se agrupan en tablas MIB). Dentro de los objetos MIB se encuentran objetos mandatorios, por ejemplo, una Tabla de Traducción de Dirección (llamada atTable). Los MIBs son periódicamente actualizados de forma de agregar nuevas funcionalidades y reparar defectos.

### 3.4.1. Simple Network Management Protocol (SNMP)

Una red con administración SNMP cuenta con tres componentes claves:

- Dispositivos administrados: Es un nodo de la red que contiene un agente SNMP y que se ubica en una red administrada. Éstos recolectan y almacenan información de administración dejando la información a disponibilidad de los NMSs usando SNMP.
- Agentes: Consiste en un software de administración de red que se encuentra en un dispositivo administrado. Éste posee conocimiento local de información administrativa y traduce esta información a una forma compatible con SNMP.

- Sistemas de Administración de Red (NMS: Network-Management System): Ejecuta aplicaciones que monitorean y controlan los dispositivos administrados. Éstos proveen la mayor parte de los recursos de procesamiento y memoria para la administración de la red.

La arquitectura SNMP cuanta con las siguientes entidades funcionales:

- Agente Master: Consiste en un software corriendo en una componente de red que soporte SNMP. Así, éste actúa como un servidor en la terminología de la arquitectura cliente-servidor. Un Agente Master se basa en sub-agentes que proveen información sobre la administración de funcionalidades específicas. Los agentes Master también pueden ser referidos como objetos administrados.
- Sub-agente: Consiste en un software corriendo en una componente de red que soporte SNMP y que implemente la información y funcionalidad de administración definida por un MIB específico de un sistema específico. Algunas capacidades del sub-agente son agrupar información y configurar los parámetros de los objetos administrados, responder a los requerimientos de los administradores, y generar alarmas.
- Estación de Administración: También llamado administrador, es la componente final de la arquitectura SNMP. Éste funciona como el equivalente del cliente en la arquitectura cliente-servidor. Además, emite requerimientos para las operaciones de administración en nombre de un administrador o aplicación y recibe información de los agentes.

### 3.4.2. MIB para el Protocolo SIP

El protocolo SIP incluye MIB para su administración lo que permite, por tanto, que el Core IMS pueda ser administrado con este método. MIB provee algunos objetos administrados para las entidades SIP Agentes de Usuario y Servidores Proxy, de Redirección y Registro. Así, se pueden monitorear el estado y estadísticas del protocolo además de configurar las entidades SIP.

La estructura del SIP MIB define cuatro módulos MIB:

- SIP-COMMON-MIB, que contiene objetos MIB comunes usados en todas las entidades SIP. Éstos incluyen el tipo de protocolo SIP, tipo de entidad, el estado operacional y administrativo, máximo número de transacciones que una entidad puede administrar, configuraciones de Timer, tablas de resumen de estadísticas, tablas de respuestas SIP y número de transacciones entre otros. Además, el SIP-COMMON-MIB contiene notificaciones para indicar si códigos de estado han sido enviados o recibidos por el sistema.
- SIP-SERVER-MIB, que contiene objetos específicos a los servidores Proxy, de Redirección y Registro. Algunos de estos son objetos de configuración común a los servidores como los modos de operación proxy, métodos de autentificación proxy, tablas de estadísticas aplicables a los servidores SIP Proxy, Registradores y tabla estadística con el número de requerimientos REGISTER que han sido aceptados o rechazados.
- SIP-UA-MIB, que contiene objetos específicos para los Agentes de Usuario. Este grupo especifica los objetos de configuración de servidores SIP aplicables a los Agentes de Usuario incluyendo la dirección IP del servidor SIP utilizado para el registro, proxy o redirección de llamadas.
- SIP-TC-MIB, que define las convenciones textuales usadas entre los módulos MIB.

## 3.5. WiMAX

En esta sección se pretende analizar las principales características de WiMAX como tecnología de acceso y sus ventajas sobre otras tecnologías ya existentes o emergentes. Como se explicó anteriormente, el estándar 802.16 ha evolucionado desde un sistema limitado en movilidad y con línea de vista a un estándar mucho más flexible con sus últimas versiones hasta a proveer conectividad móvil con su versión 802.16e o WiMAX Móvil.

WiMAX (Worldwide Interoperability for Microwave Access) consiste en un consorcio industrial que promueve el uso del estándar aéreo de la IEEE 802.16 y que se encarga del desarrollo de esta tecnología en interoperabilidad, aplicaciones y características. Como un estándar WMAN (Wireless Metropolitan Area Network), WiMAX juega un gran rol para los operadores de redes a gran escala debido a su buen potencial en operación tanto en cobertura geográfica como en velocidad de transmisión y a un bajo costo de implementación lo que lo posiciona como alternativa a líneas DSL o Cable. Existen dos versiones de WiMAX que pueden proveer soluciones optimizadas para acceso de banda ancha inalámbrico para acceso fijo, nómada, portátil y móvil:

- WiMAX 802.16-2004: Utiliza OFDM (Orthogonal Frequency Division Multiplexing) y soporta acceso fijo y nómada tanto en ambientes LOS como NLOS.
- WiMAX 802.16e: Optimizado para canales de radio dinámicos móviles, provee soporte para roaming y handoffs, utiliza SOFDMA (Scalable Orthogonal Frequency Division Multiplexing Access). Con esta técnica también se puede entregar un servicio fijo.

### 3.5.1. Principales Características de la Arquitectura de WiMAX

En la Figura 67 se muestra un diagrama de la arquitectura 802.16.

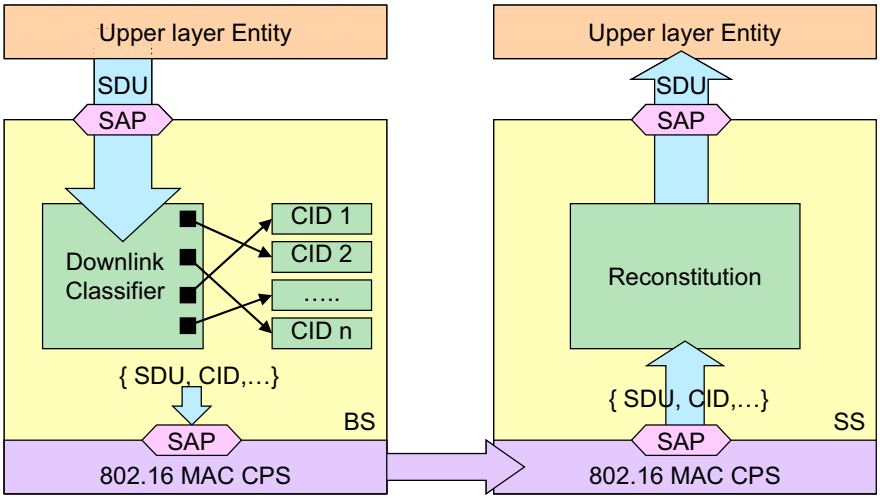



**Figura 67: Diagrama de la Arquitectura 802.16.**

El plano superior puede estar implementado ya sea como un bridge, router o un host. Cuando la Unidad de Servicio de Datos (SDU: Service Data Unit) llega a una sub-capa de Convergencia, el Clasificador de esta capa clasifica el tipo de tráfico y lo mapea a una Identidad de Conexión (CID: Connection ID) en particular y donde cada CID refiere a un profile específico. Cada profile describe varias características como el esquema de modulación o FEC (Forward Error Correction) entre

otros. De esta forma, luego de que se definen los CID entre la estación base (BS: Base Station) y la estación suscriptora (SS: Subscriber Station), el header de información de carga es suprimido.

Dentro de la arquitectura WiMAX existen dos capas que determinan en gran parte sus características, estas capas son la capa física (PHY) y la capa MAC (Media Access Control)

### 3.5.1.1.Capa Física (PHY)

El estándar 802.16 trabaja en variadas bandas de frecuencia. Estas se pueden dividir en dos grupos principales: bandas licenciadas, entre los 10 y 66 GHz; y bandas de uso libre, entre 2 y 11 GHz. Durante el desarrollo de esta tecnología, se fueron implementando distintos tipos de interfaces aéreas, donde las principales se resumen en la Tabla 14.

**Tabla 14: Resumen de Interfaces Aéreas de 802.16.**

| Designación | Aplicabilidad | Duplexación |
|---|---|---|
| Wireless MAN-SC | 10-66Ghz Licenciado<br>2-11Ghz Licenciado | TDD, FDD, HFDD<br>TDD, FDD |
| Wireless MAN-OFDM | 2-11Ghz Licenciado<br>2-11Ghz Exento de licencia | TDD, FDD<br>TDD |
| Wireless MAN-OFDMA | 2-11Ghz Licenciado<br>2-11Ghz Exento de licencia | TDD, FDD<br>TDD |

#### 3.5.1.1.1. Multiplexación

WiMAX 802.16-2004 utiliza multiplexación OFDM, lo que le permite contar con 256 canales. La técnica OFDM es un sistema digital de codificación y modulación basada en la técnica FDM o multiplexación en frecuencia donde una estación transmisora puede enviar datos a través de distintos canales en frecuencias ortogonales, es decir, frecuencias independientes bastante cercanas unas de otras por lo que los canales deben ser de banda estrecha y, aún así, los canales se traslapan.

Dentro de los principales errores que afectan a una señal aérea se encuentran la interferencia inter-símbolos y el desvanecimiento de la señal producido por trayectorias múltiples. Para evitar esto, se debe esperar un tiempo determinado entre el envío de un símbolo y otro. Este intervalo de tiempo se llama intervalo de guardia y hace ineficiente el uso del espectro. Para optimizar este efecto, OFDM divide la transmisión en sub-portadoras con el mismo tiempo de guardia, de forma que el tiempo de transmisión de los símbolos se multiplica por el número total de sub-portadoras.

Como las señales pueden presentar desvanecimientos en ciertas frecuencias, en OFDM sólo algunas sub-portadoras se ven afectadas, sin embargo, los códigos de información de errores proveen información redundante que permite a los receptores recuperar la información de estas sub-portadoras, logrando finalmente que la técnica OFDM sea más robusta al desvanecimiento.

Por otra parte, las sub-portadoras pueden modularse individualmente mediante técnicas como BPSK, QPSK, 16-QAM o 64-QAM. Luego de la modulación, los datos de todas las sub-portadoras se traspasan a una única cadena de símbolos mediante una transformada de Fourier inversa rápida (IFFT), para en el receptor aplicar una FTT que permite demodular cada sub-portadora independientemente.

Dado que las sub-portadoras son ortogonales, éstas pueden traslaparse. Pero para esto, cuando la potencia de una de las sub-portadoras esté en su máximo, la potencia del resto de las sub-portadoras debe ser nula, como se muestra en la Figura 68.

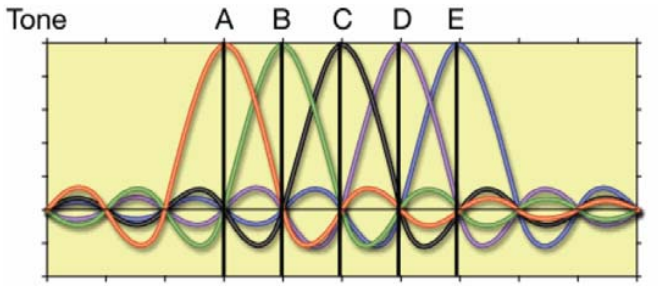



**Figura 68: Ortogonalidad en OFDM.**

En cuanto a la versión 802.16e, ésta utiliza una modificación de OFDM conocida como OFDMA. OFDMA (Orthogonal Frequency Division Multiple Access) es un esquema de múltiple-acceso/multiplexación que provee operaciones de multiplexación de los flujos de datos desde múltiples usuarios a los sub-canales downlink y acceso múltiple uplink mediante los sub-canales uplink. Así, a cada usuario se le asigna una o más sub-portadoras de forma que comportan un determinado ancho de banda. En la Figura 69 se observa la diferenciación entre OFDM y OFDMA.

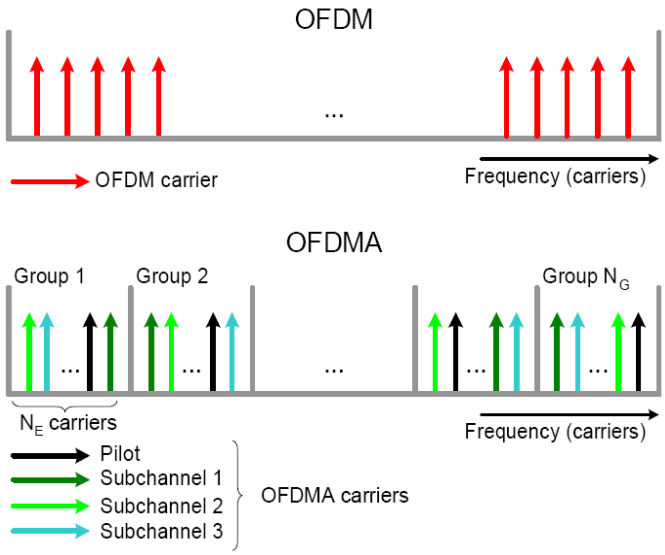



**Figura 69: OFDM y OFDMA.**

En OFDMA, la subcanalización define sub-canales que pueden asignarse a diferentes suscriptores dependiendo de las condiciones del canal y sus requerimientos de datos, de forma de permitir un uso más eficiente de los recursos.

802.16e está basado en la enmienda SOFDMA (Scalable OFDMA), la cual escala el tamaño de la Transformada Rápida de Fourier (FFT) al ancho de banda del canal de forma de mantener el espaciado entre carriers constante en canales con distinto ancho de banda. De esta forma, el espaciado constante permite una mayor eficiencia espectral en canales anchos y reducción de costos en canales angostos.

### 3.5.1.2.Capa de Control de Acceso al Medio (MAC)

La capa MAC se encarga de administrar eficientemente los recursos de la interfaz aérea. Soporta servicios de banda ancha Punto-a-Multipunto (PMP) y Mesh, además soporta QoS y seguridad, entre otros. Como la capa MAC debe soportar diversas tecnologías en el backhaul, en la parte superior de ésta existe una sub-capa de Convergencia. Además cuenta con una capa de seguridad, que permite la autentificación, acceso a la red o encriptación de datos.

#### 3.5.1.2.1. Soporte de QoS

Tanto 802.16-2004 como 802.16e implementan QoS en la capa MAC. Los parámetros de QoS son negociados durante el establecimiento de sesión entre la BS y SS. El tipo de QoS se provee a través de flujos de servicios que corresponden a flujos unidireccionales de paquetes con un conjunto de parámetros particulares de QoS. Los parámetros del flujo de servicio pueden ser administrados dinámicamente a través de mensajes MAC para acomodarse a una demanda dinámica de servicios. En la Tabla 15 se observan los tipos de aplicaciones y QoS de WiMAX móvil.

**Tabla 15: Aplicaciones y QoS para WiMAX.**

| Categoría de QoS | Aplicaciones | Especificaciones de QoS |
|---|---|---|
| UGS<br>Unsolicited Grant Service | VoIP | ➢ Máxima velocidad sostenida<br>➢ Máxima tolerancia a la latencia<br>➢ Tolerancia al Jitter |
| rtPS<br>Real-Time Polling Service | Streming de audio o video | ➢ Mínima velocidad reservada<br>➢ Máxima velocidad sostenida<br>➢ Máxima tolerancia a la latencia<br>➢ Prioridad de Tráfico |
| ErtPS<br>Extended Real-Time Polling Service | Voz con detección de actividad (VoIP) | ➢ Mínima velocidad reservada<br>➢ Máxima velocidad sostenida<br>➢ Máxima tolerancia a la latencia<br>➢ Tolerancia al Jitter<br>➢ Prioridad de Tráfico |
| nrtPS<br>Non-Real-Time Polling Service | File Transfer Protocol (FTP) | ➢ Mínima velocidad reservada<br>➢ Máxima velocidad sostenida<br>➢ Prioridad de Tráfico |
| BE<br>Best Effort Service | Transferencia de datos, navegación en la Web, etc. | ➢ Máxima velocidad sostenida<br>➢ Prioridad de Tráfico |

#### 3.5.1.2.2. Seguridad

WiMAX móvil soporta varias características de seguridad, entre ellas el soporte de autentificación mutua de dispositivo/usuario, protocolo de administración flexible de claves y una fuerte encriptación de tráfico. Los aspectos de uso de las características de seguridad son:

- Protocolo de Administración de Clave: La base de la seguridad en WiMAX Móvil es el protocolo PKMv2 (Privacy and Key Management Protocol Version 2). Se basan en este protocolo la autentificación, control de encriptación de tráfico, intercambio de clave en el handoff y mensajes de seguridad Multicast/Broadcast.
- Autentificación Dispositivo/Usuario: WiMAX Móvil soporta la autentificación de dispositivo y usuario con el protocolo EAP de la IETF, el que provee soporte para

credenciales basadas en SIP, USIM, Certificado Digital, basado en Nombre de Usuario o Password.

- Encriptación de Tráfico: Se utiliza cifrado AES-CCM para proteger los datos de usuario sobre la interfaz MAC de WiMAX Móvil. Las claves usadas para el cifrado se generan por la autentificación EAP. La máquina de estado de encriptación de tráfico posee un mecanismo de refresco de clave periódico (TEK) para mayor protección.
- Protección de mensajes de Control: El control de datos se protege usando AES o MD5.
- Soporte de Handoff Rápido: WiMAX Móvil soporta un esquema de Handshake de 3 vías para la re-autentificación de forma de soportar handoffs rápidos. Este mecanismo además es útil para prevenir ataques del tipo man-in-the-middle. El término Handshake (o "Apretón de Manos") es referido en telecomunicaciones a una comunicación en que ambas partes involucradas requieren de manifestaciones de disponibilidad y/o autenticidad de su compañero.

Existen varias otras características de WiMAX dignas de ser mencionadas, en la sección 9.5 de Anexos se mencionan las principales de ellas.

### 3.5.2. Comparativa de WiMAX con algunas Tecnologías 3G

Además de WiMAX existen variadas tecnologías que prometen conectividad inalámbrica de banda ancha. Entre estas tecnologías se encuentran UMTS y EVDO, estas técnicas se basan en la multiplexación CDMA. UMTS se basa en la variante WCDMA y EVDO en CDMA2000.

En pocas palabras, cada tecnología se puede describir de la siguiente forma:

- 1xEVDO (Evolution Data-Optimized), corresponde a una evolución de CDMA2000 desarrollado por la 3GPP2. 1xEVDO ofrece velocidades de transmisión máximas de 2.4 Mbps (Rev 0) y 3.1 Mbps (Rev A) en el enlace downlink (DL) y 153.6 kbps (Rev 0) y 1.8 Mbps (Rev A) en el enlace uplink (UL) en un canal de 1.25 MHz. EVDO-Rev B agrega mejoras a la capacidad DL, esperándose que se incremente a 4.9 Mbps en un canal de 1.25 MHz.
- UMTS HSDPA (High-Speed Downlink Packet Access), provee mejoras en el enlace downlink a WCDMA R'99 y fue definido por la 3GPP. Esta mejora ofrece velocidades de transmisión máximas de hasta 14 Mbps en un canal de 5 MHz, y con la nueva mejora HSUPA (High-Speed Uplink Packet Access), también provee mejoras en la capacidad del enlace UL. Las tecnologías combinadas de HSDPA y HSUPA se nombran HSPA.

En la Tabla 16 se muestra un resumen de las principales características técnicas de estas tecnologías y WiMAX Móvil.

**Tabla 16: Resumen Comparativo de algunas Características de 1xEVDO, HSPA y WiMAX Móvil.**

| Atributo | | 1xEVDO Rev A | HSPA | WiMAX Móvil |
|---|---|---|---|---|
| Estándar Base | | CDMA 2000/IS-95 | WCDMA | IEEE 802.16e-2005 |
| Duplexación | | FDD | FDD | TDD |
| Downlink | | TDM | CDM-TDM | OFDMA |
| Uplink Multi-Acceso | | CDMA | CDMA | |
| BW del Canal | | 1.25 MHz | 5.0 MHz | Escalable: 5, 7, 8.75, 10 MHz |
| Tamaño del Frame | DL | 1.67 ms | 2 ms | 5 ms TDD |
| | UL | 6.67 ms | 2, 10 ms | |
| Modulación DL | | QPSK/8PSK/ 16QAM | QPSK/16QAM | QPSK/16QAM/ 64QAM |
| Modulación UL | | BPSK, QPSK/8PSK | BPSK, QPSK | QPSK/16QAM |
| Peak Máximo DL | | 3.1 Mbps | 14 Mbps | 46 Mbps, DL/UL=3[4]<br>32 Mbps, DL/UL=1<br>(BW: 10 MHz) |
| Peak Máximo UL | | 1.8 Mbps | 5.8 Mbps | 7 Mbps, DL/UL=1[5]<br>4 Mbps, DL/UL=3<br>(BW: 10 MHz) |
| Programación | | Programación rápida en el enlace DL | Programación rápida en el enlace DL | Programación rápida en enlaces DL y UL |
| Handoff | | Soft Handoff Virtual | Iniciado por la Red<br>Hard Handoff | Optimizado por la Red<br>Hard Handoff |
| Cobertura Típica de Celda | | 5 – 15 Km | 1 - 5 Km | 1- 3 Km Micro-celda<br><1 Km Pico-celda |

De esta tabla se desprende que existen varias características comunes a las tres tecnologías, entre las que se incluye:

- Adaptive Modulation and Coding (AMC).
- Hybrid ARQ (HARQ).
- Programación Rápida.
- Handoff con ancho de banda eficiente.

En cuanto al desempeño de estas tecnologías, se debe tener en cuenta que EVDO y HSPA operan en un canal de frecuencia de 2 GHz mientras que WiMAX Móvil opera en los 2.5 GHz, lo que claramente pone en una ligera desventaja a WiMAX debido a los efectos de propagación. Por otra parte, al utilizar duplexación FDD, tanto EVDO como HSPA utilizan dos canales de 5 MHz y 1.25 MHz respectivamente mientras que WiMAX Móvil, al tener duplexación TDD, utiliza sólo un canal (de ancho variable, a lo más 10 MHz).

En la Tabla 17 se muestra un ejemplo de desempeño de las tecnologías EVDO, HSPA y WiMAX Móvil en distintos escenarios de implementación. En este caso, WiMAX Móvil está operando en los 10 MHz y EVDO-Rev B posee una implementación multicanal de 5 MHz comparable con la multiplexación TDD de 10 MHz de WiMAX Móvil además de considerar un uso opcional de 66QAM en el enlace DL de EVDO-Rev B. Además, tanto para EVDO como HSPA se

utiliza una única antena transmisora y dos receptoras (1x2, SIMO: Single Input Multiple Output), en cuanto a WiMAX Móvil se utiliza una implementación 2x2 MIMO con un sistema AMS.

**Tabla 17: Comparación de Desempeño de EVDO, HSPA y WiMAX Móvil.**

| Parámetro | | 1x EVDO Rev A | 3x EVDO Rev B | HSPA | WiMAX Móvil |
|---|---|---|---|---|---|
| Duplexación | | FDD | FDD | FDD | TDD |
| Espectro Ocupado (MHz) | | 2.5 | 10 | 10 | 10 |
| BW del Canal (MHz) | DL | 1.25 | 5 | 5 | DL/UL=3 |
| | UL | 1.25 | 5 | 5 | |
| Eficiencia Espectral (bps/Hz) | DL | 0.85 | 0.93 | 0.78 | 1.91 |
| | UL | 0.36 | 0.28 | 0.30 | 0.84 |
| Velocidad de Información de red por Canal/Sector (Mbps) | DL | 1.06 | 4.65 | 3.91 | 14.1 |
| | UL | 0.45 | 1.39 | 1.50 | 2.20 |

Además de estos datos, otros estudios y simulaciones se ha encontrado que la eficiencia espectral de WiMAX puede llegar a alcanzar valores muy cercanos a los 3 bps/Hz por sector.

En cuanto a los costos en los que incurre cada una de estas tecnologías, un parámetro muy común es considerar el costo de red en dólares por MByte o Gbyte bajado desde la red. Estos costos incluyen todos los gastos de operación de la red. Para la tecnología EVDO-Rev A se tiene un costo de 0.02 $ US/Mbyte (o bien, 20 $ US/Gbyte) y para HSPA se tiene un costo de 10.4 $ US/Gbyte. En cuanto a WiMAX se tiene un costo de 12 $ US/Gbyte, esto para un ancho de banda de 5 MHz y una eficiencia espectral de 0.76 bps/Hz por sector, por lo que a mayor eficiencia los costos son inferiores al aquí presentado.

Otra característica importante a considerar es la movilidad de estas tecnologías. WiMAX comenzó pensada como una tecnología inalámbrica fija o nómada. Sin embargo WiMAX Móvil está diseñado para brindar conectividad a velocidades entre 75 y 100 Km/h (con un máximo teórico de 120 Km/h). Por otra parte, las tecnologías HSPA y EVDO están diseñadas para proveer enlaces móviles a altas velocidades, permitiendo moverse a velocidades superiores a los 200 Km/h.

### 3.5.2.1. Ventajas de la Utilización de OFDM(A)

Además de las ventajas técnicas ya mencionadas, existen algunas que están relacionadas netamente con la técnica de multiplexación. A continuación se muestran algunas características diferenciadoras entre la multiplexación OFDM y técnicas derivadas de CDMA:

- Atenuación: Como WiMAX opera en bandas de frecuencia superiores a los 2 GHz y típicamente las tecnologías 3G trabajan en bandas inferiores a ésta, entonces WiMAX pude requerir mayor número de celdas que en las tecnologías 3G.
- Multipath: OFDM(A) se desempeña mucho mejor que CDMA en ambientes multipath ya que sobrelleva mejor la Interferencia Inter Símbolo (ISI), efecto que se produce cuando las señales reflejadas se traslapan con la señal transmitida.
- Desvanecimiento Selectivo de Frecuencias: OFDMA es más resistente al desvanecimiento selectivo de frecuencias ya que su naturaleza ortogonal permite corregir los errores en cada sub-canal.

- Deterioro de Frecuencia y Ruido de Fase: OFDMA es más sensitivo al deterioro de frecuencia y ruido de fase resultante de la Interferencia Inter-Canal (ICI). Aunque esto puede ser mitigado por el uso de bandas de guarda.
- Rechazo al Ruido de Impulso: Como los símbolos OFDM son de más larga duración que los símbolos CDMA, el ruido del impulso causan un menor impacto en la tasa de error. En CDMA, la pérdida de unos pocos símbolos puede llevar a un aumento del BER (Bit Error Rate).
- Adaptive Modulation and Coding (AMC): OFDMA utiliza de mejor forma AMC, logrando obtener tasas de transmisión superiores comparada con otras técnicas CDMA. Además, OFDMA es capaz de mejorar esta ventaja aplicando AMC a nivel de sub-canales.
- Reuso de Frecuencia: CDMA emplea promediación de interferencia, lo que permite mantener un reuso de frecuencia de 1 y OFDMA requiere, típicamente, un reuso de frecuencia de 1:3, lo que quiere decir que la velocidad alcanzable por celda para cierto ancho de banda debe dividirse por 3. El uso de AAS en OFDMA permite sobrellevar esta limitación, a pesar de que la técnica AAS pude ser costosa.
- Limitación de Código: Debido a la limitación de códigos disponible, la mayoría de los clientes HSDPA estará limitado a 5 códigos del máximo de 15. Aún más, como cada usuario necesitará por lo menos un código para voz o datos, esto puede tener un impacto significativo en el número de usuarios soportado por cada sistema, sobre todo comparado por el número de usuarios soportado por OFDMA.
- QoS: WiMAX posee una capa MAC orientada a transmisión de datos, al contrario de las tecnologías basadas en CDMA, que están orientadas a la conmutación de circuitos. Además, WiMAX cuenta con múltiples modos de duplexación, que pueden permitir que el ancho de banda de los enlaces UL y DL pueda asignarse dinámicamente dependiendo de las condiciones de tráfico.

# Capítulo 4
# Resultados

## 4.1. Convergencia de Telefonía Fija – Móvil

A continuación se analizan los principales motivos para adoptar IMS y los factores a considerar tanto de parte de operadores como de clientes que favorecen o retrasan su adopción.

### 4.1.1. Redes Convergentes versus Redes Superpuestas

La convergencia de redes se trata de ofrecer nuevos servicios a los clientes más que nuevas tecnologías. Para esto, el operador puede utilizar una red convergente o bien, implementar múltiples servicios de múltiples redes. Entonces, ¿Por qué decidirse por redes convergentes y no redes superpuestas? En la Tabla 18 se ilustran los principales motivos por los que una red convergente se prefiere a una superpuesta.

**Tabla 18: Comparación entre Redes Convergentes y Superpuestas.**

| Red Convergente | Red Superpuesta |
|---|---|
| Simplifica la arquitectura de red. | Dimensionado según el despliegue. |
| Comparte equipos comunes para minimizar el CAPEX. | Menor dependencia de un suministrador. |
| Reduce el OPEX (menos elementos de red, espacio, piezas de repuesto, gestión y aprendizaje). | Optimizada según los requisitos de los servicios. |
| Reutiliza estadísticamente los recursos. | Despliegue más rápido. |
| Bajo costo para cambiar servicios e introducir nuevos. | Probado despliegue a gran escala. |

Se tiene que, aunque las redes superpuestas están técnicamente más desarrolladas y existe más conocimiento del funcionamiento de éstas, las redes convergentes reducen los gastos operativos (OPEX) e inversiones (CAPEX) además de ser más flexibles y más eficientes.

## 4.1.2. Potenciadores e Inhibidores de FMC

Del desarrollo actual de las arquitecturas de telefonía y de las tecnologías de acceso se puede observar una serie de condicionantes que favorecen o limitan el desarrollo de la FMC. Estos aspectos pueden dividirse en tres grandes grupos: de la industria, de los consumidores y de las empresas.

### 4.1.2.1.Aspectos del Desarrollo para la Industria

A continuación se resumen tanto los potenciadores como inhibidores para el desarrollo de la FMC desde el punto de vista de la Industria.

