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

CONSTRUCCIÓN DE LABORATORIOS DOCENTES PARA ARQUITECTURA IMS

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL ELECTRICISTA

JAVIER ALONSO MIRANDA TORRES

PROFESOR GUÍA:
ALBERTO CASTRO ROJAS

MIEMBROS DE LA COMISIÓN:
NÉSTOR BECERRA YOMA
JORGE SANDOVAL ARENAS

SANTIAGO DE CHILE
OCTUBRE 2008

RESUMEN DEL INFORME FINAL
PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL ELECTRICISTA.
POR: JAVIER MIRANDA TORRES.
FECHA: 13/OCTUBRE/2008.
PROF. GUÍA: SR. ALBERTO CASTRO.

CONSTRUCCIÓN DE LABORATORIOS DOCENTES PARA ARQUITECTURA IMS

La masificación y crecimiento de la telefonía móvil e Internet propone un desafío para los operadores y proveedores de servicios de valor agregado. Sus modelos de redes y negocios deben adaptarse para lograr la *convergencia en redes de telecomunicaciones* y así poder competir en más nichos de mercado, en los que actualmente no son capaces de entrar, dadas las características técnicas de sus plataformas tecnológicas. La convergencia de redes y servicios permite a los usuarios de redes de telefonía móvil, fija e Internet, utilizar distintas tecnologías de acceso. Además, facilita el uso de dispositivos de comunicación, como terminales móviles, que concentran varios servicios.

Con la evolución de las arquitecturas de telefonía móvil, se han incluido nuevas plataformas que integran sistemas de comunicaciones nuevos y existentes. La solución de la organización *Third Generation Partnership Project* (3GPP) para alcanzar la convergencia de redes y servicios es IMS, *IP Multimedia Subsystem*. El desarrollo de los antecedentes técnicos de la arquitectura IMS permite introducir el funcionamiento de sus componentes principales, con el fin de elaborar un curso de capacitación para los profesionales del mercado de telecomunicaciones.

El principal objetivo del trabajo de título es la construcción de un conjunto de laboratorios docentes, que conforman el curso de capacitación. La investigación de la plataforma IMS, especificada por 3GPP, comprende principalmente los protocolos de Internet, en particular el protocolo de iniciación de sesiones SIP, utilizado ampliamente en telefonía sobre IP. El protocolo SIP y sus extensiones, definidas en los estándares, son la base de IMS y le otorgan las características necesarias para ofrecer servicios convergentes en el mercado de la telefonía móvil y fija. Las experiencias de laboratorio sirven para que los estudiantes manejen SIP y describan una arquitectura IMS con sus componentes y funciones.

Para llevar a cabo la construcción de los laboratorios se elabora y ejecuta una metodología docente. La metodología es empleada para estructurar las experiencias prácticas y distribuir en las actividades los contenidos desarrollados en los antecedentes técnicos. Las actividades permiten trabajar en detalle la señalización SIP, el comportamiento del núcleo IMS y el funcionamiento de servicios convergentes, tales como: voz sobre IP, video llamadas, mensajería instantánea, *click to dial*, *voicemail*, *IPTv*, entre otros.

Una vez expuesta la estructura del curso, se procede con el diseño, instalación e integración de una plataforma IMS basada en software de código abierto. Sobre esta plataforma, modular y portable, se realizan pruebas de funcionamiento que permiten tener una visión práctica de la plataforma IMS, además de la ejecución y revisión de los laboratorios. Los resultados del trabajo son: un conjunto de actividades prácticas que permiten el aprendizaje integral de las funcionalidades de IMS, las que conforman los laboratorios; la introducción a servicios convergentes; el uso e interacción de terminales SIP e IMS; la construcción y operación de una plataforma de pruebas IMS; y el trabajo con herramientas de análisis y pruebas, para redes y plataformas.

Finalmente, la propuesta de nuevos trabajos, consiste en agregar a la plataforma de prueba varios nodos de tareas específicas, como facturación, control de medios, control de políticas de QoS (calidad de servicio) y de comunicación con otras redes. Esto permitirá alcanzar un conocimiento amplio sobre la tecnología IMS, que está llamada a ser el medio de integración entre las redes de comunicación móvil e Internet.

“A mis queridos padres,
Gladys y Segundo.
Por su incansable esfuerzo y dedicación.”

Índice general

Índice de figuras

Capítulo 1

Introducción

Este documento presenta el desarrollo del trabajo de titulación realizado sobre una plataforma IMS *IP Multimedia Subsystem* enfocado en la creación de un curso de laboratorio. La elaboración de este curso refleja la necesidad de contar con los conocimientos sobre el nuevo subsistema de telefonía móvil que forma parte del núcleo de red en el marco de la evolución de las redes de tercera generación 3G.

La masificación y crecimiento de la telefonía móvil e Internet propone un desafío para los operadores y proveedores de servicios de valor agregado. Ellos necesitan modificar sus modelos de negocio y sus redes para lograr la *convergencia en telecomunicaciones*, de tal manera de poder competir en nichos de mercado en los que actualmente no son capaces de entrar dadas las características técnicas de sus redes. El concepto de convergencia significa poder utilizar un servicio móvil, fijo o de Internet utilizando cualquier medio de acceso y a su vez, concentrar todos los servicios en un solo dispositivo de comunicación. Para lograr esto, es necesaria la inclusión de una nueva plataforma que integre todos los sistemas de comunicaciones de manera sencilla y rápida. La solución de la organización 3GPP *Third Generation Partnership Project* para alcanzar la convergencia de redes y servicios es la arquitectura IMS.

A lo largo del documento se presentan los fundamentos teóricos de IMS, la integración de una plataforma computacional útil para la ejecución de pruebas experimentales y finalmente la creación del curso de laboratorio. A continuación se presentan los objetivos y la estructura de la memoria.

1.1. Objetivos

El objetivo principal del trabajo de título es crear el curso de laboratorio. Esto corresponde a la elaboración de guías prácticas para ser resueltas por alumnos con conocimientos previos en telecomunicaciones. El cumplimiento del objetivo se traduce en la realización de las siguientes tareas.

1. Construcción de laboratorios docentes. Es el objetivo principal de este trabajo. Consiste en crear los procedimientos para generar guías de trabajo de laboratorio de apoyo docente.
2. Estudio y despliegue de arquitectura IMS. Se requiere una completa comprensión de la arquitectura IMS para poder llevar a cabo la creación del curso. Dentro del estudio se destacan los protocolos sobre los que se sostiene IMS, tales como SIP, SDP, RTP, DHCP, Diameter, UDP, TCP, IP, entre otros.
3. Integración a un Core IMS. Corresponde a la tarea más extensa puesto que se requiere de un estudio acabado de la arquitectura, además de largos períodos de instalación y pruebas.
4. Desarrollar un plan de pruebas. Dentro de la creación de material docente, el plan de pruebas consiste en crear las directivas para ejecutar pruebas de funcionamiento de la plataforma e interconexión entre dispositivos.

5. Integrar herramientas de prueba. Son las herramientas de software y hardware que permiten ejecutar las pruebas a un nivel de usuario final.

6. Interconectar usuarios. Corresponde a la utilización de las herramientas y verificación de su funcionamiento.

1.2. Estructura de la memoria

El capítulo 2: ***IMS en redes convergentes***, da a conocer los aspectos técnicos de la plataforma IMS, comenzando con una descripción de la red de telefonía móvil conocida actualmente y su evolución hasta la aparición del núcleo de red IMS. Se presenta también el protocolo de señalización SIP que es el eje principal de la arquitectura que conecta el mundo Internet con las telecomunicaciones móviles en el marco de la convergencia de servicios y medios de acceso. Luego se presentan las características principales de IMS, sus fundamentos y requerimientos para lograr la convergencia. El paradigma de provisión de servicios cambia totalmente desde el llamado modelo vertical hacia el horizontal que permite una mayor versatilidad en la creación de servicios acortando los tiempos de llegada al mercado haciéndolo más competitivo y abierto a terceros. La compañía telefónica se encarga de la mantención del núcleo de red y la provisión de servicios de valor agregado la ejecutan los llamados operadores de servicios.

El capítulo 3: ***Construcción de un laboratorio IMS***, muestra la planificación y desarrollo del curso de laboratorio junto con la integración de la plataforma de pruebas, que sustentan las experiencias del curso. Se abordan los temas presentados en el capítulo anterior de manera práctica utilizando herramientas *open source* de fácil uso. Se otorga un amplio enfoque al protocolo de señalización SIP y las extensiones que utiliza IMS, las cuales han sido estandarizadas por la organización 3GPP *Third Generation Partnership Project*. Se plantea también una metodología docente, basada en antecedentes previos [5], utilizada en la creación de cada una de las experiencias para darle el enfoque didáctico necesario.

El capítulo 4: ***Resultados***, contiene el análisis de los resultados de las pruebas planteadas en la construcción del curso. Se detallan los flujos de señalización SIP, Diameter, RTP y SDP que conforman la interacción entre los distintos nodos de la red de pruebas. Además se muestra como resultado una experiencia de laboratorio creada a partir de las pruebas realizadas.

