ESTADO DEL ARTE DE IP MULTIMEDIA SUBSYSTEM (IMS)

Director:

JHON JAIRO PADILLA AGUILAR
Doctor en Ingeniería Telemática

Integrantes:

LUIS ALONSO OSORIO MOLINA
Ingeniero Electrónico
LUISA EDMME SUÁREZ DE AQUIZ
Ingeniera Electrónica

UNIVERSIDAD PONTIFICIA BOLIVARIANA
FACULTAD DE INGENIERÍA ELECTRÓNICA
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2009

ESTADO DEL ARTE DE IP MULTIMEDIA SUBSYSTEM (IMS)

Director:

JHON JAIRO PADILLA AGUILAR
Doctor en Ingeniería Telemática

Integrantes:

LUIS ALONSO OSORIO MOLINA
Ingeniero Electrónico
LUISA EDMME SUÁREZ DE AQUIZ
Ingeniera Electrónica

MONOGRAFÍA

UNIVERSIDAD PONTIFICIA BOLIVARIANA
FACULTAD DE INGENIERÍA ELECTRÓNICA
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2009

TABLA DE CONTENIDO

LISTADO DE TABLAS 6
RESUMEN 7
SUMMARY 8
INTRODUCCIÓN 9
1. IP MULTIMEDIA SUBSYSTEM (IMS) 11
1.1. Surgimiento de la Arquitectura IP Multimedia Subsystem (IMS) 11
1.2. Ventajas de IP Multimedia Subsystem (IMS) 13
1.3. Desventajas de IP Multimedia Subsystem (IMS) 13
2. ARQUITECTURA IMS 15
2.1. Call Session Control Function (CSCF). 15
2.2. Proxy-CSCF. 17
2.3. Interrogating-CSCF. 17
2.4. Serving-CSCF. 18
2.5. Home Subscriber Server (HSS). 18
2.6. SIP Application Server (AS). 19
2.7. Media Resource Function (MRF). 19
2.8. Breakout Gateway Control Function (BGCF). 19
2.9. Media Gateway Control Function (MGCF). 20
2.10. Media Gateway (MGW). 20
2.11. Signaling Gateway (SGW) 20
2.12. IMS Application Level Gateway (IMS ALG) 21
2.13. Session Border Controller (SBC). 21
3. INTERFACES LÓGICAS. 22
3.1. Independencia en el acceso. 24
4. PROTOCOLOS USADOS EN IMS. 27
4.1. SIP (Session Initiation Protocol). 27
4.1.1. Beneficios de SIP. 28
4.1.2. Entidades SIP 29
4.1.3. Mensajes SIP 30
4.1.4. Respuestas SIP 31
4.2. SDP (Session Description Protocol). 32
4.3. Protocolo de Internet versión 6 (IPV6). 34
4.3.1. Principales características 34

4.3.2. Direccionamiento en IPv6 35
4.3.3. Representación de las direcciones IPv6. 35
4.3.4. Representación de los prefijos de las direcciones. 36
4.3.5. Mecanismos de transición básicos. 37
4.4. RTP (Real Time Transport Protocol) 38
4.5. RTCP (Real Time Control Protocol). 39
4.6. COPS (Common Open Policy Service). 40
4.7. RSVP (Resource Reservation Protocol). 42
4.8. Diameter. 43
4.9. Megaco. 44
5. ACCESO A LOS SERVICIOS EN IMS. 45
5.1. Procedimiento de Registro. 46
5.2. Establecimiento de Sesión. 47
5.3. Descubrimiento del punto de entrada a la red IMS (P-CSCF) 48
5.4. Asignación del S-CSCF. 49
6. MECANISMOS PARA EL CONTROL DE TRÁFICO 51
6.1. Autorización de Portadora. 52
6.2. Aprobación de la función de entrega de QoS. 53
6.3. Eliminación de la función de entrega de QoS. 54
6.4. Indicación de liberación de portadora. 54
6.5. Indicación de pérdida/recuperación de portadora. 54
6.6. Revocación de autorización. 54
6.7. Intercambio de identificadores de tarificación. 54
6.8. Flujo de mensajes soportando reserva de QoS. 55
7. IDENTIFICACIÓN. 58
7.1. Identificación de Usuarios. 58
7.1.1. Identidad de Usuario Privada. 58
7.1.2. Identidad de Usuario Pública. 58
8. HERRAMIENTAS DE SIMULACIÓN. 60
8.1. Productos universitarios OPNET. 61
CONCLUSIONES 66
GLOSARIO 67
REFERENCIAS 76

LISTADO DE FIGURAS

Figura 1 Organismos de estandarización de IMS. 12

Figura 2. Estructura en capas IMS. 14

Figura 3. Arquitectura IMS. 16

Figura 4. Roles del CSCF. 16

Figura 5. Interfaces lógicas. 24

Figura 6. Protocolos usados en IMS. 27

Figura 7. Entidades SIP. 30

Figura 8. Encapsulamiento de paquetes IPv6 37

Figura 9. Encabezado RTP. 38

Figura 10. Modelo COPS. 40

Figura 11. Encabezado COPS. 41

Figura 12. Encabezado RSVP. 42

Figura 13. Procedimiento de registro. 46

Figura 14. Establecimiento de Sesión en IMS. 48

Figura 15. Mecanismo general para descubrir el P-CSCF. 48

Figura 16. Asignación del S-CSCF. 50

Figura 17. Entidades SBLP 51

Figura 18. Autorización de portador usando SBLP 53

Figura 19. Flujo de mensajes soportando reserva de QoS 55

Figura 20. Modelo de simulación OPNET 62

Figura 21. Modelamiento con OPNET Modeler® Wireless Suite. 63

LISTADO DE TABLAS

Tabla 1. Interfaces lógicas..... 23

Tabla 2. Información almacenada antes, durante y después del proceso de registro. 47

RESUMEN

Son muchos los beneficios que se logran entorno a la implementación de una arquitectura basada completamente en el Protocolo de Internet; entre otros, se pueden señalar la generación de nuevos servicios, reducción de costos, simplificación de la arquitectura, presencia global de aplicaciones avanzadas y generación de nuevos ingresos. Sin embargo, implica grandes inversiones y un cambio en la tecnología de acceso. De esta manera, con la necesidad de convergencia de las redes y frente a las dificultades de migrar radicalmente las tecnologías de las telecomunicaciones al Protocolo de Internet surge la arquitectura IP Multimedia Subsystem.

En el presente documento se consigna una descripción del estado del arte de la arquitectura IP Multimedia Subsystem. En él, se hace una recopilación de los factores que dieron origen a este modelo de red, identificando sus ventajas, desventajas, estado actual y proyecciones. También, se desglosa cada uno de los componentes que la conforman, así como las funciones, interfaces lógicas, protocolos y los procedimientos que hacen posible el establecimiento de una comunicación multimedia. Por último, se recomienda un software de simulación para el apoyo a investigaciones y desarrollos alrededor de este tema.

Esta investigación fue del tipo exploratorio y se llevó a cabo a través de la ejecución de las siguientes etapas: recopilación de la información, clasificación de la información relevante, análisis de la información y elaboración del documento final.

La arquitectura IP Multimedia Subsystem plantea una solución magnífica para la interconexión de redes con soporte de calidad de servicio; pero, por tratarse de una tecnología que todavía está en proceso de desarrollo y estandarización requiere la participación conjunta de los organismos de estandarización, fabricantes, proveedores de servicio y universidades, para así poder lograr que este modelo de red alcance a corto plazo su madurez tecnológica.

SUMMARY

There are many benefits achieved through the implementation of an architecture based entirely on the Internet Protocol; with IP based networks, it is possible to point out the generation of new services, lower costs, simplified architecture, global presence, advanced applications and generating new revenues. However, this requires large investments and a change in access technologies. In this way, the IP Multimedia Subsystem architecture emerges as a solution to networks convergence. Then, IMS decreases the difficulties to migrate radically telecommunications technologies to the Internet Protocol.

The present document describes the state of the art of the IP Multimedia Subsystem architecture. It includes a compilation of the factors that support this network model, identifying their advantages, disadvantages, current status and projections. Also, it describes every IMS technology component, as well as the functions, logical interfaces, protocols and procedures that make the establishment of a multimedia communication possible. Finally, the document suggests simulation software for supporting research and developments around this issue.

This research was exploratory and it was done through the execution of the following phases: information gathering, classification of relevant information, information analysis and elaboration of the final document.

IP Multimedia Subsystem architecture poses a great solution for the network interconnection with quality of service support, but it is an emerging technology that is still under development and under a standardization process. Therefore, it requires the joint participation of standardization bodies, manufacturers, suppliers' service and universities, to ensure that this network model will achieve in the short term its technological maturity.

INTRODUCCIÓN

Con el vertiginoso avance de las comunicaciones y el posicionamiento cada vez más fuerte de tecnologías basadas en conmutación de paquetes, surge el concepto “ALL IP”, el cual contempla la introducción de nuevos y mejores servicios en multimedia, voz y datos, garantizando calidad de servicio con esquemas de seguridad, considerado una visión industrial sobre el futuro de las redes de comunicaciones, que ofrece diversos modos de acceso que se integran de forma transparente en una capa de red basada en el protocolo de Internet IP; pero la presencia de la arquitectura “ALL IP” en el entorno de las comunicaciones no es suficiente para motivar el tráfico de datos en redes externas, como por ejemplo las redes móviles, de hecho sólo proporciona beneficios a los operadores en lo referente a la reducción de costos de operación y mantenimiento, a la flexibilidad en la prestación de servicios y a la reducción en la complejidad de su arquitectura, facilitando la migración hacía las tecnologías emergentes (1), en la mayoría de los casos transparente para los usuarios. De esta forma, buscando no sólo el beneficio de las empresas de telecomunicaciones sino también introduciendo características que resulten llamativas a los usuarios e impulsando el mercado de las comunicaciones, se incorpora la arquitectura IP Multimedia Subsystem (IMS).

Con IMS, los operadores pueden combinar la calidad y la interoperabilidad de las telecomunicaciones con el rápido e innovador desarrollo de la Internet, disponiendo para la industria de las telecomunicaciones el desarrollo de aplicaciones, mientras que al mismo tiempo se garantiza la entrega de las aplicaciones tradicionales como telefonía y mensajería (2).

IMS ofrece una forma normalizada para entregar servicios basados en IP a comunidades fijas, móviles y cableadas, gracias a la presencia de un núcleo y control común; es la piedra angular de la evolución de las redes actuales a una sola red basada en IP, donde todo tipo de servicios (mensajería, telefonía, entre otros) y los medios (voz, vídeo, imágenes, texto, entre otros) pueden integrarse en una sola experiencia de usuario. Para los consumidores, IMS posibilita opciones de comunicación que perfectamente combinan sesiones de voz en curso con elementos multimedia (vídeo simultáneo mientras se habla) o enriquecidas aplicaciones compartidas con comunicaciones de voz (hablar mientras se reproduce un juego multijugador) (2).

En su estructura interna, IMS adopta una arquitectura superpuesta, cuyo propósito es mantener una capa neutral entre las tecnologías de red heterogéneas subyacentes y las aplicaciones de usuario. De esta forma, los servicios básicos de red pueden ser adaptados a la tecnología de alguna red de acceso y por tanto ser proporcionados de manera uniforme al usuario (1).

Para su implementación, IMS ha adoptado el Protocolo de Inicio de Sesión (SIP), que permite la gestión de recursos de red y el manejo de llamadas a nivel IP. Usando los procedimientos de señalización SIP y los protocolos RTP (Real Time

Protocol), RTCP (Real Time Control Protocol), RTSP (Real Time Streaming Protocol) y RSVP (Reservation Protocol), pueden ser provistas comunicaciones multimedia de alta calidad a través de algún medio de comunicación heterogéneo que incluye acceso inalámbrico, móvil y cableado, permitiendo por ejemplo, la comunicación entre un usuario móvil y uno fijo, conectados a través de un modem XDSL usando un servicio de video telefonía (1).

1. IP MULTIMEDIA SUBSYSTEM (IMS)

La arquitectura IP Multimedia Subsystem (IMS) permite y habilita eficientemente la convergencia de servicios. Es la clave para la prestación de servicios multimedia de telecomunicaciones con un grado de calidad de servicio (QoS) a través de accesos fijos y móviles. Crea nuevas oportunidades para los operadores que quieren ofrecer servicios multimedia atractivos, fáciles de usar, fiables y rentables, incluidos voz, imágenes, texto y video, o cualquier combinación de éstos con los servicios existentes. Los usuarios se benefician, pues pueden disfrutar de atractivos servicios múltiples convergentes, independientemente de la red de acceso y dispositivo (2).

IMS es de acceso independiente; es la única arquitectura normalizada y abierta para prestar servicios basados en IP a las empresas y consumidores, habilitado por un núcleo y control común para las comunidades fijas y móviles. Combina la calidad y la interoperabilidad de las telecomunicaciones con el rápido e innovador desarrollo de la Internet.

Como se implementa con base en las normas estandarizadas, IMS permite a los operadores combinar equipos y aplicaciones de múltiples proveedores, así como a los usuarios móviles acceder a su conjunto personal de servicios dondequiera que ellos estén, sin importar a que operador de red están conectados.

IMS incluye las herramientas y funciones necesarias para manipular numerosos servicios no normalizados de una manera normalizada, garantizando la interoperabilidad, acceso consiente, soporte de políticas, tarificación, seguridad y calidad de servicio, funcionalidades necesarias para satisfacer la demanda de los consumidores a través de atractivas y convenientes ofertas. Básicamente, los servidores de aplicación se ejecutan por encima de la estandarizada arquitectura IMS (2).

1.1. Surgimiento de la Arquitectura IP Multimedia Subsystem (IMS)

IMS fue definido originalmente por 3rd Generation Partnership Project (3GPP); 3GPP es un acuerdo de colaboración que fue establecido en diciembre de 1998. El propósito original de 3GPP era el de producir especificaciones técnicas y reportes técnicos aplicables globalmente para sistemas móviles de 3ra generación (3G), basados en la evolución de redes base GSM y en las tecnologías de acceso radio que estas soportan (UTRAN). Posteriormente, el alcance fue modificado para incluir mantenimiento y desarrollo de GSM, especificaciones técnicas e Informes técnicos, incluyendo tecnologías de radio acceso evolucionadas, por ejemplo, General Packet Radio Service (GPRS) y Enhanced Data Rates for GSM Evolution (EDGE) (3).

La introducción de IMS es especificada en el Release 5, que originalmente se ocupó de la evolución de UMTS. El objetivo del Release 5 fue el de definir los conceptos relacionados con los requerimientos generales y las características de los servicios multimedia IP. El Release 6 adicionó mensajería IP IMS, interconexión con redes de conmutación de circuitos y facturación en IMS (4). En el Release 6 se desarrollaron aplicaciones adicionales que no se pudieron terminar; éstas, son retomadas y terminadas por el Release 7 (5), el cual se enfoca en la disminución de la latencia y mejoras en la calidad de servicio (QoS).

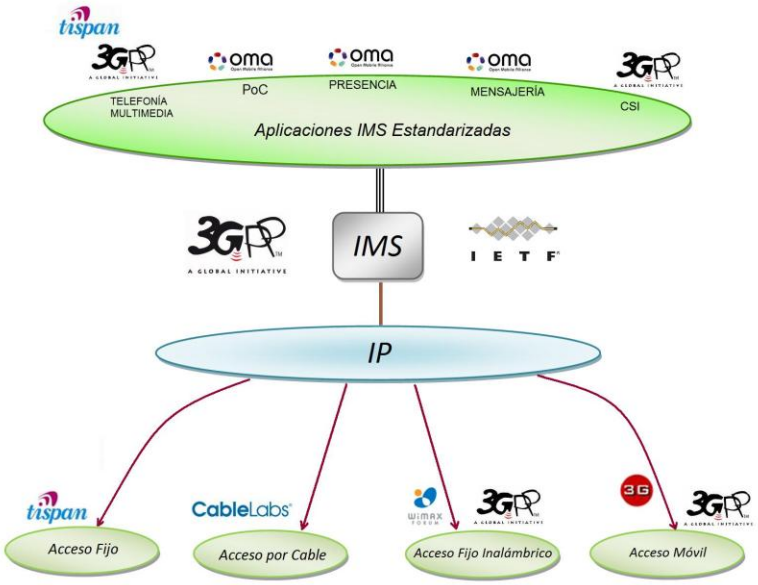
Actualmente, 3GPP trabaja en los Release 8 y 9 que se enfocan en redes completamente IP. Algunos de los temas de estudio son:

- Release 8: Interconexión móvil WLAN, interconexión multimedia entre IMS y redes de conmutación de circuitos, mejoras para el soporte de paquetes por accesos de cable, mejoras del sistema de interconexión entre dos interfaces IMS, telefonía IMS multimedia y servicios suplementarios (6).

- Release 9: Servicios de alineación y migración, registro en zonas densamente pobladas (RED), sistema de alerta pública, selección de redes para accesos No-3GPP, mejoras en el servicio prioritario multimedia, soporte de redes de área personal y mejoras a la gestión de redes personales, convergencia de datos de usuario y mejoras de la interfaz radio (6).

IMS es un estándar reconocido internacionalmente, especificado inicialmente por 3GPP/3GPP2. En la actualidad ha sido acogido por otros grupos de estandarización (Figura 1) como lo son: ETSI/TISPAN, CableLabs, JCP, OMA y WiMAX Forum (2).

Figura 1 Organismos de estandarización de IMS.



1.2. Ventajas de IP Multimedia Subsystem (IMS)

- IMS toma el concepto de arquitectura por capas mediante la definición de una arquitectura horizontal, donde servicios permitidos y funciones comunes pueden ser reutilizados por múltiples aplicaciones. La arquitectura horizontal de IMS permite a los operadores alejarse de la tradicional implementación vertical de nuevos servicios, eliminando la costosa y compleja estructura de red tradicional de superposición de funciones de tarificación, enrutamiento y abastecimiento (2).

- El estándar IMS soporta múltiples tecnologías de acceso, que incluyen GSM, WCDMA, CDMA2000, cobre, acceso de banda ancha por cable, WLAN/WiFi y WiMAX, gracias a que su diseño es completamente independiente del acceso, esto significa que con una única red de servicio se puede entregar servicios multimedia, independientemente del lugar o dispositivo de usuario.

- Se mejora la gestión de movilidad, ya que el usuario puede tener acceso a los servicios desde cualquier red.

- Comparte los recursos de control de sesión, datos de usuario y transporte entre diferentes aplicaciones, lo que supone, por un lado, una mejora en la rapidez y eficiencia con la que se desarrollan nuevas aplicaciones, y por otro, una disminución de los costos de mantenimiento del servicio final. Posibilita los mecanismos de gestión de la Calidad de Servicio necesarios para poder ofrecer al usuario una buena experiencia de servicio y a la vez permitir al operador el control sobre la eficiencia en el uso de los recursos de la red.

- Permite ofrecer servicios combinados, es decir, aquellos que hacen posible combinar diferentes tipos de contenidos multimedia (voz, vídeo, mensajería, streaming, entre otros) en un único servicio que brinda al usuario una experiencia de comunicaciones mucho más rica y valiosa.

- Facilita la creación de redes multi-proveedor. IMS, como estándar, implementa un entorno en el que las aplicaciones SIP de diferentes proveedores pueden integrarse en la red del operador de forma rápida. Además, la clara separación entre las diferentes capas permite la participación de diferentes proveedores en una misma red de forma sencilla y eficiente (7).