#### 4.1.2.1.1. Potenciadores de la Industria

- Redes de Próxima Generación (NGN): La evolución de las redes fijas y móviles ha migrado desde redes verticales y poco flexibles a redes NGN (horizontales, con arquitectura de capas y conmutación de paquetes) que se caracterizan por ser menos costosas, con más funcionalidades, mayor relación precio/desempeño y múltiples interfaces convergentes.
- Terminales Convergentes: Los teléfonos móviles están desarrollándose como dispositivos convergentes con múltiples servicios además de voz. Una característica importante de los terminales es que puedan acceder a más de una tecnología de acceso además de la celular, como por ejemplo bluetooth, Wi-Fi o WiMAX. Sin embargo, la duración de la batería necesita mejorarse.
- Crecimiento de Redes Inalámbricas: Una de las tecnologías inalámbricas más populares actualmente es Wi-Fi (con diferentes niveles de ancho de banda, alcance y seguridad) que permite la implementación de hotspots. Además, WiMAX permite el desarrollo de redes WMAN y las redes Mesh permiten una implementación fácil y rápida de redes junto con la unión de zonas Wi-Fi.

#### 4.1.2.1.2. Inhibidores de la Industria

- Disponibilidad Limitada: Actualmente existen algunos terminales convergentes en el mercado. Su rango es limitado y muchos operadores piensan que debido a los pocos terminales existentes, la habilidad del proveedor de entregar servicios atractivos se ve retrasada. Los recientes terminales lanzados y los próximos a salir cambiarán esta percepción.
- La telefonía fija y móvil son negocios separados para los operadores más integrados: Los cambios más grandes para FMC serán organizacionales y políticos más que tecnológicos.

### 4.1.2.2.Aspectos del Desarrollo para los Consumidores

A continuación se resumen tanto los potenciadores como inhibidores para el desarrollo de la FMC desde el punto de vista de los Consumidores.

#### 4.1.2.2.1. Potenciadores para los Consumidores

Los consumidores de servicios de telecomunicaciones son cada vez más exigentes, éstos desean servicios a precios razonables, simples para usar y que simplifiquen o mejoren sus vidas. De esta forma, los clientes valorarán, entre otras, las siguientes características:

- Buena cobertura de telefonía móvil indoor.
- Bajos precios y más simplicidad en los precios de planes.
- Innovadores servicios y terminales.
- Servicios auto-instalables, plug-and-play, de uso intuitivo.
- Fácil de usar y servicios de roaming con el mismo número, un buzón de voz y un terminal.

En mercados emergentes con economías de rápido crecimiento, los usuarios tienen más recursos para invertir además del servicio básico de voz.

#### 4.1.2.2.2. Inhibidores para los Consumidores

Dentro de las razones por las que los consumidores no quieran suscribir los servicios FMC se encuentran:

- No querer atarse a un sólo proveedor.
- Falta de percepción de valor en el servicio.
- Falta de terminales atractivos en comparación con actuales de uso único.
- Complejidad de los servicios ofrecidos.
- Complejidad en la implementación técnica de los servicios.

### 4.1.2.3.Aspectos del Desarrollo para la Empresa

Finalmente, se resumen los potenciadores e inhibidores para el desarrollo de la FMC desde el punto de vista de la Empresa.

#### 4.1.2.3.1. Potenciadores para las Empresas

Las empresas tienen muchos potenciadores en común con los consumidores pero están menos orientados a la calidad y se basan más en el precio. Dentro de sus potenciadores se encuentran una mejor cobertura indoor, menores cargos por roaming, simplicidad en las comunicaciones internas y externas y utilización de menos tipos de terminales para diferentes servicios.

Todas las empresas de telecomunicaciones en un mercado maduro necesitan incrementar sus retornos promedio por usuario y retener a sus clientes. Los aspectos potenciadores de las empresas pueden dividirse en tres grupos:

- Operadores móviles: FMC les permite compartir el tráfico fijo residencial y líneas alquiladas, mejorar la calidad de llamadas móviles y diferenciarse de los otros operadores móviles. FMC también puede ayudar a evitar la saturación del enrutamiento de tráfico fuera de la red.

- Operadores Integrados (Fijo-Móvil): FMC les permite lanzar paquetes o "bundles" de servicios y mejorar la calidad de servicio de sus llamadas. Además, pueden utilizar sus instalaciones celulares para disminuir la competencia de los operadores puramente móviles.
- Operadores Fijos: FMC les permite ofrecer servicios de valor agregado que atraigan a los clientes y pueden utilizar su infraestructura en packs de cuatro servicios.

#### 4.1.2.3.2. Inhibidores para las Empresas

Dentro de los aspectos inhibidores de FMC para las empresas se encuentran:

- Incertidumbre en soluciones seguras.
- Elección limitada de terminales atractivos.
- FMC no es de tan bajo costo como la telefonía IP que ya ha sido implementada puesto que esta última no es de carácter integrados de arquitecturas y tan sólo comprende un único servicio (la telefonía) dentro de la amplia gama de servicios que contempla FMC.

## 4.2. IMS como "paraguas" de la Convergencia de Redes

Como se abordó durante el desarrollo de esta memoria, IMS establece una arquitectura de red que permite unificar las diferentes redes existentes para que dos usuarios puedan comunicarse estando en cualquier parte y desde cualquier red de acceso o para que un usuario pueda acceder a sus servicios contratados en su red Home desde cualquier red. En la Figura 70 se muestra un diagrama de resumen de la arquitectura IMS.

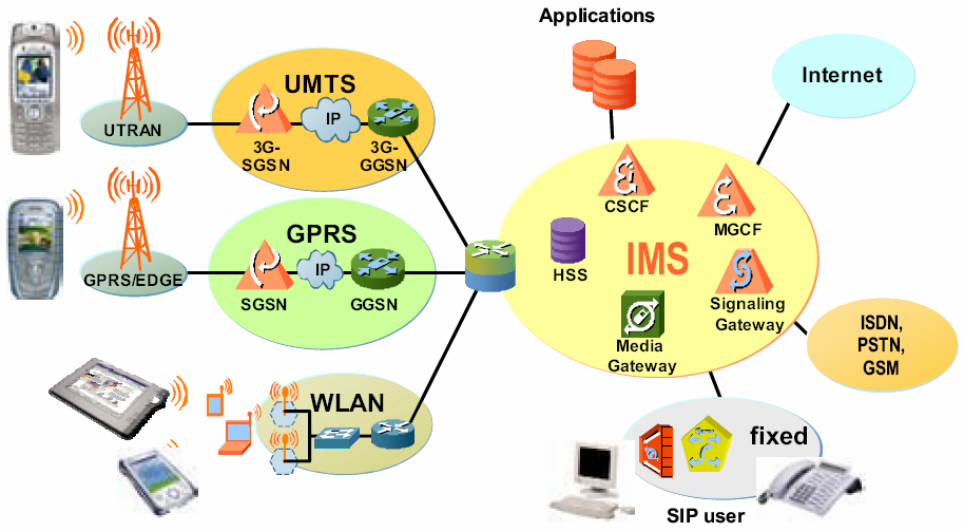



**Figura 70: Diagrama de Resumen de la Arquitectura IMS.**

En esta sección se resumen las principales redes de acceso estudiadas, junto con generalidades de procedimientos de acceso de interés y algunos factores de importancia que se deben considerar para decidir a implementar nuevas arquitecturas como IMS.

IMS tiene la ventaja de estar definida con estándares abiertos y es una de las arquitecturas más desarrolladas como candidata para proveer la convergencia de redes. Está bien definida para brindar

múltiples servicios de voz y multimedia a través de UMTS y GPRS. Sin embargo, en su última versión incluye acceso a través de redes WLAN y, aunque aún no está completamente definido, promete proveer servicios multimedia con calidad de servicio a través de este medio.

### 4.2.1. Redes de Acceso a IMS

A continuación se resumen las principales redes de acceso para acceder a IMS.

#### 4.2.1.1. Redes Celulares

En un principio IMS fue diseñado para acceder a través de redes UMTS (red de acceso UTRAN) o GPRS (red de acceso GERAN), el acceso a la red IMS se realiza a través de las entidades SGSN, que se encarga de requerir el acceso al punto de acceso a la red IMS (el Proxy-CSCF) y el GGSN, que se encarga de encontrar el Proxy-CSCF. Luego, los terminales pueden acceder a IMS. En la Figura 71 se muestra un diagrama básico del acceso a IMS mediante redes celulares.

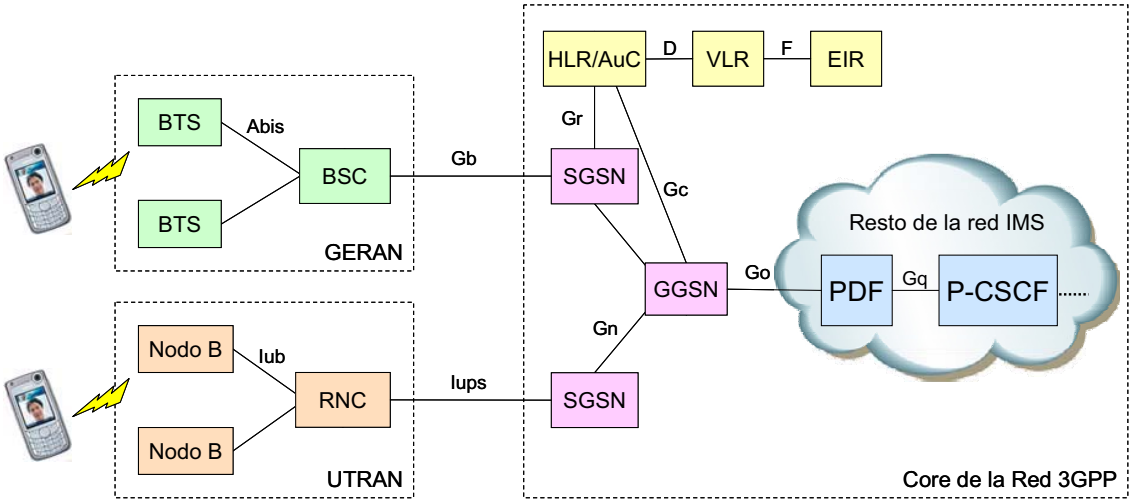



**Figura 71: Acceso a IMS a través de Redes Celulares.**

#### 4.2.1.2. Redes PSTN

La red IMS permite la comunicación hacia y desde usuarios de la PSTN. En la Figura 72 se muestran las entidades necesarias para la interacción entre un acceso PSTN y la red IMS. Cuando se inicia el proceso de comunicación, el switch PSTN se encarga de reservar un circuito de voz entre éste y el IMS-MGW (encargado de convertir el flujo TDM de la red PSTN a IP y viceversa) y envía un mensaje de señalización IAM al T-SGW (que realiza el traspaso de la señalización desde transporte TDM a IP y viceversa), luego, el T-SGW envía el mensaje de señalización al MGCF sobre transporte IP (que controla al IMS-MGW). El MGCF crea una asociación en el IMS-MGW para vincular una terminación TDM (de parte del circuito de voz) con una RTP (de parte del enlace de voz IMS). Luego, el MGCF crea una invitación SIP al destino, la que se envía a través del S-CSCF.

En este ejemplo, el acceso a IMS se hace directamente a la red Home del usuario de destino, por lo que sólo se necesita un BGCF. Si el usuario de destino se encontrara en otra red, entonces se necesitaría acceder al BGCF de esa red y luego al S-CSCF.

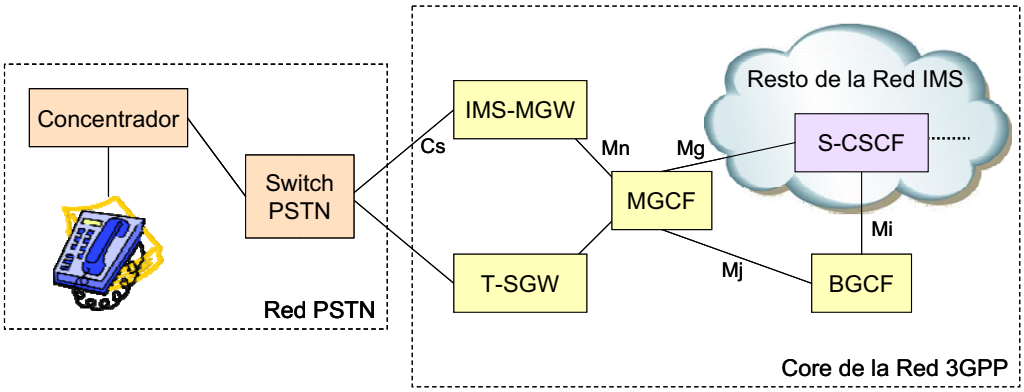



**Figura 72: Acceso a IMS a través de una red PSTN.**

### 4.2.1.3. Redes Wireless LAN

En las últimas versiones de IMS se estableció la arquitectura general de acceso a redes wireless. En particular, la 3GPP definió ciertos parámetros para la interacción de IMS con Wi-Fi pero no se descarta la inclusión de nuevas tecnologías como WiMAX. En la Figura 73 Se muestra la arquitectura general para acceder a IMS a través de una WLAN.

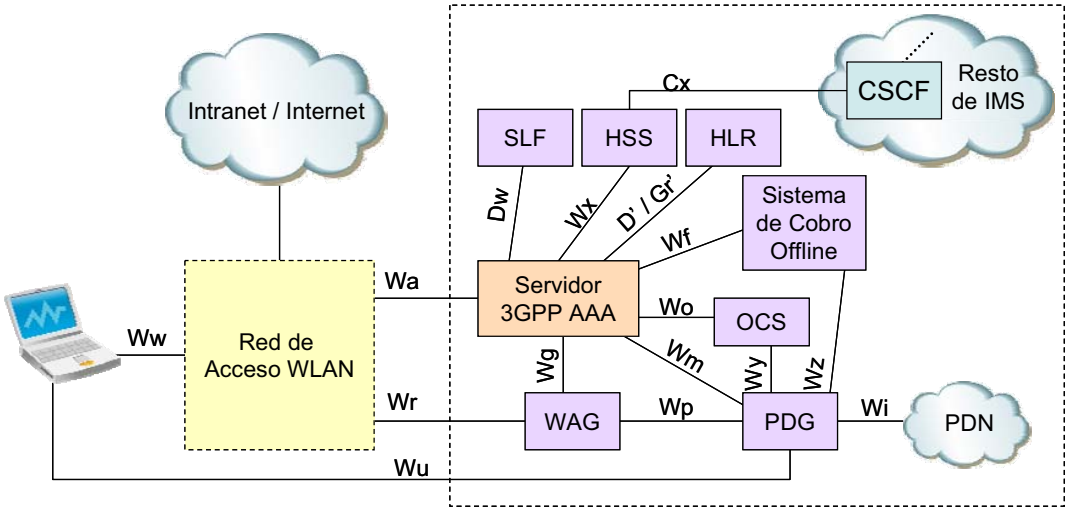



**Figura 73: Acceso a IMS a través de una red WLAN.**

El terminal accede a un servidor de Autentificación, Autorización y Accounting a través de la red WLAN para solicitar acceso a la red IMS. Este servidor consulta al SLF (en caso de que exista más de un HSS) a cuál HSS dirigirse para el usuario en particular que solicita acceso. Luego de que se autentifica y autoriza al cliente, éste puede acceder a los servicios del IMS y se utilizan los bloques de cobros para registrar los cargos que se le asignarán al usuario.

Este tipo de acceso puede extenderse a todo tipo de acceso IP, como por ejemplo redes xDSL, HFC o fibra óptica siempre y cuando exista un identificador en el terminal o equipo móvil que permita la autentificación, como por ejemplo una identidad USIM o NAI.

### 4.2.1.4. Redes de Acceso Genérico (GAN)

La 3GPP define una red de acceso genérico a IMS, esta red de basa en el uso de terminales duales (es decir, acceso a una red de celular como UMTS y a una red IP inalámbrica como Wi-Fi, Bluetooth o WiMAX, entre otras). Este terminal está predeterminado para preferir una de las redes de acceso a las que puede optar y, en caso en que no pueda acceder a esta red, entonces se decide por la otra. Las redes GAN también son conocidas como UMA y en la Figura 74 se muestra un diagrama básico de ésta.

El controlador GANC permite el acceso y seguridad al Core de la red, dependiendo del tipo de acceso utilizado (si es celular o IP), el procedimiento seguido corresponde al de redes celulares (sección 4.2.1.1) o al de redes WLAN (sección 4.2.1.3).

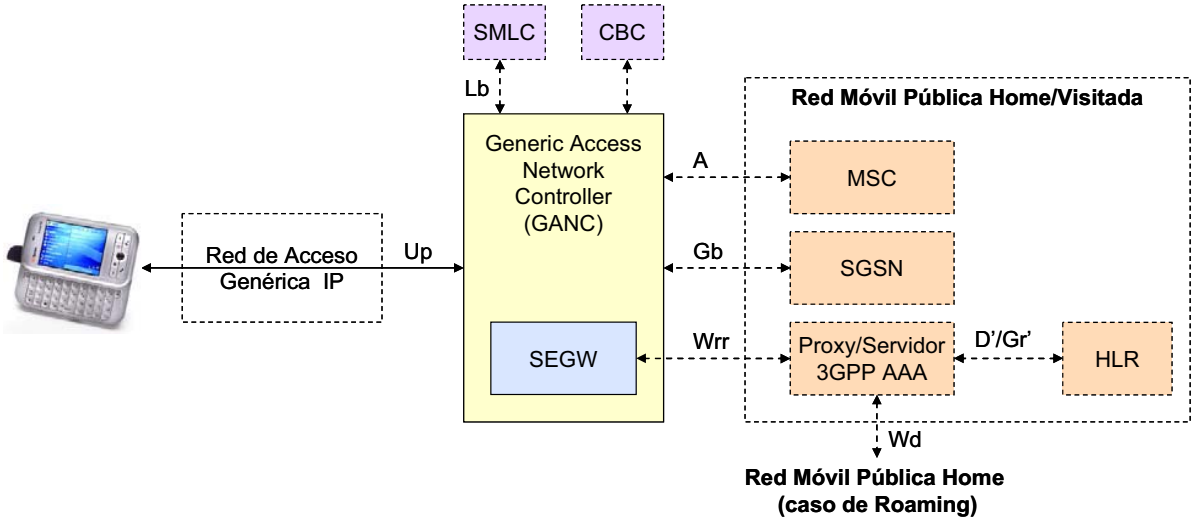



**Figura 74: Acceso a IMS a través de una red GAN.**

## 4.2.2. Algunos Procedimientos de Interacción entre redes

A continuación se pretende resumir y explicar brevemente ciertos procedimientos de interacción entre redes e IMS que son de interés.

### 4.2.2.1. Descubrimiento del P-CSCF

Antes de poder iniciar cualquier sesión, el terminal de usuario debe acceder al Core de la red IMS encontrando un punto de entrada a ésta, este punto de entrada es el P-CSCF. Existen dos métodos de descubrimiento del P-CSCF, el primero es a través de una red UMTS o GRPS en que se utilizan las entidades SGSN y GGSN para conseguir una lista de direcciones IP de los P-CSCF, el segundo está definido a través de una red de conectividad IP genérica, como se muestra en la Figura 75.

Primero, el terminal envía una consulta a un Servidor DHCP para obtener una lista de los P-CSCF en la red. El Servidor DHCP puede responder con los nombres o direcciones de los P-CSCFs, si responde con los nombres, el terminal debe realizar una consulta adicional a un servidor DNS para

obtener las direcciones. Finalmente, teniendo la dirección IP, el terminal puede encontrar un P-CSCF con el cual registrarse.

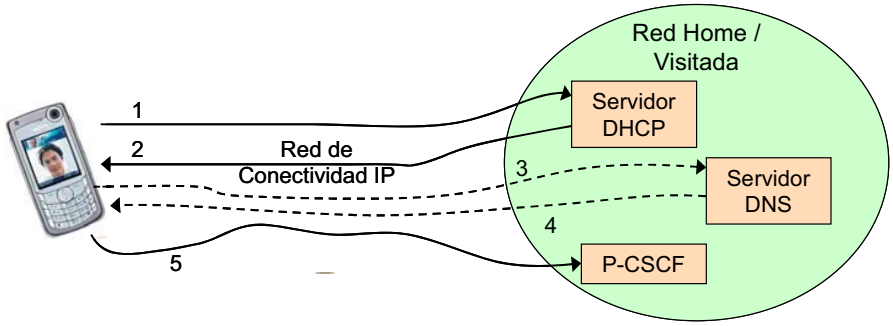



**Figura 75: Descubrimiento del P-CSCF a través de una Red de Conectividad IP.**

### 4.2.2.2. Procedimiento de Registro

Antes de que un usuario pueda iniciar cualquier tipo de sesión con una red IMS, éste debe ser registrado en dicha red. La Figura 76 muestra el proceso de registro para un usuario que se encuentra en caso de Roaming.

A través de la red de acceso, el terminal de usuario inicia un proceso de búsqueda de algún P-CSCF disponible. Luego de encontrarlo, el terminal envía al P-CSCF un requerimiento de registro. El P-CSCF determina que el usuario no es cliente de la red local (red visitada), por lo que reenvía el requerimiento a la red Home de origen del usuario, específicamente a un punto de entrada que el P-CSCF conozca (el I-CSCF). El I-CSCF consulta al HSS sobre cual S-CSCF debe iniciar el registro del usuario y, luego de determinar el S-CSCF, le envía el requerimiento de registro al S-CSCF. El S-CSCF se encarga de realizar el registro de usuario junto con verificar sus permisos y almacenar su ubicación actual. Es importante notar que, en caso de existir más de un HSS, el I-CSCF consulta a la entidad SLF a cual de los HSSs dirigirse.

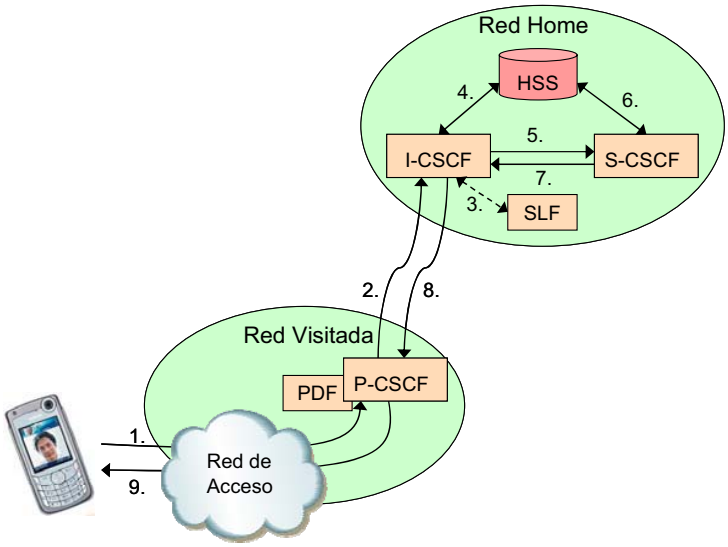



**Figura 76: Procedimiento de Registro al sistema IMS.**

El proceso de registro se repite periódicamente en caso de que las condiciones del terminal (por ejemplo, la localización) hayan cambiado.

### 4.2.2.3. Interacción entre dos redes IMS

En la Figura 77 se muestra un resumen de los procedimientos realizados para que el usuario de la red de origen pueda iniciar una sesión (por ejemplo, de voz) con el usuario en la red de destino.

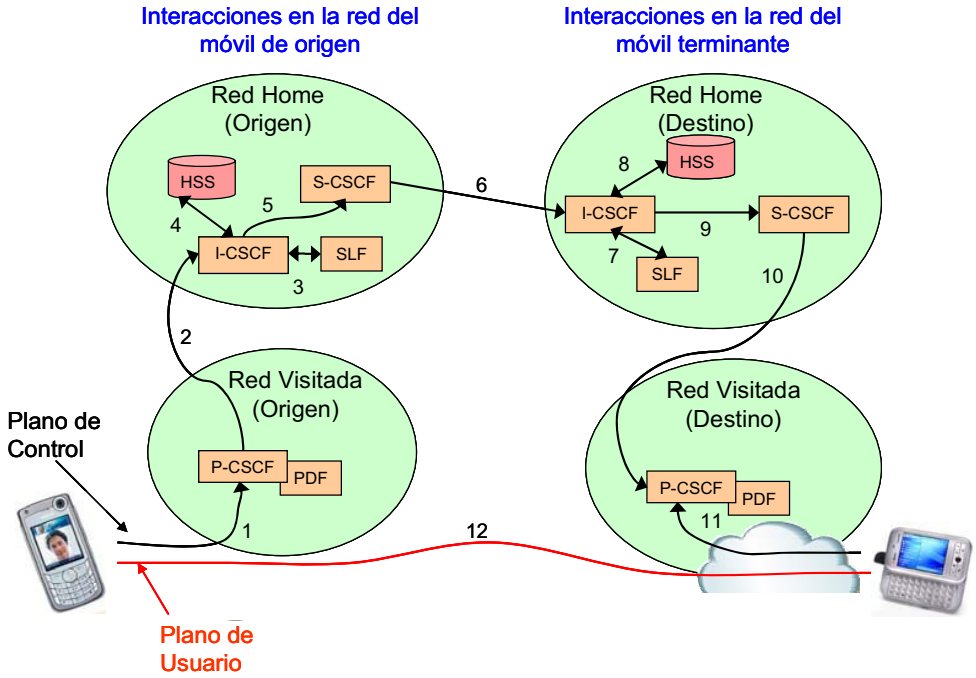



**Figura 77: Resumen de Sesión SIP End-to-End.**

En este caso se tiene que ambos usuarios se encuentran en caso de Roaming, es decir, no se encuentran en su red Home contratada sino que en redes visitadas. El acceso a la red puede ser de tipo celular o una red de acceso WLAN. Los pasos que siguen las entidades en la Figura 77 se encuentran numeradas para un mayor entendimiento del proceso.

En resumen, el usuario de origen accede a una red de acceso y, a través de ésta, está enlazado con un P-CSCF. Cuando el usuario desea establecer una sesión con el usuario de destino, éste envía una invitación al P-CSCF. Como el usuario se encuentra en Roaming, el P-CSCF se encarga de dirigir el requerimiento a un punto conocido de la red Home del usuario de origen (el I-CSCF), el cual se encarga de encontrar al S-CSCF que tratará el requerimiento del usuario de destino mediante un proceso similar al descrito en el procedimiento de registro.

Luego de que el S-CSCF recibe el requerimiento del origen, éste determina que el usuario de destino no es cliente de esta red y dirige la invitación a un punto conocido de la red de destino (el I-CSCF). Con un procedimiento igual al realizado en la red de origen, el I-CSCF de la red de destino determina al S-CSCF que servirá al usuario de destino. Este S-CSCF determina que el usuario de destino no se encuentra en la red Home, sino que en una red visitada determinada y enruta la

invitación al P-CSCF de la red visitada y, por consiguiente, al usuario de destino iniciándose así el intercambio de información.

### 4.2.2.4. Interacción entre IMS y la PSTN

En la Figura 78 se muestra el proceso y entidades necesarias para establecer una sesión iniciada desde una red de acceso celular o IP a una red PSTN para el caso de Roaming. En este caso la comunicación típicamente será de voz.

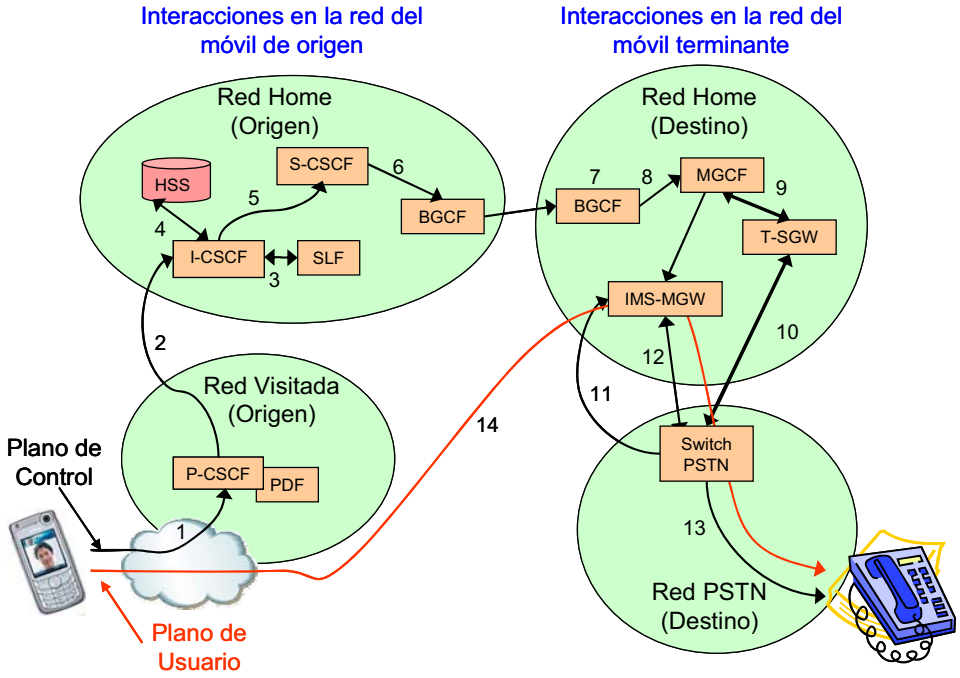



**Figura 78: Resumen de una sesión desde IMS a la PSTN.**

El proceso realizado en el lado de origen para enviar el requerimiento de inicio de sesión al S-CSCF del usuario de origen es el mismo que el descrito en la parte anterior. Sin embargo, cuando el S-CSCF del usuario de origen recibe el requerimiento, éste determina que la identidad de destino pertenece a una red PSTN por lo que deriva el requerimiento a la entidad BGCF, la que se encarga de realizar el corte entre las redes IMS y PSTN. El BGCF determina, en este caso, que el traspaso de la llamada desde IMS a la PSTN no se realiza dentro de la misma red Home de Origen por lo que decide la red en la que debe producirse este traspaso y envía el requerimiento al BGCF de dicha red.

El BGCF de la red de destino selecciona el MGCF que controlará el estado de la sesión. El MGCF realiza la traducción de señalización entre la red IMS y PSTN y la envía al T-SGW, que realiza el cambio de transporte entre dichas redes y envía la señalización al Switch de la PSTN. Este Switch reserva recursos con el IMS-MGW para establecer el mapa del flujo de voz. El T-SGW reenvía el mensaje al MGCF, el que entrega al IMS-MGW la orden para conectar las terminaciones TDM y RTP e iniciar la sesión.

### 4.2.2.5. Interacción entre IMS y una red IPv4

IMS es una arquitectura definida para IPv6. Sin embargo, cuenta con Funciones de Control de Borde que, además de ocultar la topología de la red a redes exteriores, permite que IMS interopere con redes IPv4. En la Figura 79 se muestra un diagrama de esta interacción.