Finalmente el capítulo 5: ***Conclusiones***, cierra el trabajo realizado mostrando las conclusiones más importantes del proyecto realizado. Se hace un análisis sobre el cumplimiento de los objetivos y resultados generales para terminar con una descripción de futuros trabajos posibles a partir de este.

Capítulo 2

IMS en redes convergentes

La tendencia del mercado de las telecomunicaciones de migrar hacia redes convergentes, en particular para ofrecer servicios Internet móvil de calidad, hace necesaria la creación de un sistema que permita hacer convivir los mundos de telefonía celular y de Internet. Este sistema es llamado IMS *IP Multimedia Subsystem*.

Para entender de mejor manera y justificar la aparición de IMS, se presenta en este capítulo la evolución de las redes de telefonía móvil. Luego de esta introducción se detallan las principales características de IMS, partiendo por su componente principal, el protocolo SIP.

2.1. Convergencia en redes de comunicaciones

El concepto de convergencia en telecomunicaciones responde a la necesidad de los usuarios de comunicarse independientemente del tipo de acceso que tengan disponible. Como ejemplo, un usuario utilizando su teléfono móvil puede entablar una comunicación de voz con otro que utiliza un cliente de mensajería en un computador personal con conexión a Internet. Sin embargo, el término de convergencia es más amplio que este concepto y se enfoca hacia la provisión de servicios de valor agregado. A continuación se definen las características que definen un servicio convergente.

2.1.1. Fundamentos

La tendencia de las tecnologías de comunicaciones es lograr que los usuarios logren una experiencia cada vez más cercana a la realidad. Esto significa que una persona tenga la capacidad de comunicarse a la distancia como si lo hiciera en forma presencial.

La primera generación de Internet no contaba con esta característica. A pesar de ser un medio rápido y confiable los datos no se transmitían en tiempo real. De dicha generación el servicio que ha sobrevivido a lo largo de los años es el correo electrónico. Aunque más tarde la mensajería instantánea hizo su aparición, no dejaba de ser solamente texto.

Hoy en día el escenario ha cambiado y es posible transmitir cualquier tipo de medio de manera instantánea. Sin embargo, resta todavía agregar movilidad a los servicios de tiempo real.

El concepto de convergencia se traduce básicamente en proveer servicios de telefonía fija o móvil con el modelo de negocios de Internet. El paradigma de los métodos de acceso se orienta cada vez más a la red celular, que es el medio inalámbrico que ha experimentado el mayor crecimiento en el mundo, en desmedro de otras técnologías como WiMax o el propio WiFi. Sin embargo, el tráfico de datos por esta red no es tan masivo, por el momento, como lo es el tráfico de voz. Los operadores ven un nicho de negocios

en la red de datos de alta velocidad —claro ejemplo de esto es la red de acceso de tercera generación 3G— porque pueden ofrecer servicios multimedia de la misma forma como se hace en Internet pero garantizando la calidad en la entrega y por cierto, cobrando por ella. Así, el movimiento hacia una arquitectura basada completamente en IP para ofrecer servicios es una fuerte tendencia.

2.1.2. Principios básicos

Una red de servicios convergentes para ser exitosa debe cumplir con ciertos principios. Se requiere que la administración de la red sea sencilla, puesto que el volumen de tráfico y aplicaciones tiene un crecimiento acelerado lo que influiría en el rendimiento de un sistema complejo de administrar.

El control de sesiones debe estar estrictamente separado del tráfico de datos. Por ejemplo, no se admite que el tráfico de voz circule por los mismos nodos de una red de señalización porque simplemente colapsa por capacidad.

Debe ser posible acceder a los servicios desde cualquier lugar utilizando cualquier equipo de comunicación. Esto permite la integración de servicios y estandarización en los puntos de acceso.

Se utilizan protocolos estándares y abiertos de Internet, que permiten la interoperabilidad de los elementos de la red fabricados por distintos proveedores.

Tiene la capacidad de asegurar la calidad en el servicio. Esto es un elemento importante porque es valor agregado que el operador puede ofrecer con un servicio Internet, que por sí solo no ofrece esta garantía.

Los sistemas convergentes cumplen con el paradigma del modelo horizontal en la provisión de servicios (figura 2.1). Para ser escalable en el tiempo, el operador se encarga del núcleo de red, otorgando una capa de abstracción a ella que permite la conexión con servicios principalmente desarrollados por terceros. Esto reduce el tiempo de llegada al mercado —conocido como *time to market*— de los servicios, además de hacerlos interoperables incluso si son desarrollados por proveedores distintos. El modelo vertical difiere de esto porque el operador se involucra en todos los niveles de producción de un servicio, teniendo que desarrollar plataformas independientes dentro del núcleo de red, otorgando una interoperabilidad casi nula entre servicios y con costos altísimos en desarrollo, tanto en tiempo como en dinero.

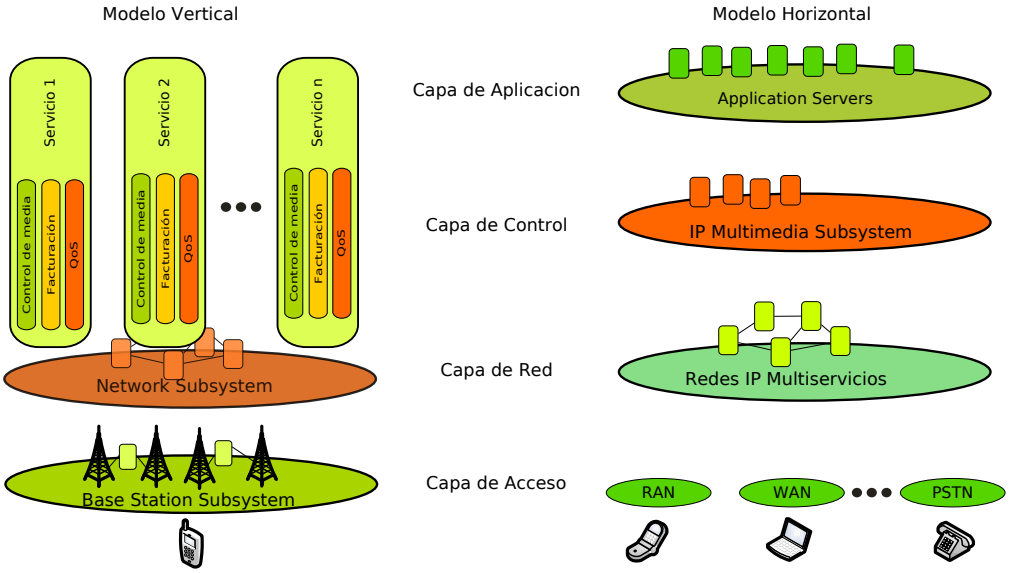

Figura 2.1: Paradigma de provisión de servicios. Modelo vertical y modelo horizontal.

2.1.3. Modelo de negocio

El negocio de una red convergente consiste en aprovechar el potencial de la red móvil para ofrecer servicios y dejar de ser meramente un acceso a Internet sin valor extra. El operador puede controlar y cobrar los contenidos ofrecidos. Asimismo el mercado se vuelve más dinámico porque permite la participación de terceros en la oferta de servicios. La creación de ellos es rápida y llegan al mercado en poco tiempo, estimulando la innovación. Decrece el costo de inversión en el desarrollo de nuevos servicios gracias a una plataforma uniforme ya existente (modelo horizontal).

Es posible por las caractéristicas topológicas de la red convergente combinar varios servicios en una misma sesión de usuario. El cliente puede interactuar por voz, video y mensajería de manera independiente o combinados sin detener la sesión o llamada. El operador conoce perfectamente el tipo de datos que trafica el cliente, por lo que puede cobrar por el servicio de manera apropiada utilizando distintos esquemas de cobros; no es lo mismo bajar 1*kByte* de un e-mail que 1*kByte* de video.

2.2. Evolución de las redes de telefonía móvil

En esta sección se define la arquitectura de red en telefonía móvil. Se entrega al lector una noción de los elementos que conforman la red móvil y además su aparición en cada versión del estándar (*Release*) de este sistema. Esto último se conoce como la evolución de la red móvil.

El fin de este apartado es mostrar el fundamento a nivel técnico de la aparición de IMS en el mundo de las telecomunicaciones. Se aclara que IMS también juega un rol fundamental con respecto a convergencia en telefonía fija (TISPAN [36]), pero sin embargo se ha optado por enfocar el estudio en la red celular, que es la que ha tenido una masificación considerable en los últimos años, comparada con el decrecimiento de la telefonía fija tradicional.

2.2.1. Subsistemas

En telefonía móvil existen los llamados subsistemas que cumplen distintas funcionalidades para proveer servicios a los usuarios. Las tareas principales de los subsistemas son: control de llamadas, tarificación, administración de movilidad, señalización, manejo de datos de suscriptores, control de rutas de radio, sincronización, codificación de señales, configuraciones y administración de fallas y rendimiento.