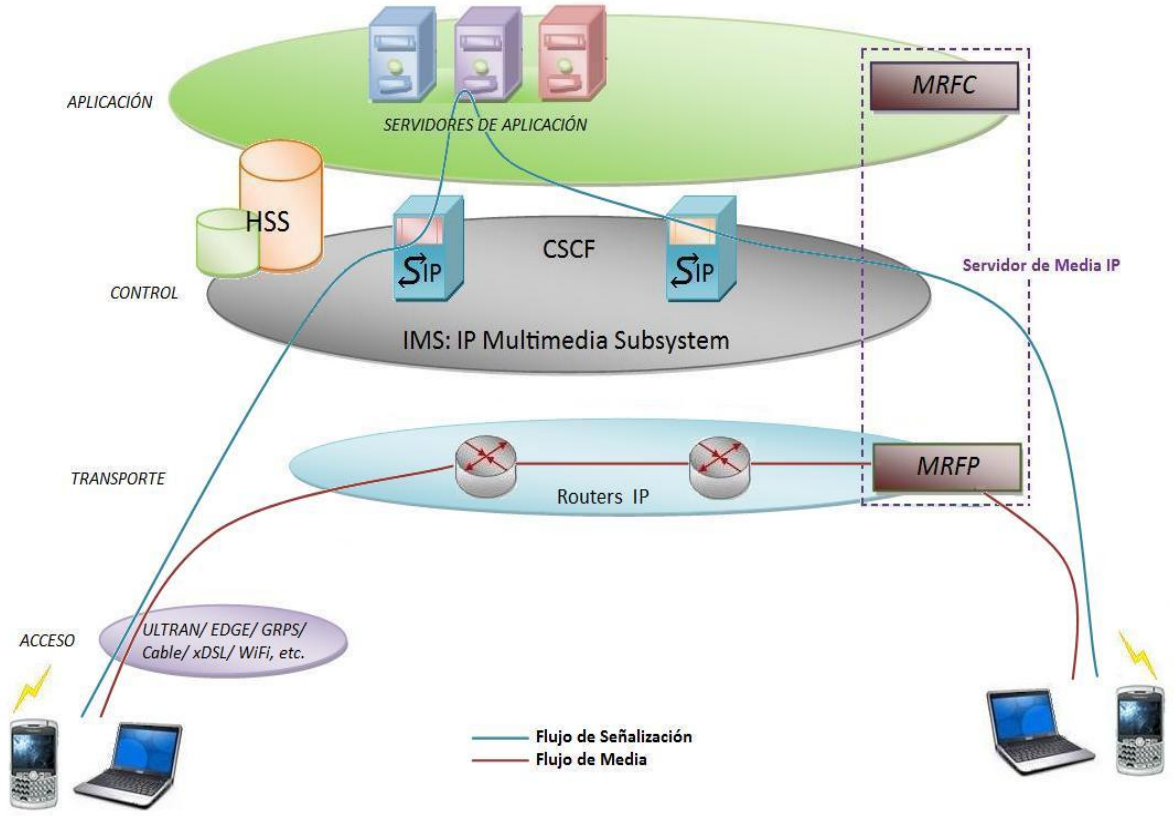
1.3. Desventajas de IP Multimedia Subsystem (IMS)

- Ya que IMS inicialmente fue desarrollada para un entorno móvil, su evolución en estas redes ha sido más acelerada que para las redes fijas.

- A pesar de que IMS es relativamente reciente describe la arquitectura general de las redes futuras y plantea muchos cambios en términos de modificaciones de terminales, políticas de desarrollo de banda ancha y modos de operación.

Es claro que los proveedores de servicio necesitan planear sus estrategias en términos de sus circunstancias particulares. La convergencia encarna una meta de largo tiempo y solo IMS proporciona la posibilidad de alcanzar convergencia técnica en las capas de red y de servicio (2). Por lo tanto, una desventaja de IMS es su relativa juventud, ya que hay temas en los que hasta ahora está incursionando; vale la pena resaltar el trabajo que se está realizando para mejorar aspectos ya incluidos en las primeras especificaciones de IMS y los estudios realizados para incluir otros aspectos que no se habían tenido en cuenta en los mismos, ya sea que estos estudios y propuestas provengan de entidades como 3GPP, 3GPP2 y TISPAN o de desarrollos de investigaciones a nivel académico.

Figura 2. Estructura en capas IMS.



2. ARQUITECTURA IMS.

La arquitectura IP Multimedia Subsystem (IMS) es definida por 3GPP. Esta arquitectura incluye numerosas funciones lógicas, que pueden estructurarse en 4 capas (Figura 2): Capa de Acceso, de Transporte, de Control y de Aplicación, cada una con componentes y funciones específicas que permiten en conjunto el desarrollo de IMS (8).

La capa de Acceso abarca todo tipo de red de acceso, como es el caso de GSM, CDMA2000, UMTS, cable, acceso de banda ancha por cable, X-DSL, WLAN/WiFi y WiMAX (2). La capa de Transporte representa una red IP conformada básicamente por routers que integran mecanismos de calidad de servicio. La capa de Control consiste de controladores de sesión responsables del encaminamiento de la señalización entre usuarios y de la invocación de los servicios. Hacen parte de ella el Call Session Control Function (CSCF) y el Home Subscriber Server (HSS). La capa de Aplicación la conforman servidores de aplicación (Aplication Server, AS) y funciones de recursos multimedia (Multimedia Resource Function, MRF), encargados de proporcionar a los usuarios servicios multimedia atractivos e innovadores (8).

Desde un punto de vista estructural, IMS es construida alrededor de un conjunto de componentes de procesamiento de señalización y entidades de manipulación y almacenaje de datos (Figura 3).

2.1. Call Session Control Function (CSCF).

El Call Session Control Function (CSCF) es el corazón de la arquitectura IMS, es usado para procesar la señalización SIP y juega un papel fundamental en el soporte de las llamadas de usuario. La función principal del CSCF es la de proporcionar control de sesión para terminales y aplicaciones usando la red IMS (2); es responsable por las tareas de enrutamiento y traducción de llamadas, gestión de calidad de servicio (QoS), configuración de las funciones de transcodificación multimedia, en caso de que las partes implicadas involucren diferentes interfaces de tecnologías de acceso y por la integración de servicios con perfiles de usuario y privilegios de comunicación (1).

El CSCF puede desempeñar tres roles diferentes (Figura 4): el de Proxy-CSCF (P-CSCF), el de Interrogating-CSCF (I-CSCF) y el de Serving-CSCF (S-CSCF) (8).

Figura 3. Arquitectura IMS.

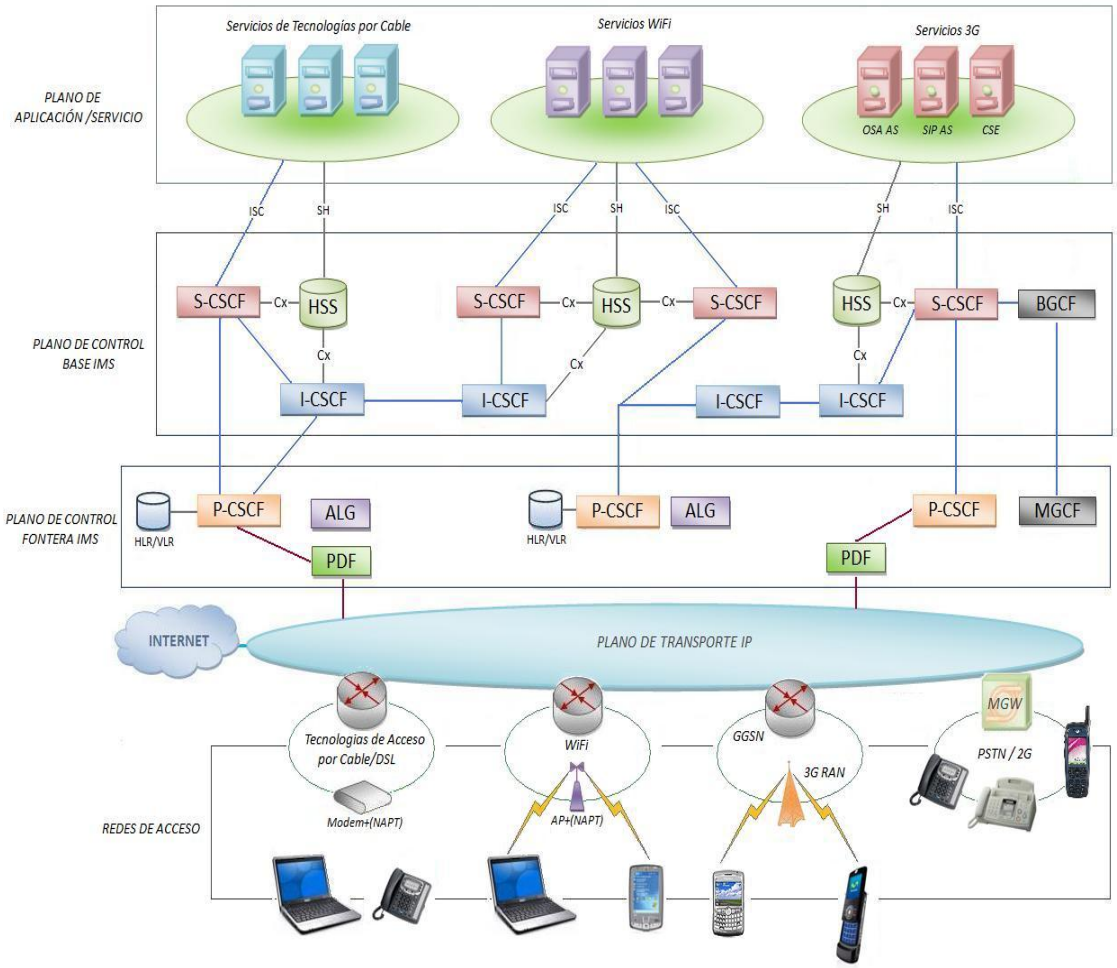
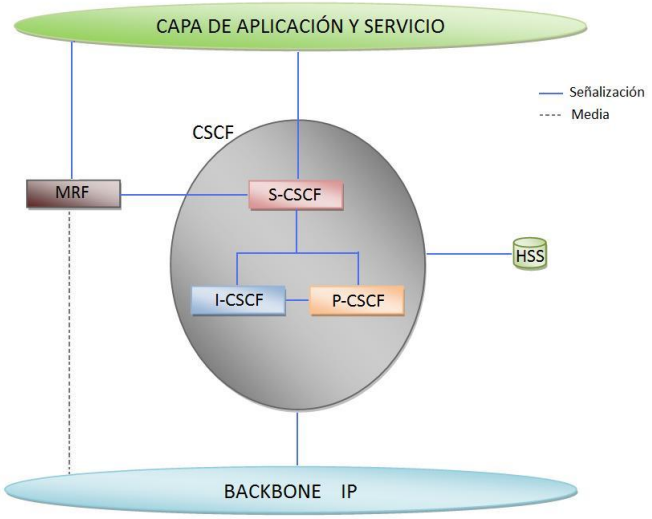


Figura 4. Roles del CSCF.



2.2. Proxy-CSCF.

El Proxy CSCF (P-CSCF) es el primer punto de contacto que el dominio IMS presenta a los terminales de usuario. Su dirección es descubierta por el terminal durante la activación de un contexto PDP para el cambio de mensajes de señalización SIP (8).

El P-CSCF realiza las siguientes funciones (8) (2):

- Proporciona una trasmisión segura de la señalización SIP con el terminal.
- Encamina la respuesta SIP REGISTER emitida por el terminal a la entidad I-CSCF desde el nombre del dominio nominal.
- Encamina las respuestas SIP emitidas por el terminal al S-CSCF cuyo nombre ha sido obtenido en la respuesta del proceso de registrarse.
- Interfaz para la arquitectura de control de políticas para la autorización multimedia.
- Compresión/Descompresión de la señalización SIP si es requerida.
- Generación de Call Detailled Record (CDRs).
- Proporciona control local para los servicios de emergencia.
- Punto donde se ejerce la política de calidad de servicio dentro de la red IMS visitada.

2.3. Interrogating-CSCF.

El Interrogating CSCF (I-CSCF) es el primer punto de contacto de la red IMS origen con otras redes IMS, realizando la interoperación entre ellas.

Las funciones realizadas por la entidad I-CSCF incluyen (8) (2):

- Asignar un S-CSCF a un usuario durante el proceso de registro.
- Dirigir las peticiones SIP recibidas desde otra red hacía el S-CSCF.
- Obtener la dirección del S-CSCF.
- Interrogar al Home Subscriber Server (HSS) para ayudar al S-CSCF a encontrar donde está registrado el usuario o a seleccionar un nuevo S-CSCF si el usuario no está registrado.
- Realizar balance de carga entre S-CSCFs.
- Ocultar la configuración y topología específica de la red origen de otros operadores de red, proporcionando un solo punto de entrada a la red.
- Soportar funciones de cortafuegos.
- Generación de Call Detailled Record (CDRs).

Pueden existir varias I-CSCF dentro de una red IMS, siendo éste un nodo opcional en la arquitectura de IMS. El sistema podría ser configurado de modo que el P-CSCF pudiera entrar en contacto con el S-CSCF directamente (9).

2.4. Serving-CSCF.

El Serving-CSCF es el nodo central para el suministro de la señalización SIP y el corazón del sistema IMS, encargado de realizar la gestión de la sesión. Pueden haber varios S-CSCFs en la red con diversas funcionalidades, elegidos basándose en los servicios solicitados o en las capacidades del móvil (2).

Las funciones realizadas por el S-CSCF son (8) (9):

- Traducción de la solicitud de llamada del P-CSCF, relacionándola con la identidad de usuario.
- Transferencia de información a los puntos finales involucrados en una sesión, a través de sus P-CSCFs asociados.
- Interacción con los servidores de aplicación después de haber analizado los criterios de disparo de los servicios correspondientes.
- Mantenimiento de la sesión.
- Interacción con otros servicios.
- Facturación.
- Generación de Call Detailled Record (CDRs).

2.5. Home Subscriber Server (HSS).

El Home Subscriber Server (HSS) es la base de datos maestra que contiene la información de usuario y suscriptor para ayudar a las entidades de red a manejar las llamadas y las sesiones (2). La información almacenada incluye: la identidad de usuario, información de registro, parámetros de acceso, así como la información que permite la invocación de los servicios de usuario (8). El HSS se comunica con el I-CSCF y el S-CSCF para proporcionar la información sobre la localización del suscriptor y la información de suscripción del cliente (2).

El HSS proporciona las siguientes funciones (2) (9):

- Tratamiento de llamadas.
- Autorización de acceso.
- Autenticación.
- Gestión de movilidad (siguiendo la pista de qué entidad de control de sesión está sirviendo al usuario).
- Ayuda en el establecimiento de sesión y en el suministro y autorización de servicios.

Cuando un usuario se registra en el dominio IMS, el perfil de usuario (información relevante de los servicios que le son proporcionados) es descargado del HSS al CSCF. Para el establecimiento de sesión, el HSS proporciona información de cual CSCF atiende al usuario. Cuando más de un HSS es desplegado en la red, se necesita una Función de Localización del Subscriptor (SLF) para localizar el HSS que tiene los datos de la subscripción para un usuario dado (2).

2.6. SIP Application Server (AS).

Todas las aplicaciones y servicios de IMS se ejecutan en los servidores de aplicación SIP. Un servidor de aplicación SIP puede estar dedicado a un solo servicio o a prestar varios servicios, pudiéndose combinar éstos desde diferentes servidores de aplicación creando una experiencia unificada para el usuario. Por ejemplo, se puede desde una sola aplicación terminal combinar simultáneamente los servicios de presencia y video llamada aunque estén localizados en diferentes servidores de aplicación (2).

2.7. Media Resource Function (MRF).

El Media Resource Function (MRF) proporciona servicios multimedia en la red e implementa funciones para gestionar y procesar flujos de voz, video, texto para hablar y tras-codificación de datos multimedia. Un MRF normalmente está sólo involucrado cuando una aplicación IMS requiere proporcionar un servicio multimedia, utilizándose únicamente durante la aplicación. Además, permite multiconferencias mezclando los flujos de varios participantes (2).

El MRF está dividido en el Media Resource Function Controller (MRFC) y en el Media Resource Function Processor (MRFP), similares en función al Media Gateway Control Function (MGCF) y al Media Gateway (MGW) (9). El MRFC es un nodo de señalización que actúa como un agente de usuario SIP para el S-CSCF y controla los flujos de medios establecidos por el MRFP, basándose en información suministrada por el S-CSCF y el servidor de aplicaciones. El MRFP es un nodo multimedia que provee la trans-codificación esencial y funciones adaptables de contenido (2).

2.8. Breakout Gateway Control Function (BGCF).

El Breakout Gateway Control Function (BGCF) es el responsable de seleccionar el operador y/o el sitio de comienzo para establecer sesiones con la PSTN. Es la entidad lógica dentro de la red IMS que decide como encaminar las sesiones de telefonía iniciadas en la red IMS y destinadas a una red de conmutación de circuitos (PSTN). Las redes de conmutación de circuitos pueden ser cualquier red heredada, PSTN u otras redes inalámbricas (2).

El BGCF elige la red en la que se realiza la salida hacia la red PSTN o de conmutación de circuitos. Si el BGCF determina que esta salida ocurre en la misma red en la que se encuentra (el BGCF), entonces elegirá el Media Gateway Control Function (MGCF) encargado de la interacción con la red PSTN. Si la salida es hacia otra red, el BGCF encaminará la señalización al BGCF de la red seleccionada (9).

2.9. Media Gateway Control Function (MGCF).

El Media Gateway Control Function (MGCF) es el nodo central de la puerta de entrada de la PSTN, responsable de controlar los recursos multimedia usados cuando el tráfico necesita fluir entre redes utilizando diferentes medios, normalmente entre una red TDM y una red IP (2).

El MGCF ejecuta las siguientes funciones (8):

- Realiza control sobre uno o más MGWs, permitiendo más escalabilidad en la red.
- Maneja la conexión entre la portadora PSTN y el flujo IP.
- Convierte mensajes SIP en mensajes de Megaco o de ISUP.
- Recibe un mensaje SIP del CSCF y determina que conexión realizar con el MGW.
- Crear el mensaje ISUP apropiado y lo envía, vía IP, al Signaling Gateway (SGW).
- Selecciona el CSCF idóneo, con el fin de entregar la señalización SIP generada a la red IMS.

Por simplicidad el MGCF podría ser integrado con el Media Gateway (MGW) (9).

2.10. Media Gateway (MGW).

El Media Gateway Control Function (MGCF) es el que controla la interconexión de redes, pero el Media Gateway (MGW) es el que hace el procesamiento de la información multimedia entre los usuarios finales. Su función principal es convertir medios de un formato a otro (9).

El MGW es responsable de proporcionar la interconexión de flujo multimedia a través de diversas redes, permitiendo ínter- funcionamiento entre diferentes formatos de transporte de medios RTP/UDP/IP y TDM, así como la transcodificación y tratamiento de flujos de voz y video, en caso de requerirse (2).

2.11. Signaling Gateway (SGW)

Una característica esencial de IMS es que la comunicación entre los componentes está basada en IP; sin embargo existen dos interfaces que no se apoyan en este protocolo y se utilizan para interactuar con una red tradicional (la PSTN o una red móvil antigua). Estas interfaces son: el camino de los flujos y el de señalización hacia la red antigua.

El SGW evita que el MGCF soporte SS7. Su función es convertir SS7 a IP, cambiando las capas más bajas de SS7 a IP (9).

2.12. IMS Application Level Gateway (IMS ALG)

El IMS ALG proporciona la funcionalidad de aplicación necesaria a la pila de protocolos SIP/SDP para que interactúen aplicaciones IPv4 e IPv6. Cuando el IMS ALG recibe un mensaje SIP de los CSCFs o de una red externa SIP IPv4, cambia los parámetros apropiados de SIP/SDP, traduciendo las direcciones IPv6 a IPv4 y viceversa (9).

2.13. Session Border Controller (SBC).

Los Session Border Controllers (SBC) realizan las funciones de control de borde en las especificaciones IMS, son puertas de entrada IP a IP desplegadas en la frontera entre una red IMS y otras redes (interface red - red, NNI). Para un acceso banda ancha, el P-CSCF y las funcionalidades de cumplimiento de políticas, pueden implementarse como un SBC soportando la interface red - usuario, UNI (2).

El SBC gestiona las sesiones IMS (correlacionando señalización y flujo multimedia) para garantizar seguridad, calidad de servicio (QoS), acuerdos de niveles de servicio (SLAs), NAT/FW transversal y otras funciones críticas para flujos IP en tiempo real. Puede ser usado para la traducción de direcciones; entre direcciones privadas y públicas IPv4 o entre direcciones IPv4 e IPv6 (2).

3. INTERFACES LÓGICAS.

Potencialmente, cada red de conmutación de paquetes es compatible con la arquitectura de IMS y puede ser integrada a este entorno implementando interfaces lógicas, que en su mayoría se presentan como diferentes manifestaciones del Protocolo de Inicio de Sesión (SIP). SIP proporciona tal flexibilidad que su estructura de mensaje se articula en el entorno del Protocolo de Descripción de Sesión (SDP), cuyo formato permite la definición de nuevos mensajes y parámetros de asociación, sin afectar los procedimientos existentes (1).

3GPP ha estandarizado esas interfaces lógicas. Las principales de estas interfaces son mostradas en la Figura 5 y se resumen en la
Tabla **1** (10).

La interfaz Gm realiza la comunicación de señalización entre el usuario IMS y la red base IMS, ejecutando las siguientes funciones (1):

- Descubrimiento y utilización del P-CSCF.
- Presentación de peticiones de utilización de servicios.
- Gestión de movilidad.

Adicionalmente a través de la interfaz Gm, un usuario puede conectarse a la red IMS y ser provisto con una serie de procedimientos genéricos (1):

- Registro de usuario: La red IMS identifica el usuario conectado a ella y realiza el registro para varios servicios.
- Roaming: El usuario puede acceder libremente a una red IMS externa, mientras usa un servicio IMS, sin sufrir interrupción del servicio o experimentar degradación en la calidad de la comunicación.
- Handover: Un usuario puede continuar usando un servicio IMS mientras se traslada y su terminal entrega su sesión a otra red de acceso.
- Servicio de tarificación: Los costos de utilización del servicio son planos e independientes de la red de acceso, permitiendo por primera vez la desvinculación de los servicios suministrados por la infraestructura de red subyacente.