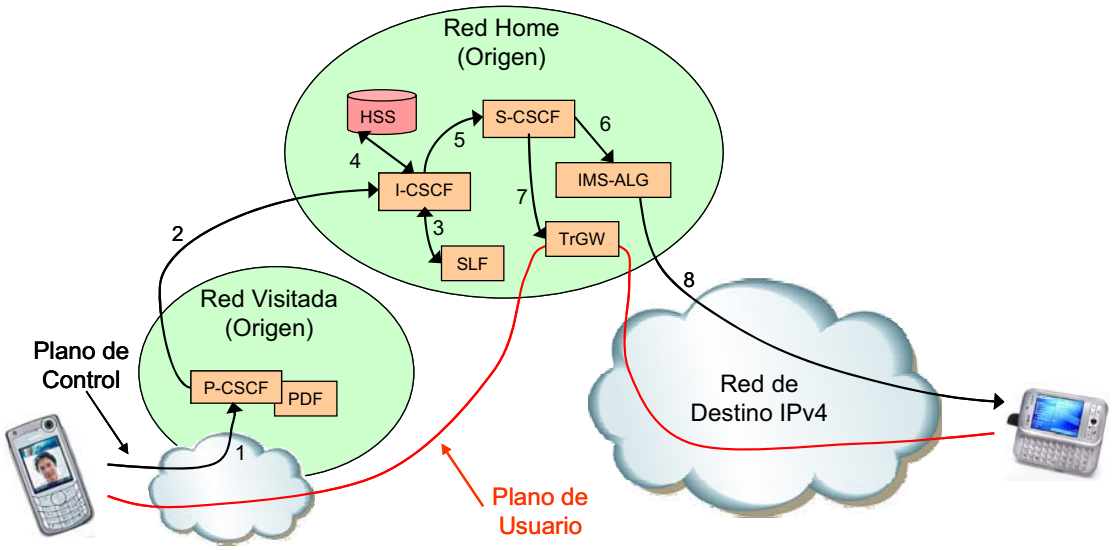



**Figura 79: Interacción entre IMS y una red IPv4.**

En este caso, un usuario desea iniciar una sesión con otro usuario que se encuentra en una red IPv4. El procedimiento para asignarle al usuario un S-CSCF es el mismo que en los casos anteriores, sin embargo, cuando el S-CSCF analiza la dirección del usuario de destino, éste determina mediante una consulta DNS que el dominio de término soporta sólo IPv4. Para poder establecer el mapa de señalización, el S-CSCF debe hacer uso del IMS-ALG y TrGW para adquirir los recursos necesarios como la dirección IPv4 y puertos en nombre del usuario de origen de forma que pueda modificar los paquetes de datos a IPv4 de forma que puedan ser interpretados por la red de destino.

Cuando la red de destino responde al requerimiento, el IMS-ALG y TrGW realizan la traducción inversa para que el tráfico sea interpretado por la red IMS y se establezca el mapa de señalización y de transmisión de media.

## 4.2.3. Factores a Considerar para la Implementación de IMS

Para implementar una red, se debe realizar un análisis para determinar que dicha red cumpla con ciertos requisitos para ser efectiva. A continuación se analizarán algunos factores de IMS que son preponderantes a la hora de decidir implementarlo. Estos factores son:

- Escalabilidad.
- Flexibilidad.
- Disponibilidad.
- Seguridad.
- Calidad de Servicio (QoS).
- Administrabilidad.

- Costo Efectividad.

#### 4.2.3.1.Escalabilidad

Existen varias razones que hacen que IMS sea escalable. Una de ellas es que la arquitectura IMS permite aprovechar las redes ya implementadas para que interactúen entre ellas. Si las redes actualmente implementadas no son suficientes, el operador puede decidir implementar más redes de acceso de variados tipos dependiendo de sus necesidades. Por otra parte, el modelo distribuido de IMS permite que se puedan implementar todas las entidades necesarias para un óptimo funcionamiento de la red:

- En caso en la base de datos HSS llegue a su límite, pueden seguir implementándose más bases de datos sin agregar muchos procedimientos extras. Esto se debe a que existe la entidad SLF, que indica al CSCF a qué HSS dirigirse, por los que sólo se agrega un paso más a los procedimientos de asignación de CSCF.
- Pueden implementarse tantos CSCFs como sea necesario, dada su condición de elemento distribuido en la red. La implementación de múltiples CSCFs optimiza el uso de los recursos y evita retardos y congestión de la red, los que pueden producirse por la existencia de demasiados clientes asignados a pocos CSCFs.

Es importante notar que en el mercado existen alternativas de entidades funcionales de IMS (por ejemplo Softswitches o servidores SIP) de gran capacidad por lo que no es necesario implementar una red engorrosa y difícil de administrar para satisfacer la demanda. Por otro lado, así como existen funciones de gran capacidad, también pueden implementarse entidades de poca capacidad. Esto, principalmente implementando softwares desarrollados como soporte como los creados por Sun en lenguaje Java y que permiten implementar entidades funcionales del tamaño ideal para la red.

#### 4.2.3.2.Flexibilidad

En IMS se pueden considerar dos tipos de flexibilidad de red. El primer tipo ya fue mencionado y tiene que ver con que IMS es agnóstica al acceso, por lo que un usuario debe poder acceder a la arquitectura IMS a través de cualquier red de acceso, incluso redes IPv4. Sin embargo, este tipo de flexibilidad sólo podrá ser apreciada por los usuarios finales si cuentan con terminales capaces de acceder a algunas de estas redes de acceso.

Por otro lado, la flexibilidad de IMS puede observarse en la cantidad de aplicaciones que pueden ser implementadas. Al ser una arquitectura separada en capas, sólo se necesita implementar más módulos en la capa de Aplicación sin necesidad de realizar cambios significativos en el resto de la arquitectura de la red. En palabras simples, la arquitectura de la capa de aplicación responde a un modelo Cliente/Servidor donde el servidor consiste en un contenedor con distintos bloques, lo que, combinados, permiten el desarrollo de distintas aplicaciones. Un ejemplo común de servidores de aplicación son los servidores SIP, siendo las aplicaciones más comunes las de presencia, mensajería instantánea, video streaming, etc. Actualmente, existen varios vendedores de plataformas de Aplicación SIP, entre ellos: IBM, Microsoft, Sun, Lucent y 3Com.

#### 4.2.3.3.Disponibilidad

IMS se puede considerar como una arquitectura robusta y resistente a los accidentes o fallas de la red. La entidad más importante en el funcionamiento de IMS es el CSCF (Proxy, Interrogating o Serving), esta entidad permite establecer, modificar y terminar las sesiones solicitadas por los clientes IMS. Estas entidades pueden implementarse en cantidad suficiente en las redes para sobrellevar la falla de una o más de ellas y el sistema IMS cuenta con procedimientos establecidos para que, en caso en que un CSCF falle, asignar otro disponible al terminal de usuario.

Algunos de los procesos que permiten que IMS se reponga a la pérdida de algún CSCF son:

- Procesos de Descubrimiento del punto de entrada al IMS: Cuando un usuario desea acceder a la red IMS, el terminal solicita los nombres o direcciones de los P-CSCFs existentes e intenta registrarse con alguno de ellos de forma que, si no puede registrarse con alguno de la lista, intenta registrarse con el otro.
- Proceso de Re-registro: Luego de que un usuario ya se registró en la red, éste se registra periódicamente. Esto permite que en caso de que falle el Proxy, Interrogating o Serving CSCF, sea asignado nuevamente otro CSCF disponible durante este proceso.

Por otra parte, IMS también permite implementar entidades redundantes como Servidores de Aplicación, Gateways o HSSs y además permite la existencia de interfaces redundantes.

#### 4.2.3.4.Seguridad

Como se analizó en el capítulo de Metodología, IMS cuenta con variados métodos de seguridad a distinto nivel. Así, IMS permite implementar seguridad cifrando los mensajes de señalización SIP, con procesos de Autentificación y Acuerdos de Clave (AKA), establece dominios de seguridad, Gateways de seguridad y seguridad en el acceso a distintos servicios de IMS.

Por otra parte, IMS cuenta con un conjunto de Funciones de Borde que protege la topología de la red de forma que no sea conocida por otros operadores ni pueda ser vulnerada debido a esta información y provee funcionalidades de Firewall y de NAT.

#### 4.2.3.5.Calidad de Servicio (QoS)

Para acceso a través de UMTS o GPRS, IMS implementa variados tipos de QoS dependiendo del tipo de servicio, profile de usuario, ancho de banda de la red de acceso, etc. El sistema utilizado para proveer QoS y administrar los portadores de tráfico se llama Control SBLP (Service-Based Local Policy Control) y es un sistema que recibe los requerimientos desde el terminal de usuario y, basado en una serie de políticas, el sistema decide asignar una calidad de servicio dada y cierto número de portadores y, finalmente, aplica esta asignación.

Para el caso de acceso a través de redes WLAN, el manejo de QoS se encuentra en desarrollo. La 3GPP plantea el uso de DiffServ para implementar distintos tipos de QoS en estas redes. Sin embargo, el trabajo en esta área aún no está maduro.

### 4.2.3.6.Administrabilidad

IMS implementa administrabilidad MIB heredado principalmente del uso del protocolo SIP entre entidades funcionales, pero también de muchos otros protocolos utilizados como TCP, UDP, DHCP, DNS, RTP, etc.

El uso de MIB en IMS permite llevar un seguimiento del desempeño de las funciones de red, y permite el uso de herramientas como SNMP que es un protocolo que permite la comunicación entre entidades controladoras de la red y las funciones controladas.

### 4.2.3.7.Costo - Efectividad

IMS permite integrar redes que estaban naturalmente separadas. Esto permite reducir costos operacionales que, de otra forma, se incurrirían en cada red por separado. Dentro de estos costos se cuenta mantención de la red, emisión de boletas y gastos en operación. Dado que el primer objetivo de los operadores es aumentar sus beneficios ofreciendo nuevos servicios, la convergencia de redes a través de IMS permite combinar servicios existentes para generar nuevos servicios. Como IMS unifica la capa de servicio, estos pueden ser expandidos a bajo costo mediante el aumento de las aplicaciones y generar más ingresos por la implementación de nuevos servicios.

Por otra parte, se debe considerar que no es difícil comenzar a implementar la arquitectura IMS en una red ya existente, por lo que no habría que incurrir en nuevos costos tales como climatización, uso de espacio o se incurriría en un aumento de los costos poco significativos por ejemplo en el uso de energía, ya que dada la naturaleza IP de las entidades funcionales, su gasto energético es reducido.

Además, dada la independencia al acceso con que cuenta IMS, ésta permite a los operadores llegar al usuario final a través de redes de acceso de bajo costo, como por ejemplo redes de acceso inalámbricas que utilizan parte del espectro no licenciado. Y por este mismo motivo, IMS permite que no sea necesario realizar cambios en las capas más bajas de la red, específicamente la de acceso, la que representa entre un 30 y 50% del costo total de una red.

## 4.3. Utilización de WiMAX como Tecnología de Acceso

En esta sección se pretende resumir las principales características de WiMAX y sus ventajas sobre otras tecnologías de acceso.

### 4.3.1. Arquitectura de Interoperación de WiMAX con IMS

Como se estudió anteriormente, la 3GPP permite la utilización de redes inalámbricas como tecnología de acceso al Core de la red IMS. En la Figura 80 se muestra la arquitectura de interoperación entre WiMAX e IMS.

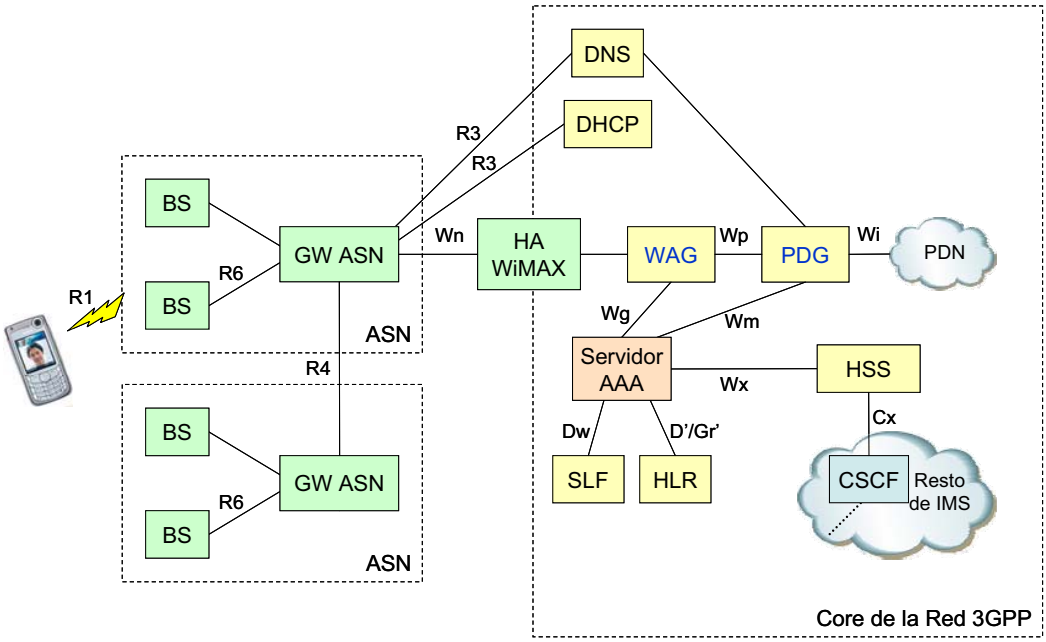



**Figura 80: Arquitectura de Interoperación entre WiMAX e IMS.**

La red de acceso WiMAX (WiMAX AN) permite acceder a los servicios IMS. La movilidad dentro de la red es administrada por el Agente Home WiMAX (WiMAX HA) que se localiza entre el Gateway ASN (Access Service Network Gateway) y el WAG (WiMAX Access Gateway). La red de acceso WiMAX se conecta a la red IMS a través del WAG y al servidor AAA 3GPP para el proceso de autentificación. Es importante recordar que el WAG es un gateway a través del cual los datos hacia/desde la WiMAX AN es enrutada para entregar al MS (Estación Móvil) los servicios de la red 3GPP. Dentro de las funciones del WAG está el enrutamiento de paquetes hacia el PDG (Packet Data Gateway), filtrado de paquetes y crear información de accounting. La principal función del PDG es enrutar los paquetes entre la PDN (Packet Data Network) y el MS.

Una implementación útil de la red sería integrar el acceso UMTS con el acceso WiMAX de forma de aprovechar la movilidad de UMTS con la alta velocidad de transmisión de datos de WiMAX. Para esto sería necesario utilizar un terminal dual que cuente con acceso a ambas tecnologías.

### 4.3.2. WiMAX Fijo y WiMAX Móvil

WiMAX Fijo (802.16-2004) y WiMAX Móvil (802.16e) son dos tecnologías bastante similares pero con enfoques a mercados bastante distintos. Ambos estándares están definidos en el mismo espectro, poseen el mismo ancho de banda de canal, duplexación y modulación. Sin embargo, 802.16-2004 utiliza acceso OFDMA y 802.16e SOFDMA.

De esta forma, WiMAX Fijo logra una gran transmisión de datos (un máximo teórico de 75 Mbps) y una eficiencia espectral que puede alcanzar los 3.75 bps/Hz mientras que WiMAX Móvil alcanza un máximo de 15 Mbps y una eficiencia espectral inferior a los 3 bps/Hz. Por otra parte, WiMAX Móvil permite una cobertura de celda entre 3 y 5 Km indoor y de 6 a 10 Km outdoor además que permite establecer conexiones a puntos móviles hasta a 120 Km/h, mientras que WiMAX Fijo posee un alcance de la celda entre 3 y 5 Km outdoor y no soporta enlaces móviles.

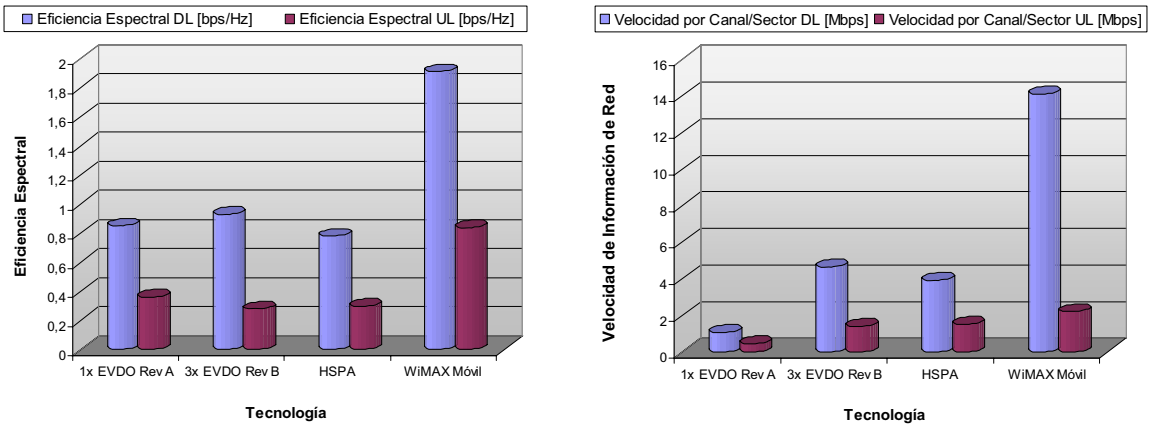
WiMAX Fijo, por tanto, se utiliza para requerimientos de altas tasas de datos sin mayor movilidad, esto lo hace útil no sólo como tecnología de acceso sino que también puede ser utilizado como parte troncal de la transmisión de datos de forma que se reduzcan los costos de implementación de la red puesto que es una tecnología inalámbrica. Por otra parte WiMAX Móvil permite mayor movilidad y mejor cobertura indoor que permite una mejor experiencia de usuario en la última milla aunque está limitada por tener una tasa de datos menor a WiMAX fijo.

Es importante considerar que, aunque WiMAX Móvil implementa celdas con mayor cobertura que WiMAX Fijo, el número de celdas también se ve determinado por la capacidad de transmisión demandada y, por tanto, es posible que en una misma área, WiMAX Móvil necesite implementar más celdas que WiMAX Móvil.

### 4.3.3. Comparación Gráfica de WiMAX Móvil con Tecnologías 3G

En la Figura 81 se muestra una comparativa del desempeño de WiMAX Móvil con HSPA y EVDO en cuanto a términos de Eficiencia Espectral y Velocidad de Información de red por Canal/Sector (datos que se observan en la Tabla 17).

Se observa en este diagrama que la utilización de WiMAX Móvil aprovecha mejor el espectro que las otras tecnologías y que logra velocidades muy superiores a las alcanzadas por las tecnologías 3G (más de 3 veces la velocidad DL de 3x EVDO Rev B y casi 1.5 veces la velocidad UL de HSPA). En este caso se tiene una eficiencia espectral de 1.91 bps/Hz para WiMAX Móvil, sin embargo, se debe recordad que esta tecnología puede alcanzar valores cercanos a los 3 bps/Hz.




**(a) Eficiencia Espectral** **(b) Velocidad de Información de Red**

**Figura 81: Comparación de Desempeño entre WiMAX Móvil, HSPA y EVDO.**

Otra característica a considerar en la comparativa entre estas tecnologías corresponde a la técnica de técnica de multiplexación utilizada: Mientras WiMAX utiliza la técnica (S)OFDMA, las tecnologías EVDO y HSPA utilizan técnicas heredadas de CDMA. En la Tabla 19 se muestra una tabla comparativa entre ambas técnicas de multiplexación.

**Tabla 19: Paralelo de características entre (S)OFDMA y CDMA.**

| Característica | (S)OFDMA | CDMA |
|---|---|---|
| Ambiente Multipath | Evita la interferencia inter-símbolo (ISI). | Necesita ecualización y mejoras al ruido. |
| Desvanecimiento Selectivo de Frecuencias | Es resistente ya que su naturaleza ortogonal permite corregir errores en cada sub-canal. | Produce errores en la transmisión disminuyendo la tasa de datos transmitida efectiva. |
| Rechazo al Ruido de Impulso | Sus símbolos de larga duración mitigan el impacto en la tasa de error | La pérdida de unos pocos símbolos puede aumentar el BER. |
| AMC | Lo soporta y mejora aplicándolo a sus sub-canales. | Lo soporta. |
| Interferencia multi-usuario en el DL | Lo evita por ser de naturaleza ortogonal. | Necesita ecualización. |
| Interferencia entre celdas | Cuanta con un reuso variable, puede evitar y promediar la interferencia. | Cuenta con promediación de interferencia. |

De esta tabla se deduce que los sistemas WiMAX tendrán un mejor desempeño en cuanto a rechazo a la interferencia, eficiencia espectral y tolerancia al multipath además de ofrecer servicios de alta calidad. Sin embargo, CDMA tiene la ventaja de responder mejor a la calidad en comunicaciones de voz.

En el diagrama de la Figura 82 ([18], [26], [43]) se observa una comparativa de resumen de variadas características de WiMAX Móvil, HSPA y EVDO. Los valores utilizados corresponden sólo a ponderadores comparativos y no a valores reales y, para efectos de gráfico, se utilizó el mayor valor

para estos tres casos como el valor "10" (por lo que los máximos reales pueden ser superiores a los aquí ilustrados).

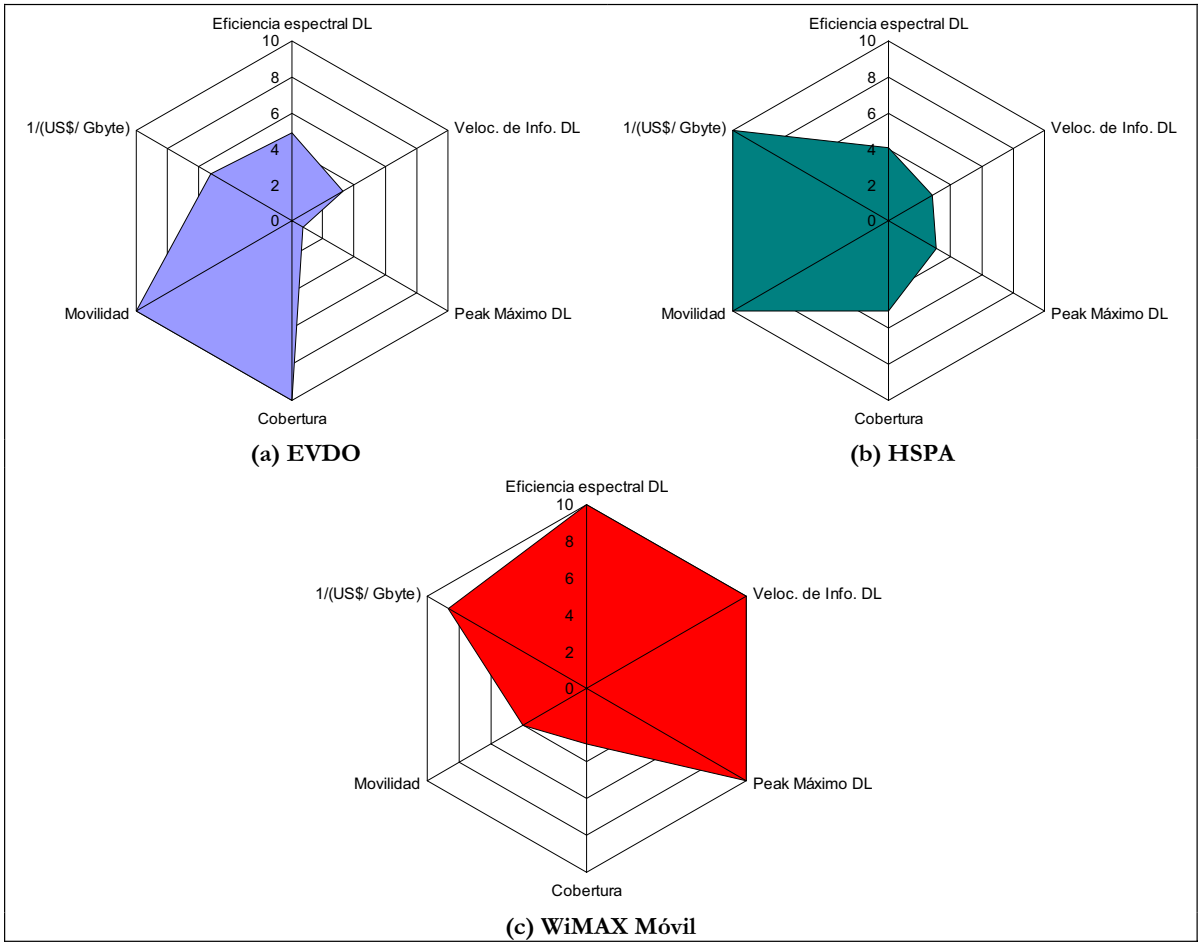



**Figura 82: Diagrama Comparativo entre EVDO, HSPA y WiMAX Móvil.**

De este diagrama se puede rescatar que WiMAX móvil posee el mejor desempeño en cuanto a transferencia de datos superando por mucho a las otras tecnologías al igual que gastos de operación por transmisión de datos bueno (y que se puede mejorar con una configuración más eficiente de antenas dado que este costo es proporcional a la eficiencia espectral). Sin embargo, el desempeño de WiMAX Móvil en cuanto a movilidad es bastante menor al de las otras tecnologías 3G.

Esto último implica que, por el desarrollo logrado por la tecnología WiMAX hasta ahora, el escenario óptimo de acceso a IMS establezca a WiMAX Móvil y a las tecnologías 3G como cooperativas. De esta forma se puede aprovechar la buena cobertura indoor de las redes inalámbricas como WiMAX y su gran capacidad en transmisión de datos con el manejo de movilidad y voz de los sistemas 3G.

# Capítulo 5
# Discusiones

## 5.1. Sobre Resultados

Las arquitecturas de interoperación descritas en el capítulo de resultados se basan únicamente en las especificaciones de la 3GPP de IMS. Estas especificaciones sobre IMS corresponden a la alternativa de red convergente más avanzada hasta el momento en cuanto a desarrollo de interfaces, funcionalidades y especificaciones. Se dejaron de lado otras alternativas propietarias principalmente por problemas de interoperación con otros tipos de redes y a que las empresas operadoras se están enfocando principalmente al uso de IMS como opción para brindar servicios convergentes costo-eficientes.

Además de los procedimientos resumidos en resultados, existen muchísimos más procesos descritos en profundidad en las especificaciones de la 3GPP. Sin embargo, los procedimientos descritos corresponden a los más ilustrativos para un fácil entendimiento de la arquitectura propuesta por IMS, de sus principales entidades funcionales y características.

Para analizar los factores determinantes en la efectiva implementabilidad de IMS, se decidió evaluar siete factores principales que debiera tener en cuenta cualquier operador antes de decidir realizar una inversión en modificar su red. IMS cumple con todas estas características, encontrándose como una alternativa bastante factible desde dicho punto de vista.

En cuanto a la evaluación de WiMAX como tecnología de acceso, los datos utilizados fueron sacados principalmente de la página del WiMAX Forum. Esta tecnología se incluyó en esta memoria como una alternativa factible y económica para brindar servicios convergentes tanto de parte de las operadoras fijas cómo móviles para abrirse paso a mercados no satisfechos. Se realizó una breve comparativa entre esta tecnología y las principales tecnologías 3G debido al desarrollo tomado por el estándar 802.16e o WiMAX Móvil que supone la abertura de WiMAX al mercado de la telefonía móvil de forma de analizar los pro y contra de utilizarlo como tecnología de acceso alternativa a los servicios móviles celulares actuales y 3G. Existen otros estándares IP que prometen conectividad móvil como el estándar de la IEEE 802.20, estos estándares se encuentran bien definidos y caracterizados en la memoria "Comparativa de Tecnologías Emergentes de Acceso a Redes Móviles y Fijas" de Priscila López ([26]). Sin embargo, se optó por evaluar WiMAX debido al gran desarrollo que ha tenido esta tecnología en cuanto a hardware, tanto de red como de terminales, a su

disponibilidad actual y a las muchas innovaciones y desarrollos de variadas empresas (como Intel) para brindar soluciones de acceso basadas en esta tecnología.

## 5.2. Sobre la Convergencia de Redes

La convergencia de redes surge de una necesidad tanto de las empresas como de los usuarios. Esta necesidad no está basada propiamente en las tecnologías sino que se orienta a la convergencia de servicios y responde a una necesidad a corto y mediano plazo, dado por un ambiente altamente competitivo en el mercado de las telecomunicaciones debido a la madurez y saturación del mercado y a que las nuevas tecnologías permiten la entrada de nuevos competidores al servicio de voz; junto con el deseo de los clientes de mejorar las comunicaciones.

De esta forma, las empresas de telecomunicaciones que necesitan consolidar sus servicios (tanto en redes fijas como móviles) se ven forzadas a migrar a redes convergentes para obtener una ventaja y no ser desplazadas por su competencia. Una razón importante de la convergencia de redes consiste en la reducción de los gastos de los operadores tanto en el CAPEX (ahorros entre un 10 y 20%) como en el OPEX (ahorros cercanos al 40%).

Una red convergente debe cumplir con los siguientes requerimientos básicos:

- La comunicación debe establecerse fácilmente por cualquier persona.
- El servicio de comunicación debe estar disponible en cualquier momento.
- El servicio de comunicación debe estar disponible en cualquier lugar.
- La red y terminal debe proporcionar cualquier servicio.
- El servicio debe estar disponible a través de cualquier acceso.
- Cualquier tipo de servicio debe de ser capaz de usar el ancho de banda necesario de la red, facilidades de seguridad y otros recursos.
- Los servicios de contenido entregados por la red o terceros deben ser proporcionados mediante interfaces abiertas.
- El costo del servicio debe ser razonable.

Para satisfacer estos requerimientos, se hace necesario crear soluciones a nivel global y, por tanto, se necesita lograr acuerdos en cuanto a soluciones basadas en estándares abiertos y en plataformas de servicios End-to-End. Como respuesta a esta necesidad surge la arquitectura IMS, definida por la 3GPP, que permite la implementación de diferentes servicios multimedia como los de Presencia o Push-to-Talk. IMS logra que las distintas redes puedan interoperar con servicios convergentes con un ambiente de servicios dinámico que permite la introducción de nuevos servicios de forma rápida y económica. Pero para esto, los operadores de distintas redes (telefonía fija, móvil y operadores de cable) deben hacer el esfuerzo de organizarse y adoptar la arquitectura IMS, de forma de que no se creen soluciones "isla".

IMS corresponde a una red NGN de carácter abierto, cuenta con una arquitectura horizontal y con interfaces abiertas en cada capa. Las capas de la arquitectura son la de Aplicación, Control, Transporte y Acceso. Una de sus principales características es la separación de tráfico en planos de control y stream media, la transmisión de datos se basa en conmutación de paquetes y permite la movilidad del usuario a través de las redes de acceso independientemente de la naturaleza de éstas.