Los subsistemas por excelencia de las redes de telefonía móvil de segunda generación son *NSS (Network Switching Subsystem*), *BSS (Base Station Subsystem)* y *NMS (Network Management Subsystem)*. En tercera generación los subsistemas se conocen como: *Core Network (CN)* , *Radio Access Network (RAN)* y *NMS*.

En los apartados siguientes se presenta la definición de los elementos presentes en cada subsistema según su aparición histórica en la evolución de la red móvil.

2.2.2. 1G AMPS

Conocida como la red celular de primera generación. Se trata de una tecnología de transmisión análoga donde su exponente en América del Norte es AMPS *Advanced Mobile Phone System*. En Europa se utilizó TACS *Total Access Communications System*. Ambas tecnologías utilizan modulación de frecuencia (FM) y el sistema FMDA (*frequency division multiple access*) para multiplexar el tráfico.

2.2.3. 2G GSM

GSM *Global System for Mobile Communications* es un sistema abierto y no propietario en constante evolución. Una de sus características más importantes es la capacidad de roaming. A diferencia de la primera generación utiliza tecnología digital y métodos de acceso TDMA (*time division multiple access*). La voz es tratada por un codificador único que emula las características de la voz humana. Este método permite una tasa de transmisión muy eficiente.

Los elementos que forman el subsistema NSS de segunda generación se describen a continuación. La figura 2.2 muestra la arquitectura GSM.

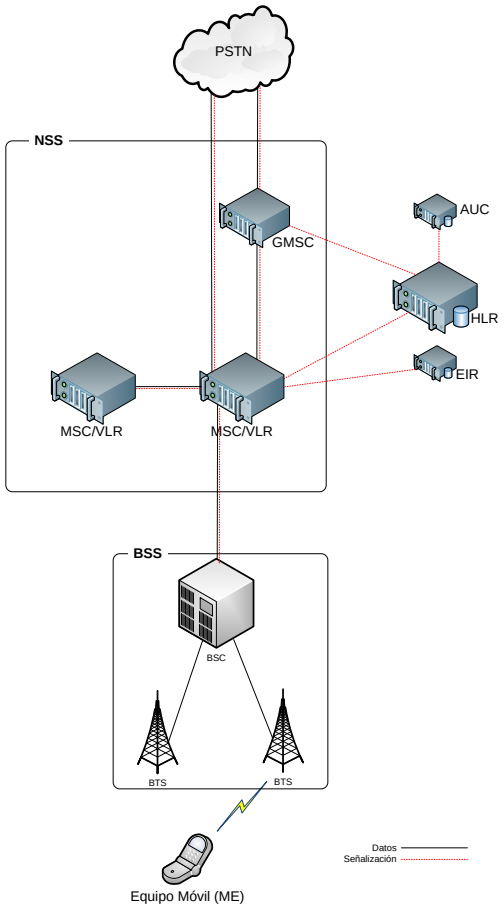

Figura 2.2: Arquitectura de la red celular de segunda generación 2G GSM.

MSC Es responsable de controlar las llamadas en la red móvil. Identifica el origen y destino de una llamada. Sus tareas más importantes son:

- Control de llamadas. El MSC identifica el tipo de llamada, el destino y el origen. Además establece, supervisa y cierra las conexiones.
- Inicia el *paging*. Es el proceso de localizar un teléfono móvil en el área de cobertura de la red en caso de recibir una llamada.
- Generación de CDR. Los CDR (*Charging Data Records*) contienen información de la utilización de la red por parte de los suscriptores. Se usa para realizar la facturación de las llamadas.

GMSC Realiza las mismas tareas que el MSC, excepto *paging*. Se utiliza para traducir la señalización proveniente de la red PSTN en los protocolos usados en la red celular.

VLR Es una base de datos que contiene información sobre los suscriptores que están bajo la cobertura de un determinado MSC. Típicamente esta integrada con el MSC en la misma máquina. La información que proporciona es: identificación de números de los suscriptores, información de seguridad para autentificación contra la tarjeta SIM[1] y servicios permitidos para el usuario.

HLR Mantiene un registro permanente de los suscriptores. Por ejemplo, almacena los números de identidad del suscriptor, y los servicios a los cuales esta suscrito. Adicionalmente a la información estática, almacena la ubicación actual de los suscriptores, útil entre otras cosas para que el GMSC encamine las llamadas.

AC Provee información de seguridad a la red, para poder verificar SIM *cards* (autentificar entre el télefono y el VLR, cifrar la información transmitida en la interfaz aérea).

EIR Es responsable de chequear el código IMEI de los aparatos móviles para verificar su válidez dentro de la red del operador. Se definen tres tipos de listas de permisos. La lista blanca permite al usuario operar normalmente. La lista gris contiene los equipos con sospecha de mala utilización. La lista negra tiene a los equipos que no pueden operar en la red porque, por ejemplo, son declarados como robados.

El subsistema de acceso por radio es la segunda componente de las redes de segunda generación. La descripción de sus elementos es la que sigue.

BSC Este elemento controla la red de radio. Algunas de sus principales características son:

- Establece la conexión entre el terminal y la NSS. Todas las llamadas hacia y desde los terminales son conectadas a través de la funcionalidad de conmutación del BSC.
- Administración de movilidad. Es responsable de iniciar los handovers[2], de acuerdo a las mediciones de señal enviadas por el terminal durante la llamada.
- Colecta datos para propósitos estadísticos. La información de los BTS, TRAU y BSC es colectada y dirigida hacia el subsistema de administración NMS para obtener una visión estadística de los parámetros de calidad del BSS.
- Control de BTS y TRAU. Todos los TC y BTS se conectan a los BSC que recolecta información de estado para fines de mantenimiento.

BTS Es el elemento responsable de mantener la interfaz de comunicación aérea y minimizar los problemas de transmisión. Maneja la señalización para establecer llamadas, actualizar la información de un cliente (terminal) cuando se conecta a la red, y realizar handovers, entre otras tareas. Como el aire es un medio inseguro de transmisión los BTS codifican y decodifican los datos transmitidos hacia y desde los terminales. Realiza procesamientos de voz que permiten garantizar las conexiones libres de errores entre el terminal y el BTS. Además utiliza métodos de modulación de señales para ser transmitidas y recibidas por los transceptores (TRX's).

TRAU Se encarga de convertir los formatos de compresión de voz para adaptarse a los requerimientos de otras redes, por ejemplo la PSTN. Típicamente la señal celular es comprimida en $12kbps$, mientras que en la PSTN las señales son de $64kbps$.

[1] SIM: Subscriber Identity Module. Contiene la información del suscriptor, por ejemplo el número telefónico, y es almacenada en un chip electrónico.

[2] Cuando un suscriptor cambia de celda que le proporciona cobertura.

2.2.4. 2.5G GPRS

Con el fin de proveer de servicios basados en datos IP se creó la arquitectura GPRS (General Packet Radio Service). Con ella es posible que los terminales trafiquen datos provenientes de Internet mediante acceso WAP (Wireless Application Protocol). La figura 2.3 muestra la arquitectura 2.5G, que es básicamente una mejora a 2G agregando el Core GPRS.

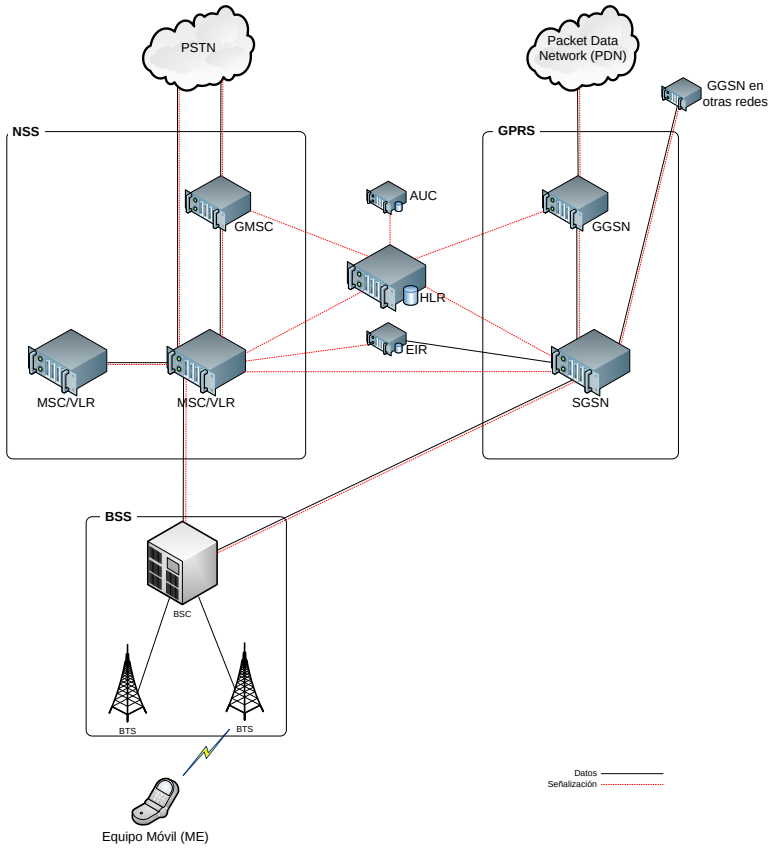

Figura 2.3: Subsistema GPRS en la arquitectura de la red celular de segunda generación 2G GSM.