La interfaz Mw tiene dos presentaciones: una para las comunicaciones red a red (NNI), usada para el manejo de los datos de usuario a través de plataformas IMS exteriores y otra para las comunicaciones entre el usuario y la red (UNI), que realiza la comunicación entre el S-CSCF y los P-CSCFs de la misma red IMS (1).

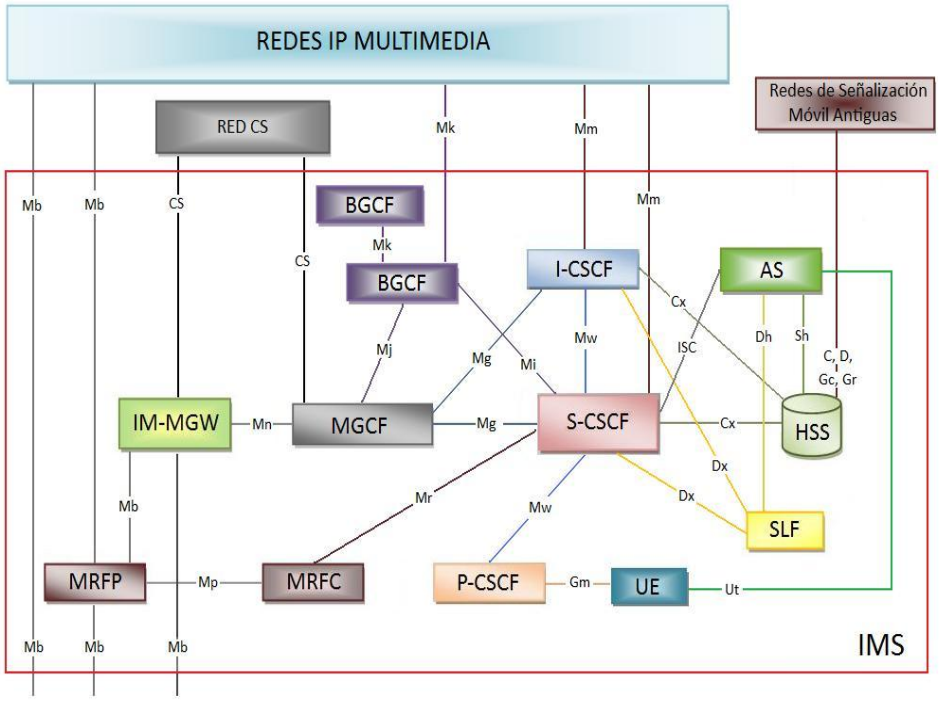
El S-CSCF se comunica con el HSS utilizando la interfaz Cx y con el AS por medio de la interfaz de control de servicio (ISC). La interfaz ISC es usada para transferir mensajes de notificación entre el AS y el S-CSCF pertinentes a la identidad de usuario, estado de registro, capacidades del terminal y características del servicio (2).

El AS se comunica con HSS por medio de la interfaz intra – operador Sh. Sobre Sh, un HSS realiza una vigilancia de la información sujeta al AS perteneciente a la red IMS origen (1).

Tabla 1. Interfaces lógicas.

Nombre de la Interfaz	Entidades IMS (Punto de referencia)	Descripción	Protocolo
Cx	I-CSCF, S-CSCF y HSS	Usada para comunicación entre I-CSCF/S-CSCF y el HSS.	Diamater
Dx	I-CSCF y un SLF	Usada por el I-CSCF para encontrar un HSS en un ambiente multi HSS.	Diamater
Gm	UE y P-CSCF	Usada para intercambiar mensajes entre UE y los CSCFs.	SIP
Go	PDF, GGSN	Permite control de QoS en el plano de usuario e intercambio de información correlacionada de tarificación entre una red IMS y una red acceso.	COPS, Diamater
Gq	P-CSCF, PDF	Usada para el intercambio de información relacionada a decisión de políticas entre P-CSCF y PDF.	Diamater
ISC	S-CSCF, I-CSCF y AS	Usada para intercambiar mensajes entre el CSCF y el AS.	SIP
Ma	AS y I-CSCF	Usada directamente para el manejo de requerimientos SIP destinados a una identidad de servicio pública almacenada por el AS.	SIP
Mg	MGCF y I-CSCF	MGCF convierte señalización ISUP a señalización SIP y remite señalización SIP al I-CSCF.	SIP
Mi	S-CSCF y BGCF	Usada para intercambiar mensajes entre el S-CSCF y el BGCF.	SIP
Mj	BGCF y MGCF	Usada para el intercambio de mensajes entre el BGCF y el MGCF de la misma red IMS.	SIP
Mk	BGCF y otro BGCF	Usada para el intercambio de mensajes entre BGCFs de diferentes redes IMS.	SIP
Mm	I-CSCF, S-CSCF y red IP externa	Usada para el intercambio de mensajes entre redes IMS y redes IP externas.	SIP
Mn	MGCF y IM MGW	Permite el control de recursos en el plano de usuario.	H.248
Mp	MRFC, MRFP	Usada para el intercambio de mensajes entre el MRFC y el MRFP.	H.248
Mr	S-CSCF y MRFC	Usada para el intercambio de mensajes entre el S-CSCF y el MRFC.	SIP
Mw	P-CSCF, I-CSCF y S-CSCF	Usada para el intercambio de mensajes entre CSCFs.	SIP
Sh	AS (SIP-AS o OSA CSCF) y un HSS	Usada para el intercambio de mensajes entre el AS y el HSS.	Diamater
Ut	UE y AS	Habilita al UE para gestionar información relacionada a sus servicios.	HTTP

Figura 5. Interfaces lógicas.



3.1. Independencia en el acceso.

Uno de los objetivos de 3GPP Release 6 consistió en mejorar la arquitectura IMS, para que en la medida de lo posible fuera independiente de la tecnología de acceso. Esto permite a los usuarios acceder a los mismos servicios sin importar que tipo de tecnología estén usando (11).

A pesar de esto, hay un número de interfaces específicas inevitables en la capa de transporte (11):

- Interfaces comunes para la recopilación de información contable desde la red de acceso (Gq).
- Interfaces para la coordinación y la ejecución de QoS a nivel de portador (Go).

Por lo tanto, estas interfaces y las funcionalidades IMS que están directamente conectadas a ellas, deben ser adaptadas a las características de las tecnologías de las capas mas bajas. Estas funcionalidades son las siguientes (11):

- El P-CSCF es la entidad IMS que tiene algunas funciones que deben ser adaptadas a su tecnología subyacente. Estas funciones de los P-CSCF son:

  - *Protocolo de compresión de mensajes SIP:* Cada tecnología de acceso puede utilizar diferentes protocolos de compresión para reducir el tamaño del

mensaje IMS. Por ejemplo, el método de compresión utilizado en WLAN puede ser diferente al usado por UTRAN. Además, en el caso de las líneas de acceso banda ancha a través de cobre, el protocolo de compresión puede ser simplemente ignorado en el P-CSCF.

- *Funciones de seguridad para la sesión*: El nivel de seguridad también depende de la tecnología de acceso. En 802,11 por causa de compartir seguridad intrínseca baja y media, el operador puede usar un túnel IPSec entre el UE y P-CSCF. Sin embargo, en X-DSL no hay necesidad de mantener una seguridad estricta. Además, el operador también puede utilizar protocolos de seguridad en la capa de sesión.

- *Funcionalidades de QoS:* El P-CSCF extraerá los parámetros multimedia de la sesión que existen en el cuerpo de los mensajes SIP/SDP enviados a la PDF. Estos parámetros describen el tipo de flujo (voz, vídeo), sus códecs y los niveles de calidad de servicio (QoS) requeridos. La PDF atendiendo los parámetros de sesión, perfil de usuario y políticas de red envía un mensaje al PEP que reside en el GGSN. Después, el GGSN reserva los recursos multimedia para la sesión de acuerdo a lo recibido en el mensaje. Sin embargo, en el caso de WLAN, no se da necesariamente el proceso de reserva de recursos. Por lo tanto, el P-CSCF no necesita comenzar el proceso de reserva de recursos y extraer los parámetros multimedia de la sesión.

- Application Level Gateway (ALG): es otro elemento funcional cuya presencia en el entorno IMS depende de las tecnologías subyacentes. ALG es requerido cuando se pretende modificar los mensajes IMS que pasan a través de NAT. Hay algunos encabezados en mensajes IMS, tales como Contact, Via, To and From que contienen la dirección IP de los puntos finales, de modo que cada modificación en la dirección IP debería ser portada en las cabeceras de estos mensajes SIP. ALG es la funcionalidad que presta especial cuidado a éstas modificaciones en IMS y es necesaria cuando la red de acceso IP (IPv4) es diferente del dominio IP IMS (IPv6), o cuando el operador utiliza NAT.

- Home Location Register (HLR): Para el multi-acceso a la red IMS, es más conveniente implementar la funcionalidad HLR separada del Home Subscriber Server (HSS). Esto es básicamente porque la información de ubicación de usuario depende de la tecnología de acceso. En 3GPP IMS, el HSS está a cargo de la localización de los usuarios, soportando las funciones del HLR. En la tecnología 3G la identificación de la celda indica el punto de acople de usuario. Los dispositivos 3G son conscientes de su ubicación y obtienen esta información durante su fase de conexión a la red, siendo capaces de ubicar la información de identificación de la celda en un encabezado dedicado en el requerimiento REGISTER y transferirlo a su dominio IMS. En consecuencia, la identificación de la celda será almacenada en el HSS. Sin embargo, en el caso de otras tecnologías de acceso, hay dos consideraciones principales que no apoyan la idea de separación entre el HLR y el HSS: en primer lugar, la definición de un punto de información de acople es de alguna manera un reto que depende fuertemente de

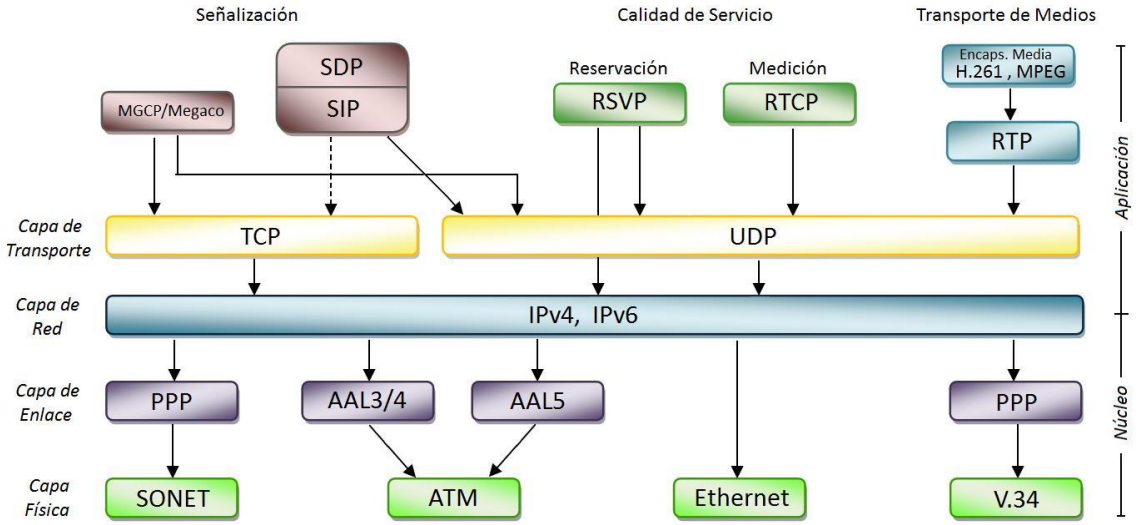
la tecnología implementada. Por ejemplo, en WiFi, el Service Set Indentifier (SSID) también puede ser utilizado para indicar el punto de acople. SSID es un carácter identificador de 32 bits adjuntado al encabezado de los paquetes enviados a través de una WLAN, que actúa como una contraseña cuando un dispositivo móvil intenta conectarse al Basic Service Set (BSS). El BSS es un punto de acceso (AP), que está conectado a la red cableada y a un conjunto de estaciones inalámbricas. El SSID diferencia entre una WLAN de otra, de modo que todos los puntos de acceso y dispositivos que intentan conectarse a una WLAN deben utilizar el mismo SSID. En segundo lugar, hay algunos dispositivos que no son capaces de capturar su información de ubicación. Esto es un problema, especialmente con dispositivos de telefonía antiguos, en tecnologías de acceso fija, como DSL y Cable. Por lo tanto, deben preverse otras funcionalidades para añadir información de localización en el encabezado del paquete.

De acuerdo a esto, la estructura del HLR y las interfaces relacionadas deben adaptarse a la tecnología de acceso. La información de ubicación del usuario será creada de acuerdo a las características del acceso y registrada en el HLR. Después, el HSS como la principal base de datos de perfil de usuario proporciona un enlace a esta información (11).

4. PROTOCOLOS USADOS EN IMS.

Para la especificación de IMS, 3GPP e IETF establecieron un acuerdo que ha ligado fuertemente el desarrollo del estándar IMS al trabajo de la IETF, al punto que ha tenido que acelerar la estandarización de los protocolos IP emergentes que se emplean en IMS, a la vez que realizar especificaciones exclusivas para 3GPP. De esta manera, en el entorno de red IMS se utilizan principalmente protocolos de la IETF (12).

Figura 6. Protocolos usados en IMS.



4.1. SIP (Session Initiation Protocol).

SIP es el principal protocolo de señalización usado en las redes IMS, definido por la Internet Engineering Task Force (IETF) y seleccionado por 3GPP como un estándar para IMS en el Release 5 (2).

SIP aporta las funciones para el registro, establecimiento, liberación y mantenimiento de las sesiones IMS, lo que incluye funciones de enrutamiento de sesiones e identificación de usuarios y nodos; también habilita todo tipo de servicios suplementarios (13). En SIP, solo hay un único protocolo que trabaja de extremo a extremo, encargado del establecimiento, finalización y gestión de sesiones. SIP está también diseñado para permitir sesiones multimedia adicionales y para que participantes sean dinámicamente añadidos o removidos de una sesión (2). Por otro lado, el protocolo SIP tiene una estructura similar a HTTP, incluso comparte los códigos de respuesta, lo que facilita el desarrollo de servicios, puesto que es similar a construir aplicaciones web. Tanto SIP como HTTP son protocolos de texto, que permiten incluir contenido MIME (Multipurpose Internet Mail Extensions) en el cuerpo de sus mensajes. De este modo, los

mensajes del protocolo SDP (Session Description Protocol) se transfieren en los mensajes SIP (12).

Un requerimiento SIP está constituido de encabezados, al igual que un mando SMTP, siendo éste un protocolo textual. SIP ha sido extendido con el fin de soportar numerosos servicios tales como mensajería instantánea, transferencia de llamada, conferencia y los servicios complementarios de telefonía, reemplazando el protocolo ISUP e INAP, utilizados para el control de llamada en la Red Telefónica Conmutada y para el control de servicio en la arquitectura de Red Inteligente, respectivamente (12).

El protocolo SIP es exclusivo de señalización. Una vez la sesión es establecida, los participantes intercambian directamente su tráfico (audio, video) a través del protocolo RTP (Real-Time Transport Protocol). Por otra parte, como SIP no es un protocolo de reserva de recursos, no puede asegurar la calidad de servicio; se trata de un protocolo de control de llamada y no de control del medio. SIP tampoco es un protocolo de transferencia de fichero tal como http, usado con el fin de transportar grandes volúmenes de datos; ha sido concebido para transmitir mensajes de señalización cortos con el fin de establecer, mantener y liberar sesiones multimedia (13).

4.1.1. Beneficios de SIP.

Los principales beneficios de SIP que lo hacen más idóneo para señalización y control en IMS son (14):

- *Simplicidad:* SIP es un protocolo muy simple. El tiempo de desarrollo del software es muy corto comparado con los productos de telefonía tradicional. Debido a la similitud de SIP a HTTP y SMTP, la reutilización de código es posible.

- *Extensibilidad:* SIP ha aprendido de HTTP y SMTP; ha construido un exquisito grupo de funciones de extensibilidad y compatibilidad.

- *Modularidad:* SIP fue diseñado para ser altamente modular. Una característica clave es su uso independiente de protocolos. Por ejemplo, envía invitaciones a las partes de la llamada independiente de la sesión misma.

- *Escalabilidad:* SIP ofrece dos servicios de escalabilidad: procesamiento de servidor, ya que tiene la habilidad para ser Stateful o Stateless y arreglo de conferencia, puesto que no hay requerimiento para un controlador central multipunto, de modo que la coordinación de la conferencia puede ser completamente distribuida o centralizada.

- *Integración:* SIP tiene la capacidad para integrarse con la Web, E-mail, aplicaciones de flujo multimedia y otros protocolos.

- *Interoperabilidad:* porque es un estándar abierto, SIP puede ofrecer interoperabilidad entre plataformas de diferentes fabricantes.

4.1.2. Entidades SIP

SIP define dos tipos de entidades: los clientes y los servidores (13):

- *El Servidor Proxy (Proxy Server):* recibe solicitudes de clientes que él mismo trata o encamina hacia otros servidores después de haber realizado eventualmente ciertas modificaciones sobre éstas solicitudes.

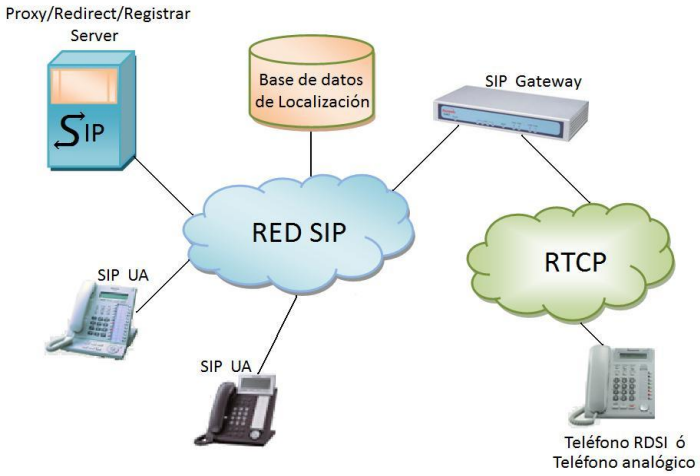
- *El Servidor de Redireccionamiento (Redirect Server):* se trata de un servidor que acepta solicitudes SIP y traduce la dirección SIP destino en una o varias direcciones de red y las devuelve al cliente. De manera contraria al Proxy Server, el Redirect Server no encamina las solicitudes SIP. En el caso de la devolución de una llamada, el Proxy Server tiene la capacidad de traducir el número del destinatario recibido en el mensaje SIP en un número de reenvió de llamada y encaminar la llamada al nuevo destino, de manera transparente para el cliente originario; para el mismo servicio, el Redirect Server devuelve el nuevo número (numero de reenvió) al cliente, el cual se encarga de establecer la llamada hacia el nuevo destino.

- *El Agente Usuario (User Agent):* se trata de una aplicación sobre un equipo de usuario que emite y recibe solicitudes SIP. Se materializa por un software instalado sobre un equipo de usuario (UE): un computador personal, un teléfono IP o una estación móvil.

- *El Registrador (Registrar):* se trata de un servidor que acepta las solicitudes SIP REGISTER. SIP dispone de la función de registro de los usuarios. El usuario indica por un mensaje REGISTER emitido al registrador la dirección donde es localizable (dirección IP). El registrador es una función asociada a un Proxy Server o a un Redirect Server que actualiza una base de datos de localización. Un mismo usuario puede registrarse sobre distintos UAs SIP, en este caso, la llamada le será entregada sobre el conjunto de estas UAs.

En una red IP Multimedia Subsystem (IMS), el Proxy Server corresponde a la entidad Call Session Control Function (CSCF) mientras la base de datos de localización es representada por la entidad Home Subscriber Server (HSS).

Figura 7. Entidades SIP.



4.1.3. Mensajes SIP

SIP usa mensajes para la conexión y control de llamadas. Hay dos tipos de mensajes SIP: mensajes de peticiones y respuestas.

Los mensajes SIP más utilizados son (14):

- *INVITE:* Solicita el inicio de una llamada. Los campos de la cabecera contienen:

• Dirección origen y dirección destino.
• El asunto de la llamada.
• Prioridad de la llamada.
• Peticiones de enrutamiento de la llamada.
• Preferencias para la ubicación de usuario.
• Características deseadas de la respuesta.

- *TRYING:* Indica que el servidor proxy está tratando de establecer la comunicación.

- *RINGING:* Indicación de aviso de llamado.

- *BYE:* Solicita la terminación de una llamada entre dos usuarios.

- *REGISTER:* Informa a un servidor de registro la ubicación actual del usuario.

- *ACK:* Usado para facilitar un intercambio confiable de mensajes entre las partes. Confirmación de diferentes campos del mensaje INVITE.

- *CANCEL:* Cancela una solicitud pendiente.

- *OPTIONS:* Solicita información a un Host acerca de sus propias capacidades. Se utiliza antes de iniciar la llamada a fin de averiguar si ese host tiene las capacidades requeridas por la sesión.