La rápida implementación de servicios convergentes por parte de los operadores será un movimiento estratégico en su crecimiento y valor percibido. Ya en Europa y Asia se han lanzado servicios que cuentan con elementos de handoff entre redes y el uso de un CPE (Customer Premise Equipment) convergente que caben en la categoría de servicios convergentes. Por ejemplo, Swisscom's Mobile Unlimited Service permite a los usuarios de empresas moverse entre diferentes tipos de redes móviles (UMTS, Wi-Fi, GPRS y EDGE) de forma que no sea percibida por el usuario, France Telecom's Business Everywhere permite a sus empleados móviles acceder a su red usando un laptop o PDA desde cualquier red de acceso (ADSL, 3G, Wi-Fi, GPRS o PSTN) utilizando sólo un password. También en Corea, Japón y Reino Unido se han lanzado servicios de convergencia con terminales duales de telefonía que conmutan entre tecnologías 3G e IP.

Aunque el desarrollo del mercado FMC se encuentra en pañales, se espera que en los próximos años se lance una gran cantidad de servicios convergentes en el mundo. IDC pronostica que, para el 2010, los usuarios FMC a nivel mundial alcanzarán los 47 millones con un retorno de US $ 24 miles de millones. En la Figura 83 se observa el desarrollo de usuarios y retornos proyectados hasta el 2010 por IDC.

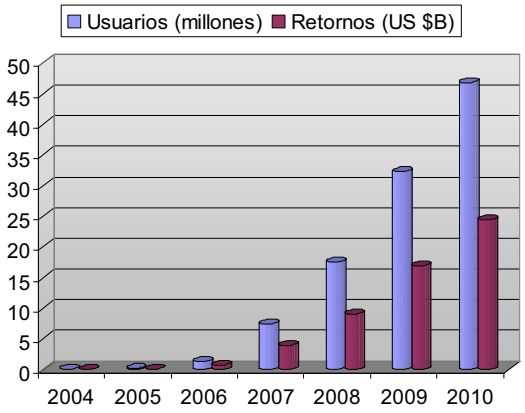



**Figura 83: Proyecciones de Usuarios y Retornos de FMC 2004-2010.**

## 5.3. Sobre IMS

Para enfrentar la convergencia de telefonía Fija-Móvil, los operadores necesitan una estrategia que defina sus objetivos como negocio y soluciones que logren metas tanto a corto, mediano o largo plazo. La solución debe sobrellevar una serie de dificultades tales como la introducción de servicios multimedia IP que deben ser soportados por variados terminales, la entrega de servicios debe ser costo-eficiente y utilizar tecnologías de acceso complementarias, además debe lograr una baja en los costos operacionales y que los servicios tradicionales se mantengan. Los primeros pasos a tomar para la evolución de redes es optimizar el Core de conmutación de paquetes de la red de forma de permitir un empleo rápido de servicios multimedia IP de valor agregado de la forma más efectiva en costos que sea posible. Una característica clave de esta estrategia es el uso de componentes comunes de la red y extensiones específicas de servicios que reduzcan el costo del desarrollo e implementación de los servicios.

Esta estrategia puede ser muy bien enfrentada utilizando IMS o IP Multimedia Subsystem como el motor para la entrega de servicios con un Core de la red unificado. IMS juega un rol crucial

en la convergencia, y con el uso de SIP (Session Initiation Protocol) permite la introducción de servicios IP, incluyendo VoIP, compartir video y otros servicios multimedia.

El estándar IMS define una arquitectura genérica para ofrecer VoIP y servicios multimedia. Corresponde a un estándar internacional especificado por la 3GPP y que ha sido adoptado por otros cuerpos de estándares como ETSI/TISPAN. Una de sus características principales es el soporte de múltiples tipos de acceso, que incluyen GSM, WCDMA, conexiones a banda ancha mediante cables y WLAN. Para los usuarios, los servicios basados en IMS permiten comunicaciones persona a persona y persona a contenido en una forma altamente personalizada y controlada y, para los operadores, IMS toma el concepto de una arquitectura estratificada horizontalmente donde los servicios y funciones comunes pueden ser reusadas para aplicaciones múltiples. Además, por sus características de interoperabilidad, roaming, control de portadores, facturación, seguridad e integración, IMS es el factor clave en la convergencia de telefonía fija-móvil.

Para los operadores fijos y móviles, IMS permite un camino seguro de migración a una arquitectura all-IP que concede al usuario final demandar servicios nuevos y enriquecidos. El éxito que logre IMS al agregar valor a los servicios de telecomunicaciones depende fuertemente de la disposición que tengan las distintas empresas de telecomunicaciones en lograr acuerdos de roaming no sólo con redes en el extranjero sino con redes dentro del mismo país en zonas donde no se tenga cobertura de forma de lograr una efectiva sensación de conectividad en todas partes de parte del usuario.

Una de las fuerzas de IMS es que separa el modelo de control de sesión en múltiples entidades funcionales con interfaces estándar entre éstas. Esto permite que IMS tenga una naturaleza multi-vendedor de forma que los operadores puedan adoptar este sistema seleccionando los mejores productos disponibles en el mercado para cada entidad de la arquitectura. El modelo distribuido de IMS crea un ambiente donde las vulnerabilidades de cada elemento varían dependiendo de las funciones proveídas, las interfaces soportadas y la plataforma utilizada. Los operadores que implementen IMS necesitan desarrollar una arquitectura de seguridad con políticas de seguridad consistentes, este puede convertirse en un reto en un ambiente donde las responsabilidades en la administración de las plataformas se dispersan en más de un grupo de operación. Por ejemplo, en un ambiente, el Core del sistema IMS (como los CSCFs) pueden estar administrados por un grupo de operación distinto al de los servidores de aplicación, en esta situación es importante para ambos grupos acordar los estándares, políticas y procesos para actividades críticas de seguridad como escaneo, Firewall o filtrado.

## 5.4. Sobre WiMAX

WiMAX corresponde a una tecnología inalámbrica orientada al mercado inalámbrico en zonas metropolitanas como una tecnología de acceso. WiMAX se basa en dos estándares: 802.16d o WiMAX Fijo, y 802.16e o WiMAX Móvil.

WiMAX Fijo abre una gran oportunidad a empresas de servicios de telecomunicaciones que no cuentan con última milla dado que sobrelleva de forma simple y baja en costos tanto en la construcción de redes de acceso como en sistemas troncales. Con WiMAX Fijo se pueden crear redes de transporte de forma de transferir grandes tasas de datos a grandes distancias utilizando sólo dos antenas y sin línea de vista. Esto permite satisfacer mercados que, sin esta tecnología, no serían

rentables como sectores rurales o de bajos recursos a bajo costo de instalación y con servicios baratos para los clientes.

Una característica de WiMAX de gran valor para la convergencia es la implementación de redes Mesh. Las redes Mesh inalámbricas son simples y fáciles de implementar y su topología reduce significativamente la necesidad de un backbone alámbrico, una de los principales obstáculos para crear grandes zonas Wi-Fi. Así, WiMAX permite el desarrollo de nuevos negocios tanto para operadores fijos como móviles de forma de proveer valor agregado a sus servicios IP inalámbricos.

Por otra parte, WiMAX Móvil promete satisfacer la demanda de usuarios que requieren transferencia de datos a altas velocidades y con cierto margen de velocidad (hasta 100 Km/h) que permite comunicaciones móviles en la mayor parte de las zonas urbanas aunque no sería capaz de funcionar en trenes, carreteras o cualquier zona en que las velocidades de transporte superen los 100 Km/h. De esta forma, WiMAX Móvil aún no es una tecnología que pueda reemplazar a las telefonías móviles de forma total.

Sin embargo, mientras WiMAX Móvil no pueda superar la movilidad de la telefonía celular o 3G, puede desempeñarse como una tecnología complementaria para los servicios celulares 3G. Mientras WiMAX es conocido por sus capacidades de transmisión a grandes distancias y a altas tasas, 3G soporta la movilidad a altas velocidades de movimiento de parte del usuario.

La Tabla 20 muestra un breve análisis FODA de WiMAX.

**Tabla 20: Análisis FODA de WiMAX.**

| | |
|---|---|
| **F** (Fortalezas) | Gran cobertura con alta capacidad, estándares unificados, Costos de equipos comparativamente más bajos que en redes alámbricas o 3G, trabajo de red rápido y flexible, utiliza tanto banda de frecuencia licenciada (para el caso chileno, las empresas Entel, TELMEX, Telsur y VTR tienen asignada la banda licenciada de 3,5 GHz para operar) como no licenciada. |
| **O** (Oportunidades) | Puede ser combinada con redes WLAN, 3G, ADSL, etc. Sirve como solución de última milla tanto para accesos fijos como móviles. |
| **D** (Debilidades) | Técnica y equipos de usuario inmaduros, el ambiente inalámbrico es complejo, desempeño inestable para transmisiones a largas distancias, sufre muchísima interferencia en el caso de operar en una banda no licenciada. |
| **A** (Amenazas) | ADSL, Cable, Fibra, MAN, WLAN y 3G. |

La tecnología WiMAX no es un sueño lejano, Telmex es una empresa de telecomunicaciones chilena que ya comenzó la implementación de WiMAX en Chile utilizando tecnología de Alcatel-Lucent. Durante la primera quincena de abril del 2007, esta red ya comenzó a estar operativa para brindar servicios de telecomunicaciones a pequeñas y medianas empresas en Santiago, Concepción, Talcahuano, Curicó, Iquique, La Serena, Coquimbo, Linares, Ovalle, Rancagua, Talca, Temuco, Valdivia, Valparaíso y Viña del Mar. Próximamente estará operando en Calama, Osorno, Puerto Montt, Requinoa y Punta Arenas y se proyecta para fines de este año, que la red WiMAX de Telmex cubra el 91% de las comunas de Chile (incluyendo Isla de Pascua), lo que equivale al 98% de la población chilena.

# Capítulo 6
# Conclusiones

En el presente trabajo se realizó un estudio y caracterización de las principales arquitecturas de telefonía tanto fija como móvil, identificándose principalmente sus entidades funcionales, interfaces y sus principales protocolos. Entre las arquitecturas estudiadas se encuentran la red PSTN, GSM, GPRS, UMTS, PacketCable e IMS. Además se repasaron los protocolos de VoIP: H.323, SIP y MEGACO.

También se abordó el concepto de FMC (Fixed Mobile Convergence) y gran parte del funcionamiento, procesos y características soportadas de la arquitectura IMS, estándar considerado como clave en la implementación de redes convergentes. Junto con esto, se estudió y evaluó la utilización de la tecnología WiMAX como alternativa de acceso para redes convergentes.

Del estudio de FMC se puede concluir que este proceso cambiará la forma en que se realizan las telecomunicaciones, cambiando la visión centrada en la red a una visión centrada en el cliente, brindándoles simplicidad, nuevos servicios a bajo precio y, desde el punto de vista de las empresas, una gran herramienta para incrementar la eficiencia y reducir costos. Sin embargo, para que FMC sea una realidad, requiere un trabajo de colaboración entre sistemas de telecomunicaciones que hasta ahora han trabajado independientemente, no sólo en el ámbito de los operadores fijos y móviles sino que también de las manufactureras de equipos de red y terminales.

El desarrollo de los terminales móviles a utilizar debe ser un proceso muy bien pensado por las agrupaciones FMC, ya que estos favorecerán una u otra tecnología de acceso de parte de los operadores. Inicialmente se espera que estos terminales cuenten con sistemas de acceso a tecnologías 3G y a otra tecnología inalámbrica, típicamente Wi-Fi o Bluetooth y en el futuro se espera la implementación de otras tecnologías como WiMAX. El precio de los terminales será una pieza determinante de la velocidad con que los servicios FMC penetrarán en el mercado. Ya en la actualidad se aprecia la aparición de terminales convergentes, principalmente de GPRS (o UMTS) y Wi-Fi (o Bluetooth); hasta la fecha los precios de estos terminales son altos por lo que se orientan a un mercado básicamente ejecutiva y son privativos para la mayoría de los usuarios móviles actuales.

La convergencia fija-móvil será un gran esfuerzo tanto para operadores como manufactureras pero con claros beneficios para ambas partes y generosos retornos (para el 2009, se estima un mercado de US $ 141 billones). Sin embargo, la convergencia no será uniforme para todas las redes sino que tendrá variaciones dependiendo del tipo de red. En el mejor de los casos, la convergencia

será lograda por un sistema que sirva tanto para el mundo fijo y móvil con las menores variaciones posibles. Este es el caso de IMS, de la 3GPP.

Del estudio realizado de IMS se saca en limpio que éste es una iniciativa basada en estándares con gran acogida dentro de la industria. IMS atrae a todos los sectores de la industria móvil incluyendo operadores de red, vendedores de infraestructura, empresas y algunos desarrolladores de aplicaciones que ya han desarrollado nuevos servicios.

IMS es una plataforma de servicios de la 3GPP creada inicialmente para redes UMTS que puede ser fácilmente exportada a redes de nueva generación. De hecho, se probó que interopera de forma exitosa con redes legacy fijas y celulares y con accesos IP como redes GSM, GPRS, UMTS, CDMA (cuya interoperación fue incluida por la 3GPP2), redes WLAN y todo tipo de acceso IP (xDSL, fibra, cable, etc.). Aunque la calidad de servicio ofrecida en redes IP aún es motivo de estudio, contemplándose el uso de DiffServ como método para proveer QoS. Una de las principales características de IMS es que distribuye las entidades encargadas de levantar y administrar sesiones en toda la red haciéndola más robusta que las redes tradicionales y más flexible en cuanto a capacidad (y por tanto, también en cuanto a costo-efectividad) y planeación de la red.

El modelo de negocios propuesto por IMS minimiza el riesgo de que los operadores de redes de próxima generación se transformen sólo en el transporte de los servicios. Además IMS permite la integración de terceras partes en la red, ofreciendo múltiples escenarios atractivos para los usuarios.

IMS será capaz de soportar los servicios de "bundles" (paquetes) de servicios, que ya se están observando en el mercado actual. IMS está diseñado para hacer que el operador de red se beneficie de este tipo de servicios. Además los "bundles" de servicios permiten la asociación de múltiples empresas para brindar servicios combinados, por ejemplo, la compra del supermercado puede ser acompañada por un aviso MMS o SMS al llegar al hogar. Con esto, se abre un amplio rango de posibilidades de aplicaciones de IMS, lo que hace difícil pronosticar el futuro de esta plataforma. IMS es una buena plataforma para implementar servicios de más de una empresa, desarrollando productos que el usuario demande.

Así mismo, IMS es clave en la evolución a redes all-IP por el hecho de proveer una forma estandarizada y bien estructurada para entregar servicios, para la interoperación con redes legacy y para la convergencia fija-móvil. Actualmente, IMS es el único estándar con comunicaciones basadas en SIP. Desde una perspectiva de red, IMS ofrece un desarrollo costo-eficiente tanto en términos de implementación, operación y mantenimiento.

Desde una perspectiva móvil, ya se está comenzando la implementación de IMS para ofrecer servicios multimedia, un ejemplo de estos servicios es el ya conocido Push-to-talk sobre Celular (PoC). Además, la arquitectura IMS permitirá enriquecer la telefonía móvil legacy (con conmutación de circuitos) combinando las capacidades de los mundos de conmutación de circuitos y de paquetes. En el futuro podrá implementarse VoIP a medida que se introduzcan las redes inalámbricas, sin embargo, este proceso tomará tiempo debido a la existencia limitada de los portadores de radio.

De esta forma, IMS soportará nuevas capacidades multimedia como video, mensajería, servicios personalizados, etc. los que pueden ser implementados a medida que crezca la demanda del mercado y en concordancia con los estándares definidos por la 3GPP y otras organizaciones preocupadas por la convergencia, como OMA.

Desde el punto de vista de las redes cableadas o wireline, muchos factores apoyan el desarrollo de redes IMS, entre ellos se encuentran: que no existen restricciones de ancho de banda, sin problemas de roaming, y los terminales cuentan con el suficiente poder de procesamiento para proveer aplicaciones avanzadas. Todas estas características implican que los operadores wireline pueden comenzar a implementar IMS para introducir nuevos servicios que generen retornos y reducciones en el OPEX y CAPEX.

El reemplazo de la telefonía de conmutación de circuitos basado en banda ancha y tecnología VoIP ya está pasando. Sin embargo, muchas de estas soluciones se basan en arquitecturas propietarias y que no interactúan con otras arquitecturas ni con IMS. Por el contrario, IMS es una gran oportunidad para los operadores fijos ya que es la única arquitectura estándar para comunicaciones basadas en SIP en redes wireline y gran parte de la comunidad wireline de telecomunicaciones se están uniendo y adoptando este estándar.

Ya existen en la actualidad variadas plataformas IMS que permiten la implementación de redes con altos requerimientos pero también redes pequeñas. Un ejemplo de implementación de plataforma IMS de bajo costo son las especificaciones Java para SIP que permite la existencia de los CSCFs, y Servidores de Aplicación (con variadas aplicaciones ya creadas). Java provee paquetes o librerías de objetos de desarrollo y programación abierta y con un alto desempeño que reduce los costos muy significativamente a los operadores de redes pequeñas.

Del análisis de WiMAX realizado se concluye que es un importante elemento en la visión de convergencia. WiMAX puede ofrecer a los proveedores de servicios una forma eficiente en costos para ofrecer servicios multimedia de gran valor a los suscriptores debido a su potencial para proveer altas tasas de transferencia y cierta movilidad. WiMAX puede ser integrado con redes wireline y 3G de forma de entregar ancho de banda a los usuarios en un amplio rango de localizaciones. Además, puede complementar los servicios DSL extendiendo su alcance a usuarios que no tengan acceso a la red o como red de acceso en los últimos 100 metros desde la red para minimizar los costos en la implementación de fibra.

WiMAX permite ser implementada como red de acceso a bajo costo bajo variadas condiciones demográficas tanto urbanas como rurales. Además, sus características permiten servir como backhaul para los Hot Spots Wi-Fi. Sin embargo, este negocio no es rentable ofrecido de forma única pero sí es un buen complemento para otros servicios del operador y que logra buenos retornos con una pequeña inversión extra. En zonas rurales de poca densidad, permite una inversión inicial reducida, la que se puede ir aumentando a medida que aumenta la demanda.

Con el desarrollo actual de la especificación WiMAX, es claro que no puede ser utilizado en forma única como tecnología de acceso, sino como tecnología complementaría tanto para unir puntos de acceso WLAN o para trabajar junto con redes celulares de hasta 3G de capacidad limitada. Esto, de todas formas, abre una gran oportunidad de mercado ya que los usuarios gradualmente comienzan a utilizar aplicaciones cada vez más sofisticadas que requieren altas tasas de transferencia. Una de las grandes oportunidades que ofrece WiMAX es que es una tecnología que permite la ampliación de servicios tanto en redes de operadores fijos como móviles pues permite a los operadores fijos brindar servicios con características móviles y, permite a los operadores móviles ofrecer servicios de banda ancha sin mayor inversión en su infraestructura, sobre todo en cuanto a la última milla.

WiMAX está direccionado a un mercado global, está basado en interfaces estándar abiertas desarrolladas por alrededor de 400 compañías contribuyendo para su adopción en todo el mundo.

Comparado con otras alternativas móviles como HSPA y EVDO, WiMAX es más flexible y dinámico en la asignación de recursos, con mejor sistema de QoS y es capaz de servicios DSL y Cable en ambientes móviles de forma efectiva en costos.

El enfoque de esta memoria es fundamentalmente teórico, un buen aporte para trabajos futuros consistiría en el desarrollo de una maqueta de arquitectura IMS con herramientas abiertas (como las ya mencionadas de Java u otras como OpenSer) que permitan verificar experimentalmente su funcionamiento con variadas tecnologías de acceso y aplicaciones. Esta arquitectura puede ser enriquecida con las múltiples aplicaciones desarrolladas por otros memoristas del Team ToIP, como los servicios de E-Learning o de Contact Center.

# Capítulo 7
# Acrónimos

- 1xEVDO: Evolution Data-Optimized.
- 3G GSM: Red GSM de Tercera Generación.
- 3GPP: Third Generation Partnership Project.
- AAA: Authentication, Authorization & Accounting.
- AAS: Adaptive Antenna System.
- ACM: Address Complete Message.
- ADSL: Asymmetric Digital Subscriber Line.
- ADSL2+: Asymmetric Digital Subscriber Line 2 Plus.
- AF: Application Function.
- AKA: Authentication and Key Agreement.
- AMC: Adaptive Modulation and Coding.
- AMS: Adaptive MIMO Switching.
- AN: Access Network.
- ANM: Answer Message.
- AMPS: Advanced Mobile Phone Service.
- ANI: Application-to-Network Interface.
- API: Application Programming Interfaces.
- AS: Application Server.
- ASN: Access Service Network.
- ASN.1: Abstract Syntax Notation One.
- ATM: Asynchronous Transfer Mode.
- AuC: Authentication Center.
- BER: Bit Error Rate.
- BGCF: Breakout Gateway Control Function.
- BS: Bearer Service.
- BS: Base Station.
- BSC: Base Station Controller.
- BSS: Base Station Subsystem.

- BTS: Base Transceiver Station.
- CBC: Cell Broadcast Centre.
- CCITT: Comite Consultatif Internationale de Telegraphique et Telephonique.
- CDMA: Code Division Multiple Access.
- CDF: Charging Data Function.
- CDR: Charging Data Records.
- CGF: Charging Gateway Function.
- CID: Connection ID.
- CM: Cable Modem.
- CMS: Call manager Server.
- CMTS: Cable Modem Termination System.
- CN: Core Network.
- COPS: Common Open Policy Server.
- CPE: Customer Premise Equipment.
- CS: Circuit Switched.
- CSCF: Call Session Control Function.
- DHCP: Dynamic Host Configuration Protocol.
- DL: Downlink.
- DNS: Domain Name System.
- DOCSIS: Data Over Cable Service Interface Specification.
- E-MTA: Embedded – Multimedia Terminal Adapter (1 MTA + 1 Cable módem).
- EAP: Extensible Authentication Protocol.
- EDGE: Enhanced Data Rates for Global Evolution.
- EGPRS: Enhanced General Packet Radio Service.
- EIR: Equipmenent Identity Register.
- EMS: Element Management System.
- ESP: IPsec Encapsulating Security Payload.
- ETSI: European Telecommunications Standards Institute.
- FA: Foreign Agent.
- FDD: Frequency Division Duplex.
- FDMA: Frequency Division Multiple Access.
- FEC: Forward Error Correction.
- FMC: Fixed-Mobile Convergence.
- GAN: Generic Access Network.
- GANC: Generic Access Network Controller.
- GGSN: Gateway GPRS Support Node.
- GMSC: Gateway Mobile Services Switching Center.
- GPRS: General Packet Radio Service.
- GRUU: Globally Routable User Agent URI.
- GSM: Global System for Mobile communications.

- GSN: GPRS Support Node.
- GUP: Generic User Profile.
- HARQ: Hybrid Auto Repeat Request.
- HFC: Hibrid Fibre Coaxial.
- HLR: Home Location Register.
- HSDPA: High-Speed Downlink Packet Access.
- HSPA: High-Speed Packet Access.
- HSS: Home Subscriber Server.
- HSUPA: High-Speed Uplink Packet Access.
- I-CSCF: Interrogating CSCF.
- I-WLAN: Interworking WLAN.
- IAM: Initial Address Message.
- IBCF: Interconnection Border Control Function.
- ICI: Inter-Channel Interference.
- IETF: Internet Engineering Task Force.
- IKE: Internet Key Exchange.
- IMEI: International Mobile Equipment Identity.
- IMS: IP Multimedia Subsystem.
- IMS-ALG: IMS – Application Level Gateway.
- IMS-MGW: IP Multimedia Subsystem – Media Gateway Function.
- IMTS: Improved Mobile Telephone System.
- IP: Internet Protocol.
- IP-CAN: IP – Connectivity Access Network.
- ISDN: Integrated Services Digital Network.
- ISI: Inter-Symbol Interference.
- ISIM: IMS Identity Module.
- ISO: International Standards Organization.
- ISUP : ISDN User Part.
- ITU: International Telecommunication Union.
- IXC: IntereXchange Carrier.
- LOS: Line of Sight.
- MAC: Media Access Control.
- MCU: MultiControl Unit.
- MGC: Media Gateway Controller.
- MGCF: Media Gateway Control Function.
- MGW: Media Gateway.
- MIB: Management Information Base.
- MIMO: Multiple Input Multiple Output.
- MRF: Media Resource Function.
- MRFC: Multimedia Resource Function Controller.

- MRFP: Multimedia Resource Function Processor.
- MS: Mobile Station.
- MSC: Mobile Services Switching Center.
- MTP: Message Transfer Part.
- NAI: Network Access Identifier.
- NAT : Network Address Translation.
- NAPT: Network Address and Port Translation.
- NCD: National Destination Code.
- NDS: Network Domain Security.
- NGN: Next Generation Network.
- NLOS: Non Line of Sight.
- NMS: Network Management System.
- NNI: Network-to-Network Interface.
- NSN: National Significant Number.
- NSS: Network and Switching Subsystem.
- OCS: Online Charging System.
- OFDM: Orthogonal Frequency Division Multiplexing.
- OFDMA: Orthogonal Frequency Division Multiple Access.
- OMA: Open Mobile Alliance.
- OSI: Open Systems Interconnection Reference Model.
- OSS: Operation and Support Subsystem.
- P-CSCF: Proxy CSCF.
- PAC: Provisioning, Activation, and Configuration.
- PBX : Private Branch eXchange.
- PCM: Pulse Code Modulation
- PDF: Policy Decision Function.
- PDG: Packet Data Gateway.
- PDN: Packet Data Network.
- PDP: Packet Data Protocol (utilizado en GPRS).
- PIN: Personal Identification Number.
- PKMv2: Privacy and Key Management Protocol Version 2.
- PS: Packet Switched.
- PSTN: Public Switched Telephone Network.
- QoS: Quality of Service.
- RAB: Radio Access Bearer.
- RAFC: Resource and Admission Control Function.
- RNC: Radio Network Controller.
- RNS: Radio Network System.
- RSVP: Resource ReSerVation Protocol.
- RTCP: Real Time Control Protocol.

- RTP: Real Time Protocol.
- S-CSCF: Serving CSCF.
- SBLP: Service-Based Local Policy.
- SCCP: Signaling Connection Control Part.
- SCP: Service Control Point.
- SDP: Session Description Protocol.
- SDU: Service Data Unit.
- SEG/SEGW: Security Gateway.
- SGSN: Serving GPRS Support Node.
- SIM: Subscriber Identity Module.
- SIMO: Single Input Multiple Output.
- SIP: Session Initiation Protocol.
- SLF: Subscription Locator Function.
- SMLC: Serving Mobile Location Center.
- SMS: Short Message Service.
- SN: Subscriber Number.
- SNMP: Simple Network Management Protocol.
- SOFDMA: Scalable Orthogonal Frequency Division Multiplexing Access.
- SS: Subscriber Station.
- SS7: Signaling System 7.
- SSP: Serving Switching Point.
- STP: Signal Transfer Point.
- STUN: Simple Traversal of UDP through NATs.
- T-SGW: Trunking Signaling Gateway.
- TCAP: Transaction Capabilities Application Part.
- TCP: Transmission Control Protocol.
- TDD: Time Division Duplex.
- TDMA: Time Division multiple Access.
- TE: Terminal Equipment.
- TGCP: PSTN Gateway Call Signaling Protocol.
- THIG: Topology Hiding Inter-network Gateway.
- TIC: Tecnologías de la Información y la Comunicación.
- ToIP: Telephony over IP.
- TrGW: Transition Gateway.
- TUP: Telephone User Part.
- UA: User Agent.
- UAC: User Agent Client.
- UAS: User Agent Server.
- UDP: User Datagram Protocol.
- UE: User Equipment.

- UICC: Universal Integrated Circuit Card.
- UL: Uplink.
- UMA: Unlicensed Mobile Access.
- UMTS: Universal Mobile Telecommunications System.
- UNI: User-to-Network Interface.
- URI: Uniform Resource Identifier.
- URL: Uniform Resource Locator.
- USIM: Universal Subscriber Identity Module.
- UTRAN: UMTS Terrestrial Radio Access Network.
- VLR: Visitor Location Register.
- VoIP: Voice over IP.
- WAG: WLAN Access Gateway.
- Wi-Fi: Wireless Fidelity.
- WiMAX: Worldwide Interoperability for Microwave Access.
- WLAN: Wireless Local Area Network.
- WMAN: Wireless Metropolitan Area Network.
- WMM: Wireless Multimedia Extensions.
- xDSL: Digital Subscriber Line.

# Capítulo 8
# Bibliografía


[1] 3GPP: "TR 21.905 v7.2.0 (2006-06): Vocabulary for 3GPP Specifications" [en línea]. http://www.3gpp.org/ftp/Specs/archive/21_series/21.905/ [Consulta: Noviembre 2006]

[2] 3GPP: "TR 23.836 v1.0.0 (2005-11): Quality of Service (QoS) and policy aspects of 3GPP – Wireless Local Area Network (WLAN) interworking" [en línea]. http://www.3gpp.org/ftp/Specs/archive/23_series/23.836/ [Consulta: Noviembre 2006]

[3] 3GPP: "TR 23.934 v1.0.0 (2002-08): 3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and architectural definition" [en línea]. http://www.3gpp.org/ftp/Specs/archive/23_series/23.934/ [Consulta: Noviembre 2006]

[4] 3GPP: "TR 23.981 v6.4.0 (2005-09): Interworking aspects and migration scenarios for IPv4 based IMS implementations" [en línea]. http://www.3gpp.org/ftp/Specs/archive/23_series/23.981/ [Consulta: Noviembre 2006]

[5] 3GPP: "TS 23.002 v7.1.0 (2006-03): Network architecture" [en línea]. http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/ [Consulta: Noviembre 2006].

[6] 3GPP: "TS 23.207 v6.6.0 (2005-09): End-to-end Quality of Service (QoS) concept and architecture" [en línea]. http://www.3gpp.org/ftp/Specs/archive/23_series/23.207/ [Consulta: Noviembre 2006].

[7] 3GPP: "TS 23.228 v7.4.0 (2006-06): IP Multimedia Subsystem (IMS); Stage 2" [en línea]. http://www.3gpp.org/ftp/Specs/archive/23_series/23.228/ [Consulta: Noviembre 2006].