SGSN Es el elemento más importante de la red GPRS. Es equivalente al MSC en la red GSM. Algunas de sus funciones son:

- Conversión de protocolos (por ejemplo de IP a FR).
- Cifrado de datos entre el terminal y SGSN.
- Compresión de datos para minimizar el ancho de banda utilizado.
- Autentificación de usuarios.
- Manejo de movilidad en caso de que el suscriptor cambia de área de cobertura.
- Interacción con el NSS utilizando señalización SS7 para obtener información del suscriptor.
- Recolección de información de facturación.

GGSN Es la puerta de enlace hacia otras redes. Sus tareas son:

- Ruteo de paquetes provenientes de redes externas hacia el SGSN correspondiente al terminal destino.

- Ruteo de paquetes hacia redes externas.
- Recolección de datos de facturación y de estadísticas.
- Asigna direcciones IP a los terminales móviles.
- Se involucra en el establecimiento de túneles con el SGSN y con otras redes externas y VPN.

Los elementos que conforman el BSS de segunda generación pasan a llamarse GERAN *GSM/EDGE Radio Access Network*.

2.2.5. 3G UMTS R3

Corresponde a una nueva actualización, pero esta vez en la interfaz de radio. El objetivo es aumentar las velocidades de transmisión de paquetes de datos. Los elementos principales de las estaciones base reciben el nombre de Nodos B y RNC (*Radio Network Controller*). En la figura 2.4 aparece esta nueva mejora en el sistema celular conocida como UTRAN (*UMTS Terrestrial Radio Access Network*).

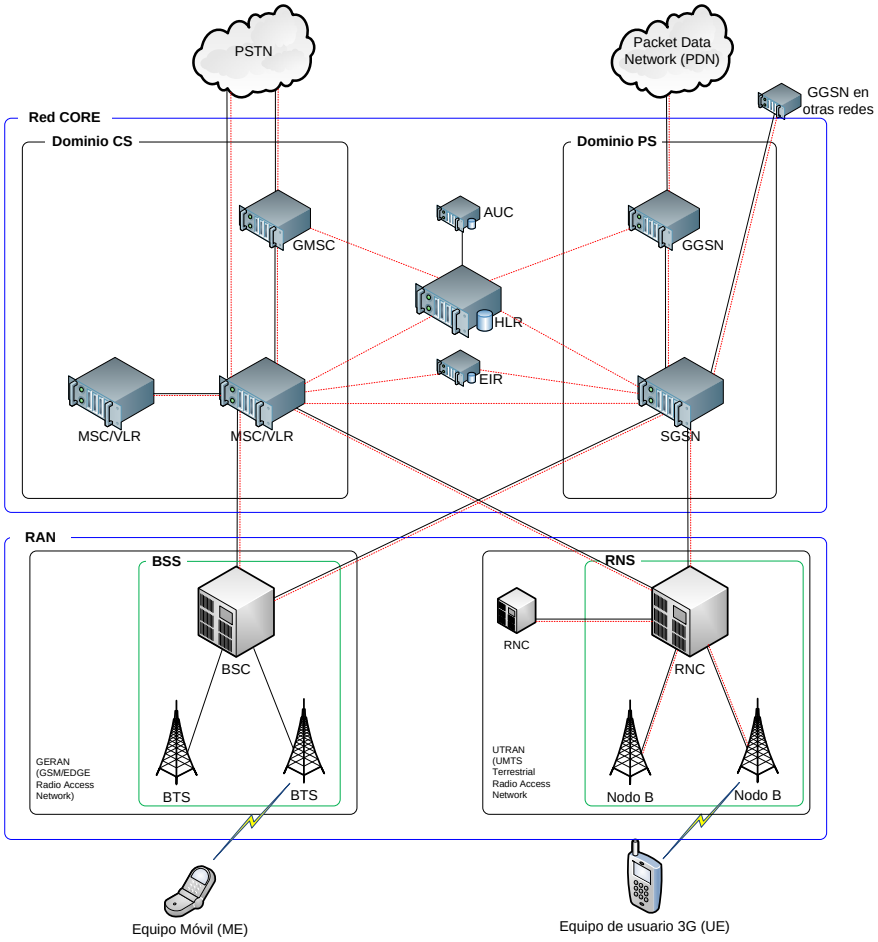

Figura 2.4: Arquitectura de la red celular de tercera generación 3G UMTS (3GPP Release 3).

A contar de esta versión los nodos del NSS junto con los de GPRS conforman el llamado *Core Network* (núcleo de red). El NSS es conocido como *Circuit Switched Domain*, y GPRS como *Packet Switched Domain*. GERAN y UTRAN se conocen en conjunto como *Radio Access Network* (RAN).

RNC Es la entidad de administración en UTRAN. Responsable de la configuración de recursos de radio (canales de tráfico) y handovers, entre otras tareas:

- Administración de ubicación y conexión.
- Cifrado.
- Asignación de canales de tráfico entre el RNC y las estaciones base.
- Conmutación y multiplexión ATM.
- GPT (Protocolo de túnel GPRS) hacia la red core de paquetes.
- Funciones de seguridad.

Nodo B Tiene prácticamente las mismas tareas que un BTS GSM. Establece la conexión física de la interfaz de radio entre el terminal de usuario y la red 3G.

- Controla el *uplink* y *downlink*. Conversión banda-base a RF.
- Mapeo de canales lógico-físico.
- Codificación/decodificación.
- Multiplexión y conmutación ATM hacia el RNC.

2.2.6. 3G UMTS R4

Es una actualización en el llamado *Core* de la red (conformado por el dominio de circuitos conmutados y por el dominio de paquetes conmutados). La finalidad es optimizar los nodos de conmutación de circuitos separando las funciones de señalización y tráfico. La figura 2.5 muestra los componentes de la arquitectura.

MSC Server Realiza básicamente las mismas tareas de señalización que un nodo MSC de segunda generación. Incorpora protocolos IP que se traducen en mayor capacidad y mejor manejo en el control de llamadas.

GMSC Server Cumple las funciones de señalización del nodo GMSC, con las mismas finalidades que el MSC Server.

CS-MGW Se especializa en la función de conmutación de tráfico de voz que antes hacía el MSC y el GMSC.

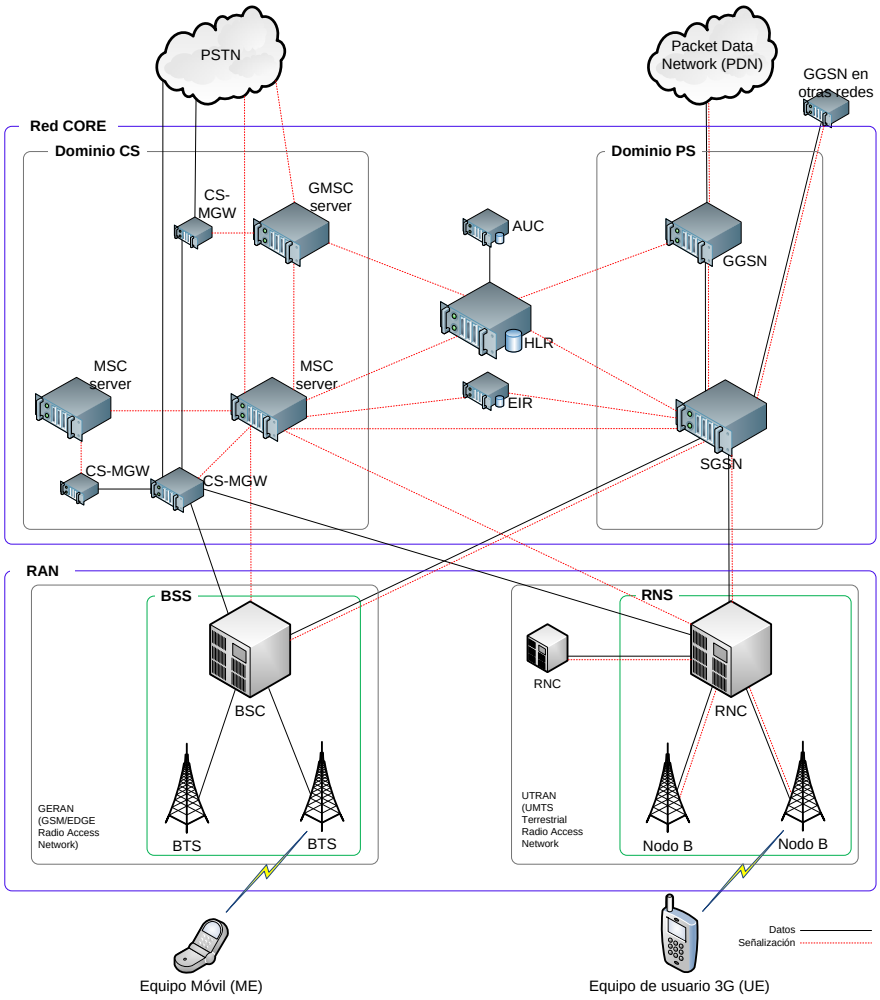

Figura 2.5: Arquitectura de la red celular de tercera generación 3G UMTS (3GPP Release 4).