- *200OK:* Sirve para enviar confirmaciones satisfactorias de diferentes sucesos.

- *SUBSCRIBE:* Permite la subscripción de una entidad SIP a un evento.

- *NOTIFY:* Notifica una subscripción.

- *PUBLISH:* Publica el estado de una subscripción.

- *REFER:* Reenvía el receptor hacia un recurso identificado. También permite emular distintos servicios o aplicaciones incluyendo la transferencia de llamada.

- *MESSAGE:* Permite la transferencia de mensajes instantáneos.

- *INFO:* Permite transferir informaciones de señalización durante la llamada. Por ejemplo los dígitos DTMF e informaciones relativas a la tasación de una llamada.

- *PRACK:* Satisface la recepción de respuestas temporales de tipo 1XX.

- *UPDATE:* Permite a un terminal SIP actualizar los parámetros de una sesión multimedia (ejemplo: el tipo de flujo y sus códecs). El método UPDATE puede ser enviado antes de que la sesión sea establecida.

4.1.4. Respuestas SIP

Después de haber recibido e interpretado un requerimiento SIP, el destinatario de este requerimiento devuelve una respuesta SIP. Existen seis clases de respuestas (13):

- *Clase 1xx:* Información; el requerimiento ha sido recibido y está en curso de tratamiento.

- *Clase 2xx:* Éxito; el requerimiento ha sido recibido, entendido y aceptado.

- *Clase 3xx:* Re-enrutamiento; la llamada requiere otros procesamientos antes de poder determinar si puede ser realizada.

- *Clase 4xx:* Error requerimiento cliente; el requerimiento no puede ser interpretado o prestado por el servidor. El requerimiento tiene que ser modificado antes de ser reenviado.

- *Clase 5xx:* Error servidor; el servidor fracasa en el procesamiento de un requerimiento aparentemente válido.

- *Clase 6xx:* Fracaso global; el requerimiento no puede ser procesado por ningún servidor.

Las respuestas finales 2xx, 3xx, 4xx, 5xx y 6xx a un requerimiento INVITE son satisfechas por el requerimiento ACK mientras las respuestas provisorias de tipo 1XX son satisfechas por el requerimiento PRACK.

4.2. SDP (Session Description Protocol).

El protocolo SDP se emplea para describir la sesión que se negocia con SIP. Mediante SDP, los extremos de una sesión pueden indicar sus capacidades multimedia y definir el tipo de sesión que se desea mantener. Además, con SDP los extremos deciden qué flujos multimedia compondrán la sesión (audio, video, etc.), los códecs que soportan para cada flujo y la configuración específica de los mismos. Mediante este intercambio de señalización se negocia la QoS, tanto en el establecimiento como durante la sesión en curso, si es necesario.

Este dinamismo es una novedad en el sector de las telecomunicaciones, donde la QoS es estática y viene impuesta por las redes y el servicio final solicitado. Por otro lado, en las redes 3GPP el operador puede configurar IMS para elegir qué tipo de flujo multimedia y códecs desea soportar en su red, incluso puede personalizar cada perfil de usuario IMS para que éste pueda realizar un determinado tipo de sesiones IP multimedia, rechazando cualquier otra comunicación IMS que difiera de sus políticas (12).

Una descripción SDP incluye (15):

- Nombre de sesión y propósito.
- Tiempo (s) de sesión activa.
- Los flujos que comprende la sesión.
- Información necesaria para recibir los flujos multimedia (direcciones, puertos, formatos).

Como los recursos necesarios para participar en una sesión pueden ser limitados, es conveniente alguna información adicional:

- Información sobre el ancho de banda usado por la sesión.
- Información de contacto de la persona responsable de la sesión.

Una descripción de sesión SDP consiste de un nivel de sesión seguido por cero o más niveles de medios. El nivel de sesión comienza con “v=” y continua hacía el primer nivel de medios. Cada nivel de medios comienza con “m=” y avanza a la próxima sesión de nivel de medios o al final de la descripción de la sesión. En general, los valores de cada nivel de sesión son por defecto aquellos de los medios menos predominantes (15).

Algunas de las líneas son requeridas, otras son opcionales, pero todas deben aparecer exactamente en el siguiente orden (15):

Descripción de sesión:
v = (versión del protocolo).
o = (dueño/creador e identificador de sesión).
s = (nombre de la sesión).
i = * (información de la sesión).
u = * (URI de la descripción).
e = * (email address).
p = * (número de teléfono).
c = * (información de conexión - no requerida si está incluido en todos los medios).
b = * (información de ancho de banda).
Descripciones de tiempo (líneas "t=" y "r="; ver abajo).
z = * (ajustes de la zona de tiempo).
k = * (llave del cifrado).
a = * (cero o más líneas de atributos de sesión).
Descripción de medios.

Descripción de tiempo:
t = (tiempo activo de la sesión).
r = * (cero o más tiempos de repetición).

Descripción de medios, si se presenta:
m = (nombre de los medios y dirección de transporte).
i = * (título de los medios).
c = * (información de conexión - opcional si está incluido a nivel de sesión).
b = * (información de ancho de banda).
k = * (llave de cifrado).
a = * (cero o más líneas de atributos de medios).

Las líneas opcionales aparecen con “*”.

A continuación se presenta un ejemplo de descripción SDP:

v=0
o=jdoe 2890844526 2890842807 IN IP4 10.47.16.5
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.example.com/seminars/sdp.pdf

e=j.doe@example.com (Jane Doe)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 99
a=rtpmap:99 h263-1998/90000

4.3. Protocolo de Internet versión 6 (IPV6).

El protocolo de Internet versión 6 (IPv6) es un estándar IP de capa de red usado como mecanismo para intercambiar datos a través de una red de conmutación de paquetes. Originalmente, IMS fue especificado para usar IPv6; sin embargo, con el Release 6 de 3GPP, IMS proporciona soporte para IPv4 y esquema de dirección privada (2).

4.3.1. Principales características (16).

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y nodos direccionables.

- Simplificación del formato del encabezado. Algunos campos del encabezado IPv4 se quitan o se hacen opcionales.

- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del router.

- Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.

- Seguridad en el núcleo del protocolo (IPsec). El soporte de IPsec es un requerimiento del protocolo IPv6.

- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio por defecto o servicios de tiempo real; por ejemplo video conferencia.

- Autoconfiguración. La autoconfiguración de direcciones es más simple.

- Renumeración y multihoming, facilitando el cambio de proveedor de servicios.

- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.

- Calidad de servicio (QoS) y clase de servicio (CoS).

- Capacidades de autenticación y privacidad.

4.3.2. Direccionamiento en IPv6

Las direcciones son de 128 bits e identifican interfaces individuales o conjuntos de interfaces. Al igual que en IPv4, se asignan a interfaces.

Se clasifican en tres tipos (16):

- *Unicast:* identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección.

- *Anycast:* identifican a un conjunto de interfaces. Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto, al cual pertenece esa dirección anycast.

- *Multicast:* identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todos las interfaces del grupo identificadas con esa dirección. En el IPv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast.

4.3.3. Representación de las direcciones IPv6.

Existen tres formas de representar las direcciones IPv6 como cadenas de texto (16).

- *x:x:x:x:x:x:x:x* donde cada x es el valor hexadecimal de 16 bits de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir un número en cada campo.

Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:417A

- Existe la posibilidad de usar sintácticamente ***::*** para representar cadenas de bits en cero. El uso de *::* indica uno o más grupos de 16 bits de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección.

Por ejemplo:

1080:0:0:0:8:800:200C:417A	unicast address
FF01:0:0:0:0:0:0:101	multicast address
0:0:0:0:0:0:0:1	loopback address
0:0:0:0:0:0:0:0	unspecified addresses

Podrán ser representadas como:

1080::8:800:200C:417A	unicast address
FF01::101	multicast address
::1	loopback address
::	unspecified addresses

- Para escenarios con nodos IPv4 e IPv6 es posible utilizar la siguiente sintaxis:

x:x:x:x:x:x:d.d.d.d, donde cada x representa valores hexadecimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y las d son valores decimales de las 4 partes menos significativas (de 8 bits cada una) de la representación estándar del formato de direcciones IPv4.

Ejemplos:

0:0:0:0:0:0:13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38

o en la forma comprimida:

::13.1.68.3
::FFFF:129.144.52.38

4.3.4. Representación de los prefijos de las direcciones.

Los prefijos de identificadores de subredes, routers y rangos de direcciones IPv6 son expresados de la misma forma que en la notación CIDR utilizada en IPv4. Un prefijo de dirección IPv6 se representa con la siguiente notación (16):

dirección-ipv6/longitud-prefijo, donde:

dirección-ipv6: es una dirección IPv6 en cualquiera de las notaciones mencionadas anteriormente.
longitud-prefijo: es un valor decimal que especifica cuantos de los bits más significativos, representan el prefijo de la dirección.

4.3.5. Mecanismos de transición básicos.

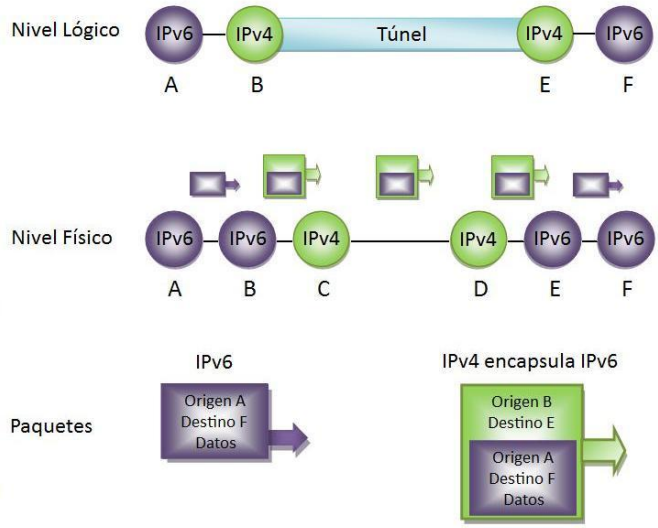
Los mecanismos de transición son un conjunto de mecanismos y de protocolos implementados en hosts y routers, junto con algunas guías operativas de direccionamiento designadas para hacer la transición de la Internet al IPv6 con la menor interrupción posible. Dichos mecanismos están diseñados para ser usados por hosts y routers IPv6 que necesitan interoperar con hosts IPv4 y utilizar infraestructuras de enrutamiento IPv4.

Existen dos mecanismos básicos (16):

- *Dual Stack:* provee soporte completo para IPv4 e IPv6 en hosts y routers. La forma más directa para nodos IPv6 ser compatibles con nodos IPv4 es proporcionar una implementación completa de IPv4. Los nodos IPv6 que proveen una implementación completa de IPv4 (además de su implementación de IPv6) son llamados nodos IPv6/IPv4. Estos nodos tienen la habilidad de enviar y recibir paquetes IPv6 e IPv4, operando directamente con nodos IPv4 usando paquetes IPv4 y también con nodos IPv6 usando paquetes IPv6.

- *Tunneling:* encapsula paquetes IPv6 dentro de encabezados IPv4, de manera que se transportan usando la infraestructura de enrutamiento IPv4. Los nodos o redes IPv6 que se encuentran separados por infraestructuras IPv4 pueden construir un enlace virtual, configurando un túnel (Figura 8). Paquetes IPv6 que van hacia un dominio IPv6 serán encapsulados dentro de paquetes IPv4. Los extremos del túnel son dos direcciones IPv4 y dos IPv6. Se pueden utilizar dos tipos de túneles: configurados y automáticos. Los túneles configurados son creados mediante configuración manual; los túneles automáticos no necesitan configuración manual. Los extremos se determinan automáticamente usando direcciones determinadas IPv6/IPv4-compatibles.

Figura 8. Encapsulamiento de paquetes IPv6



4.4. RTP (Real Time Transport Protocol)

El protocolo de transporte en tiempo real (RTP) es un protocolo de nivel de aplicación utilizado para la transmisión de información en tiempo real, tal como audio y vídeo, a través de diferentes redes. El propósito de RTP es facilitar la entrega, el monitoreo, la reconstrucción, la mezcla y la sincronización de flujos de datos. Aunque RTP no proporciona calidad de servicio en redes IP, sus mezcladores pueden ser utilizados para facilitar la entrega de servicios multimedia en una amplia gama de tipos de enlaces y velocidades. RTP está diseñado para utilizar protocolos de transporte tanto unicast como multicast (17).

El encabezado RTP tiene el siguiente formato (18):

Figura 9. Encabezado RTP.

+ Bits	0 - 1	2	3	4 -7	8	9 - 15	16 - 31
0	Ver	P	X	CC	M	PT	Número de secuencia
32	Marca de tiempo						
64	Identificador SSRC						
96	Identificador CSRC (opcional)						
96 + (CCx32)	Extensión de Cabecera (opcional)						
96 + (CCx32) + (X*((EHL+1)*32))	Datos						

- *Número de la versión RTP (V - versión number):* 2 bits. La versión definida por la especificación actual es 2.

- *Relleno (P - Padding):* 1 bit. Si el bit de relleno está presente, hay uno o más bytes al final del paquete que no hacen parte de la carga útil. El último byte del paquete indica el número de bytes de relleno. El relleno es usado por algunos algoritmos de cifrado.

- *La extensión (X - Extensión):* 1 bit. Si el bit de extensión está presente, entonces el encabezado fijo es seguido por una extensión del encabezado. Este mecanismo de extensión posibilita implementaciones para añadir información al encabezado RTP.

- *Conteo CSRC (CC):* 4 bits. El número de identificadores CSRC que sigue el encabezado fijo. Si la cuenta CSRC es cero, entonces la fuente de sincronización es la fuente de la carga útil.

- *El marcador (M - Marker):* 1 bit. Un bit de marcador definido por el perfil multimedia.

- *La carga útil Type (PT):* 7 bits. Un índice en una tabla de perfiles multimedia que describe el formato de carga útil. Los mapeos de carga útil para audio y vídeo están especificados en el RFC 1890.

- *El número de secuencia:* 16 bits. Un único número de paquete que identifica la posición de éste en la secuencia de paquetes. El número del paquete es incrementado en uno para cada paquete enviado.

- *Sellado de tiempo:* 32 bits. Refleja el instante de muestreo del primer byte en la carga útil. Varios paquetes consecutivos pueden tener el mismo sellado si son lógicamente generados en el mismo tiempo. (por ejemplo, si son parte del mismo frame de vídeo).

- *SSRC:* 32 bits. Identifica la fuente de sincronización. Si la cuenta CSRC es cero, entonces la fuente de carga útil es la fuente de sincronización. Si la cuenta CSRC es distinta a cero, el SSRC identifica el mixer (mezclador).

- *CSRC:* 32 bits cada uno. Identifica las fuentes contribuyentes de carga útil. El número de fuentes contribuyentes está indicado por el campo de la cuenta CSRC; allí puede haber más de 16 fuentes contribuyentes. Si hay fuentes contribuyentes múltiples, entonces la carga útil son los datos mezclados de esas fuentes.

- *EH:* El tamaño de este dato debe ser CC×32 en bits.

- *Datos:* El tamaño de los datos debe ser de (X)*((EHL+1)*32), donde EHL es la longitud de la extensión de la cabecera en unidades de 32 bits.

4.5. RTCP (Real Time Control Protocol).

El protocolo de control de tiempo real (RTCP), es un protocolo de comunicación que proporciona información de control asociada con un flujo de datos para una aplicación multimedia. El protocolo RTCP se basa en transmisiones periódicas de paquetes de control que realizan todos los participantes de la sesión (18).

El encabezado RTCP contiene la siguiente información sesión (18):

- *Versión:* 2 bits. Indica la versión RTCP; es la misma de los paquetes RTP.

- *Relleno (Padding):* 1 bit. Si está activado quiere decir que el paquete contiene algunos bits de relleno al final, que no forman parte de la información de control. El último byte de relleno indica cuántos bytes de relleno se tienen que ignorar.

- *Conteo:* 5 bits. Indica el número de bloques de informes de receptor contenidos en este paquete.

- *Tipo:* 8 bits. Indica el tipo de paquete RTCP.

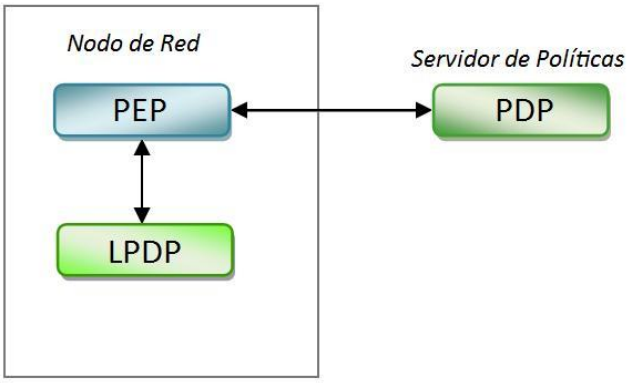
- *Longitud:* 16 bits. Indica la longitud del paquete RTCP.

4.6. COPS (Common Open Policy Service).

El protocolo COPS (Common Open Policy Service) define un modelo sencillo cliente/servidor que proporciona control de políticas para protocolos con señalización de calidad de servicio (19).

El protocolo COPS utiliza mensajes sencillos de petición y respuesta para intercambiar información acerca de políticas de tráfico entre un servidor de políticas (PDP, Policy Decision Point) y distintos tipos de clientes (PEPs, Policy Enforcement Points) (19).

Figura 10. Modelo COPS.



Las características principales del protocolo COPS son las siguientes (19):

- El protocolo emplea un modelo cliente/servidor en el que el PEP envía peticiones y actualizaciones al PDP y el PDP responde con las decisiones tomadas.

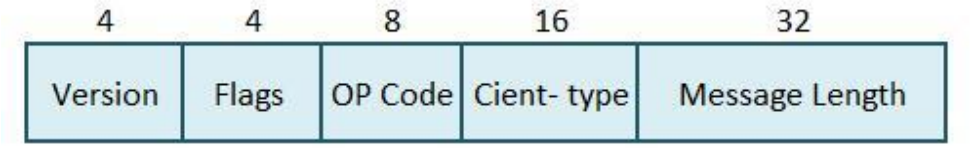
- El protocolo utiliza TCP como protocolo de transporte para asegurar así fiabilidad en el intercambio de mensajes entre los clientes y el servidor.

- El protocolo es extensible en el sentido de que está diseñado para permitir el uso de objetos autoidentificativos y soporta distintos tipos de información específica de clientes, sin tener que realizar modificaciones sobre el protocolo. COPS se creó para la administración general, configuración y aplicación de políticas en una red.

- COPS proporciona seguridad a nivel de mensaje mediante autenticación, protección frente al reenvío (replay) e integridad. COPS permite además reutilizar otros protocolos de seguridad existentes para proporcionar autenticación y proteger el canal entre el PEP y el PDP.

Cada mensaje COPS consiste del encabezado COPS seguido por un campo de objetos. El encabezado COPS es mostrado en la Figura 11.

Figura 11. Encabezado COPS.



Los campos en el encabezado son los siguientes (20):

- *Versión:* 4 bits. Número de la versión COPS. La versión actual es 1.

- *Banderas (Flags):* 4 bits. Define los valores de las banderas. La bandera es alertada cuando el mensaje es solicitado por otro mensaje COPS.

- *Op Code:* 8 bits. Operaciones COPS.

1 = Solicitud	(REQ), Request
2 = Decisión	(DEC), Decision
3 = Informe Estado	(RPT), Report State
4 = Eliminar Solicitud	(DRQ), Delete Request State
5 = Estado de sincronización	(SSQ), Synchronize State Req
6 = Cliente-Abierto	(OPN), Client-Open
7 = Cliente-Aceptado	(CAT), Client-Accept
8 = Cliente-Cerrado	(CC), Client-Close
9 = Keep-Alive	(KA), Keep-Alive
10 = Sincronización completa	(CDC), Synchronize Complete

- *Client-type:* 16 bits. Identifica la política del cliente. La interpretación de todos los objetos encapsulados es relativa al tipo de cliente.

- *Message Length:* 32 bits. Tamaño del mensaje en octetos.

4.7. RSVP (Resource Reservation Protocol).

El Protocolo de reserva de recursos (RSVP) permite a las aplicaciones de la Internet obtener distintas calidades de servicio (QoS) para sus flujos de datos (21). RSVP no es una aplicación de transporte, es más bien un protocolo de control de la Internet, que reserva canales o rutas para la transmisión por unidifusión y multidifusión con escalabilidad y robustez (22).

RSVP puede ser utilizado tanto por hosts como por routers para pedir o entregar niveles específicos de calidad de servicio (QoS) a los flujos de datos de las aplicaciones, define cómo las aplicaciones deben hacer reservas y cómo liberar los recursos reservados una vez que han terminado. Las operaciones RSVP generalmente dan como resultado una reserva de recursos en cada nodo a lo largo de un camino (22).