[8] 3GPP: "TS 23.234 v7.4.0 (2006-12): 3GPP system to Wireless Local Area Network (WLAN) interworking; System Description" [en línea]. http://www.3gpp.org/ftp/Specs/archive/23_series/23.234/ [Consulta: Diciembre 2006].

[9] 3GPP: "TS 29.162 v7.1.0 (2006-03): Interworking between the IM CN subsystem and IP networks" [en línea]. http://www.3gpp.org/ftp/Specs/archive/29_series/29.162/ [Consulta: Noviembre 2006].

[10] 3GPP: "TS 29.207 v6.5.0 (2005-09): Policy Control over Go interface" [en línea]. http://www.3gpp.org/ftp/Specs/archive/29_series/29.207/ [Consulta: Noviembre 2006].

[11] 3GPP: "TS 43.318 v7.0.0 (2006-11): Radio Access Network; Generic access to the A/Gb interface; Stage 2" [en línea]. http://www.3gpp.org/ftp/Specs/archive/43_series/43.318/ [Consulta: Diciembre 2006].

[12] BECERRA, Néstor: "Apuntes EL55A: Sistemas de Telecomunicaciones", Departamento de Ingeniería Eléctrica, Universidad de Chile, 2005.

[13] BILDERBEEK, Pim; FINGER, Jill y VESTERGAARD, Lars: "Fixed-Mobile Convergence: Unifying the Communications Experience" [en línea]. http://www.thefmca.com/assets/pdf/idc_fmca_09_11_05.pdf [Consulta: Agosto 2006].

[14] CableLabs®: "PacketCable 2.0™: Architecture Framework Technical Report" [en línea]. http://www.packetcable.com/downloads/specs/PKT-TR-ARCH-FRM-V02-061013.pdf [Consulta: Noviembre 2006].

[15] DAUPHIN, Jean-Louis; ZNATY, Simon: "IP Multimedia Subsystem: Principles and Architecture" [en línea]. http://www.efort.com/media_pdf/IMS_ENG.pdf [Consulta: Noviembre 2006].

[16] Digital Engineering Library @ McGraw Hill: "Broadband Telecommunications Handbook", Capítulo 16: xDSL [en línea]. http://www.digitalengineeringlibrary.com [Consulta: Noviembre 2006].

[17] Digital Engineering Library @ McGraw Hill: "Softswitch Architecture for VoIP", Capítulo 2: The Public Switched Telephone Network (PSTN) [en línea]. http://www.digitalengineeringlibrary.com [Consulta: Noviembre 2006].

[18] GASPAROLLO, Luigi: "Guidelines on the Smooth Transition of Existing Mobile Networks to IMT-2000 for Developing Countries ARB Region" [en línea]. http://www.itu.int/ITU-D/imt-2000/documents/Damascus2005/Presentations/Day%201/Damascus_1_4_2.PDF [Consulta: Marzo 2006].

[19] IEEE: "An Architecture UMTS-WiMAX Interworking" [en línea]. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?isnumber=34792&arnumber=1662289&count=28&index=21 [Consulta: Diciembre 2006].

[20] Intel: "Understanding WiMAX and 3G for Portable/Mobile Broadband Wireless" [en línea] http://www.itr-rescue.org/bin/pubdocs/mtg-weekly/9-16-05%20Intel_WiMAX_White_Paper%20(Hassib).pdf [Consulta: Octubre 2006].

[21] ITU, Unión Internacional de Telecomunicaciones: "Informe sobre el Desarrollo de las Telecomunicaciones 2003: Indicadores de acceso para la sociedad de la información" [en línea]. http://www.itu.int/ITU-D/ict/publications/wtdr_03/material/WTDR03Sum_s.pdf [Consulta: Septiembre 2006].

[22] ITU, Unión Internacional de Telecomunicaciones: "Informe sobre el Desarrollo de las Telecomunicaciones 2006: Evaluación de las TIC para el desarrollo económico y social" [en línea]. http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-WTDR-2006-SUM-PDF-S.pdf [Consulta: Septiembre 2006].

[23] KORHONEN, Juha: "Introduction to 3G Mobile Communications", Artech House, 2003.

[24] LARRABEITI, David; MORENO, José; SOTO, Ignacio: "Protocolos de Señalización para el transporte de Voz sobre redes IP" [en línea]. http://www.it.uc3m.es/~jmoreno/articulos/protocolssenalizacion.pdf [Consulta: Octubre 2006].

[25] LEIVA, Nicolás: "Comparación de Estructuras de Costo de Sistemas de Telefonía sobre IP y Tradicional". Memoria de Título para optar a la Carrera de Ingeniero Civil Electricista. Santiago, Chile. Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, 2006.

[26] LÓPEZ, Priscila: "Comparativa de Tecnologías Emergentes de Acceso a Redes Móviles y Fijas". Memoria de Título para optar a la Carrera de Ingeniero Civil Electricista. Santiago, Chile. Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, 2007.

[27] Lucent Technologies: "The WiMAX Option for Delivering Converged Services"

[28] MONTIEL, Alejandro: "Historia de la Telefonía Inalámbrica" [en línea]. http://alejovzla.tripod.com/sitebuildercontent/sitebuilderfiles/HistoriaTelefoniaCelular.pdf [Consulta: Octubre 2006].

[29] NAVEAS, Pablo: "Telefonía IP: sus características y protocolos utilizados" [en línea]. http://profesores.elo.utfsm.cl/~agv/ipd438/2s03/projects/Protocols4Multimedia/Informes/Informe2.pdf [Consulta: Noviembre 2006].

[30] OLEXA, Ron: "Implementing 802.11, 802.16, y 802.20 Wireless Networks – Planning, Troubleshooting, and Operations", Elsevier Inc., 2005. ISBN: 0-7506-7808-9.

[31] PACHÓN, Álvaro: "Evolución de los sistemas móviles celulares GSM" [en línea]. http://dspace.icesi.edu.co/dspace/bitstream/item/408/1/apachon_gsm.pdf [Consulta: Octubre 2006].

[32] PAREKH, Shyam; LEE, Jiwoong: "EE228a – Lecture 6 – Spring 2006: IEEE 802.16 / WiMAX" [en línea]. http://walrandpc.eecs.berkeley.edu/228S06/L6.pdf [Consulta: Octubre 2006].

[33] POIKSELKÄ, Miikka; MAYER, Georg; KHARTABIL, Hisham; NIEMI, Aki: "The IMS – IP Multimedia Concepts and Services in the Mobile Domain", John Wiley & Sons Ltd, 2004. ISBN: 0-470-87113-X.

[34] SANDOVAL, Jorge: "Diapositivas del curso EL64E, Redes de Computadores", Departamento de Ingeniería Eléctrica, Universidad de Chile, 2006.

[35] SANTARELLI, Omar: "Convergencia Redes IP, Fijas y Móviles" [en línea]. http://ingenieros.cl/archivos_show.cfm?id=832 [Consulta: Septiembre 2006].

[36] SIP Working Group: "Management Information Base for the Session Initiation Protocol (SIP); draft-ietf-sip-mib-12.txt" [en línea]. http://www.ietf.org/internet-drafts/draft-ietf-sip-mib-12.txt [Consulta: Diciembre 2006].

[37] SUBTEL, Subsecretaría de Telecomunicaciones: "Informe Estadístico 10: Estadísticas de Desempeño del Sector de Telecomunicaciones en Chile: Junio 2004 – Junio 2005" [en línea]. http://www.subtel.cl/pls/portal30/docs/FOLDER/WSUBTEL_CONTENIDOS_SITIO/SUBTEL/ESTDEMERCADO/INFESTAD/INFESTAD2/INFO_ESTADISTICO_10_JUN.PDF [Consulta: Septiembre 2006].

[38] SUBTEL, Subsecretaría de Telecomunicaciones: "Series conexiones internet (Fecha Publicación 27 de diciembre de 2006) (Período Información Enero 2000 - Marzo 2006)" [en línea]. http://www.subtel.cl/servlet/page?_pageid=58&_dad=portal30&_schema=PORTAL30 [Consulta: Marzo 2006].

[39] WIKIPEDIA, La Enciclopedia libre [en línea]. http://www.wikipedia.org [Consulta: Octubre 2006 – Febrero 2007].

[40] WiMAX Forum: "Business Case Models for Fixed Broadband Wireless Access based on WiMAX Technology and the 802.16 Standard" [en línea]. http://www.wimaxforum.org/news/downloads/WiMAX-The_Business_Case-Rev3.pdf [Consulta: Diciembre 2006].

[41] WiMAX Forum: "Fixed, nomadic portable and mobile applications for 802.16-2004 and 802.16e WiMAX networks" [en línea]. http://www.wimaxforum.org/technology/downloads/Applications_for_802.16-2004_and_802.16e_WiMAX_networks_final.pdf [Consulta: Octubre 2006].

[42] WiMAX Forum: "Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation" [en línea]. http://www.wimaxforum.org/technology/downloads/Mobile_WiMAX_Part1_Overview_and_Performance.pdf [Consulta: Enero 2007].

[43] WiMAX Forum: "Mobile WiMAX – Part II: A Comparative Analysis" [en línea]. http://www.wimaxforum.org/technology/downloads/Mobile_WiMAX_Part2_Comparative_Analysis.pdf [Consulta: Diciembre 2006].

# Capítulo 9
# Anexos

## 9.1. Modelos de Referencia de Red

Dado el gran crecimiento de las redes de computadores desde su creación, el manejo e interoperación de dichas redes se fue volviendo cada vez más complejo. Con el objetivo de simplificar el diseño de las redes de telecomunicaciones y lograr una compatibilidad y comprensión más abiertos, éstas se dividen en un conjunto de niveles o capas que conforman la arquitectura de la red, entendiéndose por capa una entidad que realiza por sí sola una función específica.

Además de simplificar la comprensión de las redes y de permitir la interoperación entre estas, los modelos de capas permiten cambiar o agregar funcionalidades en una capa sin tener que cambiar las otras y simplifican la detección de fallas (troubleshooting).

Así, han surgido una serie de modelos de referencia, donde los más masificados son:

- Modelo OSI.
- Modelo TCP/IP.
- Modelo Jerárquico de Redes.

### 9.1.1. Modelo OSI

A finales de los 70's, la ISO (International Standards Organization) comenzó a desarrollar un modelo conceptual para la conexión de red llamado modelo OSI (Open Systems Interconnection Reference Model). En el año 1984, este modelo se convirtió en el estándar internacional de las comunicaciones entre redes.

Los principios aplicados para la división en capas son:

- Se debe crear una capa siempre que se necesite un nivel diferente de abstracción.
- Cada capa debe realizar una función bien definida.
- La función de cada capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente.

- Los límites de las capas deben elegirse a modo de minimizar el flujo de información a través de las interfaces.
- La cantidad de capas debe ser suficientes para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

El modelo OSI define en 7 capas los protocolos de comunicación. Los niveles inferiores se encargan de acceder al medio, mientras que los superiores, definen como las aplicaciones acceden a los protocolos de comunicación. Las dos únicas capas del modelo con las que, de hecho, interactúa el usuario son la primera capa, la capa Física, y la última capa, la capa de Aplicación. A continuación se explica brevemente la funcionalidad de cada capa.

#### 9.1.1.1.Capa Física

La capa física del modelo OSI es la encargada de las conexiones físicas de la computadora hacia la red, es decir en esta capa la información es manejada bit a bit sobre un medio de transporte.

La capa física estandariza el medio físico por los que viajará la información, características de materiales y eléctricas usadas en la transmisión, características funcionales de la interfaz, transmisión del flujo de bits a través del medio, administración de señales eléctricas y electromagnéticas. Un ejemplo de estas características son niveles de voltaje y disposición de pines.

#### 9.1.1.2.Capa de Enlace

Esta capa es la encargada de transmitir la información en "paquetes" denominados frames o tramas a un conjunto de terminales en una red local. Además, a partir de cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores.

Para cumplir su objetivo, algunas responsabilidades de esta capa son: estructurar frames, direccionamiento y mecanismo de acceso, crear y reconocer los límites de las tramas, resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. Además, esta capa debe incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.

Para poder transmitir los frames a un terminal dentro de la red local, cada terminal debe tener una dirección, que permita indicar cual es el o los destinatarios del frame. Un equipo que se caracteriza con esta capa en temas de redes es el switch.

#### 9.1.1.3.Capa de Red

La función de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Es decir, transmitir "paquetes de información" a estaciones, en otras redes locales (red Global).

La capa de red se encarga del funcionamiento de la subred de comunicaciones, enrutamiento de los "paquetes" (mediante una tabla de enrutamiento) y control de congestión, y la comunicación entre redes que no necesariamente utilizan el mismo protocolo en niveles inferiores.

Además, la capa de red estandariza la estructura de los paquetes, direccionamiento global y enrutamiento. El router es ejemplo de equipos que se manejan en esta capa.

#### 9.1.1.4.Capa de Transporte

La capa de transporte es la capa límite entre las capas de procesamiento de datos y el transporte de éstos. Su función es permitir el establecimiento, mantención y término de "canales" de comunicación o circuitos virtuales entre aplicaciones en estaciones remotas.

Entre las responsabilidades de la capa de transporte se encuentran el comunicar aplicaciones mediante la modalidad de intercambio de datagramas o el establecimiento de sesiones persistentes, identificar aplicaciones, estandarización de estructuras de datagramas, sesiones, identificadores de aplicación, mecanismos de establecimiento de sesiones y la multiplexación de mensajes provenientes de distintas aplicaciones.

#### 9.1.1.5.Capa de Sesión

La capa de sesión tiene la función de comunicar las aplicaciones, por medio de algún protocolo previamente acordado, por sobre las sesiones de capa transporte

Las tareas de esta capa son el control de la sesión a establecer entre el emisor y el receptor y control de la concurrencia y sincronización, la mantención de puntos de verificación (checkpoints) y la estandarizar los protocolos de comunicación entre aplicaciones.

#### 9.1.1.6. Capa de Presentación

El objetivo de esta capa es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas los datos lleguen de manera reconocible. En otras palabras, esta capa se encarga de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos.

Dentro de sus tareas, se encuentra que la información enviada por la capa de aplicación sea entendible y la verificación de la estructura semántica y sintaxis de los datos a enviar.

#### 9.1.1.7.Capa de Aplicación

La capa de aplicación corresponde a la capa más cercana al usuario, por lo que es la encargada de relacionar al usuario con la comunicación proporcionada por las capas inferiores. La capa de

aplicación contiene los programas del usuario, además que contiene los protocolos que se necesitan frecuentemente.

Además, la capa de aplicación define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros y que pueden emular terminales virtuales o ser utilizados para transferencia de archivos u otras labores.

En la Tabla 21, a continuación, se presentan algunos ejemplos de protocolos de redes de computadores ordenados según las capas del modelo OSI a las que pertenecen.

**Tabla 21: Ejemplos de Protocolos por Capas.**

| | |
|---|---|
| Capa 7: Aplicación | FTP, HTTP, Telnet, SNMP |
| Capa 6: Presentación | JPEG, MPEG, ASCII, MIDI, HTML, XML |
| Capa 5: Sesión | NFS, SQL |
| Capa 4: Transporte | UDP, TCP |
| Capa 3: Red | IP, IPX, OSPF |
| Capa 2: Enlace | MPLS, SNA |
| | Ethernet, Token Ring, LocalTalk, FDDI, X.21, X.25, Frame Relay, BitNet, CAN, ATM, Wi-Fi, HDLC, SDLC |
| Capa 1: Física | RS-232, RS-449, EIA-422, EIA-485, V.21-V.23, V.90 |
| | Códigos NRZ, Codificación Manchester, Cable coaxial, Par trenzado,10Base2, 10BASE5, 10BASE-T, 100BASE-TX, PDH, SDH, T-carrier, E-carrier, SONET, DSSS, FHSS |

### 9.1.2. Modelo TCP/IP

El modelo TCP/UDP fue desarrollado por la Agencia de Investigación de Defensa de los Estados Unidos (ARPA o DARPA) de forma que la principal característica de esta red fuera ser funcional para cualquier tecnología de red y ser robusta a la pérdida de algún nodo causada por ataques nucleares.

Así, DARPA creó el grupo de protocolos de TCP/IP (stack TCP/IP), cuyo nombre está compuesto por las siglas de los dos estándares principales: Transmission Control Protocol (TCP) e Internet Protocol (IP). Este modelo hace posible la comunicación entre un par de terminales en cualquier lugar del mundo.

El modelo TCP/IP está basado en el modelo OSI; sin embargo, posee menos capas agrupando funcionalidades en algunas de sus capas. Es importante mencionar que el modelo TCP/IP no específica protocolos en la capa de hardware, por lo que éstos dependerán de la arquitectura de red física utilizada. En la Figura 84 se observa un paralelo entre las capas de ambas arquitecturas.

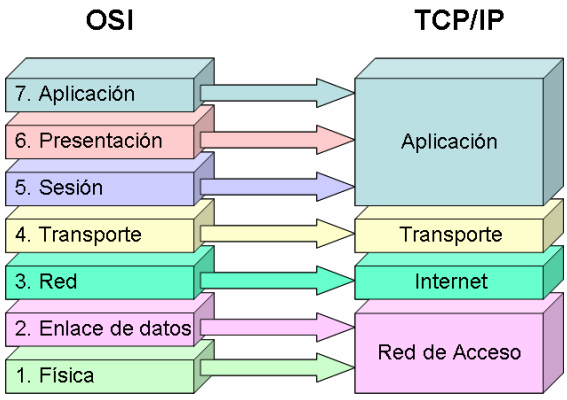



**Figura 84: Comparación entre el Modelo OSI y TCP/IP.**

#### 9.1.2.1. Capa de Internet

Es una capa orientada hacia un servicio sin conexión de forma que se puedan ingresar paquetes a la red sin importar su destino. Su función es, por tanto, enrutar los paquetes de información a su destino a través de los distintos nodos de red.

La capa de Internet, por tanto, no es confiable y posee una política de mejor esfuerzo (best effort), el protocolo oficial de esta capa es el protocolo IP (Internet Protocol).

#### 9.1.2.2. Capa de Transporte

En esta capa se realiza una comunicación punto a punto entre emisor y receptor. El modelo TCP/IP utiliza para esto dos tipos de protocolos:

- TCP (Transmission Control Protocol): Implementa servicios orientados a la conexión, confiables y con control de flujo.
- UDP (User Datagram Protocol): Implementa servicios no orientados a la conexión ni confiable.

#### 9.1.2.3. Capa de Aplicación

En esta capa corren los protocolos que prestan servicios específicos al usuario. Algunos ejemplos de estos protocolos son: TELNET, FTP, HTTP, etc.

### 9.1.3. Modelo Jerárquico de Red

El modelo jerárquico de red, propietario de Cisco, es un diseño de 3 capas cuya finalidad es la simplificación del diseño, planificación y operación de las redes. En la Figura 85 se aprecia un diagrama con las capas del modelo jerárquico.

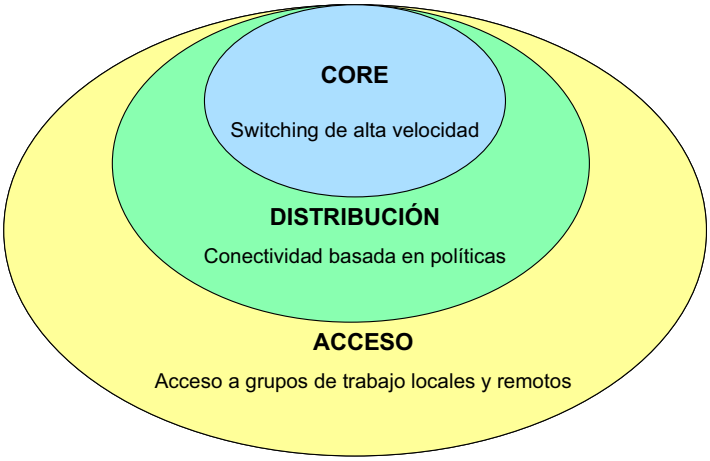



**Figura 85: Modelo Jerárquico de Red.**

#### 9.1.3.1.Capa Core

La capa Core, es la capa que transporta la mayor cantidad de tráfico, por lo que corresponde al backbone de una red. Para cumplir con su función debe tener una serie de características como son la alta velocidad de transmisión de datos, alta confiabilidad (como lo pueden ser redes redundantes) y baja latencia (este último punto, es muy importante el tiempo de convergencia y adaptabilidad de los protocolos de enrutamiento). La capa Core, por lo general es transparente al usuario final.

#### 9.1.3.2.Capa de Distribución

La capa de distribución corresponde a la capa de servidores y es la interfaz de acceso entre las capas Core y Acceso. Dentro de sus funciones se encuentra el enrutamiento, filtrado, políticas, seguridad, enrutamiento entre VLANs y separación entre protocolos de enrutamiento estáticos y dinámicos.

#### 9.1.3.3.Capa de Acceso

Como lo indica el nombre, esta capa provee acceso a los recursos de parte de los usuarios y se caracteriza por ser conmutada y compartir el ancho de banda. La capa de acceso segmenta la red, conecta a los usuarios a la LAN y aísla de broadcast a los servidores.

## 9.2. Arquitecturas de Redes de Telefonía (Continuación)

### 9.2.1. GSM

#### 9.2.1.1.Protocolos Utilizados

En la Figura 86 se observa la pila de protocolos existentes entre las entidades MS (estación móvil), BTS, BSC y MSC.

En esta figura se observan tres capas de protocolos que coinciden con la capa de red, en el modelo OSI:

- CM (Connection Management): Responsable de la gestión de las llamadas (establecer, mantener y terminar llamadas) a solicitudes de los usuarios.
- MM (Mobility Management): Responsable del mantenimiento de la información de localización del usuario.
- RR (Radio Resource Management): Responsable del establecimiento y mantenimiento del enlace entre el MS y el MSC.

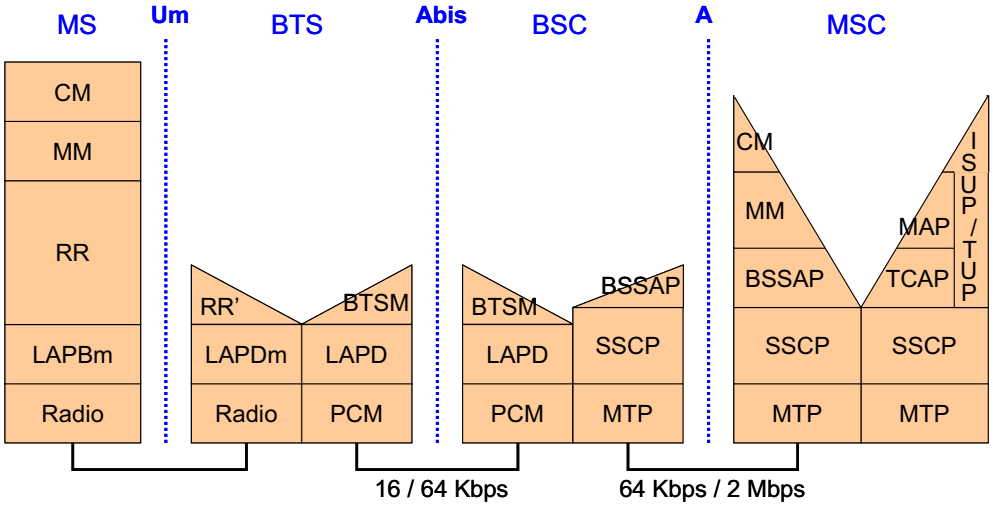



**Figura 86: Pila de Protocolos utilizados en GSM.**

Además de estas capas se encuentran las siguientes:

- RR': Parte de la funcionalidad de RR administrada por el BTS.
- LAPD y LAPDm (Link Access Protocol on Dm Channel): Coinciden con la capa de enlace del modelo OSI.
- BTSM (Base Transceiver Station Management): Responsable de transferencia de información de capa RR al BSC.
- SCCP (Signalling Connection Control Part): Forma parte de la señalización SS7.
- MTP (Message Transfer Part): Junto con SCCP, forma parte de la señalización SS7 y es responsable de la seguridad de la transmisión entre el BSC y MSC.
- BTSM (BTS Management).
- BSSAP (Base Station System Application Part): Recibe los mensajes RR para enviarlos a la MSC.
- TCAP (Transaction Capabilities Application Part): Se utiliza para transmitir información en tiempo real entre MSC, HLR y VLR.
- MAP (Mobile Application Part): Define la capa de aplicación, protocolos de señalización, procesos para registrar usuarios móviles y manejo de handoff entre sistemas celulares.
- ISUP (ISDN Part User).
- TUP (Telephone User Part).

### 9.2.1.2.Canales Físicos y Lógicos

Los canales físicos en GSM corresponden a los time-slots antes mencionados. Sin embargo, estos canales físicos pueden transmitir dos tipos de información o "canales lógicos":

- Canal de tráfico o TCH (Traffic Channel): transporta la información de voz o datos.
- Canal de control o CCH (Control Channel): transporta información de señalización.

En la Tabla 22 se observa cada uno de estos canales.

**Tabla 22: Canales Lógicos en GSM.**

<table>
<tr><th>Tipo de canal</th><th colspan="2">Denominación</th><th>Descripción</th></tr>
<tr><td rowspan="7">Canales de Tráfico (TCH)</td><td colspan="2">TCH/FS</td><td rowspan="7">S: Voz (Speech)<br>9.6: Datos a 9600 bps.<br>4.8: Datos a 4800 bps.<br>2.4: Datos a 2400 bps.<br>F: Full Rate. La información de un usuario se envía en una ranura de tiempo, en cada trama.<br>H: Half Rate. La información de un usuario se envía en una ranura de tiempo, trama de por medio. Dos usuarios comparten una misma ranura en diferentes instantes de tiempo.</td></tr>
<tr><td colspan="2">TCH/F9.6</td></tr>
<tr><td colspan="2">TCH/F4.8</td></tr>
<tr><td colspan="2">TCH/F2.4</td></tr>
<tr><td colspan="2">TCH/HS</td></tr>
<tr><td colspan="2">TCH/H4.8</td></tr>
<tr><td colspan="2">TCH/H2.4</td></tr>
<tr><td rowspan="9">Canales de Control (CCH)</td><td rowspan="3">Canales de Broadcast BCH (Broadcast Channels)</td><td>BCCH</td><td rowspan="3">Utilizados para permitir el enganche de los móviles y el monitoreo de las potencias de los móviles en celdas vecinas (MAHO).</td></tr>
<tr><td>FCCH</td></tr>
<tr><td>SCH</td></tr>
<tr><td rowspan="3">Canales Comunes de Control CCCH (Common Control Channels)</td><td>PCH</td><td rowspan="3">Permiten el establecimiento de las llamadas y la asignación de canales de control.</td></tr>
<tr><td>RACH</td></tr>
<tr><td>AGCH</td></tr>
<tr><td rowspan="3">Canales de Control Dedicados DCCH (Dedicated Control Channels)</td><td>SDCCH</td><td rowspan="3">Canales bidireccionales utilizados para señalización y supervisión al usuario.</td></tr>
<tr><td>SACCH</td></tr>
<tr><td>FACCH</td></tr>
</table>

### 9.2.1.3.Interfaces entre Entidades Funcionales

En la Tabla 23 se encuentran listadas las diferentes interfaces de la arquitectura GSM.

**Tabla 23: Interfaces en GSM.**

| Interfaz | Se ubica entre | Descripción | Intercambio de Información | |
|---|---|---|---|---|
| | | | Tráfico Usuario | Protocolo Señalización |
| **A** | MSC – BSC | Permite el intercambio de información sobre la administración del BSS, de las llamadas y de la movilidad. A través de ella, se negocian los circuitos que serán utilizados entre el BSS y el MSC. | Si | SS7 |
| **Abis** | BSC – BTS | Permite el control del equipo de radio. | Si | LAPD |
| **B** | VLR – MSC (asociados) | Permite al MSC acceder a información sobre algún cliente que se encuentre en el área de influencia de dicho MSC en el VLR. Esta interfaz NO debe ser externa (por desempeño, por el volumen de información intercambiado). | No | MAP/B |
| **C** | HLR – MSC | Utilizada por los GMSC para enrutar la llamada hacia el MSC destino. | No | MAP/C |
| **D** | HLR – HLR | Permite intercambiar información entre ambas HLRs, esta información se encuentra relacionada con la posición del móvil y la gestión del servicio contratado por el usuario. | No | MAP/D |
| **E** | MSC – MSC | Permite el intercambio entre MSCs cuando el móvil cambia de área de influencia de un MSC a otro. | Si (64 Kbps) | MAP/E, RDSI, ISUP |
| **F** | MSC – EIR | Utilizada cuando el MSC desea comprobar el IMEI de un equipo. | No | |
| **G** | VLR – VLR | Permite la interconexión entre dos VLRs de diferentes MSCs | No | MAP/G |
| **H** | HLR – AuC | Permite la comunicación entre las bases de datos HLR y AuC | Si | MAP/H |
| **I** | MSC – MS | Permite el intercambio transparente de datos entre el MSC y el MS a través del BSS. | | |
| **Um** | BSS – MS | Interfaz de radio, se encuentra entre la estación móvil y el BSS. | Voz: 13 Kbps<br>Datos: 9,6 Kbps | LAPDm |

## 9.2.2. GPRS

### 9.2.2.1. Protocolos Utilizados

La pila de protocolos utilizados en la arquitectura GPRS puede dividirse en dos partes: protocolos de transmisión y protocolos de señalización. A continuación se explicará cada una de estas partes.

El plano de transmisión se encarga de la transmisión de datos del usuario junto con la señalización para el control de flujo, detección y corrección de errores. En la Figura 87 se muestra la pila de protocolos de transmisión entre las entidades MS, BSS, SGSN y GGSN.

A continuación se explican algunos de los protocolos más importantes de la pila de transmisión:

- GTP (GPRS Tunneling Protocol): Responsable del transporte de los datos de usuario y la señalización entre los nodos de GSN. Sus paquetes contienen los paquetes IP o X.25 del usuario.
- SNDCP (Subnetwork Dependent Convergence Protocol): Responsable de transportar los paquetes de datos entre los SGSN y el MS. Se encarga de la multiplexación de varias conexiones de la capa de red en una conexión lógica virtual de la capa LLC.
- RLC/MAC: Estos protocolos actúan en la interfaz de aire y permiten la multiplexación multiusuario en los canales de datos compartidos.
- LLC (entre MS y SGSN): Corresponde a parte de la capa de enlace y se encarga del control de secuencia, de flujo, entrega en orden y detección de errores. Se puede interpretar como una adaptación del protocolo LAPDm de GSM.