2.2.7. 3G UMTS R5

Finalmente aparece el subsistema conocido como IMS. Su función es proporcionar los mismos servicios multimedia presentes en Internet pero con la característica de movilidad que ofrece la red celular. El detalle de esta arquitectura aparece más adelante. La ubicación de esta arquitectura en las redes de tercera generación se muestra en la figura 2.6.

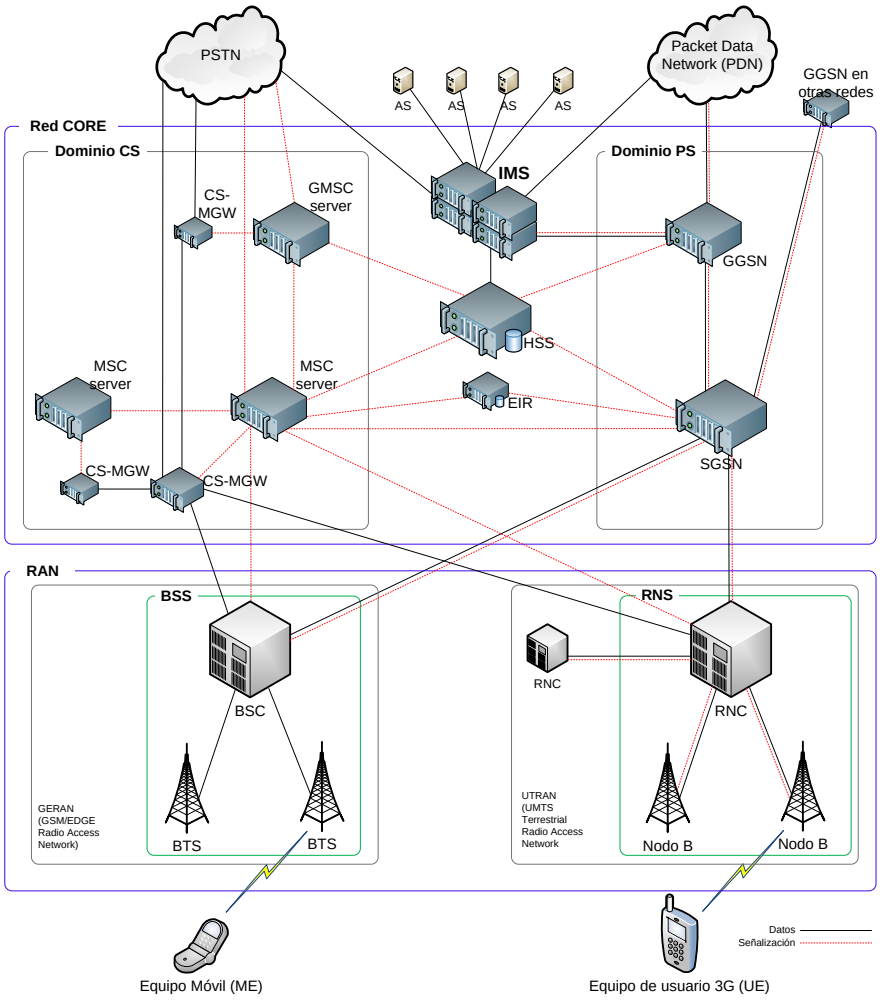

Figura 2.6: Subsistema IMS en la arquitectura de la red celular de tercera generación 3G UMTS (3GPP Release 5).

2.3. El protocolo SIP

SIP *Session Initiation Protocol* [7] es un protocolo de control de la capa de aplicación en TCP/IP (figura 2.7) basado en texto, similar a HTTP (web) y SMTP (mail), para iniciar sesiones de comunicación interactiva entre usuarios. Dichas sesiones incluyen voz, video, chat, juegos, y realidad virtual.

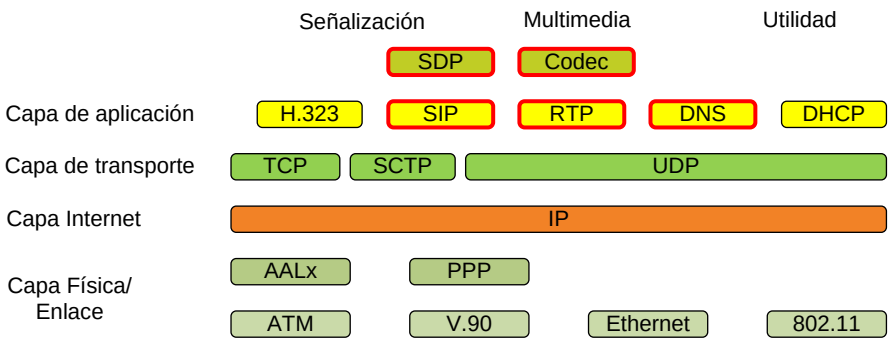

Figura 2.7: Modelo de capas TCP/IP. Ubicación de SIP y otros protocolos de aplicación complementarios.

Diversos protocolos están diseñados para transportar varias formas de sesiones multimedia en tiempo real. SIP trabaja en conjunto con dichos protocolos para conectar a los terminales (*end-points*) y caracterizarlos con una determinada sesión.

SIP es una herramienta ágil de propósito general para crear, modificar y terminar sesiones trabajando independientemente de los protocolos de transporte de la capas inferiores y del tipo de datos de la sesión establecida.

2.3.1. Características

Las descripción básica del modelo y arquitectura SIP corresponde a:

- Los servicios y características son provistos punto a punto siempre cuando sea posible.
- Los complementos y nuevas características a los estándares deben ser aplicables en general, y no sólo a un set específico de tipos de sesiones.
- La simplicidad es clave.
- La reutilización de arquitecturas y protocolos Internet existentes y su uso con otras aplicaciones de Internet es crucial.

2.3.1.1. Funcionalidad de SIP

SIP soporta cinco facetas para establecer y terminar comunicaciones:

User Location: Se determina el sistema final a ser usado para la comunicación.

User availability: Determinación de la disponibilidad del destinatario para entablar la comunicación.

User capabilities: Determinación del tipo de medios y sus parámetros a ser usados.

Session setup: *Ringing*, etapa de establecimiento de los parámetros de sesión entre las dos partes.

Session management: Incluye transmisión y terminación de sesiones, modificación de los parámetros de sesión e invocación de servicios.

2.3.1.2. Estructura del protocolo

SIP está estructurado como un protocolo de capas. La capa más baja es de **sintáxis y codificación**. Esta última está especificada usando BNF (*Backus-Naur Form*) [8].

La segunda capa es de **transporte**. Define la manera en que un cliente o servidor envía peticiones y recibe respuestas sobre la red. Todos los elementos de SIP contienen una capa de transporte.

La tercera capa es de **transacción**. Una transacción es una petición enviada por un cliente usando la capa de transporte a un servidor de transacciones. Esta capa maneja las retransmisiones de la capa de aplicación, la combinación de respuestas y peticiones, y los *timeouts* de la capa de aplicación.

La siguiente capa es **transacción de usuario**. Cada una de las entidades SIP es un usuario de transacción (*Transaction User* TU), excepto los llamados *stateless proxies*. Cuando un usuario desea enviar una petición, crea una instancia de transacción y pasa la petición con la dirección IP de destino, puerto y transporte.

SIP funciona mediante peticiones y respuestas entre dos *Agentes de Usuario* o *User Agents* (UA). Una petición es enviada con un formato definido en el estándar RFC3261 [7]. Cada petición, también conocida como *método* tiene una respuesta asociada llamada *estado* (*Status Response*). Los métodos del estándar SIP son `REGISTER`, `INVITE`, `ACK`, `BYE`, `CANCEL` y `OPTIONS`.

2.3.2. Sesión SIP

Una sesión es una colección de participantes, y un flujo de medios (por ej. voz, mensajería, video) entre ellos, entablando una comunicación. Una sesión SIP corresponde al flujo de mensajes necesarios para establecer una comunicación entre dos terminales UA (*User Agents*) los cuales transfieren datos multimedia entre sí. Típicamente una sesión se establece con el método INVITE y se termina con el método BYE. La figura 2.8 muestra una sesión SIP típica.

Para establecer y terminar una sesión se utilizan los llamados **diálogos** que son un conjunto de mensajes desde que se envía una petición hasta que se recibe la respuesta. Por ejemplo en el flujo de la figura 2.8 los mensajes (1) `INVITE` al (12) `ACK` corresponden al primer diálogo que precisamente es el que inicia la sesión de medios. El segundo diálogo es conformado por los mensajes (13) `BYE` y (14) `200 OK`. En general, se efectúan varios diálogos dentro de una sesión. No obstante lo anterior pueden generarse diálogos fuera de ella, por ejemplo para tareas adicionales de los servidores SIP.