El protocolo de reserva de recursos (RSVP) tiene las siguientes características principales (22):

- RSVP pide recursos para los flujos simplex: un flujo de tráfico en una sola dirección desde el emisor a uno o más receptores.

- RSVP no es un protocolo de encaminamiento; pero trabaja con los protocolos de enrutamiento actuales y futuros.

- RSVP está orientado hacia el receptor: es el receptor de un flujo de datos el que inicia y mantiene la reserva de recursos para ese flujo.

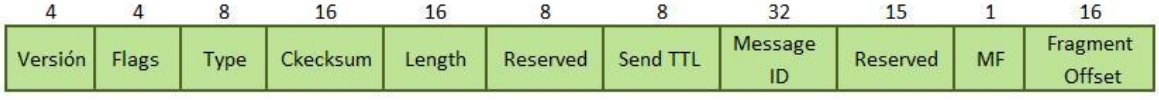
- RSVP es soft state (la reserva necesita actualizarse periódicamente en cada nodo), mantiene solo temporalmente el estado de las reservas de recursos del host y de los routers, de aquí que soporte cambios dinámicos de red.

- RSVP proporciona varios estilos de reserva (un conjunto de opciones) y permite que se añadan futuros estilos permitiéndole adaptarse a diversas aplicaciones.

- RSVP transporta y mantiene parámetros de tráfico y de la política de control.

El encabezado RSVP (Figura 12) consta de lo siguiente (20):

Figura 12. Encabezado RSVP.



- *Versión:* 4 bits. Indica la versión del protocolo. La versión actual es 1.

- *Flags:* 4 bits. Define el valor de las banderas. Normalmente no definidas.

- *Type:* 8 bits. Campo con siete posibles valores enteros:

1: Path
2: Reservation-request
3: Path-error
4: Reservation-request error
5: Path-teardown
6: Reservation-teardown
7: Reservation-request acknowledgment

- *Checksum:* 16 bits. Representa un estándar (TCP/UDP) sobre el contenido del mensaje RSVP.

- *Length:* 16 bits. Representa la longitud del mensaje RSVP en bytes, incluyendo la longitud común del encabezado y la longitud de variables del campo objeto.

- *Send TTL:* 8 bits. Indica el valor de tiempo de vida con el cual el valor del mensaje fue enviado.

- *Message ID:* 32 bits. Provee una etiqueta compartida por todos los fragmentos de un mensaje desde un salto RSVP dado (siguiente/anterior).

- *More fragments (MF) flag:* 1 bit. Bandera para tener o no en cuenta la información en el campo fragment offset.

- *Fragment offset:* Representa el offset del fragmento en el mensaje.

4.8. Diameter.

Diameter es una evolución del protocolo RADIUS, escogido como el soporte de políticas y protocolo de contabilidad, autenticación y autorización (AAA) para IMS. Diameter es usado por el S-CSCF, I-CSCF y los servidores de aplicación SIP en la capa de servicio y en los intercambios con el HSS que contiene la información de usuario y subscripción (2).

Las principales características del protocolo diameter son (2):

- Utiliza protocolos de transporte fiables (TCP o SCTP, no UDP).
- Usa seguridad a nivel de transporte (IPSEC o TLS).
- Tiene compatibilidad transicional con RADIUS.
- Es un protocolo peer-to-peer en lugar de cliente-servidor.

- Tiene negociación de capacidades.
- Admite ACKs en el nivel de aplicación, definiendo métodos de fallo y máquinas de estado.
- Tiene notificación de errores.
- Tiene mejor compatibilidad con roaming.
- Es más fácil de extender, pues se pueden definir nuevos comandos y atributos.
- Incluye una implementación básica de sesiones y control de usuarios.

4.9. Megaco.

Megaco conocido como H.248 es un protocolo de control usado entre las funciones de control y recursos de medios. Ejemplos de nodos con funciones de control de medios son el MGCF y el MRFC; recursos típicos de medios son el Media Gateway y el MRFP (2).

El H.248 es un protocolo del tipo maestro-esclavo, en el que se espera que los gateways ejecuten los comandos enviados por los agentes de llamada. Un sistema H.248 está formado por uno o más gateways y como mínimo por un agente, el cual es notificado de la ocurrencia de cualquier evento (23).

5. ACCESO A LOS SERVICIOS EN IMS.

Para acceder a un servicio IMS y establecer una sesión, un usuario necesita cumplir cinco fases (11):

- Conexión a la red (Registro) y autenticación.
- Conectividad IP.
- Descubrimiento del P-CSCF.
- Registro a nivel de aplicación.
- Configuración de la sesión y reserva de recursos.

Inicialmente, el usuario será acoplado y autenticado en la red. Luego, el router frontera le asignará una dirección IP en el dominio de red. Seguidamente, el usuario deberá descubrir el P-CSCF como el punto de entrada a la red IMS (11).

Una vez el usuario descubre el P-CSCF podrá registrarse en la red. Este proceso se denomina registro de nivel de servicio. En esta fase, el usuario enviará un mensaje “REGISTER” desde su dominio de origen. Este mensaje será transmitido por el P-CSCF al I-CSCF adecuado. Inicialmente, el I-CSCF interroga al HSS para conocer el perfil de usuario y verificar si tiene permitido conectarse a la red IMS a través del actual P-CSCF. Si el perfil de usuario cumple con la condición, el I-CSCF pregunta al HSS para asignar el adecuado S-CSCF de acuerdo con sus criterios de filtrado de servicios (11).

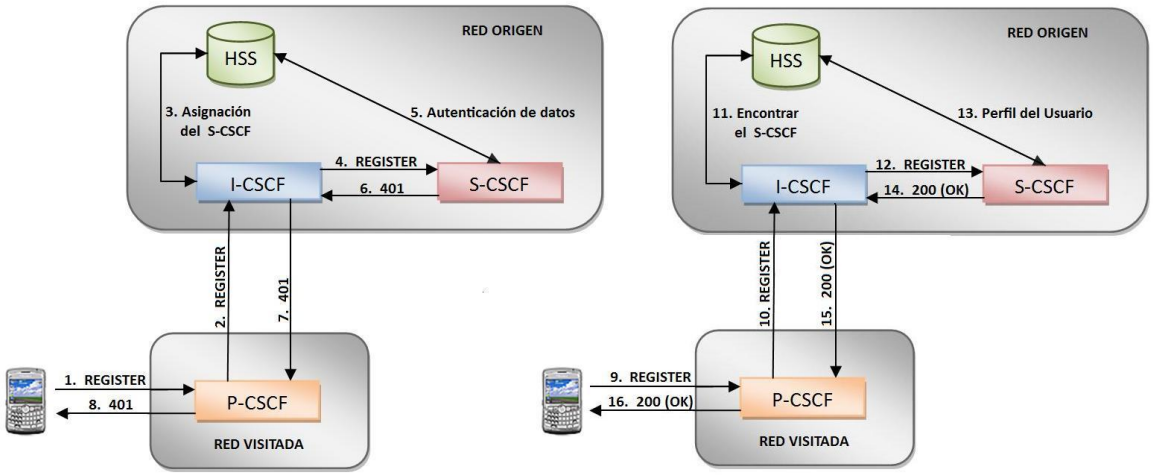
Posteriormente, el mensaje REGISTER será enviado al S-CSCF y el usuario se localizará con este servidor. Esto significa que el S-CSCF vinculará la actual dirección IP del usuario con su identidad pública o su SIP URI (11).

Después del registro en el dominio IMS, el usuario podrá establecer una sesión y beneficiarse de los servicios IMS. Para esto, realiza un requerimiento INVITE a otra entidad o a un servidor IMS. Esta petición, contiene los parámetros propuestos para la sesión por la parte que llama y se encaminan a la parte llamada. Si los parámetros de la sesión son aprobados por la parte llamada, los recursos requeridos serán reservados a nivel de transporte (11).

Sin embargo, cabe mencionar que el proceso de reserva de recursos depende de la tecnología de la red de acceso y de las políticas del operador. La arquitectura IMS habilita una política basada en la reserva de recursos solicitados. El P-CSCF extrae los parámetros de calidad de servicio (QoS) y transfiere esta información al PDF a través de la interfaz Gq. La PDF de acuerdo con el perfil de usuario y las políticas de red determina la cantidad de recursos que deberían ser asignados a la sesión y transfiere su decisión a los routers que soportan las funcionalidades PEP (Policy Enforcement Point) (11).

5.1. Procedimiento de Registro.

Figura 13. Procedimiento de registro.



Antes del registro IMS, el cual permite al UE utilizar los servicios IMS, se debe obtener conectividad IP y descubrir un punto de entrada a la red IMS, es decir, localizar el P-CSCF. El registro en la red IMS contiene dos fases: en la primera fase, la red reta al UE (Figura 13 - parte izquierda); en la segunda fase, el UE responde al desafío y completa el registro (Figura 13 - parte derecha).

En primer lugar, el UE envía una solicitud SIP REGISTER para descubrir al P-CSCF, que contendrá, por ejemplo, una identidad para ser registrada y un nombre de dominio (Dirección del I-CSCF). El P-CSCF procesa el requerimiento REGISTER y usa el nombre de dominio origen para resolver la dirección IP del I-CSCF. El I-CSCF, a su vez, se pondrá en contacto con el HSS para la selección del S-CSCF. Después de la selección del S-CSCF, el I-CSCF remite el mensaje REGISTER al S-CSCF. El S-CSCF se da cuenta de que el usuario no está autorizado, recupera los datos de autenticación desde el HSS y reta al usuario con una respuesta 401 Unauthorized (24).

En segundo lugar, el UE calcula una respuesta al desafío y envía otro requerimiento REGISTER al P-CSCF. Una vez más, el P-CSCF encuentra el I-CSCF y éste por su parte al S-CSCF. Por último, el S-CSCF comprueba la respuesta y, si es correcta, descarga el perfil de usuario desde el HSS y acepta el registro con una respuesta 200 OK. Una vez que el UE es autorizado satisfactoriamente, está habilitado para iniciar y recibir sesiones. Durante el procedimiento de registro, tanto el UE como el P-CSCF aprenden cual S-CSCF en la red sirve al UE (24). Las entidades implicadas en el proceso de registro aprenden y almacenan información antes, durante y después de que el usuario logra registrarse satisfactoriamente en la red (Tabla 2).

Es responsabilidad de los UE's mantener activo su registro, refrescando periódicamente su inscripción en la red IMS. Si el UE no actualiza su registro, el S-

CSCF silenciosamente eliminará el registro cuando caduque el temporizador de registro. Cuando el UE quiere re-registrarse desde la red IMS establece un temporizador de registro en 0 y envía un requerimiento REGISTER (24).

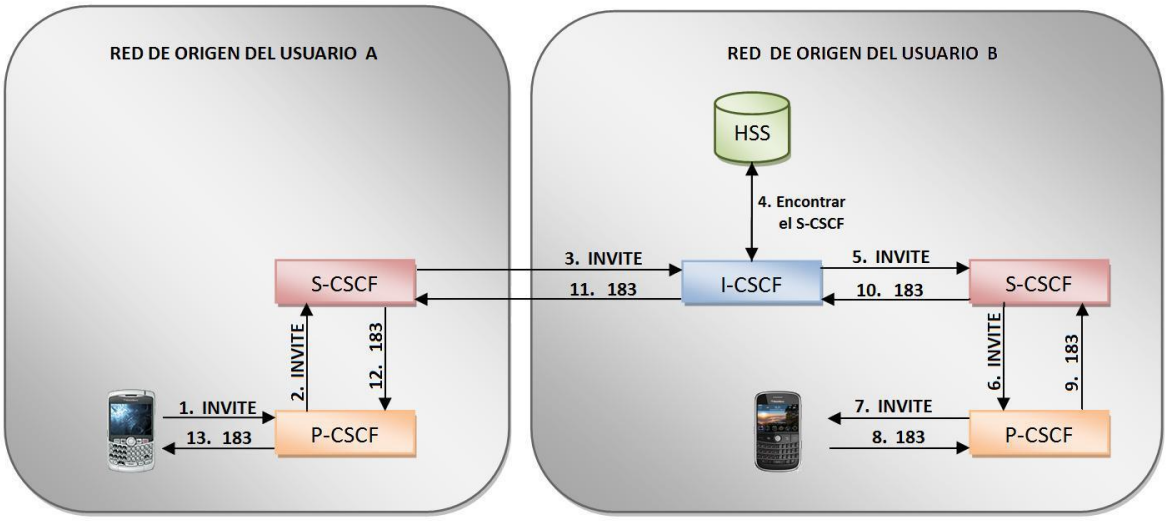
Tabla 2. Información almacenada antes, durante y después del proceso de registro.

Nodo	Antes del registro	Durante el registro	Después del registro
UE	Dirección del P-CSCF, nombre de dominio, identidad pública de usuario, identidad privada de usuario.	Dirección del P-CSCF, nombre de dominio, identidad pública de usuario, identidad privada de usuario, seguridad asociada.	Dirección del P-CSCF, nombre de dominio, identidad pública registrada, identidad privada de usuario, seguridad asociada, información de encaminamiento (S-CSCF).
P-CSCF	No almacena información.	Punto inicial de entrada a la red, dirección IP del UE, identidades públicas y privadas, seguridad asociada.	Punto final de entrada a la red (S-CSCF), dirección del UE, identidad pública registrada, identidad privada, seguridad asociada, dirección del CDF (Charging Data Function).
I-CSCF	Dirección del HSS o SLF.	Entrada al HSS o SLF, dirección del P-CSCF, dirección del S-CSCF.	Direcciones del HSS o SLF.
S-CSCF	Dirección del HSS o SLF.	Nombre/dirección del HSS, perfil de usuario, nombre/dirección del proxy, identificación pública/privada, dirección IP de usuario.	Nombre/dirección del HSS, perfil de usuario, nombre/dirección del proxy, identificación pública/privada, dirección IP del usuario.
HSS	Perfil de usuario, parámetros de selección del S-CSCF.	Perfil de usuario, parámetros de selección del S-CSCF, información de red visitada (roaming).	Perfil de usuario, parámetros de selección del S-CSCF, información de cuales identidades de usuario están registradas, nombre del S-CSCF asignado.

5.2. Establecimiento de Sesión.

Cuando un usuario A quiere tener una sesión con un usuario B, el UE A genera un requerimiento SIP INVITE y lo envía, a través del punto de referencia Gm al P-CSCF. El P-CSCF procesa la solicitud, por ejemplo, descomprime la solicitud y verifica la identidad de usuario antes de reenviar la solicitud a través de la interfaz Mw al S-CSCF. El S-CSCF analiza la solicitud, ejecuta control de servicio que puede incluir interacción con servidores de aplicación (AS's) y determina el punto de entrada del operador del usuario B, basándose en la identidad de B y en el requerimiento SIP INVITE. El I-CSCF recibe el requerimiento a través del punto de referencia Mw y contacta el HSS sobre la interfaz Cx para encontrar el S-CSCF que esta sirviendo al usuario B. El requerimiento se traslada al S-CSCF usando el punto de referencia Mw. El S-CSCF se encarga de procesar la terminación de la sesión, la cual puede requerir interacciones con otros servidores de aplicación y entrega el requerimiento al P-CSCF. Después, el P-CSCF encamina el requerimiento SIP INVITE al UE B, que genera una respuesta 183 Session Progress hacía el UE A, a través de la ruta que fue creada desde el UE A (UE B, P-CSCF, S-CSCF, I-CSCF, S-CSCF, P-CSCF, UE A, Figura 14). Por ultimo, ambos conjuntos de UE establecen sesión y se habilitan para iniciar una aplicación (24).

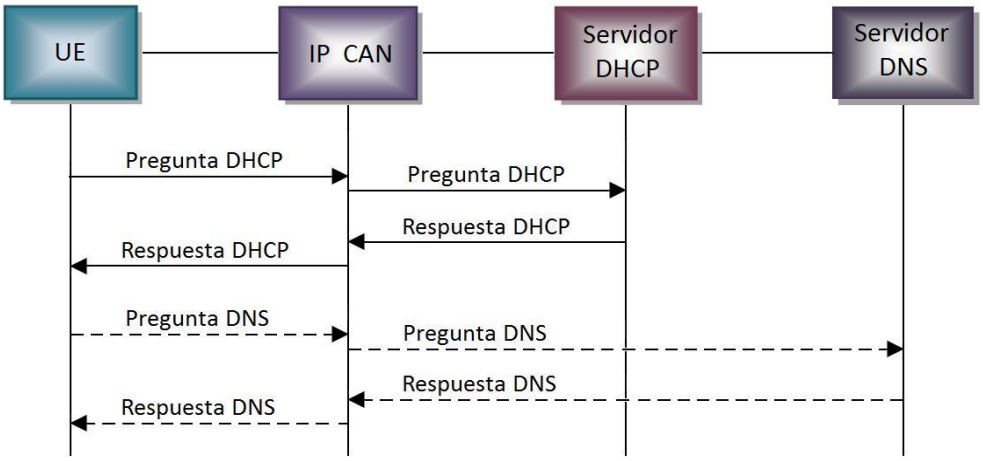
Figura 14. Establecimiento de Sesión en IMS.



5.3. Descubrimiento del punto de entrada a la red IMS (P-CSCF)

Con el fin de comunicarse con la red IMS, el UE tiene que conocer por lo menos una dirección IP del P-CSCF. El mecanismo por el cual el UE recupera éstas direcciones es llamado “descubrimiento del P-CSCF”. Para este fin, 3GPP ha estandarizado dos mecanismos: el procedimiento DHCP DNS (Dynamic Host Configuration Protocol) y el procedimiento GPRS. Adicionalmente, es posible configurar en el UE el nombre del P-CSCF o su dirección IP (24).

Figura 15. Mecanismo general para descubrir el P-CSCF.



En el procedimiento DHCP DNS (Figura 15), el UE envía una consulta DHCP a la red de acceso con conectividad IP (Por ejemplo, GPRS), la cual retransmite la solicitud al servidor DHCP. El UE podría requerir una lista de los nombres de

dominio o las direcciones IPv6 de los P-CSCF´s. Cuando se retornan nombres de dominio, el UE necesita realizar una solicitud DNS (NAPTR/SRV) para encontrar la dirección IP del P-CSCF. El mecanismo DHCP DNS es un método independiente de la red de acceso para descubrir el P-CSCF (24).

5.4. Asignación del S-CSCF.

Una vez el P-CSCF es encontrado se asigna el S-CSCF al UE. Hay tres casos en los cuales un S-CSCF es asignado:

- Cuando un usuario se registra con la red IMS.
- Cuando un usuario no registrado recibe una solicitud SIP.
- Cuando un S-CSCF asignado previamente no está respondiendo.

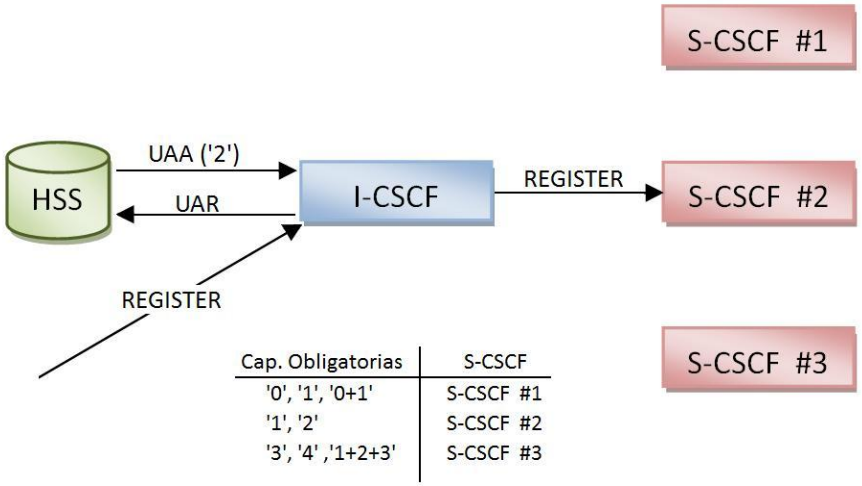
Cuando un usuario está registrándose en una red IMS, el UE envía un requerimiento REGISTER para descubrir el P-CSCF, el cual se encarga de encontrar el I-CSCF. Luego, el I-CSCF intercambia mensajes con el HSS. Como resultado, el I-CSCF recibe capacidades del S-CSCF siempre y cuando, éste no haya sido asignado previamente. Basándose en las capacidades recibidas el I-CSCF selecciona un adecuado S-CSCF. La información de capacidad es transferida entre el HSS y el I-CSCF dentro del servidor de capacidades AVP (Attribute Value Pair) (24). El servidor de capacidades AVP contiene:

- *Capacidades obligatorias AVP.* Este tipo de AVP contiene las capacidades obligatorias del S-CSCF. Cada capacidad obligatoria disponible en una red de operador individual será asignada a un único valor.
- *Capacidades opcionales AVP.* Esta clase de AVP contiene las capacidades opcionales del S-CSCF. Cada capacidad opcional disponible en una red de operador individual será asignada a un único valor.
- *Nombre del servidor AVP.* Este tipo de AVP contiene un SIP URI usado para identificar un servidor SIP.