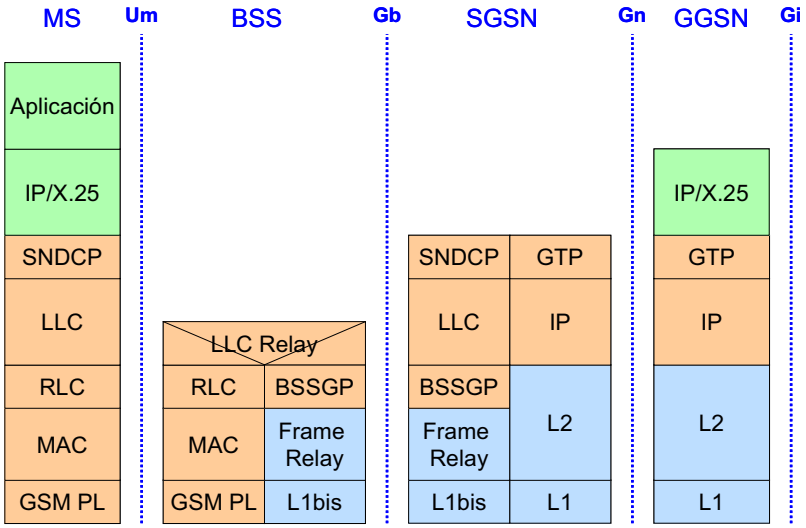



**Figura 87: Pila de Protocolos de transmisión utilizados en GPRS.**

En cuanto a la pila de protocolos de señalización de GPRS, en la Figura 88 se observan los respectivos protocolos entre el MS, BSS y SGSN.

Esta pila incluye los protocolos relacionados con el control y mantenimiento de las funciones del plano de transmisión, conexión, activación y localización de recursos de la red, entre otros.

La nueva capa que aparece corresponde a GMM/SM (GPRS Mobility Management / Session Management) y que se encarga de la movilidad y la gestión de sesión mientras se realizan las funciones de seguridad y otros.

Ahora, la interacción del SGSN con las bases de datos HLR, VLR y EIR se produce a través de los mismos protocolos utilizados en GSM.

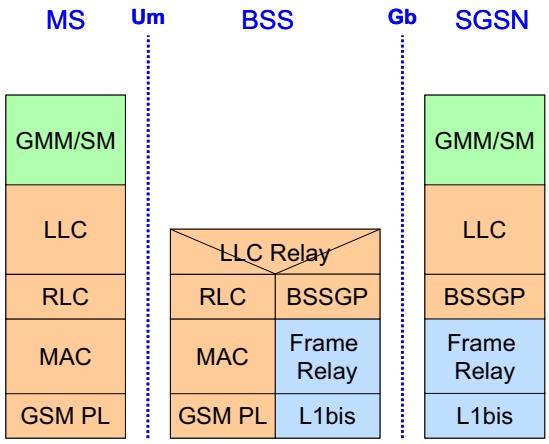



**Figura 88: Pila de Protocolos de Señalización utilizados en GPRS.**

### 9.2.2.2. Canales Físicos y Lógicos

Al igual que GSM, GPRS divide sus canales físicos en canales lógicos de tráfico y señalización. La Tabla 24 muestra los canales físicos y lógicos aportados GPRS a la arquitectura celular de GSM.

**Tabla 24: Canales Físicos y Lógicos agregados por GPRS.**

| Tipo de canal | Denominación | | Descripción |
|---|---|---|---|
| Canales Físicos | Canales de Paquetes de Datos PDCH (Packet Data CHannel) | Canales PDCH dedicados | Son asignados exclusivamente para el servicio GPRS. |
| | | Canales PDCH bajo demanda | Son utilizados para GPRS si no son necesarios para GSM. |
| Canales Lógicos | Canales de control común | Packet Paging Channel: PPCH | Utilizado para localizar una estación móvil antes de la transferencia de paquetes. |
| | | Packet Random Access Channel: PRACH | Utilizado por la estación móvil para solicitar canales para GPRS. |
| | | Packet Access Grant Channel: PAGCH | Utilizados para comunicar a la estación móvil los canales de tráfico asignados. |
| | Canales de difusión | Packet Broadcast Control Channel: PBCCH | Utilizado para difundir información de control general del sistema GPRS. |
| | Canales de tráfico | Packet Data Traffic Channel: PDTCH | Usado para la transferencia de paquetes de datos. |
| | Canales dedicados de control | Packet Associated Control Channel: PACCH | Canal de señalización asociado con un canal de tráfico PDTCH. Permite transferir el nivel de potencia e información del sistema. |
| | | Packet Timing Control Channel- PTCCH. | Utilizado para el envío de información relacionada con el avance del tiempo. |

#### 9.2.2.3. Interfaces entre Entidades Funcionales

En la Tabla 25 se muestran las nuevas interfaces introducidas por GPRS y las entidades funcionales que une cada una de estas interfaces.

**Tabla 25: Interfaces en GPRS.**

| Interfaz | Descripción |
|---|---|
| Ga | Interfaz entre los nodos GSN (GGSN, SGSN) y el Gateway CG (Charging Gateway) |
| Gb | Interfaz entre el SGSN y la BSS; normalmente usa Frame Relay |
| Gc | Interfaz entre el GGSN y el HLR |
| Gi | Interfaz entre la red GPRS (GGSN) y alguna red de paquetes de datos externa (PDN: Packet Data Network) |
| Gn | Interfaz entre dos nodos GSN (por ejemplo entre GGSN y SGSN); éste se conecta con el backbone de una red interna |
| Gp | Interfaz entre dos nodos GSN en diferentes PLMNs; esto a través de un gateway de borde |
| Gr | Interfaz entre el SGSN y el HLR |
| Gs | Interfaz entre el SGSN y el MSC/VLR |
| Gf | Interfaz entre el SGSN y el EIR |

### 9.2.3. UMTS

#### 9.2.3.1. Clases de Servicio en UMTS

**Tabla 26: Clases de Servicios en UMTS.**

| Clase de Servicio | Naturaleza | Características Básicas | Ejemplos |
|---|---|---|---|
| Conversacional | Servicios de tiempo real | Mantener un retardo pequeño y constante al igual que la variación de tiempo entre paquetes. | Voz, videoteléfono |
| Streaming | Servicios de tiempo real | Mantener la variación de tiempo entre paquetes. Retardo constante, no necesariamente muy pequeño. | Streaming de video o audio |
| Interactivo | Servicios de tiempo no real | Modelo de petición y respuesta. Mantiene el contenido de los datos. Retardo moderado y bajas tasas de error. | Navegación en Internet |
| Diferido (Background) | Servicios de tiempo no real | No se necesita interacción. Mantiene el contenido de los datos. | Correo electrónico, descarga de datos. |

### 9.2.3.2. Protocolos Utilizados

A continuación se presentarán en forma breve los protocolos utilizados en UMTS, tanto en el plano de usuario como el de control o señalización. En la Figura 89 y Figura 90 se muestran los protocolos de correspondientes a cada plano entre el UE, Nodo B, RNC y MSC. Ahora, se debe tener en cuenta que los protocolos en cada pila es un ejemplo que puede ir variando a distintos protocolos específicos dependiendo del tipo de canal.

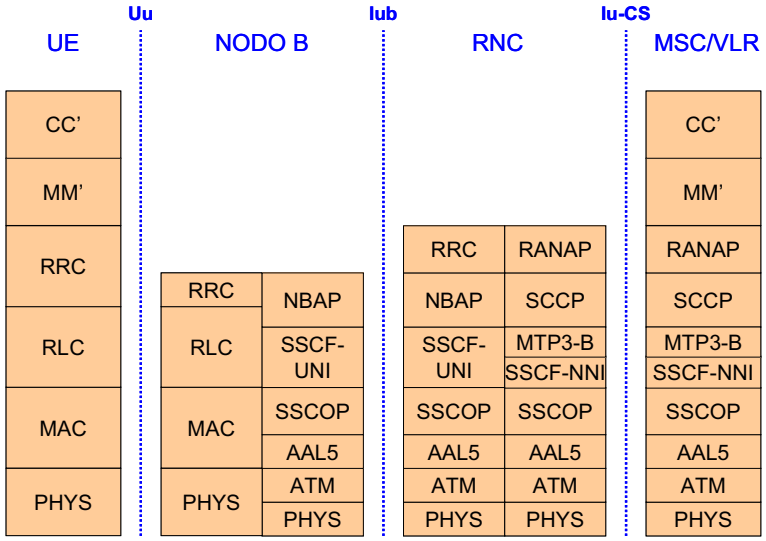



**Figura 89: Pila de Protocolos del Plano de Señalización utilizados en UMTS.**

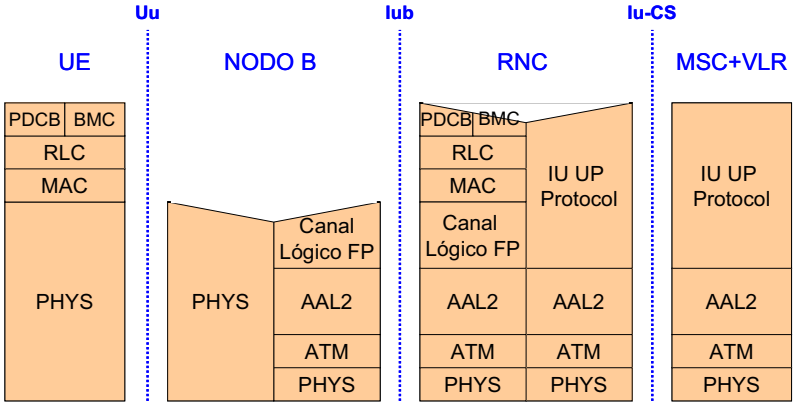



**Figura 90: Pila de Protocolos del Plano de Usuario utilizados en UMTS.**

- ATM (Asynchronous Transfer Mode): Protocolo utilizado en el transporte en el Core de la red, se basa en la multiplexación de división de tiempo asíncrona de paquetes de datos de largo fijo.
- AAL2 y AAL5 (ATM Adaptation Layer): Su función es procesar los datos de capas superiores para la transmisión en ATM. Es decir, segmenta los datos a enviar y reensambla los datos recibidos. AAL2 se encarga de la transmisión de flujos de datos en tiempo real con velocidades variables y AAL5 se encarga de la transmisión de flujos de datos con velocidades variables sin necesidad de cumplir con tiempo real.

- Iu UP (User Plane) Protocol: retransmite los datos de usuario desde la UTRAN al CN y viceversa.
- Capa de Adaptación de Usuario SS7 MTP3: También llamada M3UA, soporta el transporte de cualquier señalización SS7 MTP3-U (en el caso de la UTRAN, será SCCP) utilizando los servicios de SCTP (Stream Control transmisión Protocol).
- MAP: Corresponde a un conjunto de protocolos utilizados por los elementos del CN para su comunicación mutua.
- MTP (Message Transfer Part): Se encarga del enrutamiento de mensajes, discriminación y distribución, administración del enlace de señalización y distribución de carga.
- NBAP (Node B Application Part): Usado por el RNC para administrar al Nodo B a través de la interfaz Iu. Dentro de sus funciones está la administración de la configuración de celda, del canal de transporte, información de sistema, enlace de radio, medidas y recursos dedicados, corrección de potencia entre otros.
- Capa Física (PHYS): El estándar ATM no indica ningún medio físico específico. La capa física en la interfaz Iu consta de dos sub-capas: PMD (Physical Media Dependent) y TC (Transmission Convergence).
- ALCAP (Access Link Control Application Part): Llamada genéricamente Q.2630.1, es utilizado para establecer conexiones del plano de usuario a través del dominio CS. También se conoce como protocolo de señalización AAL2.
- Q.2150.1: Corresponde a un convertidor entre los protocolos ALCAP y MTP3-B.
- RANAP (Radio Access Network Application Part): Entrega el servicio de señalización entre la UTRAN y el CN. RANAP posee tres tipos de servicios: Servicios de control general (referidos a toda la interfaz Iu), servicios de notificación (referido a UEs específicos o a todos los UEs dentro de un área) y servicios de control dedicado (referidos a un sólo UE).Además, el transporte de señalización cuenta con dos tipos de servicio: transferencia de datos orientada a la conexión y transferencia de datos no orientada a la conexión. Dentro de las funciones del protocolo RANAP está la reubicación del RNC que está sirviendo, liberación de los recursos de todas las conexiones Iu, control de sobrecarga en la interfaz Iu, reseteo de la Iu, reporte de las situaciones generales de error, entre otros.
- RNSAP (Radio Network Subsystem Application Part): Especifica los procedimientos de señalización en la red de radio entre dos RNCs. Dentro de los servicios de RNSAP están los procedimientos básicos de movilidad, procedimientos globales, administración y supervisión del enlace de radio, reconfiguración del canal físico, entre otros.
- SSCF (Service-Specific Coordination Function): Mapea los requerimientos de capas superiores a requerimientos de SSCOP.
- SSCOP (Service-Specific Connection-Oriented Protocol): Define mecanismos para establecer conexiones y liberarlas, e intercambio de la información de señalización entre entidades de señalización.
- SCCP (Signaling Connection Control Part): Posee dos clases de mensajes, la clase 0 provee servicios no orientados a la conexión y la clase 2, servicios orientados a la conexión.
- SCTP (Stream Control Transmission Protocol): Permite transmitir varios protocolos de señalización sobre redes IP.

### 9.2.3.3. Canales Físicos y Lógicos

En la Tabla 27, a continuación, se presentan los canales lógicos y físicos definidos en UMTS.

**Tabla 27: Canales Físicos y Lógicos utilizados en UMTS.**

| Tipo de Canal | Nombre | Sentido | Tipo | Descripción |
|---|---|---|---|---|
| Canales Lógicos | BCCH | Downlink | Control | Difusión de información de la red |
| | PCCH | | | Aviso a móviles no localizados |
| | CCCH | | | Señalización con móviles sin conexión RRC |
| | DCCH | | | Señalización con un móvil específico |
| | DTCH | | Tráfico | Transferencia de información con un móvil específico |
| | CTCH | | | Transferencia de información punto-a-multipunto |
| Canales de Transporte | BCH | Downlink | Común | Difusión de información de la red y la celda |
| | FACH | | | Envío de información a móviles cuya ubicación es conocida |
| | PCH | | | Envío de información a móviles cuya ubicación NO es conocida |
| | DSCH | | | Asignación de recursos |
| | RACH | Uplink | Común | Acceso aleatoria de los móviles |
| | CPCH | | | Transmisión de paquetes sin asignación exclusiva. |
| | DCH | Bidireccional | Dedicado | Transmisión de información y señalización en un móvil específico |
| Canales Físicos | P-CCPCH | Downlink | Común | Soporta el canal BCH |
| | S-CCPCH | | | Soporta los canales FACH y el PCH |
| | PDSCH | | | Soporta el canal DSCH |
| | PRACH | Uplink | Común | Soporta el canal RACH |
| | PCPCH | | | Soporta el canal CPCH |
| | DPDCH | Bidireccional | Dedicado | Tráfico de datos del DCH |
| | PDCCH | | | Tráfico de señalización del DCH |

### 9.2.3.4. Interfaces entre Entidades Funcionales

UMTS define cuatro nuevas interfaces además de las definidas en GPRS. Estas interfaces se muestran en la Tabla 28.

**Tabla 28: Interfaces en UMTS.**

| Interfaz | | Situada entre |
|---|---|---|
| Uu | | Equipo de Usuario (UE) y Nodo B |
| Iu | Iu-CS | Interfaz para Conmutación de Circuitos (RNC-MSC/VLR) |
| | Iu-PS | Interfaz para Conmutación de Paquetes (RNC-SGSN) |
| Iub | | RNC a Nodo B |
| Iur | | RNC a RNC (No tiene equivalencia en GSM). |

## 9.2.4. PacketCable

### 9.2.4.1. Arquitectura (Continuación)

#### 9.2.4.1.1. Borde (Edge)

Dentro del bloque de borde se encuentras las siguientes entidades funcionales:

- P-CSCF (Proxy CSCF): Esta entidad cumple la misma función que el P-CSCF de IMS (descrito en la sección 2.6.2.3.1). El UE accede a la infraestructura SIP a través del P-CSCF. El P-CSCF protege la red SIP de los detalles de protocolos específicos de la red de acceso (como QoS) y permite que la infraestructura sea escalable a través de la manipulación de ciertos recursos de tareas intensivas cuando se interactúa con el UE.
- Servidores STUN y STUN Relay: Un Servidor STUN es una entidad que recibe requerimientos STUN, y envía respuestas STUN. Los requerimientos STUN son típicamente requerimientos vinculantes usados para determinar los vínculos asignados por los NATs. El UE envía un requerimiento de vinculación al servidor sobre UDP. El servidor examina la dirección IP y el puerto fuente del requerimiento, y los copia dentro de una respuesta, la que es enviada de vuelta al UE.

  La red PacketCable emplea tres servidores STUN, uno como componente funcional del P-CSCF (no ilustrado en la Figura 33) y dos más como servidores STUN autónomos:

  - El servidor STUN como componente funcional dentro del P-CSCF es utilizado por los UEs SIP para mantener los vínculos NAT para la señalización. Estos mensajes STUN también actúan como keepalives, permitiendo al UE determinar la disponibilidad del P-CSCF y detectar reinicios del NAT.
  - El servidor STUN mostrado en la Figura 33 se usa para determinar una de las posibles direcciones de media candidatas a través del protocolo STUN.
  - El servidor STUN Relay es una entidad que recibe requerimientos STUN de ubicación, y envía respuestas STUN. Es servidor es capaz de actuar como un relay de datos, recibiendo datos en la dirección proveída a los UE, y reenviándola a los UE. Esta funcionalidad permite que los datos multimedia atraviesen NATs para los casos en otras técnicas de atravesamiento de NATs resulten insuficientes.

- Administrador de Aplicación PacketCable: El Administrador de Aplicación PacketCable es responsable de variadas tareas. La más importante de ellas es determinar los recursos de QoS necesarios para una sesión basado en los descriptores de sesión recibidos y administrar los recursos de QoS asignados para una sesión.

  Determinar los recursos de QoS para una sesión implica interpretar el descriptor de sesión y calcular el ancho de banda necesario, determinando el tipo de programación de tráfico, y trasladar los clasificadores de tráfico. Esto también implica determinar el número de flujos necesarios para la sesión (sólo voz vs. voz y video) y administrar la asociación de los flujos a la sesión.

#### 9.2.4.1.2. Core

El Core de PacketCable, como se observa en la Figura 33, está conformado por entidades cuyas funciones son las mismas descritas para la arquitectura IMS. Estas entidades son:

- S-CSCF (Serving CSCF): Descrito en la sección 2.6.2.3.3.
- I-CSCF (Interrogating CSCF): Descrito en la sección 2.6.2.3.2.
- HSS (Home Subscriber Server): Descrito en la sección 2.6.2.2.
- SLF (Subscription Locator Function): Descrito en la sección 2.6.2.4.

#### 9.2.4.1.3. PacketCable Multimedia

PacketCable Multimedia define una plataforma basada en IP para entregar servicios multimedia con QoS mejorada sobre redes de acceso DOCSIS 1.1 (o superior). Esta plataforma permite que las capacidades del Core de PacketCable (por ejemplo autorización de QoS y control de admisión, mensajes de evento para la cobranza y seguridad) para soportar un amplio rango de servicios IP, más allá de la telefonía. Así, mientras el CMS PacketCable es óptimo para brindar servicios de telefonía residencial, los componentes de PacketCable Multimedia ofrecen una plataforma de servicios IP que requieren un método de QoS.

La arquitectura PacketCable Multimedia define la interacción entre un CMTS, Servidor de Políticas y Administración de Aplicación. A continuación se describe el Servidor de Políticas:

- Servidor de Políticas: El Servidor de Políticas actúa principalmente como un intermediario entre Administrador(es) de Aplicación y CMTS(s) para la administración de sesión de QoS. Éste aplica políticas de red a los requerimientos del Administrador de Aplicación y actúa como proxy para los mensajes entre el Administrador de Aplicación y el CMTS.

#### 9.2.4.1.4. Aplicación

- AS (Servidor de Aplicación): Un AS provee servicios con aplicaciones específicas. Un AS puede influenciar una sesión SIP basado en los servicios soportados. También puede realizar el papel de Host y ejecutar servicios. Además puede iniciar o terminar servicios en nombre de un usuario.
- Servidor de Presencia: Corresponde a un servidor de aplicación especializado. Actúa como el punto focal para la conexión de fuentes de información de presencia y las partes interesadas.

#### 9.2.4.1.5. Interconexión

- Elemento de Borde: Se interconecta con las redes que pueden ser soportadas a través de un elemento de borde. El elemento de borde contiene una función Proxy de Interconexión y puede contener una función Media Proxy. La funcionalidad Proxy de Interconexión incluye interoperación de protocolos, aplicaciones de registro SIP, servicios de seguridad, administración de direcciones IP, interoperación con redes IPv4 e IPv6.

  PacketCable no define requerimientos funcionales específicos que el Elemento de Borde deba soportar, sino que cada operador determina los requerimientos de éste de acuerdo a sus necesidades.
- BGCF (Breakout Gateway Control Function): Provee la selección de red para enrutamiento a la PSTN y dentro de su propia red determina cual MGC se utilizará para conectarse a la PSTN.
- PSTN GW (Gateway PSTN): Está formado por el SG (Signaling Gateway, que realiza la conversión de señalización a nivel de la capa de transporte entre SS7 y transporte basado en IP), MGC (Media Gateway Controller, que realiza la conversión de protocolos entre mensajes SS7 ISUP y protocolos PacketCable) y el MG (Media Gateway, que realiza la conversión de los canales portadores entre la red conmutada y la de PacketCable, basada en flujos RTP).
- CMS (Call Managment Server): Entrega soporte a los servicios de telefonía para clientes con señalización de llamadas de red (como los E-MTAs). Entrega la mayor parte de las cualidades de la telefonía mientras actúa directamente con los servidores de aplicación para entregar aplicaciones adicionales a los E-MTAs. Además, el CMS se comunica con los CSCFs como un igual.

### 9.2.4.2.Sistemas de Soporte Operacional

Se espera que la red PacketCable posea los siguientes servidores como parte del Sistema de Soporte Operacional:

- Servidor DHCP (Dynamic Host Configuration Protocol): Se utiliza un servidor DHCP cuando la red local del UE esté bajo el control del Proveedor de Servicios. Éste entrega información de participación de la red IP. Los UEs en ambientes que no estén bajo el control del proveedor de Servicios puede no ser capaz de utilizar los servicios del DHCP, en esos casos se asume que la información de participación de la red IP es entregada al UE por la red local.
- Servidor DNS (Domain Name System): Se utiliza para resolver entidades DNS a direcciones de red y viceversa.
- Servidor ENUM: Se utiliza para almacenar y traducir números E.164 a SIP URIs o Registros NS (Name Server) apuntando al Servidor de Nombre para el operador con la delegación de ese número E.164 específico.
- Elemento PAC (Provisioning, Activation, and Configuration): Es la componente responsable de aprovisionamiento, activación y configuración de los UEs. es la responsable de mantener la información de configuración del UE. Los datos de configuración contienen la información necesaria para que un UE entregue servicios. También es el elemento que comunica los cambios en la configuración de la red al usuario o viceversa.

- EMS y NMS (Element Management y Network Management Systems): Un EMS o NMS relaciona a una o más entidades asociadas con el monitoreo y administración de elementos de red específicos o de una red completa, respectivamente.
- Servidor de Tiempo: Usado por los UEs para obtener el tiempo.
- CDF/CGF (Charging Data Function / Charging Gateway Function): El CDF recibe eventos de cobranza de los distintos elementos de la red PacketCable. Así, puede utilizar la información contenida en los CDRs. Los CDRs producidos por el CDF son transferidos al CGF, el que actúa como un gateway al Sistema de Soporte de Cuentas.

### 9.2.4.3.Principales Protocolos

Dentro de los protocolos utilizados por PacketCable se encuentran:

- RTP (Real Time Protocol) y RTCP (Real Time Control Protocol).
- TGCP (PSTN Gateway Call Signaling Protocol), que es una extensión MGCP para Media Gateways.

Uno de los protocolos más importantes para el funcionamiento de PacketCable corresponde al protocolo DOCSIS, el se describe brevemente a continuación.

DOCSIS® corresponde a un estándar internacional creado por CableLabs® que define los requerimientos de interfaz para cable módems utilizados para la distribución de datos de alta velocidad sobre sistemas de red de televisión por cable. Se han adoptado distintas variantes de las versiones de DOCSIS dependiendo de los sistemas de bandas que utilice cada país para la televisión por cable.

DOCSIS provee una gran variedad de opciones en la capa física PHY y la capa de Control de Acceso al Medio MAC (correspondientes a las capas 1 y 2 del modelo OSI respectivamente),

- Capa PHY: DOCSIS 1.0 y 1.1 especifica canales de ancho entre 200 KHz y 3,2 MHz mientras que DOCSIS 2.0 especifica 6,4 MHz. En cuanto a modulación DOCSIS especifica 64-QAM o 256-QAM para el flujo downstream y QPSK o 16-QAM para el flujo upstream.
- Capa MAC: DOCSIS 1.0 y 1.1 utilizan TDMA y DOCSIS 2.0 utiliza TDMA y S-CDMA (Synchronous CDMA). Además, desde su versión 1.1, DOCSIS incluye características de QoS que permiten soportar aplicaciones eficientemente.

En la Tabla 29 se aprecian las velocidades de transferencia de las distintas versiones de DOCSIS, tanto downstream como upstream.

**Tabla 29: Velocidades de Transferencia de DOCSIS.**

| DOCSIS | Downstream | Upstream |
|---|---|---|
| 1.1 | 38 Mbps | 10 Mbps |
| 2.0 | 40 Mbps | 30 Mbps |
| 3.0 | 160 Mbps | 120 Mbps |

### 9.2.4.4. Interfaces entre componentes funcionales

PacketCable define un conjunto de interfaces o puntos de referencia entre entidades funcionales. Estas interfaces pueden ser propias o tomadas de la arquitectura IMS. Los puntos de referencia propios de PacketCable tienen un formato de nombre estandarizado con las siguientes características: pkt-<área funcional>-<número del punto de referencia>.

En la  se muestran las principales interfaces de PacketCable adicionales a las de IMS.

**Tabla 30: Principales Interfaces de PacketCable.**

| Interfaz | Une las entidades | Breve Descripción |
|---|---|---|
| pkt-sig-1 | MGC – MG | Corresponde a una interfaz del tipo TGCP (Trunking Gateway Control Protocol). |
| pkt-sig-2 | CMS – (S/I)-CSCF<br>MGC – (S/I)-CSCF<br>MGC – BGCF | Permite establecer sesiones de voz a los E-MTAs con los elementos PacketCable. Además permite al BGCF, S-CSCF e I-CSCF intercambiar señalización de sesión con un MGC para interoperar con la PSTN. Usa el protocolo CMSS (CMS to CMS Signaling) |
| pkt-qos-1 | P-CSCF – Administrador de Aplicación | Interfaz de Servicio Web Multimedia. Permite al P-CSCF hacer requerimientos de QoS al Administrador de Aplicación. |
| pkt-qos-2 | Servidor de Políticas - CMTS | El servidor de políticas usa el protocolo CPD (Control Point Discovery) para determinar el CMTS que sirva a un UE dado. |
| pkt-mm-1 | CM – CMTS | Permite al CMTS instruir al CM para montar, desechar, o cambiar un flujo de servicio DOCSIS. |
| pkt-mm-2 | Servidor de Políticas - CMTS | Permite al servidor de políticas traspasar sus decisiones al CMTS y a este último, entregar respuestas. |
| pkt-mm-3 | Administrador de Aplicación – Servidor de Políticas | Permite al administrador de aplicación pedir al servidor de políticas que instale decisiones en el CMTS. |
| pkt-nat-1 | UE – Servidor TURN | Permite al UE acceder al servidor TURN para que soporte el cruce del NAT. |
| pkt-nat-2 | UE – Servidor STUN externo | Permite al UE determinar una de las posibles direcciones media usando STUN. |
| pkt- pacm-1 | UE - DHCP | Provee la información de participación de la red. |
| pkt- pacm-2 | UE – DNS | Permite al UE resolver nombres DNS para la localización de elementos de red o enrutamiento de mensajes. |
| pkt- pacm-3 | UE - PDS | Permite al UE, a través del uso de SIP, suscribir el estatus de información y características de datos. |
| pkt- pacm-4 | UE -XDS | Usado para distribuir y administrar la configuración y características de datos. |
| pkt- pacm-5 | UE – Tiempo | Permite al UE obtener el tiempo. |
| pkt- pacm-6 | UE – EMS & NMS | Permite a los EMSs y NMSs monitorear y administrar UEs. |

### 9.2.4.5.Adaptación de Identidades de IMS.

Además de las identidades públicas y privadas de usuario definidas por IMS, PacketCable agrega la identidad GRUU (Globally Routable User Agent URI), en que cada GRUU se asocia con una identidad pública de usuario y un UE. En PacketCable, cuando un UE se registra se le asigna una ID de Instancia en un tiempo dado, de esta forma, el GRUU sirve como un URI (Uniform Resource Identifier) que puede usarse desde cualquier dominio y se enrutará sólo al UE con la específica identidad pública asociada y la ID de Instancia. Los GRUUs son asignados por el S-CSCF del UE y los requerimientos destinados a un GRUU son enrutados al S-CSCF responsable de la identidad de usuario pública asociada con el GRUU.

En la Figura 91 se observa la relación entre las identidades públicas de usuario, GRUUs y UEs. Si un UE se registra con múltiples identidades públicas a cada una se le asigna un GRUU separado. De la misma forma, si varios UEs se registran con la misma identidad pública, a cada uno se le asigna un diferente GRUU.