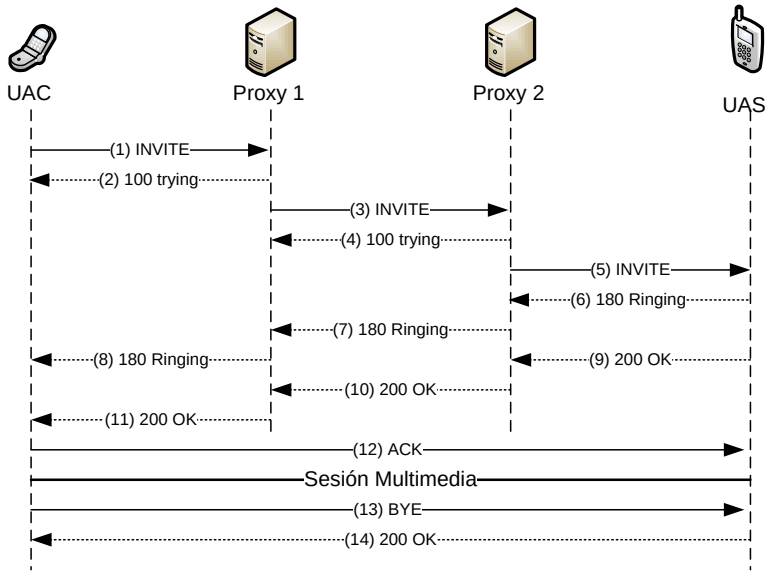

Figura 2.8: Sesión SIP

2.3.2.1. Componentes de un mensaje SIP.

Se muestra un mensaje SIP `INVITE` con el fin de detallar cada uno de los encabezados tradicionales presentes en el protocolo.

```
INVITE sip:javier@playsip.org SIP/2.0
Via: SIP/2.0/UDP pc33.uchile.cl;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Javier <sip:javier@playsip.org>
From: diego <sip:diego@uchile.cl>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.uchile.cl
CSeq: 314159 INVITE
Contact: <sip:diego@pc3-die.uchile.cl>
```

```
Content-Type: application/sdp
Content-Length: 142
```

REQUEST LINE: MÉTODO, Request-URI, SIP version.

- `MÉTODO`: Corresponde al tipo de mensaje que se está enviando. Por ejemplo INVITE, OPTIONS, BYE, etc.
- `Request-URI`: Indica el cliente destino.

Via: Contiene la dirección a la cual debe ser devuelta la respuesta a la petición. También contiene un parámetro `branch` que identifica la transacción.

To: Contiene un nombre y un URI SIP al cual está dirigido el mensaje.

From: Contiene un nombre y un URI SIP que indica el origen del mensaje. Tiene también un parámetro `tag` agregado para propósitos de identificación en el cliente destino, por ejemplo en un *softphone*.

Call-ID: Identificador global formado por un número aleatorio y por el nombre del host o su dirección IP. La combinación de `To`, `From` y `Call-ID` definen completamente una relación peer-to-peer, es decir un diálogo.

Cseq: Contiene un número entero y el nombre del método. El número se incrementa por cada nueva petición dentro de un diálogo.

Contact: Contiene un URI compuesto por un nombre FQDN[3]. También se permite el uso de direcciones IP. Sirve para indicar donde enviar peticiones futuras al cliente (a diferencia de `Via` que indica donde enviar la respuesta solamente a la petición en curso).

2.3.2.2. SDP *Session Description Protocol*

Definido en el estándar RFC 4566 [9] para realizar el proceso de negociación básico para *streams* de medios. Incluye la tasa de transferencia y el codec a ser utilizado, además de otros atributos de medios. Un cuerpo SDP normalmente contiene las opciones descritas en los cuadros siguientes.

- Descripción de la sesión:

```
v=  (Versión del protocolo)
o=  (Identificador de sesión y originador)
s=  (nombre de sesión)
i=* (información de sesión)
u=* (URI de descripción)
e=* (dirección email)
p=* (número telefónico)
c=* (información de conexión)
b=* (lineas de información de ancho de banda)
z=* (ajustes de zona horaria)
k=* (llave de encriptación)
a=* (lineas de atributos de sesión)
```

- Descripción de tiempo:

```
t=  (tiempo en que la sesión está activa)
r=* (cero o más tiempos de repetición)
```

[3]FQDN: Fully Qualified Domain Name

- Descripción de medios, si están presentes:

```
m=  (nombre del medio y dirección de transporte)
i=* (título del medio)
c=* (información de conexión -- opcional si se incluye a nivel de sesión)
b=* (líneas de información de ancho de banda)
k=* (llave de encriptación)
a=* (líneas de atributos de medios)
```

2.3.3. Servidores SIP

Son intermediarios de los UAs para enviar y recibir peticiones y respuestas. Los servidores proxy SIP tienen la capacidad de encontrar los *hops* (nodos de red adyacentes) mediante el acceso a una base de datos o un servicio de ubicación (*location service*) con el fin de localizar al cliente destino de una llamada. La interfaz que comunica los proxies con los *location service* no está definida por el protocolo SIP. Para ubicar servidores en otros dominios se utiliza el mecanismo DNS SRV [28].

Un proxy no realiza peticiones, excepto con el método `CANCEL`. Sólo responde a las peticiones de los UAs. No tiene habilidad para procesar medios. No revisa el cuerpo del mensaje, por ejemplo SDP, sólo se preocupa de los encabezados (*header fields*).

En general los mensajes son transportados directamente entre los *end-points* (clientes) sin pasar por los proxies, lo que se conoce como el trapezoide SIP (figura 2.9). Los servidores únicamente hacen el contacto entre dos clientes y luego se desentienden de la sesión. Este comportamiento no es útil cuando un operador (el que presta servicios de telefonía IP) necesita conocer los contenidos traficados por los clientes para realizar cobro de servicios, por lo que se puede forzar el mecanismo para que los mensajes atraviesen los nodos deseados y así mantener controlada la sesión.

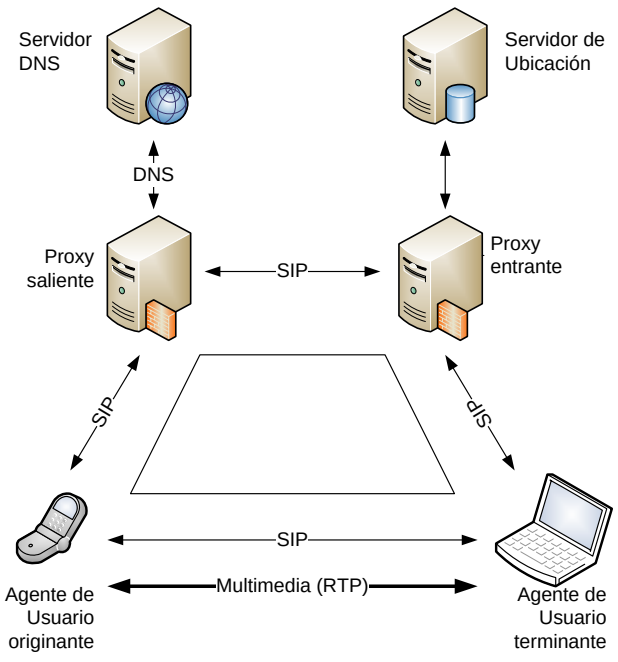

Figura 2.9: Trapezoide SIP

También existen servidores SIP con funciones específicas que se diferencian de los servidores proxies comunes. Por ejemplo un servidor de redirección (*Redirect Server*) responde peticiones pero no las encamina. Dichos servidores (figura 2.10) utilizan *location service* para encontrar la ubicación de los UAs. La información es devuelta al cliente mediante respuestas `3xx`.

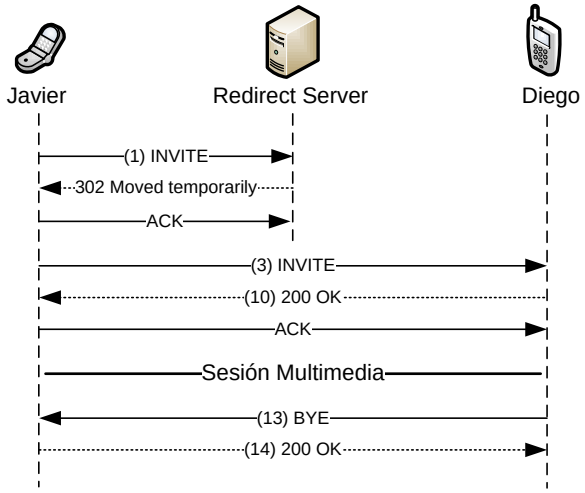

Figura 2.10: Redirect Server

Los servidores de registro (*Registrar Server*) están especializados en aceptar las peticiones `REGISTER`. El resto de las peticiones las responde con `501 (Not Implemented)`. Posteriormente al registro del cliente la información de contacto (provista en el encabezado `Contact`) está disponible para todos los servidores del dominio donde el cliente se registra (*registrar, proxies, redirect servers*). Usualmente en dominios de seguridad se requiere que los UAs se autentifiquen contra el servidor *Registrar*.