Basado en las capacidades AVPs obligatorias y opcionales, un operador es capaz de distribuir a los usuarios entre los S-CSCFs, dependiendo de las capacidades requeridas que cada S-CSCF pueda tener. Es responsabilidad del operador definir el exacto significado de las capacidades obligatorias y opcionales. Como primera opción, el I-CSCF seleccionará el S-CSCF que tenga todas las capacidades obligatorias y opcionales para el usuario. Si esto no es posible, el I-CSCF aplicará un algoritmo best fit **(**24**)**. El proceso es resumido en la Figura 16.

Usando el nombre del servidor AVP, un operador tiene la posibilidad de dirigir a los usuarios a S-CSCFs seguros; por ejemplo, teniendo un S-CSCF dedicado a la misma compañía/grupo para implementar un servicio de VPN o simplemente facilitando la asignación de un S-CSCF (24).

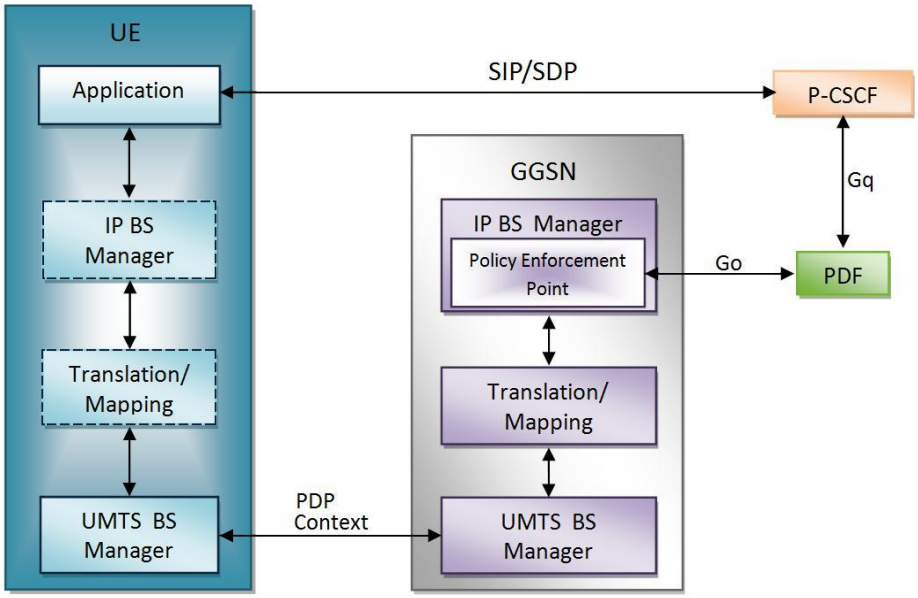
Figura 16. Asignación del S-CSCF.



6. MECANISMOS PARA EL CONTROL DE TRÁFICO

La separación del plano de control y el plano de usuario es la principal característica del diseño IMS. Independencia plena de capas no es factible porque sin interacción entre el plano de usuario y el de control, los operadores no son capaces de controlar calidad de servicio (QoS), el origen / destino del tráfico de medios IMS y cuándo comienza y termina un flujo multimedia. De esta manera, se creó un mecanismo para autorizar y controlar el uso de tráfico multimedia en IMS; éste se basa en los parámetros de negociación de sesión IMS del protocolo SDP. Esta interacción global entre GPRS e IMS es llamada control SBLP (Service Based Local Policy) (24).

Figura 17. Entidades SBLP



Las entidades funcionales SBLP son (Figura 17) (24):

- *IP Bearer Service (BS) Manager:* gestiona el servicio de portadora IP usando un mecanismo estándar IP. Reside en el GGSN (Gateway GPRS Support node) y opcionalmente en el UE.
- *Función Translation/Mapping:* provee la interconexión entre los mecanismos y parámetros usados dentro del UMTS BS y los usados en el IP BS. Reside en el GGSN y opcionalmente en el UE.
- *UMTS BS Manager:* manipula los requerimientos de reserva de recursos desde el UE. Reside en el GGSN y en el UE.
- *Punto de aplicación de políticas:* es una entidad lógica que hace cumplir las decisiones de políticas tomadas por la PDF. Reside en el IP BS Manager del GGSN.

- *Función de decisión de políticas (PDF):* es un elemento de decisión de políticas lógico que usa un mecanismo estándar IP para implementar SBLP en la capa de medios IP, siendo una entidad autónoma que define una estructura para control de admisión basado en políticas.

Hay siete funciones SBLP (24):

- Autorización de portadora.
- Aprobación de la función de entrega de QoS.
- Eliminación de la entrega de QoS.
- Indicación de liberación de portadora.
- Indicación de pérdida/recuperación de portadora.
- Revocación de autorización.
- Intercambio de identificadores de tarificación.

6.1. Autorización de Portadora.

El establecimiento de sesión y modificación en IMS involucra un intercambio de mensajes end to end usando SIP y SDP. Durante el intercambio de mensajes, los UE's negocian un conjunto de características multimedia. Si un operador aplica la arquitectura SBLP, el P-CSCF enviará la información SDP relevante al PDF junto con una indicación de quién lo originó. El PDF nota y autoriza el flujo IP de los componentes multimedia escogidos, mapeados desde los parámetros SDP para autorizar las características de QoS IP y transferirlas al GGSN a través de la interfaz Go.

Cuando el UE está activando o modificando un contexto PDP multimedia, éste tiene que desarrollar su propio mapeo desde los parámetros SDP y demandas de aplicación para algunos parámetros de QoS UMTS. La activación o modificación de un contexto PDP también contendrá la señal de autorización recibida, los identificadores de flujo y la información de vinculación.

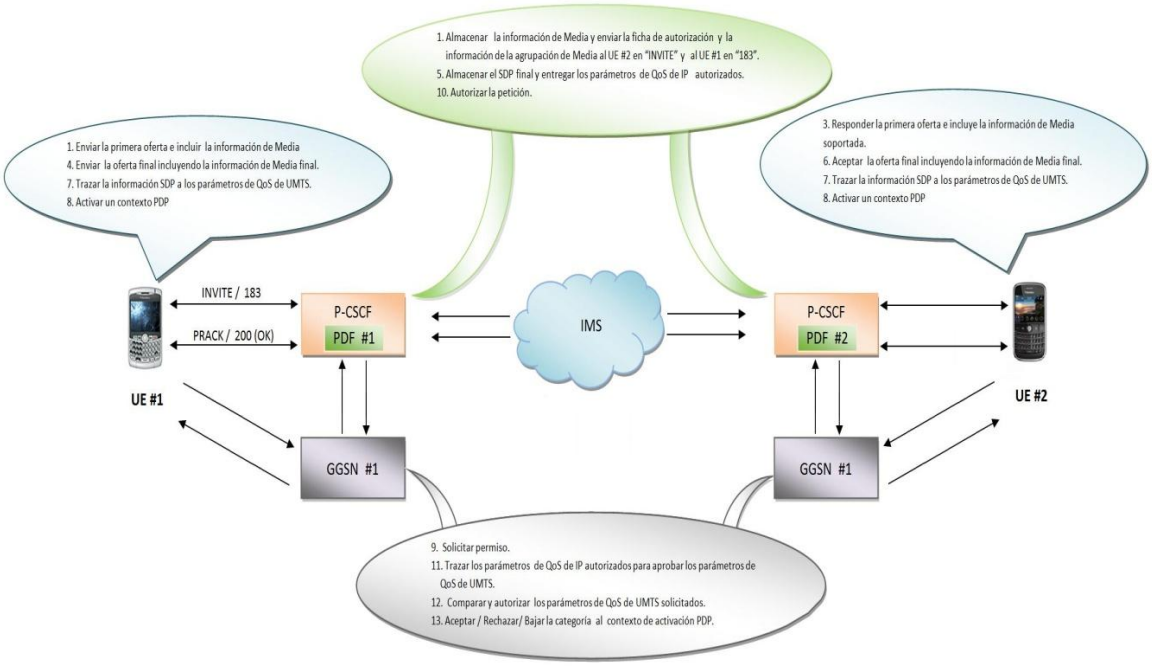
En el recibimiento del contexto de activación o modificación PDP, el GGSN pregunta por información de autorización desde la PDF. La PDF compara la información de vinculación recibida con la información de autorización almacenada y retorna una decisión de autorización. Si la información de vinculación es validada como correcta, la PDF comunica detalles de la autorización multimedia en la decisión al GGSN. Estos detalles contienen los parámetros de QoS IP y clasificadores de paquetes relacionados al contexto PDP.

El GGSN mapea los parámetros de QoS IP autorizados a los parámetros de QoS UMTS autorizados y, finalmente, el GGSN compara los parámetros de QoS UMTS otra vez con los parámetros de QoS UMTS autorizados del contexto PDP. Si los parámetros de QoS UMTS desde el contexto PDP están dentro de los límites autorizados por la PDF, la activación o modificación del contexto PDP será aceptada. La Figura 17 muestra esta funcionalidad; por simplicidad la PDF es

parte del P-CSCF. Cuando un PDF autónomo existe, el P-CSCF necesita mapear información de señalización SIP/SDP para apropiarse de los elementos de información Diameter y enviar un requerimiento apropiado Diameter a la PDF a través del punto de referencia Gq.

En la Figura 18 aparece el proceso completo y se pueden identificar dos fases: autorización de recursos de QoS (Pasos 1-6) y reserva de recursos (Pasos 7-14)

Figura 18. Autorización de portador usando SBLP



6.2. Aprobación de la función de entrega de QoS.

Durante el procedimiento de reserva de recursos la PDF envía paquetes clasificados al GGSN. Basado en la clasificación de paquetes, el GGSN formula una puerta para el control de políticas de tráfico de llegada y de salida. Es decisión de la PDF cuando abrir la puerta. Cuando la puerta está abierta, el GGSN permite el tráfico a través de él. La apertura de la puerta podría ser enviada como una respuesta a un requerimiento de autorización inicial desde el GGSN o la decisión puede ser enviada como una decisión autónoma. Si esta última opción es usada, un operador puede asegurar que los recursos del plano de usuario no son usados antes que la sesión IMS es aceptada (por ejemplo, cuando un mensaje 200OK es recibido). En este caso, usuarios finales perderán todos los anuncios que son entregados antes de completar la sesión, ya que el GGSN desechará los paquetes IP de llegada al plano de usuario (24).

6.3. Eliminación de la función de entrega de QoS.

Esta función cierra la puerta en el GGSN cuando la PDF no permite tráfico a través del GGSN; es usada, por ejemplo, cuando un componente multimedia de una sesión es puesto en espera debido a la re-negociación multimedia (24).

6.4. Indicación de liberación de portadora.

Cuando el GGSN recibe un requerimiento de eliminación de contexto PDP y el contexto PDP ha sido previamente autorizado a través del punto de referencia Go, el GGSN informa a la PDF de la liberación de portadora relacionada a la sesión SIP, enviando un mensaje COPS DELETE. La PDF remueve la autorización para los componentes multimedia correspondientes. Cuando la PDF recibe un reporte que indica que el portador ha sido liberado, podría requerir al P-CSCF liberar las sesiones y revocar las autorizaciones multimedia (24).

6.5. Indicación de pérdida/recuperación de portadora.

Cuando la máxima tasa de bit es igual a 0 Kbps en una solicitud de actualización de contexto PDP, el GGSN necesita enviar un mensaje de reporte COPS al PDF. Similarmente, cuando la máxima tasa de bits es modificada desde 0 kpbs, el GGSN envía un mensaje de reporte COPS al PDF después de recibir una actualización desde el SGSN (Serving GPRS Support Node) (24).

Usando este mecanismo la red IMS es capaz de aprender que UE tiene perdida/recuperada su portadora cuando un flujo o clase de tráfico conversacional está en uso en el sistema GPRS.

6.6. Revocación de autorización.

Está función es usada para forzar la liberación de recursos de portadora autorizados previamente en una red GPRS. Con este mecanismo la PDF es capaz, por ejemplo, de asegurar que el UE libera un contexto PDP cuando una sesión SIP es finalizada o que el UE modifica el contexto PDP cuando un componente multimedia es removido de la sesión. Si el UE no lo hace dentro de un tiempo pre-definido fijado por el operador, entonces la PDF revoca los recursos (24).

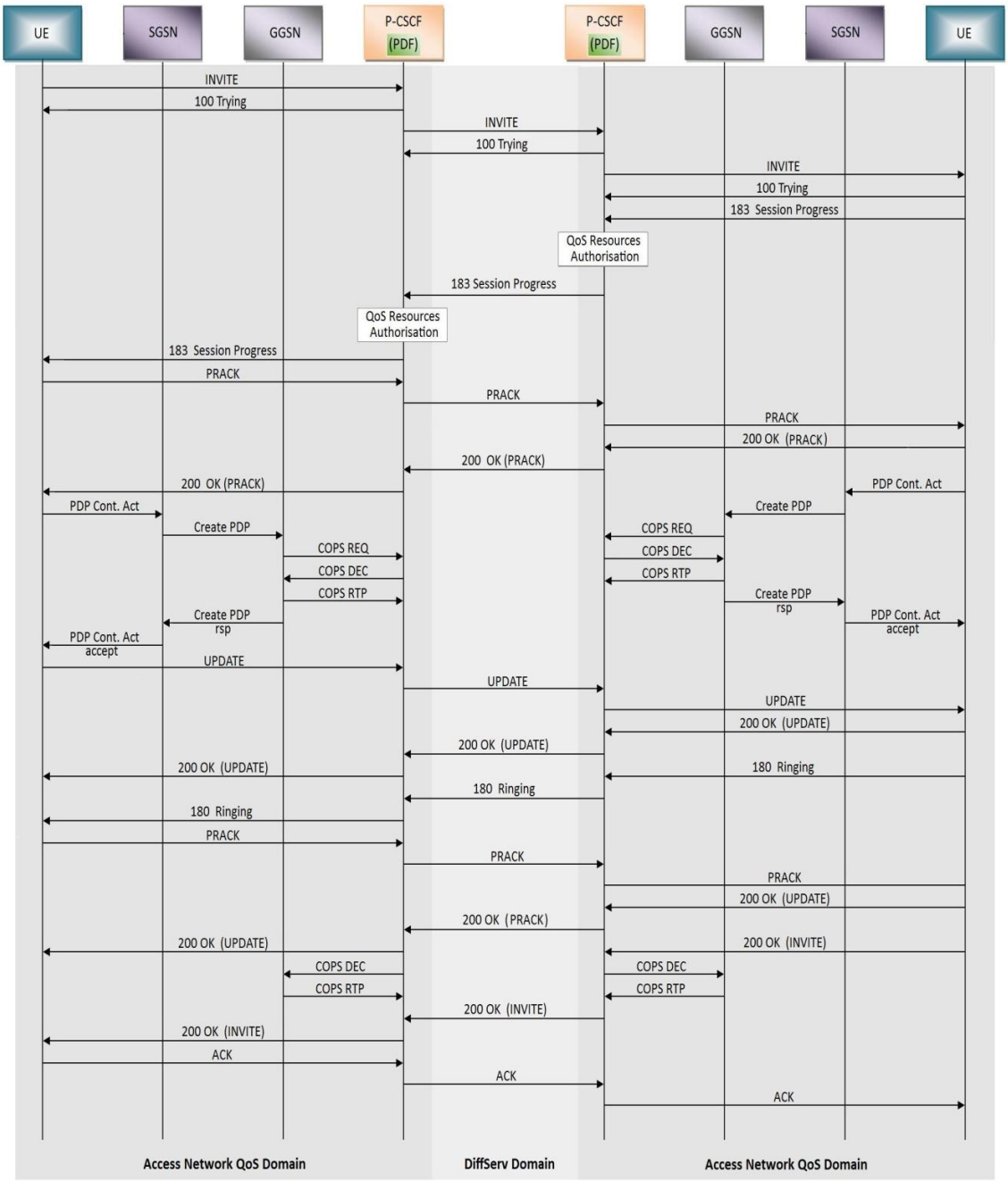
6.7. Intercambio de identificadores de tarificación.

El punto de referencia Go es el enlace entre la red IMS y la red GPRS. Para efectuar el proceso de tarificación, la capa IMS necesita conocer el identificador de tarificación GPRS correspondiente y viceversa. Estos identificadores son

intercambiados durante la fase de autorización de portadora. Un identificador de tarificación IMS es entregado al GGSN dentro del mensaje de decisión de autorización, igualmente un identificador de tarificación GPRS es transmitido al PDF como parte del reporte de autorización (24).

6.8. Flujo de mensajes soportando reserva de QoS.

Figura 19. Flujo de mensajes soportando reserva de QoS



En la Figura 19, se ilustra como la reserva lógica de QoS puede ser introducida en la sesión IMS establecida, entre dos usuarios finales en la red de transporte.

Asumiendo que un usuario satisfactoriamente registrado y autenticado en la red IMS desea llamar a otro usuario en la misma red IMS, su User Equipment (UE) envía un mensaje INVITE indicando la parte llamada con la cual la sesión debería ser establecida en la red de transporte (1).

De acuerdo a los procedimientos previstos por 3GPP, el mensaje de la parte llamante se propaga vía S-CSCF (no mostrada en la Figura 19 por razones de simplicidad) hacía la otra entidad, causando activación de los mecanismos de autorización de recursos de QoS en la PDF en ambos lados de la red de acceso, de manera que el PCSCF dispara los procedimientos de reserva de QoS y obtiene una señal de autorización multimedia, que es un indexado de las características de QoS de la red backbone requeridas por el usuario para la sesión dada (1).

Como resultado, el mensaje de señalización “183 Session Progress” indica la reserva satisfactoria de los recursos requeridos por la parte llamante y se comunica la señal resultante de autorización de medios a la entidad PDF correspondiente de la red llamante. El mismo mensaje se propaga al UE (User Equipment), donde este es usado para la generación de un identificador de flujo de sesión de llamada. El identificador de flujo y el mensaje de autorización identifican únicamente un flujo de medios IP (1).

Una vez los recursos son reservados en la red backbone, el UE envía una descripción de la sesión a la parte llamante con un mensaje “PRACK”. Este procedimiento involucra la generación de un protocolo de descripción de sesión, el cual, ambas partes, la llamada y llamante deberían usar para reservar recursos de sesión en la red de acceso adjunta (1).

A continuación, el usuario originario envía un mensaje de contexto PDP de activación al SGSN. Usando este mensaje GPRS, el usuario asocia el contexto PDP de la red UMTS a la sesión IMS que se ejecutará en la parte superior de ésta, incluyendo la información del mensaje de autorización multimedia y la información del identificador o identificadores de flujo (1).

El SGSN comprueba el perfil de usuario para la QoS requerida y recursos disponibles y envía un mensaje de contexto de creación PDP al GGSN; este mensaje contiene la información de la señal de autorización de medios y la información del identificador o identificadores de flujo (1).

En el GGSN, el punto de ejecución de políticas envía un mensaje COPS REQ al PDF adjuntado. El PDF verifica que la información de la señal de autorización de medios y la información del identificador o identificadores de flujo estén como se espera y finalmente, envía un mensaje COPS DEC (DECision) de retorno al GGSN. En respuesta, el GGSN envía en mensaje COPS RPT (RePorT) al PDF con una respuesta de recibo y/o error (1).

El GGSN comprueba si hay recursos disponibles en la red UMTS y envía un mensaje de respuesta al usuario a través del SGSN en el contexto PDP creado, que contiene el valor negociado de QoS UMTS del elemento de información (IE).

Concluyendo el proceso de reserva de QoS en ambos direcciones ascendente y descendente de la red de acceso, el usuario originario envía un mensaje UPDATE de solicitud al otro usuario, el cual en el campo SDP de la parte llamada indica las características de QoS de la red de acceso (1).

Cuando la parte llamada recibe un mensaje 200 OK (UPDATE), ésta envía una notificación PRACK de los acuerdos de recursos al usuario que llama, y finalmente el PDF de ambas redes de acceso envía un mensaje COPS DEC al GGSN para habilitar al usuario los recursos autorizados de QoS, permitiendo el flujo de paquetes de datos en ambas direcciones en acuerdo con las políticas de decisión del punto de ejecución de políticas del GGSN. Como un paso final del proceso, el GGSN retorna un mensaje COPS RTP, indicando al PDF que los recursos requeridos han sido concedidos en la red backbone y en la red de acceso (1).

El proceso completo finaliza con un mensaje 200 OK correspondiente a la solicitud inicial INVITE, enviada por la parte llamada. Esta recepción por el llamante desencadena un mensaje ACK que indica el éxito de la configuración de la ruta de los datos (1).

7. IDENTIFICACIÓN.

7.1. Identificación de Usuarios.

7.1.1. Identidad de Usuario Privada.

La identidad de usuario privada es única y global definida por el operador de red y puede ser usada dentro de la red origen para identificar exclusivamente al usuario desde una perspectiva de red. Ésta no identifica al usuario por sí misma; de lo contrario, identifica la subscripción del usuario y es usada principalmente para propósitos de autenticación. También, es posible utilizar identidades de usuario privadas con motivos de tarificación y administración (24).