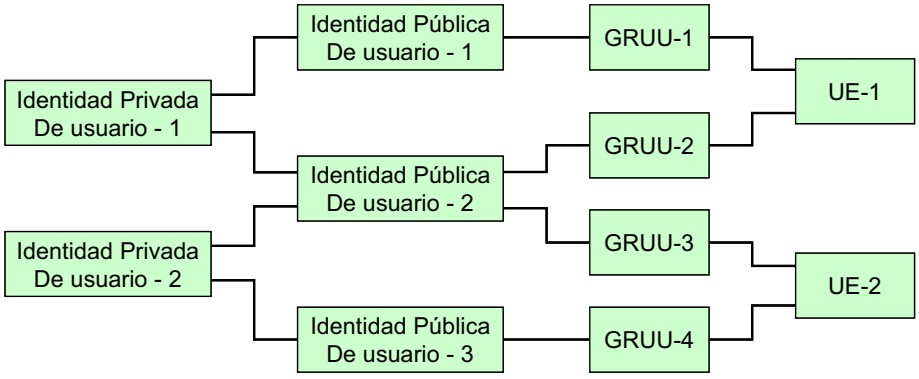



**Figura 91: Relación entre Identidades Públicas de Usuario, GRUUs y UEs.**

## 9.3. Diagrama Resumen de IMS

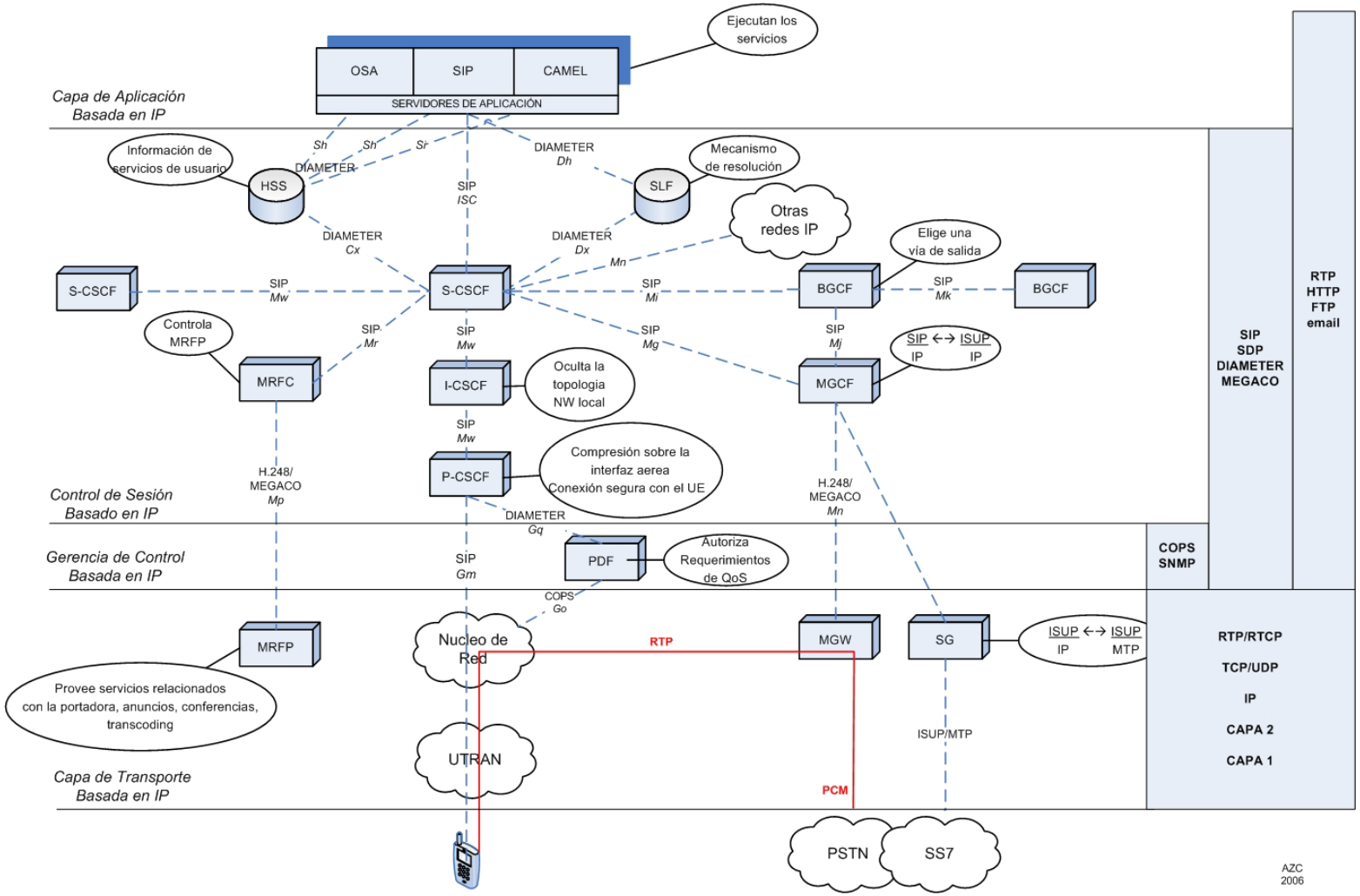



**Figura 92: Diagrama Resumen de IMS.**

# 9.4. Conceptos y Funcionamiento de IMS (Continuación)

## 9.4.1. Ejemplos de Control de Portadores de Tráfico

### 9.4.1.1. Proceso de Reservación de Recursos en UMTS

En la Figura 93 se observa, a modo de ejemplo, el proceso de reservación de recursos para un servicio basado en una política local. El proceso realizado se resume a continuación:

1. El UE envía un mensaje de Activar Contexto PDP al SGSN con los parámetros de QoS e información vinculada.
2. El SGSN envía al GGSN el mensaje de Crear Contexto PDP.
3. El GGSN envía un mensaje COPS de Requerimiento al PDF con la información vinculada para obtener información relevante de políticas.
4. Mediante un token de autorización, el PDF identifica el estatus de información de la autorización y envía un requerimiento de autorización al AF (en este caso, el P-CSCF).
5. El AF (P-CSCF) envía la información de servicio al PDF.
6. El PDF autoriza los recursos de QoS requeridos para la sesión e instala las políticas a nivel de portadores IP en su base de datos interna.
7. El PDF envía un mensaje COPS "Dec" (Decision) de vuelta hacia el GGSN.
8. El GGSN envía un mensaje COPS RTP hacia el PDF, lo que gatilla un mensaje de reporte a ser enviado desde el PDF al AF.
9. El GGSN mapea el flujo IP basado en la información de políticas en el contexto PDP basado en la información de políticas y usa esta información para aceptar el requerimiento de activación PDP, y envía un mensaje de respuesta de Crear un contexto PDP al SGSN.
10. Se realiza un procedimiento de asignación RAB (Radio Access Bearer).
11. El SGSN envía un mensaje de contexto PDP de activación de aceptación.

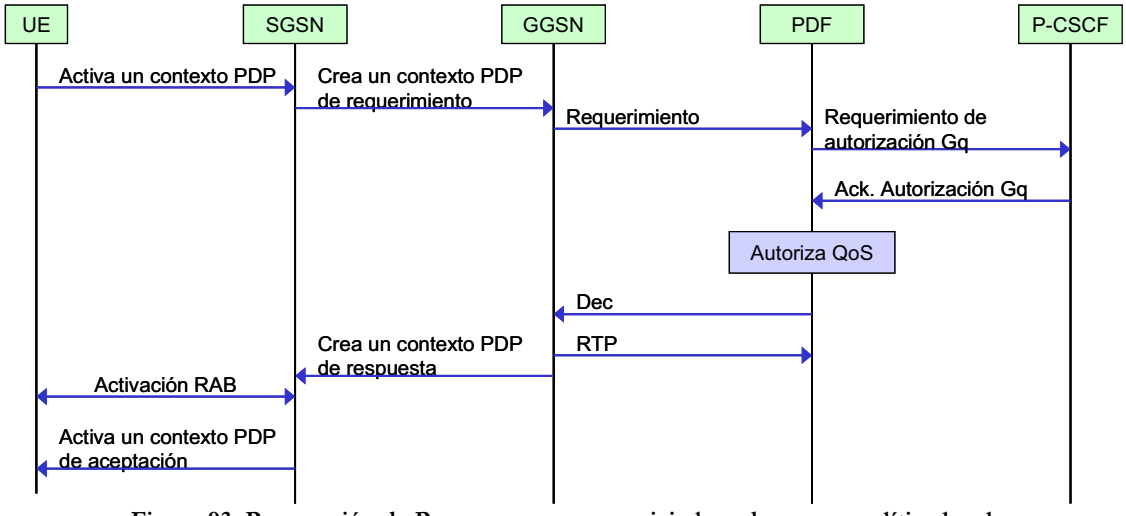



**Figura 93: Reservación de Recursos para un servicio basado en una política local.**

### 9.4.1.2. Proceso de Reservación de Recursos a través de una WLAN

A continuación se muestra un proceso de asignación de QoS a través de una WLAN. Los pasos de este proceso son:

1. El UE comienza el proceso de autentificación para el acceso WLAN.
2. La WLAN envía sus capacidades junto con el requerimiento de acceso del usuario a un Servidor AAA 3GPP.
3. El profile de QoS del usuario es bajado desde el HSS/HLR al Servidor AAA.
4. Se realizan los intercambios de autentificación.
5. El requerimiento de acceso del usuario es aceptado y se envía el mensaje correspondiente junto con el profile de QoS autorizado desde el Servidor AAA 3GPP a la WLAN.
6. La WLAN informa al UE de la autentificación exitosa.
7. Los mensajes de accounting desde la WLAN incluyen el profile de QoS que está siendo utilizado.

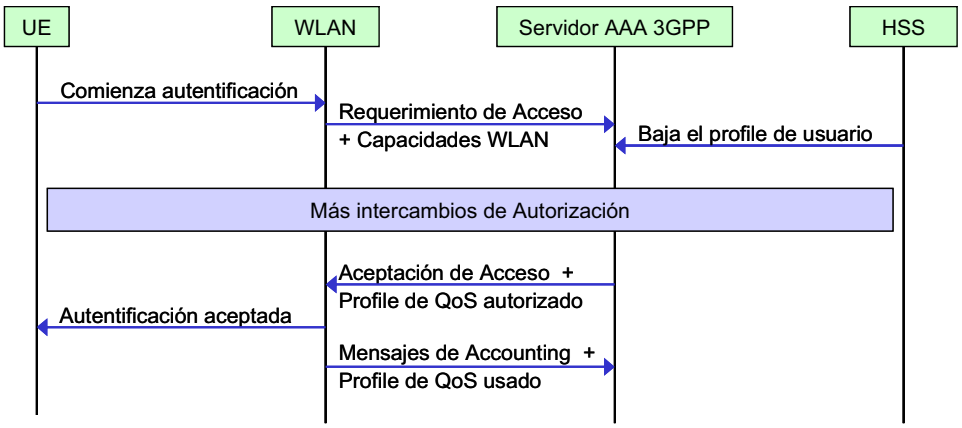



**Figura 94: Flujo de Mensajes para entregar QoS con una WLAN de acceso.**

### 9.4.1.3. Implementación de QoS en redes Inalámbricas

Para la implementación de QoS en redes inalámbricas probablemente se utilizarán protocolos ya existentes. Un protocolo de gran utilidad para la implementación de QoS puede ser el protocolo de la IEEE 802.1D que es una especificación que entrega pautas para la priorización de diferentes tráficos de usuario en la Capa 2 del modelo OSI. El protocolo 802.1D define un parámetro llamado "user_priority" que corresponde a la prioridad requerida por el usuario que origina el servicio y consiste en un número natural desde 1 hasta 7 (aunque cero es el valor de la prioridad de usuario por defecto). En la Tabla 31 se observan los valores de prioridad de usuario para distintas clases de tráfico existentes.

Con el este protocolo se pueden implementar clases de tráfico en redes inalámbricas. Por ejemplo, la Alianza Wi-Fi definió un perfil llamado WMM (Wireless Multimedia Extensions) que se basa en las especificaciones de la tecnología de la IEEE 802.11e. El perfil WMM provee soporte para aplicaciones multimedia definiendo cuatro categorías de acceso derivadas del protocolo 802.1D. En la Tabla 32 se muestran estas categorías de acceso.

**Tabla 31: Mapeo de la Clase de Tráfico de acuerdo al Número de Colas.**

| N° de Colas del sistema | Tipos o Clases de Tráfico soportados por las Colas |
|---|---|
| 1 | {Best Effort, Excellent effort, Background, Voice, Controlled Load, Video, Network Control} |
| 2 | {Best Effort, Excellent effort, Background} {Voice, Controlled Load, Video, Network Control} |
| 3 | {Best Effort, Excellent effort, Background}, {Controlled Load, Video}, {Voice, Network Control} |
| 4 | {Background}, {Best Effort, Excellent effort}, {Controlled Load, Video}, {Voice, Network Control} |
| 5 | {Background}, {Best Effort, Excellent effort}, {Controlled Load}, {Video}, {Voice, Network Control} |
| 6 | {Background}, {Best Effort}, {Excellent effort}, {Controlled Load}, {Video}, {Voice, Network Control} |
| 7 | {Background}, {Best Effort}, {Excellent effort}, {Controlled Load}, {Video}, {Voice}, {Network Control} |

**Tabla 32: Mapeo de Categorías de Acceso WMM y Etiquetas 802.1D.**

| Categoría de Acceso | Etiquetas 802.1D |
|---|---|
| WMM Prioridad de Voz | 7, 6 |
| WMM Prioridad de Video | 5, 4 |
| WMM Prioridad de Best Effort | 0, 3 |
| WMM Prioridad de Background | 2, 1 |

## 9.4.2. Procedimientos de Inicio de Sesión

### 9.4.2.1. Origen desde la PSTN

Cuando un usuario trata de iniciar una sesión través de IMS desde la red PSTN, se requiere de la entidad funcional MGCF (Media Gateway Control Function), la que en IMS es un punto final SIP que inicia los requerimientos en nombre de la PSTN y MGW. Así, las entidades subsiguientes involucradas en la señalización consideran la señalización como si viniera de un S-CSCF.

Debido al enrutamiento de sesión dentro de la PSTN, el procedimiento de origen sólo podrá ocurrir en la red Home del suscriptor de destino. El flujo de mensajes para el procedimiento de origen se muestra en la Figura 95.

El procedimiento de origen desde la PSTN es como sigue:

1. La PSTN establece un mapa de portadores hacia el MGW, y señaliza al MGCF con un mensaje IAM (Initial Address Message) dando la identidad troncal e información de destino.
2. El MGCF inicia un comando H.248, para fijar la troncal desde la PSTN a un puerto IP.

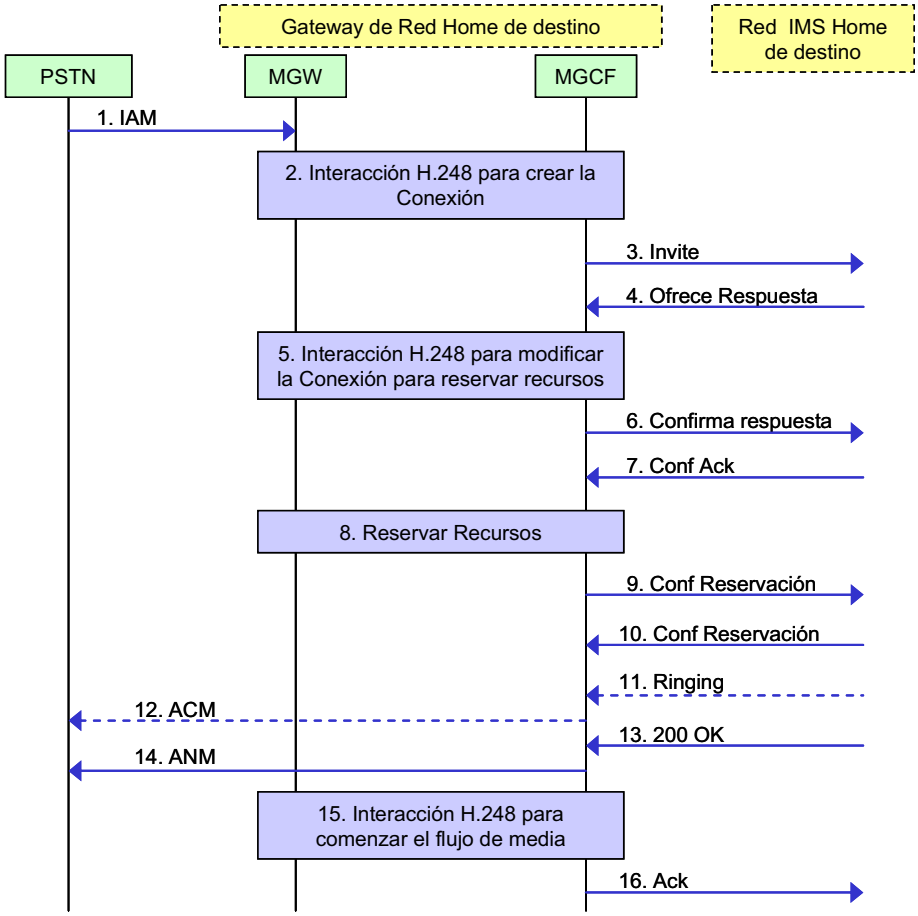



**Figura 95: Origen desde la PSTN.**

3. El MGCF inicia un requerimiento SIP INVITE en dirección a un identificador telefónico o, si es dirigido por una política del operador local, a un identificador SIP, y envía el requerimiento a un I-CSCF configurado.
4. Se retornan las capacidades del stream media del destino por el mapa de señalización.
5. El MGCF inicia un comando H.248 para modificar los parámetros de conexión e indicar al MGW que reserve los recursos necesarios para la sesión.

6-7. El MGCF decide el stream media para esa sesión, confirma la recepción del mensaje y envía una confirmación. Luego, el punto de término responde a la confirmación.

8. El MGW reserva los recursos necesarios para la sesión.

9-10. Cuando la reservación de recursos está completa, el MGCF envía el mensaje de Reservación de Recursos exitosa al punto de término y éste último responde al de origen cuando ocurrió la reservación de recursos exitosa.

11-12. Opcionalmente, el punto de término puede realizar alertas. Si es así, éste señala a la parte de origen con una respuesta provisional indicando "ringing". Este mensaje se envía al MGCF y éste envía un mensaje ACM (Address Complete Message) a la PSTN.

13-14. Cuando la parte de destino responde, los procedimientos de término y S-CSCF a S-CSCF entregan una respuesta final SIP 200 OK enviada al MGCF. Éste último envía un mensaje ANM (Answer Message) a la PSTN.

15. El MGCF inicia un comando H.248 para alterar la conexión al MGW y hacerla bidireccional.
16. El MGCF reconoce la respuesta final SIP y responde con un mensaje SIP ACK.

### 9.4.2.2. Origen desde un Cliente externo SIP No-IMS

Como se mencionó anteriormente, SIP (Session Initiation Protocol) es un protocolo para iniciar, modificar y terminar sesiones muy utilizado para VoIP. De esta forma, pueden existir muchos clientes SIP que no soporten algunas extensiones SIP IMS y, sin embargo, deseen realizar una sesión a través de esta arquitectura. Para estos casos, el UE debe levantar la sesión sin activar la transferencia de información media hasta que la sesión haya sido aceptada y se haya completado la reservación de recursos.

En la Figura 96 se muestra un ejemplo para un cliente SIP No-IMS y un usuario de término que se encuentra en su red Home (en este caso, no se encuentra en alguna red visitada).

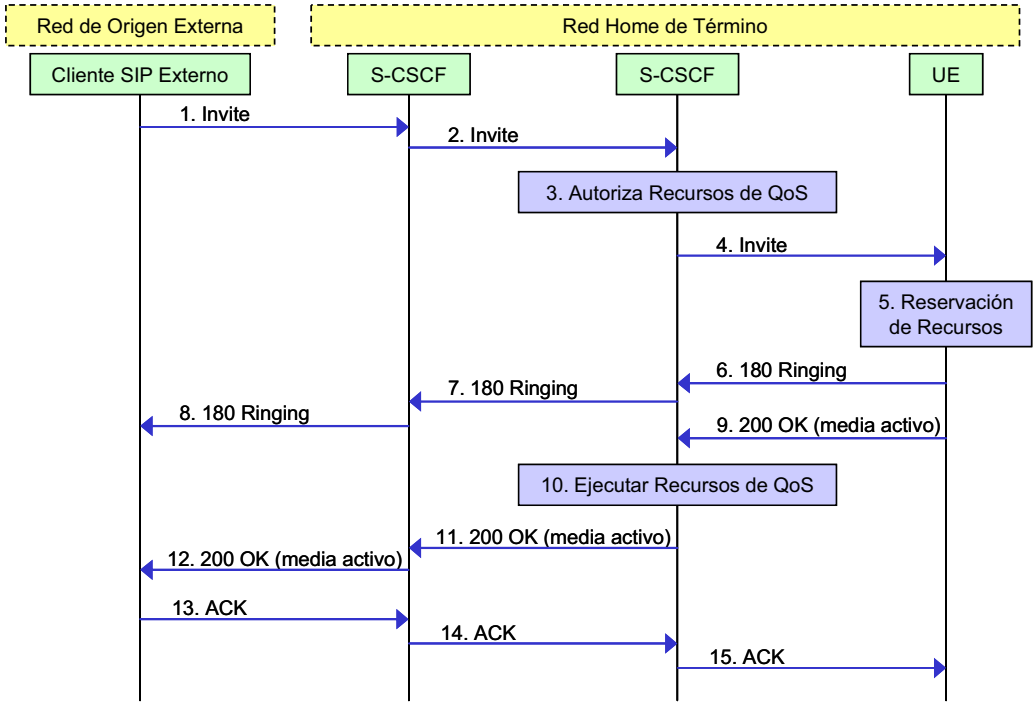



**Figura 96: Origen desde un Cliente Externo No-IMS.**

Para este ejemplo, el procedimiento de origen para un cliente externo es:

1-2. Llega al UE en la red IMS un requerimiento de sesión con la información de media pero sin la precondición de capacidad requerida.
3. El P-CSCF (utilizando el PDF) se basa en las políticas del operador para autorizar los recursos necesarios para la sesión y se genera un token de autorización. Sin embargo, los parámetros no han sido negociados aún.
4. El P-CSCF reenvía el requerimiento INVITE al UE.
5. El UE inicia la reservación de recursos de acuerdo a la sesión y parámetro de media.
6-8. La información de "ringing" se envía a la parte de origen.

9-12. Cuando el UE completa la reservación de recursos y el usuario acepta la sesión, el UE envía una respuesta 200 OK. Basado en las políticas del operador el P-CSCF/PDF puede actualizar la autorización de media de acuerdo a los parámetros negociados y entrega los recursos autorizados para la sesión.

13-15. La parte de origen envía un reconocimiento de la sesión (Acknowledgement).

## 9.4.3. Procedimientos S-CSCF/MGCF ↔ S-CSCF/MGCF

### 9.4.3.1. Terminación PSTN en una Red distinta a la del S-CSCF

En la Figura 97 se muestran los flujos necesarios para establecer una sesión hacia una terminación PSTN en que la red de término no se encuentra en la misma red que el S-CSCF de la red de origen utilizada. En estos casos se utiliza la entidad funcional BGCF (Border Gateway Control Function) que se encarga de hacer la transición entre la red IMS y la red PSTN si ésta si el cambio ocurre en la misma red de origen o, si el cambio ocurre en otra red, se encarga de entregar el requerimiento a otro BGCF dentro de esa red.

A continuación se explican, en resumen, los procedimientos realizados:

1. El requerimiento SIP INVITE se envía desde el UE al S-CSCF de la red de origen.
2. El S-CSCF de origen realiza la lógica de servicio necesaria para levantar la sesión.
3. El S-CSCF de origen analiza la dirección de destino y determina que es para la PSTN, y entrega el requerimiento al BGCF en la red de origen.
4. El BGCF de la red de origen determina que la transición a la PSTN debe ocurrir en otra red y reenvía el requerimiento al BGCF de esa red de destino.
5. El BGCF de la red de destino determina que el MGCF (recordar que el MGCF es el punto final SIP que inicia requerimientos en nombre de la PSTN) debe estar en esa red y selecciona un MGCF apropiado. El requerimiento SIP INVITE es reenviado al MGCF y, por tanto, al punto de término en la PSTN.

6-9. Las capacidades de stream media del destino son retornados a través del mapa de señalización desde el punto de término en la PSTN hacia el punto de origen.

10-13. El punto de origen decide las capacidades de flujo entre las características ofrecidas y confirma la recepción del mensaje enviando un mensaje de confirmación al S-CSCF de la red de origen y luego es reenviado hasta llegar al punto de término en la PSTN.

14-21. El punto de término responde un reconocimiento a través del mapa de sesión hasta el punto de origen. Luego de que el punto de origen completa los procedimientos de reserva de recursos, envía un mensaje de reservación de recursos exitosa al S-CSCF de la red de origen, el que es reenviado al punto de término mediante el mapa de sesión establecido.

22-29. El punto de término responde el mensaje hacia el punto de origen y puede generar un mensaje de "ringing" hacia el punto de origen.

30-37. El punto de término envía 200 OK cuando la parte de destino responde la sesión y el punto de origen envía un reconocimiento del establecimiento de la sesión.

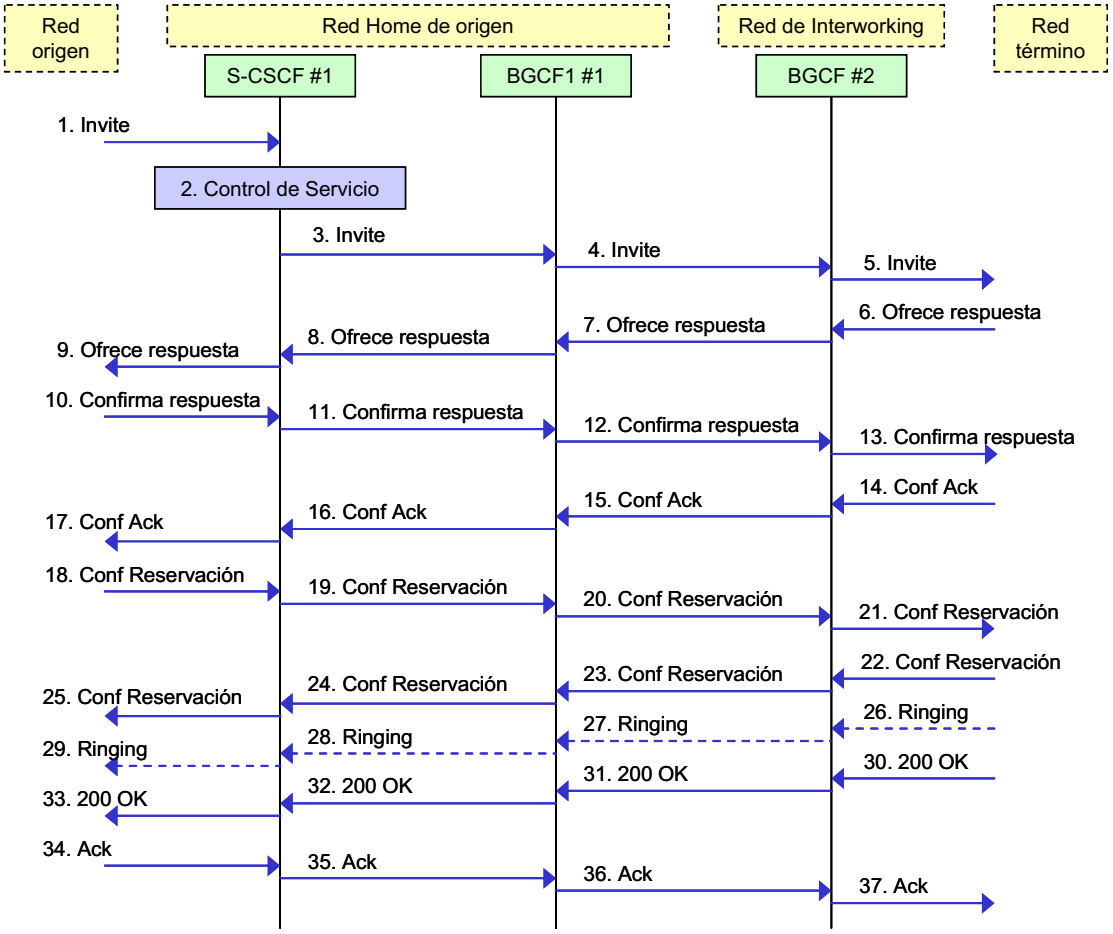



**Figura 97: Inicio de Sesión con término PSTN en una Red distinta a la del S-CSCF.**

## 9.4.4. Procedimientos de Término de Sesión

### 9.4.4.1. Término en una red PSTN

Cuando se debe realizar una terminación hacia la PSTN, la transición debe realizarse en la misma red Home de origen. Sin embargo, pueden existir acuerdos entre los operadores que permitan realizar la terminación hacia la PSTN en una red distinta a la red Home de origen.

En la Figura 98 se muestra el flujo de mensajes para realizar una sesión con la parte de término en una red PSTN. A continuación se resume la secuencia de mensajes realizada:

1. El MGCF recibe un requerimiento SIP INVITE mediante algún procedimiento de inicio de sesión y de S-CSCF/MGCF a S-CSCF/MGCF.

2-3. El MGCF inicia una interacción H.248 para tomar un canal saliente y determinar las capacidades media del MGW. Luego, determina el tipo de stream media que soporta de entre los que le propone la parte de origen y le envía un mensaje de respuesta.

4. La parte de origen envía una confirmación o puede continuar ofreciendo nuevos tipos de stream media.

5-6. El MGCF inicia una interacción H.248 para modificar la conexión establecida en el paso 2 y dirige al MGW para que reserve los recursos necesarios para el stream media y luego responde los medios ofrecidos a la parte de origen.

7. El MGW reserva los recursos necesarios.

8-10. Luego de que la parte de origen reserva sus recursos necesarios exitosamente envía un mensaje de confirmación al MGCF, el que envía un mensaje IAM a la PSTN y luego envía una respuesta al mensaje de reserva exitosa hacia la parte de origen.

11-12. Luego de que se establece el mapa de destino, la parte de término puede alertar al usuario de término sobre el intento de sesión; si es el caso, éste responde con un mensaje ACM y el MGCF indica un mensaje "ringing" a la parte de origen.

13. Cuando la parte de término responde, la PSTN envía un mensaje ANM al MGCF.

14-16. El MGCF inicia una interacción H.248 para que la conexión en el MGW se haga bidireccional y envía una respuesta SIP 200 OK a la parte de origen, la que envía un mensaje de reconocimiento de vuelta al MGCF.