2.3.4. Ruteo de mensajes SIP

A continuación se describe el detalle del ruteo de mensajes SIP entre clientes y servidores. En particular, se muestran algunas definiciones y encabezados presentes en los mensajes que determinan su camino dentro de una red SIP.

2.3.4.1. URI

Identifica un recurso (cliente, servidor) perteneciente a una red de tal forma de poder comunicarse con él. Contiene la información necesaria para iniciar y mantener una sesión de comunicación con el recurso.

Ejemplos de estos recursos son los siguientes:

- Un usuario de un servicio online.
- Una casilla de correo en un sistema de mensaje.
- Un número PSTN en un servicio de gateway.
- Un grupo en una organización.

Los esquemas `sip:` o `sips:`[4] siguen las directivas del RFC 2369 [13]. Es similar a los URI `mailto` donde se especifican los encabezados y el cuerpo del mensaje.

La forma general de un URI SIP es la siguiente:

```
sip:user:password@host:port;uri-parameters?headers
```

[4]SIPS: SIP sobre un protocolo de seguridad (típicamente TLS).

user: Identifica al recurso presente en un host.

Password: Contraseña asociada con el usuario. Su uso no es recomendado porque el transporte de mensajes es texto plano resultando ser muy inseguro.

Host: El host que provee el recurso SIP. Puede ser un nombre o una dirección IPV4 o IPV6.

Port: El puerto donde las peticiones son enviadas.

uri-parameters: Opciones que pueda requerir una petición. Van separados por ";" y tienen la forma:

```
nombre opción \=" valor opción
```

Los parámetros disponibles son: `transport`, `maddr`, `ttl`, `user`, `method`, `lr`.

Ejemplos de SIP URIs:

```
sip:javier@playsip.org
sip:javier:password@playsip.org;transport=tcp
sips:javier@playsip.org?subject=project\%20x\&priority=urgent
sip:+1-212-555-1212:1234@gateway.com;user=phone
sips:1212@gateway.com
sip:javier@192.0.2.4
sip:playsip.org;method=REGISTER?to=javier\%40playsip.org
sip:javier;day=tuesday@playsip.org
```

2.3.4.2. Via, Route y Record-Route

Cuando un mensaje es enviado desde un UA a otro, cada proxy y UA dentro del camino del mensaje agrega su campo `Via`. El propósito del este campo es asegurar que las respuestas a un mensaje siguen el mismo camino, es decir atraviesan el mismo set de proxies pero en forma inversa. En otras palabras, este campo es utilizado para enrutar las respuestas. Los campos `Route` y `Record-Route` tienen un propósito distinto: se usan para rutear peticiones futuras.

El campo `Contact` es utilizado para dar a conocer al UA la dirección en la cual puede ser ubicado. Un *user agent* A agrega el campo `Contact` con su IP en el método INVITE para que el UA B pueda comunicarse directamente con A en el futuro. De la misma forma el *user agent* B agrega el campo `Contact` con su IP en la respuesta `200 OK`. Así la comunicación entre los *user agents* puede prescindir de los proxies intermedios.

Cuando es necesario evitar la comunicación directa entre UAs, por ejemplo para realizar tarificación, los proxies utilizan el campo `Record-Route` para que los mensajes pasen por ellos.

El proxy agrega el campo `Record-Route` al `INVITE` enviado por el *user agent* A con su IP asegurando que el UA B envíe futuras peticiones al UA A a través del proxy.

Por otra parte, en una petición futura el cliente agrega el campo `Route` construído con la información presente en `Record-Route` de los mensajes anteriores indicando a los UA y a los proxies la dirección donde debe ser enviada la petición que contiene dicho campo `Route`. Con esto el proceso de búsqueda de servidores y clientes (mediante DNS y Location Service) se realiza una sola vez por sesión.

Cuando un UA envía una petición dentro de un diálogo, siempre pondrá el URI presente en `Contact` del cliente destino en el Request-URI y copiará todas las URI's extraídas desde `Record-Route` en el campo `Route`.

Resumiendo lo anterior se concluye lo siguiente:

- `Via` es usado para enrutar respuestas en un diálogo.
- `Route` y `Record-Route` son usados para enrutar peticiones futuras.
- Los proxies usan `Record-Route` para señalizar que quieren permanecer dentro del camino de futuras peticiones.
- Los UAs usan `Record-Route` de peticiones anteriores para construir encabezados `Route` en peticiones posteriores.
- La dirección presente en `Contact` es puesta en el Request-URI de los mensajes futuros.
- La primera URI en el campo `Route` tiene prioridad sobre el Request-URI, por lo tanto el Request-URI sólo es usado cuando no hay encabezado `Route`.

2.3.5. Mensajes SIP y sus respuestas.

Los mensajes SIP originales son INVITE, REGISTER, BYE, ACK, CANCEL y OPTIONS, todos definidos en el estándar RFC 3261. A continuación se muestra una descripción de estos 6 mensajes.

REGISTER Este método es usado por un *user agent* para notificar a la red SIP (a través de un servidor Registrar) de su actual `Contact` URI (dirección IP) y del URI para las peticiones enrutadas a este `Contact`. Es necesario para que el proxy del dominio pueda hacer llegar peticiones al UA.

INVITE Es usado para establecer sesiones multimedia entre *user agents*. El acuso de recibo de INVITE es enviado con el método ACK. Si no contiene la información de la sesión multimedia (SDP), la contendrá el método ACK. Si la información no es aceptada se debe cancelar con un BYE (no con un CANCEL, puesto que la sesión está iniciada). El método se puede utilizar múltiples veces (re-INVITE) para cambiar las características de la sesión o actualizar el estado del diálogo.

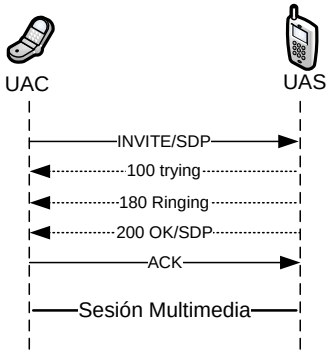

Figura 2.11: Mensaje SIP INVITE

```
INVITE sip:diego@chile.lab SIP/2.0
Record-Route: <sip:172.16.231.213:9060;lr=on;ftag=9555100d>
Via: SIP/2.0/UDP 172.16.231.213:9060;branch=z9hG4bK699a.5a87ddc5.0
Via: SIP/2.0/UDP 172.20.85.100:32382;branch=z9hG4bK-d87543
Max-Forwards: 69
Contact: <sip:javier@172.20.85.100:32382>
To: "diego@chile.lab"<sip:diego@chile.lab>
From: "javier"<sip:javier@china.lab>;tag=9555100d
Call-ID: OWQ5YzI1ZTg1MDk5MDZiYTQwMDA4YjFkNmRjMGVjNzY.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
```

```
Content-Type: application/sdp
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 372

v=0
o=- 5 2 IN IP4 172.20.85.100
s=CounterPath X-Lite 3.0
c=IN IP4 172.20.85.100
t=0 0
m=audio 26724 RTP/AVP 107 119 100 106 0 105 98 8 101
a=fmtp:101 0-15
a=rtpmap:100 SPEEX/16000
a=rtpmap:101 telephone-event/8000
a=sendrecv
```

BYE Es usado para terminar una sesión multimedia establecida. Es similar al mensaje *release* usado en telefonía convencional. Las sesiones se consideran establecidas si INVITE recibe una respuesta exitosa (2xx) o si un ACK ha sido enviado. BYE es enviado sólo por los *user agents* que participan en la sesión, nunca por proxies o terceras partes. Es un método end-to-end, por lo que las respuestas sólo son generadas por el otro *user agent*.

```
BYE sip:diego@172.16.231.184:34336;rinstance=3aa4598645df2824 SIP/2.0
Via: SIP/2.0/UDP 172.20.85.100:32382;branch=z9hG4bK-d87543-6562fe0c3e44d743-1--d87543-
Max-Forwards: 70
Route: <sip:172.16.231.213:9060;lr;ftag=9555100d>
Route: <sip:172.16.231.213:8060;lr=on;ftag=9555100d>
Contact: <sip:javier@172.20.85.100:32382>
To: "diego@chile.lab"<sip:diego@chile.lab>;tag=75158706
From: "javier"<sip:javier@china.lab>;tag=9555100d
Call-ID: OWQ5YzI1ZTg1MDk5MDZiYTQwMDA4YjFkNmRjMGVjNzY.
CSeq: 2 BYE
User-Agent: X-Lite release 1011s stamp 41150
Reason: SIP;description="User Hung Up"
Content-Length: 0
```