La arquitectura IMS impone los siguientes requerimientos para la identidad de usuario privada (24):

- Debe tomar la forma de un identificador de acceso de red (NAI). Por ejemplo: form_user@realm.
- Estará presente en todos los requerimientos de registro, entregada desde el UE a la red IMS.
- Será autenticada solo durante el registro de usuario.
- El S-CSCF necesitará obtener y almacenar la identidad privada durante el proceso de registro.
- No será usada para enrutamiento de mensajes SIP.
- Será permanentemente asignada a un usuario y almacenada en una aplicación ISIM (IMS Identity Module). La identidad privada será válida durante la subscripción del usuario dentro de la red IMS.
- No será posible para el UE modificar la identidad de usuario privada.
- El HSS necesitará almacenar la identidad de usuario privada.

7.1.2. Identidad de Usuario Pública.

Las identidades de usuario en redes IMS son llamadas identidades de usuario públicas. Son usadas para los requerimientos de comunicación con otros usuarios y pueden ser publicadas, por ejemplo en directorios o en páginas web. Los usuarios IMS están habilitados para iniciar y recibir sesiones desde diferentes redes. La identidad de usuario pública para ser accesible desde redes de conmutación de circuitos, debe ajustarse a la numeración de telecomunicaciones (Por ejemplo, +358501234567). De igual manera, para requerimientos de comunicación con clientes de la Internet, la identidad de usuario pública debe concordar con el dominio de la Internet (Por ejemplo, joe.doe@example.com) (24).

La arquitectura IMS impone los siguientes requerimientos para la identidad de usuario pública (24):

- Tomará las siguientes formas: un SIP URI (SIP Uniform Resource Identifier) o un tel URL (telephone Uniform Resource Locator).
- Al menos una identidad de usuario pública se almacenará en una aplicación ISIM.
- No será posible para el UE modificar la identidad de usuario pública.
- Una identidad de usuario pública debe ser registrada antes de ser usada para originar sesiones IMS y procedimientos no relacionados a sesiones IMS (Por ejemplo, MESSAGE, SUBSCRIBE, NOTIFY).
- Una identidad de usuario pública será registrada antes del término de una sesión IMS y terminando los procedimientos no relacionados a la sesión IMS será entregada al UE del usuario al que pertenece la identidad de usuario pública. Esto no impide la ejecución de servicios en la red para los usuarios no registrados.
- Será posible registrar múltiples identidades de usuario públicas a través de un único requerimiento del UE.
- La red no autenticará identidades de usuario públicas durante el registro.

7.2. Identificación de Servicios.

En el Release 6 se introdujo la identidad de servicio pública para aquellas capacidades de servicio estandarizadas como presencia, mensajería y conferencia. La identidad de servicio pública toma la forma de un SIP URI o el formato de un tel URL. Por ejemplo, en servicios de mensajería hay una identidad de servicio pública para el servicio de lista de mensajes, a la cual los usuarios envían mensajes y luego los mensajes son distribuidos a los miembros de la lista de mensajes, utilizando el servidor destinado para ello. Lo mismo se aplica para el servicio de conferencia, donde un URI es creado para este servicio (24).

7.3. Identificación de Entidades de Red.

Además de los usuarios, los nodos de red que manipulan el enrutamiento SIP deben ser identificables usando un SIP URI válido. Estos SIP URI identifican los nodos de red en el encabezado de los mensajes SIP. Sin embargo, no requieren ser publicados globalmente en un sistema de nombre de dominio (DNS). Por ejemplo, un operador de red podría nombrar su S-CSCF como: sip:finland.scscf1@ims.example.com (24).

8. HERRAMIENTAS DE SIMULACIÓN

Las simulaciones de sistemas utilizando equipos informáticos son en la actualidad de gran aplicación en el ámbito de la ingeniería. En éstas, se puede observar la evolución del sistema, sus características y propiedades sin la necesidad de acudir al sistema real.

En el campo de las redes de telecomunicaciones la presencia de los simuladores ha experimentado un crecimiento exponencial a nivel mundial, siendo cada vez mayor la necesidad de versatilidad de los mismos. Los simuladores de red resultan ser herramientas poderosas que facilitan el diseño de modelos, evaluación y análisis de redes y la simulación de datos.

Con respecto a la simulación de redes IMS, por tratarse de una arquitectura neutral que involucra la convergencia de redes fijas, móviles e inalámbricas, con soporte de calidad de servicio en comunicaciones multimedia, se requiere una herramienta de simulación exigente, que permita ejecutar modelos de interconexión entre redes, utilización de protocolos y procedimientos de transcodificación entre éstos, presencia de flujos multimedia, efectuar simulación de señalización de registro, autenticación, establecimiento, mantenimiento y liberación de una comunicación, entre otras características.

Para estas exigencias, una de las herramientas más utilizada en la simulación de redes IMS es el Simulador de OPNET Technologies Inc. Investigaciones llevadas a cabo a nivel mundial así lo ratifican; es el caso de los trabajos realizados por el departamento de Ingeniería electrónica de la Universidad Nacional de Ilan, en conjunto con otras Universidades Taiwanesas (Universidad Nacional Dong Hwa de Hualien, la Universidad Tamkang de Taipei y la Universidad Nacional de Cheng Kung de Tainan), que dieron como resultado el desarrollo de un mecanismo eficiente de seguridad extremo a extremo para IMS utilizando la herramienta de simulación de redes de OPNET. Igualmente, la Escuela de Ingeniería y Diseño de la Universidad de Brunel, en Londres, en conjunto con el Grupo de Software y Sistemas de Telecomunicaciones del Instituto de Tecnología Waterford en Carriganore Waterford, Irlanda, desarrollaron una investigación apoyada en la herramienta de simulación de OPNET sobre el uso de SHIM6 para la movilidad en redes IMS (25). De la misma forma, en la Universidad de Sídney Australia se verificó la Interconexión de redes WLAN y UMTS mediante la herramienta OPNET Modeler® (26).

OPNET Technologies es un proveedor líder de soluciones para la administración de redes y aplicaciones; posee soluciones para gestión de desarrollo de aplicaciones, planeamiento, ingeniería, operación e investigación y desarrollo de redes(27). Ofrece su software de forma gratuita a Universidades de países que califiquen para las licencias académicas libres en todo el mundo, para investigaciones académicas y enseñanza (28). Posee un programa de asociaciones en el que se destaca la asociación de alianza establecida con

CISCO; OPNET es miembro del programa de desarrollo de tecnología de CISCO, y está certificado como CISCO compatible (29). También posee socios de integración, como son Checkpoint, Cisco, Juniper Nokia, IBM, Oracle, Microsoft, Hewlett Packard, entre otros, con los que trabaja para proporcionar integración técnica entre las soluciones respectivas (30).

El software de simulación de OPNET ® posee las siguientes características:

- Modelo de biblioteca completa con código fuente: más de 800 protocolos, modelos de equipos y modelos de vendedores de dispositivos están disponibles con código fuente, incluyendo modelos especializados como UMTS, MANET, MPLS, WIMAX, IPv6 y más.

- Modelamiento y simulación avanzada: Simulación de eventos discretos, modelamiento analítico y tecnologías híbridas que proporcionan alta fidelidad y simulaciones escalables.

8.1. Productos universitarios OPNET.

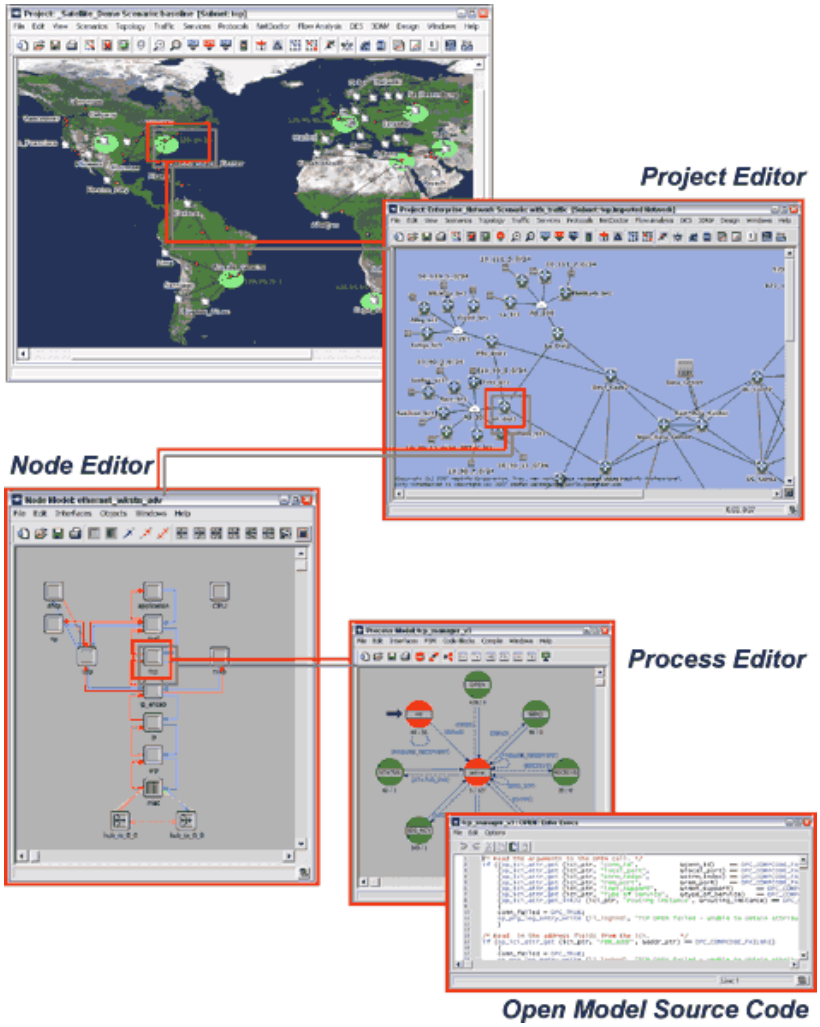
OPNET ha destinado una gama de productos de software para programas universitarios, éstos son:

- *IT Guru®:* Con los módulos adecuados esta plataforma es usada para emprender gestión de desarrollo de aplicaciones.

- *OPNET Modeler®:* Acelera los procesos de investigación y desarrollo para el análisis y diseño de redes de comunicaciones, dispositivos, protocolos y aplicaciones. Los usuarios pueden analizar redes simuladas para comparar el impacto extremo a extremo de diversos diseños tecnológicos. Modeler incorpora una amplia gama de protocolos y tecnologías e incluye un ambiente de desarrollo para habilitar el modelamiento de todo tipo de redes y tecnologías, incluyendo (30):

    - VoIP
    - TCP
    - OSPFv3
    - MPLS
    - IPv6
    - Otras

Figura 20. Modelo de simulación OPNET



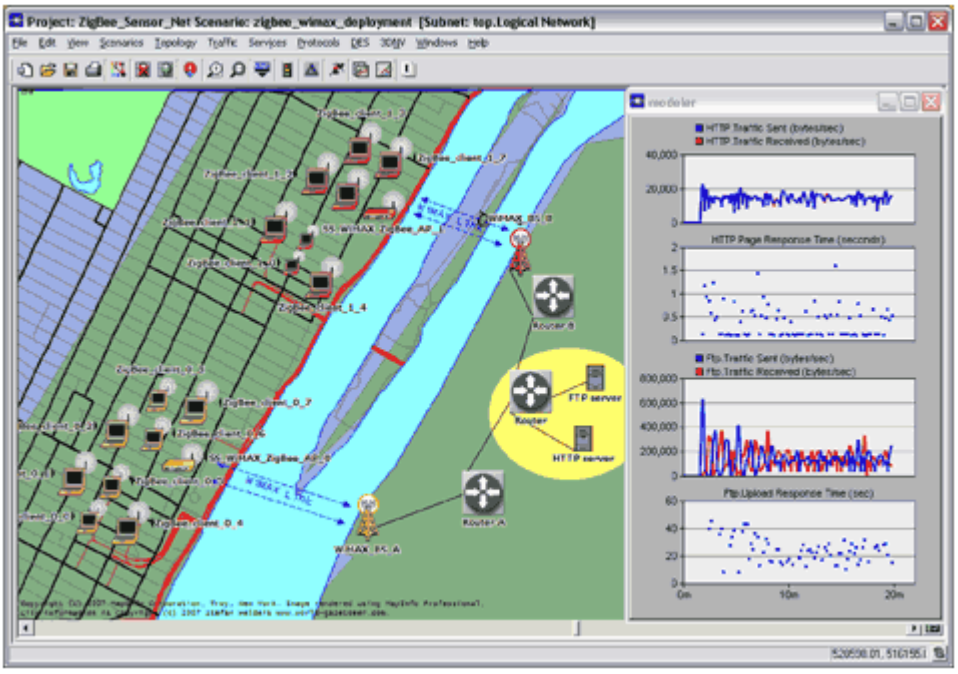
Las principales características de OPNET Modeler® son:

- Simulación discreta rápida de soluciones industriales.
- Cientos de protocolos y modelos de dispositivos de proveedores con código fuente.
- Simulación orientada a objetos.
- Ambiente de simulación jerárquico.
- Simulación discreta, híbrida y opcionalmente analítica.
- Núcleo de simulación paralelo de 32 y 64 bits.
- Interfaces de simulación de sistemas en vivo.
- Interfaces abiertas para la integración de objetos externos, librerías y otros simuladores.
- GUI basada en depuración y análisis.

- *OPNET Modeler® Wireless Suite:* Provee modelamiento de alta fidelidad, simulación y análisis para un amplio rango de redes inalámbricas. Los proveedores de tecnología aprovechan las capacidades avanzadas de simulación y el amplio conjunto de protocolos para diseñar y optimizar protocolos inalámbricos, tales como control de acceso y programación de algoritmos. Las simulaciones incorporan los movimientos presentes en las redes móviles, incluidos los de la tierra, el aire y sistemas de satélites. Modeler Wireless Suite soporta algunas redes con dispositivos móviles, incluidos los celulares (GSM, CDMA, UMTS, WiMAX IEEE 802.16, LTE, entre otros), móviles ad hoc, redes de área local inalámbricas (IEEE 802.11), redes de área personal (Bluetooth, ZigBee, entre otras) y redes satelitales (28).

Los planificadores de redes inalámbricas, arquitectos y profesionales de operación pueden analizar el comportamiento extremo a extremo, sintonizar el desempeño de la red y evaluar escenarios de crecimiento para generación de ingresos por concepto de servicios de red.

Figura 21. Modelamiento con OPNET Modeler® Wireless Suite.



Las principales características de OPNET Modeler® Wireless Suite (28)*:*

- Simulación discreta rápida de soluciones industriales.
- Cientos de protocolos para redes cableadas e inalámbricas y modelos de dispositivos de proveedores con código fuente.
- Simulación orientada a objetos.
- Ambiente de simulación jerárquico.

- Simulación inalámbrica escalable incorporando terreno, movilidad y múltiples modelos pathloss.
- Modelamiento de comportamiento habitual inalámbrico.
- Simulación discreta, híbrida y opcionalmente analítica.
- Núcleo de simulación paralelo de 32 y 64 bits.
- Interfaces de simulación de sistemas en vivo.
- Interfaces abiertas para la integración de objetos externos, librerías y otros simuladores.
- GUI basada en depuración y análisis.

- *SP Guru® Transport Planner:* Usada para la planificación e ingeniería de redes de transporte.

Adicionalmente, OPNET Technologies cuenta con una serie de módulos complementarios (28):

- *3DNV™:* Visualización de redes en 3D para simulaciones discretas en OPNET.

- *ACE™:* Análisis y planificación de aplicaciones extremo a extremo.

- *Circuit Switching™:* Simulación discreta de redes de conmutación de circuitos, para investigación y desarrollo.

- *Flow Analysis™:* Predice y visualiza enrutamiento de tráfico en redes, para análisis de capacidad y resistencia.

- *High-Level Architecture™:* Crea y ejecuta simulaciones distribuidas utilizando el estándar HLA.

- *IPv6:* Simulación discreta del protocolo de enrutamiento IPv6, para planificación e investigación y desarrollo.

- *MPLS:* Simulación discreta del protocolo MPLS, para planificación e investigación y desarrollo.

- *PNNI:* Simulación discreta del enrutamiento PNNI, para planificación e investigación y desarrollo.

- *Server Modeling™:* Planificación de capacidades de servidor y modelamiento con simulación discreta.

- *System-in-the-Loop:* Interfaz para la conexión de aplicaciones de hardware o software con la herramienta de simulación discreta de OPNET.

- *TIREM™:* Simulación discreta con modelamiento de propagación inalámbrica, usando el algoritmo DoD's TIREM.

- *UMTS:* Simulación discreta del protocolo UMTS, para planificación e investigación y desarrollo.

- *WiMAX:* Simulación discreta del protocolo WiMAX 802.16e, para planificación e investigación y desarrollo.

De esta forma, con los módulos adecuados de simulación de OPNET se pueden realizar simulaciones completas de redes IMS. Si bien, en el software todavía no se encuentran entidades IMS, éstas pueden ser creadas y almacenadas en una nueva librería; además, es evidente que se requiere adquirir uno o varios de los módulos de simulación adicionales para realizar una comunicación en el entorno heterogéneo IMS.

CONCLUSIONES

La arquitectura IP Multimedia Subsystem (IMS) propone la interconexión de las diferentes redes de acceso (móviles, inalámbricas y fijas) existentes en el mundo de las telecomunicaciones, soportando nuevos y mejores servicios multimedia con garantía de calidad de servicio. Con IMS se prestarán todo tipo de servicios multimedia (transmisión de audio, vídeo, cualquier tipo de información de usuario, servicios de presencia, mensajería, nuevos servicios de emergencia, multiconferencia, entre otros) ofrecidos por las plataformas de servicios CAMEL, OSA y SIP. Sin embargo, en torno al estudio de IMS, por tratarse de una tecnología emergente que todavía está en proceso de desarrollo y estandarización, hay diversos temas particulares sobre los cuales se puede profundizar; es el caso de la arquitectura de servicios IMS, la garantía de seguridad y calidad de servicio, la necesidad de regulación a nivel mundial, el funcionamiento lógico de las interfaces que hacen posible la interconexión entre las diferentes redes de acceso y el manejo de simuladores como el de OPNET.

Se puede simular una red IMS utilizando la gama de productos universitarios de OPNET Technologies; para ello, se requiere como mínimo el paquete *OPNET Modeler*® y el *OPNET Modeler*® *Wireless Suite* así como el modulo complementario *Circuit Switching*™, involucrando los ambientes de conmutación de paquetes, inalámbricos y móviles y de conmutación de circuitos, respectivamente.

Uno de los mayores inconvenientes de IMS se presenta cuando se realiza interconexión con la red telefónica pública conmutada (PSTN), ya que inicialmente se desarrolló solo para aplicarse a entornos móviles como evolución de las redes de tercera generación y en la medida que avanzó en su proceso de diseño y revisión se le fueron adicionando las redes inalámbricas y las redes fijas; con la dificultad de que en las redes fijas la señalización y los procedimientos seguidos para establecer una comunicación varían en gran proporción con los utilizados en el entorno móvil.

Gracias a la implementación de un modelo de capas IMS ofrece a los operadores el despliegue de una nueva actividad de negocios basada en servicios, dejando a un lado los tradicionales servicios de arquitectura vertical por el modelo de servicios horizontales, donde éstos pueden ser fácilmente creados e incorporados gracias a la utilización de protocolos de la IETF. La arquitectura horizontal de IMS permite a los operadores generar atractivos servicios finales, requiriéndose para tal fin, que el equipo de usuario utilizado en la comunicación soporte el tipo de servicio que registró en la red.

GLOSARIO

ALL IP: Modelo de red basado en el uso del protocolo IP.

ATTRIBUTE VALUE PAIR (AVP): Método de encapsulamiento de información utilizado en un mensaje de tipo Diameter.

BASIC SERVICE SET (BSS): Subsistema de estación base. En la arquitectura ETSI GSM se denomina BSS al conjunto formado por el controlador de estaciones base (BSC) y todas las estaciones base (BTS) que dependen de él.

BREAKOUT GATEWAY CONTROL FUNCTION (BGCF): Es la entidad lógica dentro de la red IMS que decide como encaminar las sesiones de telefonía iniciadas en la red IMS y destinadas a una red de conmutación de circuitos (PSTN).

CABLELABS: Consorcio encargado de investigar y desarrollar los protocolos usados en redes por cable coaxial.

CALIDAD DE SERVICIO (QOS): Término genérico para definir el conjunto de parámetros que definen el tipo y la calidad del servicio proporcionado.

CALL SESSION CONTROL FUNCTION (CSCF): Entidad de red IP Multimedia Subsystem encargada del control de sesión de llamada para terminales y aplicaciones.

CDMA2000: Tecnología hibrida 2.5G/3G de estándares de telecomunicaciones móviles que utilizan CDMA, un esquema de acceso múltiple para redes digitales, para enviar voz, datos, y señalización entre teléfonos celulares y estaciones base.