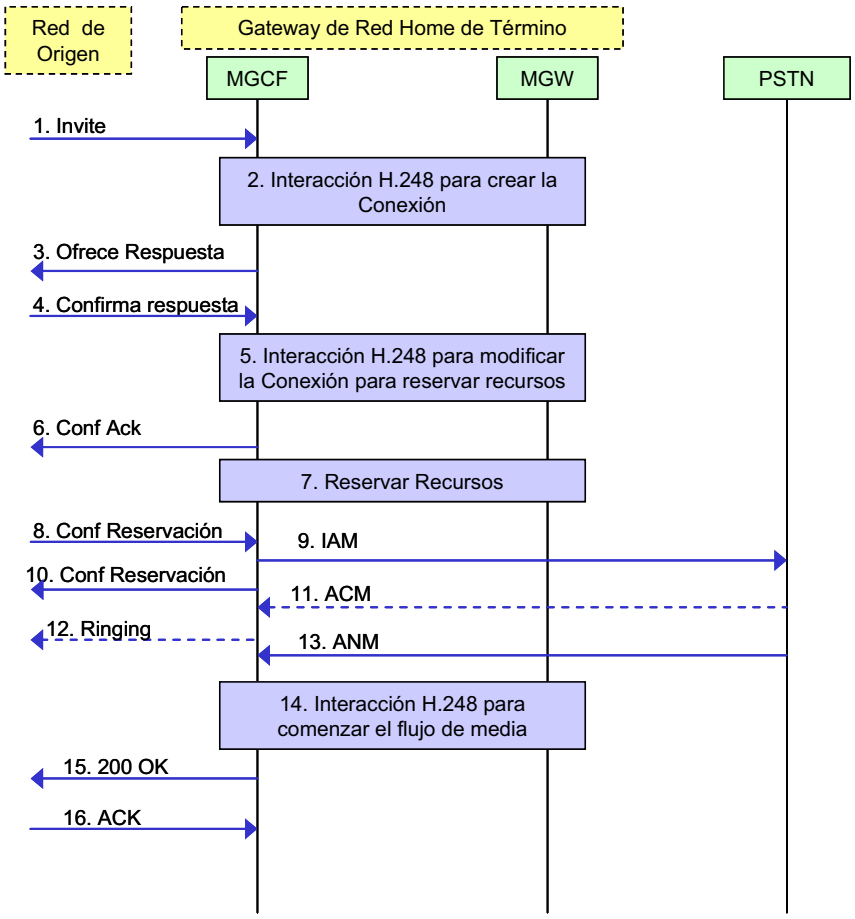



**Figura 98: Procedimiento de Término de Sesión en la PSTN.**

### 9.4.4.2. Término en un Cliente externo SIP No-IMS

Es posible que un cliente IMS desee iniciar sesión con un cliente SIP externo que no soporte las precondiciones necesarias en IMS. Cuando pasa esto, existe proceso de tres etapas para iniciar la sesión. En la Figura 99 se muestran los flujos de mensajes para las tres etapas definidas en el párrafo

siguiente. En este escenario, se supone que ambos usuarios están en su red Home como forma de simplificación.

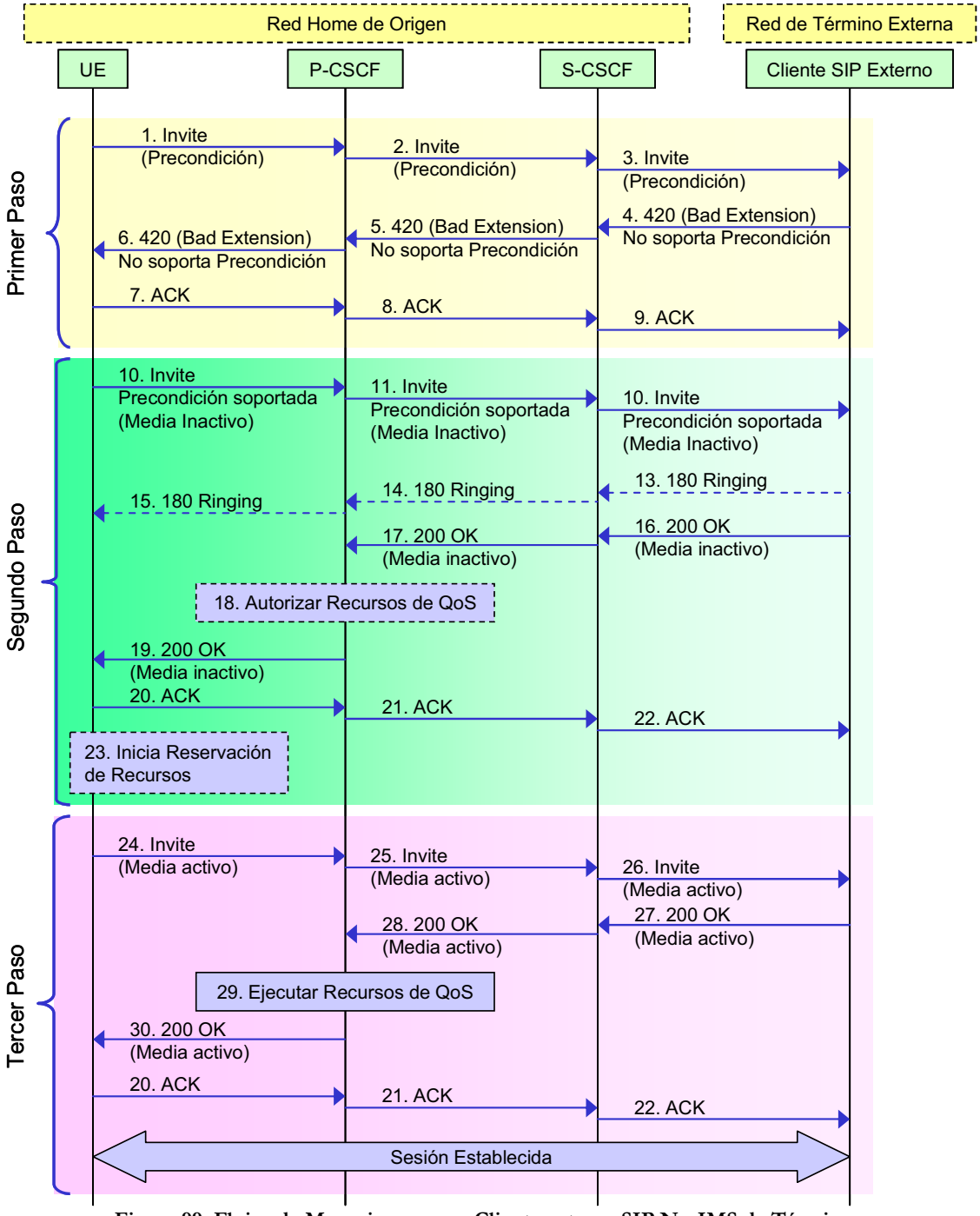



**Figura 99: Flujos de Mensajes para un Cliente externo SIP No-IMS de Término.**

Los pasos seguidos son:

1. El UE de origen inicia un requerimiento de sesión IMS con precondiciones de capacidades que no son soportadas por el cliente SIP externo. Cuando llegan a la parte de término, ésta

responde que no soporta estas precondiciones a lo que la parte de origen responde con un reconocimiento.

2. Basado en la respuesta que no existe soporte, el UE de origen reinicia la sesión anulando sus requerimientos e indicando sólo su propio soporte. El UE ajusta todas sus componentes media como inactivas hasta que la información de media ya ha sido negociada por el P-CSCF/PDF de forma de establecer la sesión pero sin que se hayan asignado los recursos aún. Finalmente, el UE inicial la reservación de recursos.
3. Una vez acordados los parámetros de la sesión y ya que el UE ha reservado recursos exitosamente, la sesión continúa levantándose pasando los componentes media a activos. De esta forma el P-CSCF/PDF asigna los recursos reservados y luego de un reconocimiento del UE, se establece la sesión entre los dos puntos.

## 9.4.5. Funciones de Control de Borde

### 9.4.5.1. Transporte del Plano de Usuario

Como se mostró anteriormente, el TrGW se encarga de hacer la traducción de información necesaria entre redes IPv4 e IPv6. Cuando el TrGW recibe un mensaje desde una red a otra realiza una de las siguientes acciones:

- Reemplaza la (o las) dirección IPv4 recibida y número de puerto en el mensaje con la dirección y puerto IPv6 correspondiente.
- Reemplaza la (o las) dirección IPv6 recibida y número de puerto en el mensaje con la dirección y puerto IPv4 correspondiente.

En el primer caso, si el TrGW recibe un mensaje IPv4 debe reemplazarlo por un mensaje con headers IPv6 para enviarlo a la red IPv6. Así, se distinguen dos alternativas:

- Si el paquete no está fragmentado (indicado por el bit DF, que está activado), los headers IPv6 se configuran como lo indica la Tabla 33.
- Si el paquete está fragmentado (bit DF no activado), los headers IPv6 se configuran como se muestra en la Tabla 33.

**Tabla 33: Derivación de Headers IPv4 a IPv6 (sin fragmentación).**

| Campo IPv6 | Valor |
|---|---|
| Versión | 6 |
| Clase de Tráfico | El comportamiento por defecto es que el valor de este campo IPv6 es el valor del campo IPv4 "Tipo de Servicio" (los 8 bits correspondientes son copiados). Sin embargo, el TrGW puede implementar la opción de ignorar el valor de este campo IPv4 y dejar el campo "Clase de Tráfico" en cero. |
| Etiqueta de Flujo | Este campo se configura en cero (todos los bits cero). |
| Largo de Carga Útil (Payload) | Su valor es el campo de largo total IPv4 menos el tamaño del header IPv4 y el largo del campo de opciones IPv4, si existe. |
| Próximo Header | El valor del Próximo Header IPv6 se copia del campo del protocolo IPv4. |
| Límite de Saltos | Su valor es el valor del campo IPv4 "Time to Live" menos 1. |
| Dirección Fuente | Puede administrarse como las direcciones del mensaje de carga útil como se describió en el primer párrafo (cambiar las versiones de direcciones y puertos). |
| Dirección de Destino | Puede administrarse como las direcciones del mensaje de carga útil como se describió en el primer párrafo (cambiar las versiones de direcciones y puertos). |

**Tabla 34: Derivación de Headers IPv4 a IPv6 (con fragmentación).**

| Campo IPv6 | Valor |
|---|---|
| Versión | 6 |
| Clase de Tráfico | El comportamiento por defecto es que el valor de este campo IPv6 es el valor del campo IPv4 "Tipo de Servicio" (los 8 bits correspondientes son copiados). Sin embargo, el TrGW puede implementar la opción de ignorar el valor de este campo IPv4 y dejar el campo "Clase de Tráfico" en cero. |
| Etiqueta de Flujo | Este campo se configura en cero (todos los bits cero). |
| Largo de Carga Útil (Payload) | Su valor es el campo de largo total IPv4 menos el tamaño del header IPv4 y el largo del campo de opciones IPv4, si existe. |
| Próximo Header | Este campo se activa como header de Fragmento (44). |
| Límite de Saltos | Su valor es el valor del campo IPv4 "Time to Live" menos 1. |
| Dirección Fuente | Puede administrarse como las direcciones del mensaje de carga útil como se describió en el primer párrafo (cambiar las versiones de direcciones y puertos). |
| Dirección de Destino | Puede administrarse como las direcciones del mensaje de carga útil como se describió en el primer párrafo (cambiar las versiones de direcciones y puertos). |
| **Headers de Fragmentos:** | |
| a) Próximo Header | Copiado del campo del Protocolo IPv4. |
| b) Fragmento de Compensación (Offset) | Copiado del Fragmento de Compensación IPv4. |
| c) Bit de más fragmentos | Copiado del valor de más fragmentos del campo de flags IPv4 de bit de más fragmentos. |
| d) Identificación | Los 16 bits de menor orden son copiados del campo de Identificación IPv4, los 16 bits de mayor orden se dejan en cero. |

En el segundo caso, si el TrGW recibe un mensaje IPv6 que va hacia una red IPv4, entonces se distinguen dos casos, igual que en el caso anterior:

- Si el paquete IPv6 no está fragmentado, el paquete IPv4 es como en la Tabla 35.
- Si el paquete IPv6 está fragmentado, el paquete IPv4 es como en la Tabla 36.

**Tabla 35: Derivación de Headers IPv6 a IPv4 (sin fragmentación).**

| Campo IPv4 | Valor |
|---|---|
| Versión | 4 |
| Largo del Header de Internet | 5 (sin opciones IPv4). |
| Tipo de Servicio | El comportamiento por defecto es que el valor de este campo IPv4 es el valor del campo IPv6 "Clase de Tráfico" (los 8 bits correspondientes son copiados). Sin embargo, el TrGW puede implementar la opción de ignorar el valor de este campo IPv6 y dejar el campo "Clase de Tráfico" en cero. |
| Largo Total | Su valor es el valor del campo de largo de carga útil IPv6 más el tamaño de los headers IPv4. |
| Identificación | Todos los bits son puestos en cero. |
| Flags | El flag de más fragmentos (more fragment) es puesto en cero. El flag no fragmentos (Don't fragment) es puesto en uno. |
| Time to Live (TTL) | Su valor es el valor del campo IPv6 "Límite de Saltos" menos 1. |
| Protocolo | Su valor es el del campo IPv6 del Próximo Header |
| Header Checksum | Se calcula una vez que el header IPv4 se ha creado. |
| Dirección Fuente | Puede administrarse como las direcciones del mensaje de carga útil como se describió en el primer párrafo (cambiar las versiones de direcciones y puertos). |
| Dirección de Destino | Puede administrarse como las direcciones del mensaje de carga útil como se describió en el primer párrafo (cambiar las versiones de direcciones y puertos). |

**Tabla 36: Derivación de Headers IPv6 a IPv4 (con fragmentación).**

| Campo IPv4 | Valor |
|---|---|
| Versión | 4 |
| Largo del Header de Internet | 5 (sin opciones IPv4). |
| Tipo de Servicio | El comportamiento por defecto es que el valor de este campo IPv4 es el valor del campo IPv6 "Clase de Tráfico" (los 8 bits correspondientes son copiados). Sin embargo, el TrGW puede implementar la opción de ignorar el valor de este campo IPv6 y dejar el campo "Clase de Tráfico" en cero. |
| Largo Total | Su valor es el valor del campo de largo de carga útil IPv6 más el tamaño de los headers IPv4 menos 8, por el header de Fragmento. |
| Identificación | Es copiada de los 16 bits de menor orden en el campo de Identificación IPv6, en el header de Fragmento IPv6. |
| Flags | El flag IPv4 de más fragmentos (more fragment) es copiado del flag IPv6 M en el header de fragmento IPv6. El flag no fragmentos (Don't fragment) es puesto en cero para permitir que el paquete IPv4 sea fragmentado por los routers IPv4. |
| Time to Live (TTL) | Su valor es el valor del campo IPv6 "Límite de Saltos" menos 1. |
| Protocolo | Su valor es el del campo IPv6 del Próximo Header |
| Header Checksum | Se calcula una vez que el header IPv4 se ha creado. |
| Dirección Fuente | Puede administrarse como las direcciones del mensaje de carga útil como se describió en el primer párrafo (cambiar las versiones de direcciones y puertos). |
| Dirección de Destino | Puede administrarse como las direcciones del mensaje de carga útil como se describió en el primer párrafo (cambiar las versiones de direcciones y puertos). |

### 9.4.6. Puntos de Referencia para la Interoperación entre IMS y una WLAN

En la Tabla 37 se muestra una breve descripción de los puntos de referencia en la arquitectura de interoperación entre IMS y redes de acceso WLAN.

**Tabla 37: Puntos de Referencia para la Interoperación con una WLAN.**

| Punto de Referencia | Descripción General |
|---|---|
| Wa | Conecta la WLAN AN a la red 3GPP de acceso (que puede ser la red Home o visitada). Transporta información de autentificación, autorización y cobro de forma segura. |
| Wx | Conecta al Servidor 3GPP AAA al HSS. Permite la comunicación entre la infraestructura WLAN AAA y el HSS. |
| D' / Gr' | Es opcional entre el Servidor 3GPP AAA y el HLR para versiones antiguas (anteriores a la 6) de IMS. |
| Wo | Usado por el Servidor 3GPP AAA para comunicarse con el OCS. Transporta información de cobro en línea para el control de crédito del suscriptor. |
| Wf | Enlaza al Servidor/Proxy 3GPP AAA con el Sistema de Cobro Offline. Transporta o reenvía información de cobro offline entre los sistemas de cobro offline de la red visitada o Home. |
| Wg | Interfaz AAA entre el Servidor/Proxy 3GPP AAA y el WAG. Usado para entregar información al WAG para que aplique políticas y, para roaming, transporte de información de cobro desde el WAG al Proxy. |
| Wn | Enlaza la WLAN AN con el WAG. Usada para forzar el tráfico en un túnel a viajar a través del WAG. |
| Wp | Enlaza el WAG con el PDG. |
| Wi | Enlaza el PDG con la Red de Paquetes de Datos (por ejemplo un operador externo público o privado). |
| Wm | Enlaza al PDG con el Servidor/Proxy 3GPP AAA. Permite al Servidor/Proxy recuperar atributos de tunneling y configuración de parámetros IP del WLAN UE, transporte de mensajes relacionados con autorización y cobro, entre otros. |
| Wd | Conecta al Proxy 3GPP AAA con el Servidor. Transporta información relacionada con autentificación y autorización de forma segura. |
| Wu | Enlaza el WLAN UE y el PDG y representa el túnel entre estas entidades. |
| Ww | Enlaza el WLAN UE con la WLAN AN a través de la especificación IEEE 802.1x u otro sistema. Transporta mensajes de señalización. |
| Dw | Enlaza el Servidor 3GPP AAA y el SLF. Permite al Servidor 3GPP AAA encontrar la dirección del HSS que tiene los datos del suscriptor en un escenario de red con más de un HSS. |
| Wy | Enlaza el PDG con el OCS. Transporta información relacionada con el cobro en línea para el control de crédito del suscriptor. |
| Wz | Enlaza al PDG con el Sistema de Cobro Offline. Transporta información relacionada con el cobro offline. |

### 9.4.7. Escenarios de Interoperación entre Redes IMS IPv4 e IPv6

Es importante definir sistemas de interoperación entre redes IMS que soporten distintas versiones de Internet. En una primera instancia, para permitir la interoperación entre ambos tipos de redes, se debe considerar la existencia de terminales IMS (UE) de stack dual, es decir, un terminal que puede utilizar tanto IPv4 como IPv6 para acceder a la red IMS (este terminal debe elegir inteligentemente qué versión IP utilizar). También se consideran redes Core IMS de stack dual, es decir, que operan con ambos tipos de versiones IP. A continuación se muestran los requerimientos que deben cumplir estas redes para su interoperación y se presentan algunos escenarios de migración.

#### 9.4.7.1. Acceso del UE a IMS

Antes de que el UE se comunique con el Core de la red IMS, éste debe establecer una conexión con el IP-CAN, obtener una dirección IP y adquirir la dirección de un P-CSCF. Si la red IMS está basada en IPv4, se deben considerar mecanismos para el descubrimiento del P-CSCF que aún no han sido definidos como opciones en el IMS de la 3GPP.

Se necesitan evaluar mecanismos del descubrimiento de P-CSCF para los siguientes casos:

a) Acceso a través de GPRS: El UE necesita obtener una dirección del P-CSCF IPv4 desde el GGSN en un contexto PDP. Si el contexto PDP establecido es de tipo IPv4, entonces el GGSN debiera entregar direcciones IPv4 de P-CSCFs. Esto no descarta escenarios en que el GGSN envíe direcciones IPv6 de P-CSCFs en un contexto PDP IPv4. En el periodo de migración, es recomendable que las redes de stack dual ofrezcan un sistema de descubrimiento común a terminales IPv4 e IPv6 de forma de enviar direcciones IPv4 "embebidas" en direcciones IPv6.

b) Acceso basado en DHCP: Actualmente el uso de DHCP se limita a redes IPv6. Para que sea usado por un UE IPv4. Una posible solución es usar un P-CSCF y un UE IPv4 que soporten la configuración del P-CSCF apropiado a través de DHCPv4, de esta forma, al UE se le entrega una completa capacidad de resolver el nombre del P-CSCF.

c) Otros Mecanismos de acceso: Estos mecanismos pueden ser de administración de terminales tipo SMS (Short Message Service), OTA (Over the Air Activation), OMA (Open Mobile Alliance) u otros esquemas de configuración. El método más recomendable para descubrir P-CSCFs IPv4 es OMA, ya que la mayoría de los UE IPv4 soportan este mecanismo.

   OMA es un cuerpo de estándares que desarrolla estándares abiertos para la industria de la telefonía móvil de forma de entregar servicios que sean capaces de interoperar sin importar el país, operador, terminales móviles o tecnología de acceso utilizada. OMA se enlaza con otros cuerpos de estándares como la 3GPP, 3GPP2 o la IETF y tiene especificaciones para MMS, IMPS (Instant Messaging and Presence), PoC (Push to talk over Cellular) entre otros.

Un UE IMS de stack dual puede acceder a la red IMS usando IPv4 o IPv6 dependiendo de la versión de la red IMS, que puede ser IPv4, de stack dual o IPv6. Para esto, el UE debe descubrir la versión IP de la red IMS. Una posibilidad es tener el UE preconfigurado para alguna versión o bien, tratar primero con una versión y luego con la otra. Un comportamiento del UE de stack dual puede ser:

- EL UE de stack dual siempre intentará iniciar la comunicación con el sistema IMS con IPv6. En caso de que falle, utilizará IPv4.
- Si el UE se comunicó en forma exitosa mediante una comunicación IPv6, éste utilizará esta versión para encontrar al P-CSCF.

Es importante tomar en cuenta los siguientes puntos:

- Si el UE se registró mediante IPv6 con una red IMS de stack dual, ésta debe utilizar IPv6 para toda la comunicación aún cuando parte de ella se haya realizado mediante IPv4.
- El UE y el P-CSCF crean un túnel IPSec entre ellos para asegurar la información enviada, por lo que cualquier entidad entre ambos que modifique los mensajes IP intercambiados puede crear serios problemas de seguridad. Más aún, si se utiliza compresión SIP, ésta no puede ser modificada de ningún modo.

### 9.4.7.2. Escenarios de Interoperación

Ya anteriormente se explicó la arquitectura de Funciones de Control de Borde que definen la interoperación entre redes IPv4 e IPv6 utilizando el concepto de IMS-ALG y TrGW (NATs). Esta arquitectura también es aplicable para la migración de redes IMS IPv4 a IPv6.

Los escenarios a considerar para la interoperación en IMS asumen empleos de IPv4 e IPv6. Los distintos escenarios se pueden dividir en cuatro categorías:

1. Escenarios de No-Roaming: El UE está conectado directamente a la red de su propio operador o red Home.
2. Escenarios de Roaming: El UE se encuentra en un red distinta a la de su operador o red Visitada.
3. Escenarios de Acceso GPRS: El UE accede a servicios IMS (a través de una red Home o Visitada) mediante la red de acceso GPRS.
4. Escenarios End-to-End interconectados: Corresponde a la mezcla de los distintos tipos de escenarios anteriores e interconectados a redes IMS/SIP de forma de soportar sesiones en escenarios End-to-End

En todos los casos es necesario considerar la versión IP del UE, junto con el uso de direccionamiento privado y de NAT en el borde de las redes IPv4. En todos los escenarios, el término NAT puede además abarcar el uso de NA(P)T y de ALG (Application Level Gateway). Además, las redes de interconexión asumen el soporte de IPv4 o de IPv4 con IPv6.

En la Tabla 38 se observan ejemplos de escenarios End-to-End. La "X" en la columna "NATx" indica que es esta entidad es necesaria para la comunicación entre redes. Las entidades "NAT1" y "NAT2a" se encuentran en los bordes de la red 1 (red de origen) y la red de tránsito, mientras que la entidad "NAT2b" se encuentra entre el S-CSCF y el P-CSCF de la red 2 (supone casos de Roaming en la red de término).

En el caso en que las redes usen Stack Dual, la red 1 decide la versión IP a utilizar en la red de tránsito basado en las capacidades de dicha red y de la red 2 junto con las políticas definidas entre las redes 1 y 2.

**Tabla 38: Algunos Escenarios End-to-End.**

| Esc. | UE 1 | Red 1 | NAT1 | Tránsito | NAT2a | Red 2 | NAT2b | UE 2 |
|---|---|---|---|---|---|---|---|---|
| 1 | IPv4 | IPv4 | X | IPv4 | - | IPv4 | - | IPv4 |
| 2 | Stack Dual (IPv4) | IPv4 | X | IPv4 | - | IPv4 | - | IPv4 |
| 3 | IPv4 | IPv4 | X | IPv4 | - | Stack Dual (IPv6) | X | Stack Dual (IPv6) |
| 4 | Stack Dual (IPv4) | IPv4 | X | IPv4 | - | Stack Dual (IPv6) | X | Stack Dual (IPv6) |
| 5 | IPv4 | IPv4 | X | IPv4 | - | Stack Dual (IPv6) | X | IPv6 |
| 6 | Stack Dual (IPv6) | IPv6 | - | IPv6 | - | IPv6 | - | IPv6 |
| 7 | IPv6 | IPv6 | X | IPv4 | X | IPv4 | - | IPv4 |
| 8 | IPv6 | IPv6 | - | IPv6 | - | Stack Dual (IPv4) | X | IPv4 |
| 9 | IPv6 | IPv6 | - | IPv6 | - | Stack Dual (IPv4) | X | IPv4 |
| 10 | IPv6 | IPv6 | - | IPv6 | - | IPv6 | - | Stack Dual (IPv6) |

### 9.4.7.3. Escenarios de Migración

En un escenario de migración, algunos usuarios IMS estarán usando UE IPv4 a pesar de que la red haya migrado desde IMS IPv4 a IPv6. De esta forma, el P-CSCF debe soportar IPv4 para comunicarse con el UE ya que otra entidad entre el UE y el P-CSCF podría arriesgar la seguridad del enlace. Si el S-CSCF ya ha evolucionado a IPv6, el registro del UE IPv4 puede realizarse a través de una dirección IPv6 mediante un NAT entre el P-CSCF y el S-CSCF.

Aunque esta posibilidad no ha sido estudiada en profundidad, es claro que puede comprometer la seguridad del enlace ya que cambiaría la correlación y otros servicios o capacidades que usan la dirección IP, por lo que se recomienda implementar redes de Stack dual en vez de solamente una red IPv6 con un NAT. Así mismo, en una etapa de migración temprana, se recomienda el uso de terminales UE de stack dual para facilitar la migración de IPv4 a IPv6 y evitar los problemas mencionados anteriormente.

Aunque la red objetivo es una red IMS IPv6, temporalmente pueden coexistir elementos IPv4 e IPv6 en la misma red. Una forma de afrontar la migración puede ser dividir la red en dos partes lógicas cada una con versiones IP distintas y comunicadas mediante el uso de NATs, otra forma es emplear entidades de red con capacidades duales en cuanto a la versión IP durante las primeras etapas de la migración, alternativa mucho más simple.

## 9.5. Características Avanzadas de WiMAX (Continuación)

### 9.5.1. Adaptive Modulation and Coding (AMC)

Adaptive modulation and coding (AMC) fue introducida en WiMAX para mejorar la cobertura y capacidad para WiMAX en aplicaciones móviles. El soporte para QPSK, 16QAM y 64 QAM son mandatorios en el DL de WiMAX móvil. En el UL, 64QAM es opcional.

OFDM utiliza QPSK y QAM. La modulación y tasas de códigos se pueden cambiar para enfrentar tasas de transferencia más altas, pero un mayor orden de modulación requiere mejores condiciones del canal. La Figura 100 muestra cómo modulaciones de mayor orden como QAM 64 son usadas más cerca de la estación base.

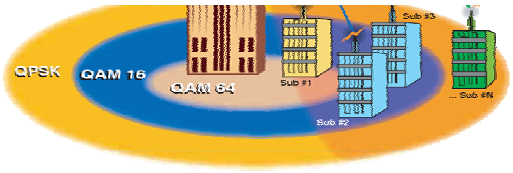



**Figura 100: Utilización de AMC en WiMAX.**

### 9.5.2. Hybrid Auto Repeat Request (HARQ)

A grandes rasgos, HARQ es un recurso utilizado para recuperar información en caso de que sea recibida con errores. En caso de que la detección y corrección de errores (proveídos por FEC) no sean suficientes para corregir un error en el lado del receptor, en vez de descartar el paquete con errores, el receptor puede enviar un mensaje ARQ al transmisor y éste retornará al receptor información con un FEC más fuerte. El receptor utilizará ambos mensajes para recuperar el paquete original.

HARQ es activado en un canal utilizando el protocolo "Stop and Wait", el que provee una respuesta rápida a los errores de paquetes. Además se provee un canal de señalización de ACK (reconocimiento) en el enlace uplink. Sin embargo, también se permite el uso de canales múltiples para ARQ stop-and-wait.

### 9.5.3. Frequency Selective Scheduling

En canales inalámbricos de banda ancha las condiciones de propagación varían dependiendo de la porción del espectro que se esté utilizando y, por tanto, también varía el enlace para los usuarios que estén utilizando dicho espectro. De esta forma, WiMAX soporta una programación selectiva de frecuencias tomando ventaja de la diversidad de frecuencias multi-usuario de forma de mejorar la QoS. Con la permutación de sub-canales adyacentes, se puede asignar un subconjunto de sub-canales a los usuarios móviles basándose en la potencia de la señal para que cada MS cuente con el mapa de ganancia más fuerte.

### 9.5.4. Técnicas de Radio

En WiMAX, las técnicas de transmisión de radio utilizan esquemas de diversidad para tomar ventaja de las señales multipath y reflejadas que ocurren en ambientes NLOS. El uso de múltiples antenas (en transmisión y/o recepción) puede reducir los efectos del fading, interferencia y pérdidas. La diversidad de transmisión en OFDMA se permite porque utiliza codificación espacio-tiempo, de forma que en la recepción se utilicen las dos señales combinadas para tomar ventaja de ambas.

Una de las alternativas más básicas de antenas múltiples es MIMO (Multiple Input Multiple Output) que mejora la velocidad de transmisión e incrementa la señal. Como lo indica el nombre, MIMO utiliza múltiples antenas receptoras y transmisoras para la multiplexación espacial. Cada antena puede transmitir diferentes datos, los que son decodificados en el receptor.

Otra alternativa es el uso de AAS (Adaptive Antenna System). Con AAS, las estaciones base pueden crear rayos dirigidos de forma de focalizar la energía de transmisión al receptor y abarcar un mayor rango de distancia. Además, este sistema permite eliminar interferencias indeseadas de otras fuentes y se aumenta la eficiencia espectral de la frecuencia.

**Figura 101: Sistema Adaptivo de Antenas.**

Por otra parte, WiMAX Móvil soporta AMS (Adaptive MIMO Switching), una técnica en que se selecciona una configuración MIMO de varias disponibles para maximizar la eficiencia espectral sin reducir el área de cobertura.