CODEC: Abreviatura de Compresor-Descompresor. Describe una especificación desarrollada en software, hardware o una combinación de ambos, capaz de transformar un archivo con un flujo de datos (stream) o una señal. Los códecs pueden codificar el flujo o la señal (a menudo para la transmisión, el almacenaje o el cifrado) y recuperarlo o descifrarlo del mismo modo para la reproducción o la manipulación en un formato más apropiado para estas operaciones.

COMMON OPEN POLICY SERVICE (COPS): Protocolo común abierto para políticas de servicio. Es un protocolo simple de petición y respuesta que puede ser utilizado para intercambiar información entre un servidor de políticas (punto de decisión de políticas o PDP) y sus clientes (Puntos de aplicación de políticas o PEPs).

DIAMETER: Protocolo de red para la autenticación de los usuarios que se conectan remotamente a la Internet a través de la conexión por línea conmutada o TLC, también provee servicios de autorización y auditoría para aplicaciones tales como acceso de red o movilidad IP.

DOMAIN NAME SYSTEM (DNS): Es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como la Internet. Aunque como base de datos, el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP): Protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Es de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

ENHANCED DATA RATES FOR GSM EVOLUTION (EDGE): Tecnología de telefonía móvil celular, que actúa como puente entre las redes 2G y 3G; considerada una evolución de la tecnología GPRS (General Packet Radio Service).

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI): Instituto Europeo de Normas de Telecomunicaciones. Es una organización de estandarización de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) de Europa, con proyección mundial.

GATEWAY GPRS SUPPORT NODE (GGSN): Nodo de red que actúa como gateway entre una red de datos inalámbrica GPRS y otras redes, como la Internet o redes privadas.

GENERAL PACKET RADIO SERVICE (GPRS): Servicio de datos móviles orientado a paquetes, disponible para los usuarios de sistemas de comunicación celular 2G GSM así como para sistemas 3G.

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS (GSM): Sistema Global para las Comunicaciones Móviles. Sistema estándar para la comunicación mediante teléfonos móviles que incorporan tecnología digital. Por su velocidad de transmisión y otras características se considera un estándar de segunda generación (2G).

HOME LOCATION REGISTER (HLR): Base de datos que almacena la posición del usuario dentro de la red, si está conectado o no y las características de su abonado (servicios que puede y no puede usar, tipo de terminal, entre otros). Es de carácter permanente; cada número de teléfono móvil está adscrito a un HLR determinado y único, que administra su operador móvil.

HOME SUBSCRIBER SERVER (HSS): Base de datos maestra que soporta las entidades de red IMS que efectúan llamadas. Contiene información relacionada al perfil de usuario, efectúa las funciones de autenticación y autorización de usuarios y puede proveer información acerca de la localización física de los usuarios. Es similar al HLR y al AUC de la red GSM.

HYPERTEXT TRANSFER PROTOCOL (HTTP): Protocolo usado en cada transacción de la Web (WWW); define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse.

IMS APPLICATION LEVEL GATEWAY (IMS ALG): Componente de red IMS que proporciona la funcionalidad de aplicación necesaria a la pila de protocolos SIP/SDP para que interactúen aplicaciones IPv4 e IPv6.

IMS SUSCRIBER IDENTITY MODULE (ISIM): Módulo de identificación de usuario IMS. Ejecuta funciones de autenticación de abonado durante su registro en IMS, contiene además datos de suscripción del abonado.

IMS SERVICE CONTROL (ISC): Interfaz de control de servicio que transfiere mensajes de notificación entre el AS y el S-CSCF.

INTELLIGENT NETWORK APPLICATION PROTOCOL (INAP): Protocolo que ofrece comunicación en tiempo real entre los elementos de una red inteligente.

INTERNET ENGINEERING TASK FORCE (IETF): Organización internacional abierta de normalización, que tiene como objetivos contribuir a la ingeniería de la Internet, actuando en diversas áreas, tales como transporte, enrutamiento y seguridad.

INTERNET PROTOCOL SECURITY (IPSec): Conjunto de protocolos para implementar seguridad y capacidades de autenticación en redes IP.

INTERROGATING - CALL SESSION CONTROL FUNCTION (I-CSCF): Entidad de red IMS encargada de la interoperación entre redes IMS. Pueden existir varias I-CSCF dentro de una red IMS, siendo éste un nodo opcional en la arquitectura IMS.

IP MULTIMEDIA SUBSYSTEM (IMS): Arquitectura de red diseñada para la entrega de servicios multimedia utilizando el Protocolo de Internet IP.

ISDN USER PART (ISUP): Protocolo de circuitos conmutados, usado para configurar, manejar y gestionar llamadas de voz y datos sobre PSTN; usado para llamadas ISDN y no ISDN y es parte de la señalización ANSI.

JAVA COMMUNITY PROCESS (JCP): Proceso formalizado que permite a las partes interesadas involucrarse en la definición de futuras versiones y características de la plataforma Java.

MEDIA GATEWAY (MGW): Nodo de red que actúa como una unidad de traducción entre redes de telecomunicaciones dispares tales como PSTN y redes de acceso como 2G, 2,5G, 3G o PBX de radio.

MEDIA GATEWAY CONTROL FUNCTION (MGCF): Entidad de red IMS que provee la función de interfuncionamiento de señalización entre los elementos de la red IMS y la red PSTN.

MEDIA RESOURCE FUNCTION (MRF): Entidad de red IMS que proporciona los servicios multimedia e implementa funciones para gestionar y procesar flujos de medios como voz, video, texto para hablar y tras-codificación de datos multimedia.

MEDIA RESOURCE FUNCTION CONTROLLER (MRFC): Entidad de red IMS que controla los recursos multimedia del MRFP. Este dispositivo utiliza SIP para comunicarse con el AS y H.248 con el MRFP.

MEDIA RESOURCE FUNCTION PROCESSOR (MRFP): Entidad de red IMS que lleva a cabo el procesamiento de servicios multimedia que requieren las aplicaciones del AS.

MEGACO: Protocolo que define el mecanismo necesario de llamada para permitir a un controlador Media Gateway el control de puertas de enlace para soporte de llamadas de voz/fax entre redes RTC-IP o IP-IP.

MULTIPURPOSE INTERNET MAIL EXTENSIONS (MIME): Especificaciones que permiten intercambiar a través de la Internet todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario.

NETWORK ADDRESS TRANSLATION (NAT): Mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Convierte en tiempo real las direcciones utilizadas en los paquetes transportados.

NETWORK TO NETWORK INTERFACE (NNI): Interfaz de señalización que especifica las funciones de gestión entre dos redes. El circuito de NNI se puede utilizar para la interconexión de cualquier señalización de redes IP o ATM.

OPEN MOBILE ALLIANCE (OMA): Organización de estándares que desarrolla estándares abiertos para la industria de telefonía móvil.

POLICY DECISION FUNCTION (PDF): Función lógica que implementa la decisión en relación a la política a ser aplicada y hace uso de mecanismos de QoS en la capa de conectividad IP.

POLICY DECISION POINT (PDP): Entidad lógica que realiza control de admisión y decisión de políticas, en respuesta a una petición de un usuario que espera acceder a un recurso en un ordenador o en un servidor de red.

POLICY ENFORCEMENT POINTS (PEP): Entidad donde las políticas son aplicadas. Es el cliente del PDP, su tarea es recuperar las peticiones del SSVM o de los Proxies SIP sobre decisiones basadas en políticas, y preguntarle al PDP. Entonces, y si fuera necesario, el PEP aplicará las reglas de política recibidas e informará al cliente de los resultados.

PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6): Nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF para reemplazar en forma gradual a la versión actual, el IPv4.

PROXY - CALL SESSION CONTROL FUNCTION (P-CSCF): Entidad de red IMS encargada de proporcionar una trasmisión segura de señalización SIP con el terminal de usuario. Constituye el primer punto de contacto que el dominio IMS presenta a los terminales de usuario.

PUBLIC SWITCHED TELEPHONE NETWORK (PSTN): Red Telefónica Pública Conmutada, constituida por todos los medios de transmisión y conmutación necesarios que permiten enlazar a voluntad dos equipos terminales mediante un circuito físico que se establece específicamente para la comunicación y que desaparece una vez se ha completado la misma.

REAL TIME CONTROL PROTOCOL (RTCP): Protocolo de comunicación que proporciona información de control que está asociado con un flujo de datos para una aplicación multimedia (flujo RTP).

REAL TIME PROTOCOL (RTP): Protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una videoconferencia.

RESOURCE RESERVATION PROTOCOL (RSVP): Protocolo de reserva de recursos. Técnica de gestión de calidad en la transmisión de datos que se realiza mediante la reserva de recursos para cada flujo de datos individual.

ROUTER: Nodo de una red TCP/IP que se encarga de la conexión con otras redes, efectuando funciones de encaminamiento y filtrado.

SERVICE BASED LOCAL POLICY (SBLP): Mecanismo de control de calidad de servicio que suele ser empleado en redes celulares.

SERVICE SET IDENTIFIER (SSID): Identificador de una red WLAN. Permite distinguir entre las redes existentes en un mismo lugar, de cara a la asociación entre un terminal y un punto de acceso.

SERVING - CALL SESSION CONTROL FUNCTION (S-CSCF): Entidad de red IMS encargada de realizar la gestión de la sesión. Puede haber varios S-CSCFs en la red con diversas funcionalidades, elegidos diferentemente basándose en los servicios solicitados o en las capacidades del móvil.

SERVING GPRS SUPPORT NODE (SGSN): Entidad encargada del control de una red GPRS.

SESSION BORDER CONTROLLER (SBC): Dispositivo de red que controla la admisión de llamadas en la frontera de la red.

SESSION DESCRIPTION PROTOCOL (SDP): Protocolo de descripción de sesión, destinado a la gestión de sesiones (anuncio, invitación e iniciación), definido por la IETF.

SESSION INITIATION PROTOCOL (SIP): Protocolo de señalización desarrollado por la IETF, con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como video, voz, mensajería instantánea, juegos online y realidad virtual.

SIGNALING GATEWAY (SGW): Entidad que provee la conversión de señalización en ambas direcciones en la capa de transporte entre SS7 y señalización basada en IP (por ejemplo ISUP/SS7 e ISUP/SCTP/IP).

SIMPLE MAIL TRANSFER PROTOCOL (SMTP): Protocolo de red basado en texto, utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

SIP APPLICATION SERVER (AS): Servidor de aplicación SIP. Dispositivo de red en el que residen las aplicaciones ofrecidas al usuario.

TELECOMS & INTERNET CONVERGED SERVICES & PROTOCOLS FOR ADVANCED NETWORKS (TISPAN): Grupo del ETSI dedicado a la estandarización de servicios y redes fijas, particularmente en la evolución de las redes de circuitos a redes de paquetes.

THE 3RD GENERATION PARTNERSHIP PROJECT (3GPP): Acuerdo de colaboración en tecnología de telefonía móvil. Su Objetivo es hacer global aplicaciones de tercera generación 3G, con especificaciones de sistemas ITU's IMT-2000.

THE 3RD GENERATION PARTNERSHIP PROJECT 2 (3GPP2): Acuerdo de colaboración entre las asociaciones de telecomunicaciones para hacer una especificación aplicable globalmente de los sistemas de telefonía móvil de tercera generación (3G) en el ámbito del proyecto IMT-2000 de la UIT. En la práctica, 3GPP2 es el grupo de normalización de CDMA2000, el conjunto de normas 3G basado en la tecnología 2G CDMA anterior.

TIME DIVISION MULTIPLEXING (TDM): Técnica de multiplexación en la que el ancho de banda total del medio de transmisión es asignado a cada canal durante una fracción del tiempo total (intervalo de tiempo).

TRANSMISSION CONTROL PROTOCOL (TCP): Protocolo de comunicación orientado a conexión, que garantiza la entrega de datos al destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. TCP da soporte a muchas de las aplicaciones más populares de la Internet, incluidas HTTP, SMTP, SSH y FTP.

UNIFORM RESOURCE IDENTIFIER (URI): Cadena corta de caracteres que identifica inequívocamente un recurso (servicio, página, documento, dirección de correo electrónico, enciclopedia); normalmente estos recursos son accesibles en una red o sistema.

UNIFORM RESOURCE LOCATOR (URL): Cadena de caracteres, de acuerdo a un formato estándar, con la cual se asigna una dirección única a cada uno de los recursos de información disponibles en la Internet.

UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM (UMTS): Sistema Universal de Telecomunicaciones móviles. Es una de las tecnologías usadas por los móviles de tercera generación (3G, también llamado W-CDMA), sucesora de GSM.

UNIVERSAL TERRESTRIAL RADIO ACCESS NETWORK (UTRAN): Red de acceso radio terrestre UMTS que proporciona la conexión entre los terminales móviles y la red principal.

USER AGENT (UA): Aplicación que utiliza un protocolo particular de red.

USER DATAGRAM PROTOCOL (UDP): Protocolo del nivel de transporte basado en el intercambio de datagramas. UDP no otorga garantías para la entrega de sus mensajes y el origen UDP no retiene estados de los mensajes UDP que han sido enviados a la red. UDP sólo añade multiplexado de aplicación y suma de verificación de la cabecera y carga útil. Cualquier tipo de garantías para la transmisión de la información, deben ser implementadas en capas superiores.

USER EQUIPMENT (UE): Cualquier dispositivo usado por el usuario final para comunicarse, puede ser un teléfono móvil, un computador portátil o cualquier otro dispositivo.

USER NETWORK INTERFACE (UNI): Interfaz entre la red del proveedor de servicios y el equipo de usuario (tales como routers IP y otros sistemas finales).

VIRTUAL PRIVATE NETWORK (VPN): Red de computadores, en la cual los enlaces entre nodos se realizan a través de circuitos virtuales en lugar de circuitos físicos.

WIDEBAND CODE DIVISION MULTIPLE ACCESS (WCDMA): Técnica de acceso múltiple para la tecnología móvil inalámbrica de tercera generación que aumenta las tasas de transmisión de datos de los sistemas GSM utilizando la interfaz aérea CDMA en lugar de TDMA.

WIFI: Sistema de envío de datos sobre redes computacionales que utiliza ondas de radio en lugar de cables. Wi-Fi es una marca de la Wi-Fi Alliance, organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11.

WIMAXFORUM: Consorcio de empresas dedicadas a diseñar los parámetros y estándares de la tecnología WIMAX y a estudiar, analizar y probar los desarrollos implementados.

WIRELESS LAN (WLAN): Sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.

WORLDWIDE INTEROPERABILITY FOR MICROWAVE ACCESS (WIMAX): Norma de transmisión por ondas de radio de última generación orientada al denominado bucle local inalámbrico (última milla) que permite la recepción de datos por microondas y retransmisión por ondas de radio (protocolo 802.16), proporcionando acceso compartido con varios repetidores de señal superpuestos, ofreciendo cobertura total en áreas de hasta 48 km de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa con las estaciones base (a diferencia de las microondas). WiMax es un concepto parecido a WiFi pero con mayor cobertura y ancho de banda.

X-DIGITAL SUBSCRIBER LINE (X-DSL): Tecnología de transmisión que permite que los hilos telefónicos de cobre convencionales transporten hasta 16 Mbps (megabits por segundo) mediante técnicas de compresión. Hay diversas modalidades de esta tecnología, tales como ADSL, HDSL y RADSL, siendo ADSL la más utilizada actualmente.

REFERENCIAS

1. **Tompros, Spyridon y Denazis, Spyridon.** *Interworking of heterogeneous access networks and QoS provisioning via IP multimedia core networks.* Universidad de Patras. 8 de septiembre 2007. Disponible: http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6VRG-4PMJK6C-5-N&_cdi=6234&_user=2620291&_orig=search&_coverDate=01%2F18%2F2008&_sk=999479998&view=c&wchp=dGLzVtz-zSkWA&md5=23bec3e813019432ac5fc4e1f6fabd00&ie=/sdarticle.pdf.

2. **Ericsson.** *Introduction to IMS, White Paper.* 2007. Disponible: http://www.ericsson.com/technology/whitepapers/8123_Intro_to_ims_a.pdf.

3. **3GPP.** 3rd Generation Partnership Project. [En línea] http://www.3gpp.org/About/about.htm.

4. **3rd Generation Partnership Project (3GPP).** Release 6. [En línea] http://www.3gpp.org/specs/releases-contents.htm.

5. **3rd Generation Parnetship Project (3GPP).** Release 7. [En línea] http://www.3gpp.org/specs/releases-contents.htm.

6. **3rd Generation Partnership Project (3GPP).** [En línea]

7. **Orange.** Fundación ORANGE. [En línea] http://www.fundacionorange.es/areas/25_publicaciones/Nota_18_DEF.pdf.

8. **Znaty, Simón, Dauphin, Jean Louis y Geldwerth, Roland.** *IP Multimedia Subsystem: Principios y Arquitectura.* EFORT. Disponible: http://www.efort.com/media_pdf/IMS_ESP.pdf.

9. **Pechuán, Luis Miralles.** *El nuevo sistema multimedia conocido como IMS que adoptarán las redes UMTS.* Universidad de Valencia. Disponible: http://www.uv.es/montanan/redes/trabajos/index.html.

10. **3rd Generation Partnership Project.** *TS 23.228: IP Multimedia Subsystem (IMS); Stage 2.* Disponible: http://www.3gpp.org/ftp/Specs/html-info/23228.htm.

11. **Mani, Mehdi y Crespi, Noel.** *Adopting IMS in WiFi Technology.* 2007. Disponible: http://portal.acm.org/citation.cfm?id=1378117.

12. **Telefónica.** *Evolución al dominio IMS.* Disponible:http://www.telefonica.es/sociedaddelainformacion/pdf/publicaciones/movilidad/capitulo_12.pdf.

13. **Znaty, Simon, Dauphin, Jean Louis y Geldwerth, Roland.** *SIP : Session Initiation Protocol.* Efort. Disponible: http://www.efort.com/media_pdf/IMS_ESP.pdf.

14. **Bounoure, Francois, y otros.** *Laboratorio de redes: Session Initiation Protocol.* Universidad de Buenos Aires. 2006. Disponible: http://www.fiuba6662.com.ar/6648/presentaciones/2006/Informe%20SIP.pdf.

15. **The Internet Engineering Task Force.** *RFC 4566: SDP: Session Description Protocol.* 3rd Generation Partnership Project. 2006. Disponible:http://www.ietf.org/rfc/rfc4566.txt?number=4566.

16. **Real Académia Uruguaya.** *Introducción al IPv6.* http://www.rau.edu.uy/ipv6/queesipv6.htm.

17. **Hallivuori, Ville.** *Real time Transport Protocol (RTP) security.* Helsinki University of Technology. 2000. Disponible: http://kotiweb.kotiportti.fi/vhallivu/files/rtp_security.pdf.

18. **The Internet Engineering Task Force.** *RFC 3550: RTP: A Transport Protocol for Real-Time Applications.* Disponible: http://www.ietf.org/rfc/rfc3550.txt.

19. **Salazar, Jorge Escribano, y otros.** *Diffserv como solución a la provisión de QoS en Internet.* Universidad Carlos III de Madrid. Disponible: http://www.ist-mobydick.org/publications/cita2002.pdf.

20. **The Internet Engineering Task Force.** *RFC 2748: The COPS (Common Open Policy Service) Protocol.* Disponible: http://www.ietf.org/rfc/rfc2748.txt?number=2748.

21. **Cisco.** *Resource Reservation Protocol.* Disponible: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/RSVP.pdf.

22. **The Internet Engineering Task Force.** *RFC 2205: Resource ReSerVation Protocol (RSVP).* Disponible: http://www.ietf.org/rfc/rfc2205.txt?number=2205.

23. **Jalercom.** *Infraestructura y Equipos de VoIP.* Disponible: http://www.jalercom.com/Brochures/brochure_infraestructura%20y%20equipo%20de%20voip.pdf.

24. **Poikselka, Miikka, y otros.** *The IMS IP Multimedia Concepts and Services.* s.l. : John Wiley & Sons Ltd, 2006. Vol. Segunda Edición.

25. **John Ronan, Sasitharan Balasubramaniam, Adnan K Kiani, Wenbing Yao.** *On the use of SHIM6 for Mobility Support in IMS Networks.*

26. **Munasighe, Kumudu y Jamalipour, Abbas.** *Interworking of WLAN-UMTS Netwoks: An IMS based Pltaform for Session Mobility.* s.l. : IEEE, 2008.

27. **OPNET Tecnologies Inc.** [En línea]
http://www.opnet.com/corporate/fact_sheet.html.

28. **OPNET.** University Program. [En línea]
http://www.opnet.com/university_program/index.htm.

29. —. Alliance Partners. [En línea]
http://www.opnet.com/corporate/partners/alliance_partners/index.html.

30. —. Integration Partners. *Integration Partners.* [En línea]
http://www.opnet.com/corporate/partners/integration_partners/index.html.