ACK Es usado para hacer acusos de recibo final de peticiones INVITE. Para otras peticiones no se realizan acusos de recibo final. Las respuestas finales están definidas como clases de respuesta 2xx, 3xx, 4xx, 5xx o 6xx. Participan los end-to-end en el caso de 2xx. Si ocurren otras respuestas, pueden participar los proxies intermedios.

```
ACK sip:diego@172.16.231.184:34336;rinstance=3aa4598645df2824 SIP/2.0
Via: SIP/2.0/UDP 172.20.85.100:32382;branch=z9hG4bK-d87543-4a4b6b72431ec407-1--d87543-
Max-Forwards: 70
Route: <sip:172.16.231.213:9060;lr;ftag=9555100d>
Route: <sip:172.16.231.213:8060;lr=on;ftag=9555100d>
Contact: <sip:javier@172.20.85.100:32382>
To: "diego@chile.lab"<sip:diego@chile.lab>;tag=75158706
From: "javier"<sip:javier@china.lab>;tag=9555100d
Call-ID: OWQ5YzI1ZTg1MDk5MDZiYTQwMDA4YjFkNmRjMGVjNzY.
CSeq: 1 ACK
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 0
```

CANCEL Este método es usado para terminar búsquedas pendientes o intentos de llamada. Puede ser generado por *user agents* o servidores proxy (es la única petición que puede efectuar un servidor proxy).

```
CANCEL sip:javier@playsip.lab SIP/2.0
Via: SIP/2.0/UDP 172.16.231.213:4060;branch=z9hG4bKea71.cd9f0b72.0
```

```
From: "Diego" <sip:diego@playsip.lab>;tag=152834176
Call-ID: 354270617
To: <sip:javier@playsip.lab>
CSeq: 20 CANCEL
Route: <sip:orig@scscf.playsip.lab:6060;lr>
User-Agent: Sip EXpress router(2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0
```

OPTIONS Es usado para consultar las capacidades de un *user agent* o un servidor y si está actualmente disponible. Es respondido como si fuera un INVITE (es decir, si no acepta llamadas responde con un 4xx o un 6xx).

```
OPTIONS sip:user@carrier.com SIP/2.0
Via: SIP/2.0/UDP cavendish.kings.cambridge.edu.uk
 ;branch=z9hG4bK1834
Max-Forwards:70
To: <sip:user@proxy.carrier.com>
From: J.C. Maxwell <sip:james.maxwell@kings.cambridge.edu.uk>
 ;tag=34
Call-ID: 9352812@cavendish.kings.cambridge.edu.uk
CSeq: 1 OPTIONS
Content-Length: 0
SIP/2.0 200 OK
Via: SIP/2.0/UDP cavendish.kings.cambridge.edu.uk;tag=512A6
 ;branch=z9hG4bK0834 ;received=192.0.0.2
To: <sip:user@proxy.carrier.com>;tag=432
From: J.C. Maxwell <sip:james.maxwell@kings.cambridge.edu.uk>
 ;tag=34
Call-ID: 9352812@cavendish.kings.cambridge.edu.uk
CSeq: 1 OPTIONS
Allow: INVITE, OPTIONS, ACK, BYE, CANCEL, REFER
Accept-Language: en, de, fr
Content-Length: ...
Content-Type: application/sdp
v=0
etc...
```

2.3.5.1. Respuestas

Existe una variedad de respuestas, cada una para un determinado propósito de acuerdo a la petición entrante. Se resumen en el siguiente cuadro.

Clase	Descripción	Acción
1xx	Informativa	Indica el estado de un llamado previo a completarse.
2xx	Exitosa	Petición es exitosa. Para un INVITE, ACK debe ser respondido, de otra forma se detienen las retransmisiones de petición.
3xx	Redirección	El servidor retorna posibles ubicaciones. El cliente debe reintentar en otro servidor.
4xx	Error de Cliente	La petición falla debido a un error del cliente. Se debe reintentar la petición reformulada.
5xx	Falla de Servidor	La petición ha fallado debido a un error en el servidor. La petición se debe efectuar hacia otro servidor.
6xx	Falla global	La petición falla. No se debiera hacer otra petición ni en el servidor actual ni en otros.

2.4. IMS

La organización 3GPP define este subsistema en el marco de la evolución de la red de telefonía móvil de tercera generación para lograr una convergencia entre el mundo Internet y telefónico en los medios de acceso y la provisión de servicios de valor agregado de calidad. En esta sección de describen los fundamentos y algunos aspectos técnicos de la arquitectura.

2.4.1. Beneficios/Ventajas

Las razones que fundamentan la necesidad de una arquitectura como IMS dentro de las redes de telecomunicaciones se describen a continuación:

Plataforma común para desarrollar servicios multimedia a bajo costo y en plazos cortos. El problema de los proveedores es que para poner en el mercado un nuevo servicio multimedia incurre en un proceso largo de desarrollo que implica grandes costos. IMS soluciona este problema proporcionando una plataforma estandarizada y componentes reutilizables. Esto permite que el proveedor de servicios pueda adoptar fácilmente los servicios creados por él e incluso por terceros. Adicionalmente, se abre la posibilidad de que varios proveedores que implementen esta plataforma puedan ofrecer sus servicios. Esta estrategia de múltiples proveedores tiene como ventaja el desarrollo de una gran cantidad de servicios multimedia cada vez de mejor calidad.

Calidad de servicio presente en los servicios multimedia. A pesar de que las redes 3G ofrecen un mayor ancho de banda, no existen garantías acerca de la calidad del servicio. Estas redes proveen lo que es conocido como "mejor esfuerzo", lo que significa que la red se esforzará lo mejor posible para asegurar un ancho de banda requerido, pero no se garantiza que se mantendrá en un nivel constante. Para solucionar este problema IMS provee mecanismos que garantizan QoS (calidad de servicio) dentro de la red IP y toma ventajas de ellos para garantizar la calidad de transmisión.

Los operadores pueden realizar cobros por sesiones multimedia apropiadamente. IMS otorga al operador la posibilidad de realizar cobros bajo diferentes esquemas. Por ejemplo, en una llamada de video-conferencia sobre una red 3G, el operador puede realizar el cobro de la llamada de acuerdo a la cantidad de bytes transmitidos, como también lo puede hacer tomando en cuenta el tiempo de duración de la llamada, o utilizando otro esquema de cobros. En general, el operador elegirá el esquema de cobro a realizar de acuerdo al tipo de servicio utilizado (voz, video y voz, mensajería, conferencia, etc).

Los servicios están disponibles independientemente de la ubicación de los usuarios. IMS utiliza tecnologías Internet y sus protocolos permitiendo a los usuarios moverse entre otras ubicaciones fuera de la cobertura de su operador, y aún ser capaces de ejecutar todos sus servicios como si estuvieran dentro las redes de su propio operador.

2.4.2. Características y requerimientos de la arquitectura

La organización 3GPP define en sus estándares [30] las funciones necesarias que debe proporcionar IMS para ser un sistema completo y útil en el mercado de la telefonía móvil.

Conectividad IP. Para acceder a los servicios provistos por IMS el cliente debe tener conectividad IP. Se requiere soporte para IPv6. Dicha conectividad puede ser obtenida desde la red *home* o *visited*[5].

[5]Se conoce como red home (*home network*) a aquella donde pertenece el cliente manteniendo una subscripción o contrato. Cuando un cliente adquiere conectividad y accede a sus servicios mediante la infraestructura de una red a la que no pertenece se dice que el cliente está haciendo *Roaming*. Dicha red de acceso de denomina *visited network*.

Se requiere que un cliente pueda acceder a la red IMS mediante *roaming*. La red *visited* podría no ofrecer servicios IMS, pero si ofrece conectividad IP el cliente puede acceder a sus servicios IMS a través de esta red.

Independencia de acceso. IMS esta diseñado para ser independiente del acceso. De esta manera los servicios IMS pueden ser provistos sobre cualquier red con conectividad IP (por ejemplo: GPRS, WLAN, xDSL).

3GPP utiliza el término *IP connectivity access network* (IP-CAN) para referirse a la colección de entidades de red e interfaces que proveen conectividad IP entre el UE[6] y las entidades IMS.

QoS para servicios IP multimedia. Mediante IMS, el UE negocia sus capacidades y expresa sus requerimientos de QoS durante la iniciación de una sesión SIP o un procedimiento de modificación de sesión. El UE es capaz de negociar parámetros tales como:

- Tipo de medios, dirección del tráfico.
- Tasa de transferencia de medios, tamaño de paquetes, frecuencias de transporte de paquetes.
- Utilización de datos RTP para los tipos de medios.
- Adaptación de ancho de banda.

Después de negociar los parámetros al nivel de aplicación, los UEs reservan recursos adecuados de la red de acceso. Se asume que los operadores negocian acuerdos de nivel de servicio para garantizar el QoS requerido en la interconexión del *backbone*[7].

Control de políticas IP, para asegurar la utilización correcta de los recursos multimedia. IMS tiene la capacidad de autorizar y controlar el tráfico en el canal portador de medios, basado en los parámetros de señalización en una sesión IMS. Esto requiere interacción entre la red de acceso con conectividad IP (IP-CAN) e IMS. Esta interacción es dividida en tres diferentes categorías:

- El elemento de control de políticas es capaz de verificar que los valores negociados en la señalización SIP sean efectivamente los utilizados cuando se activan los portadores para el tráfico de medios. Esto permite que un operador verifique que sus recursos no sean usados inadecuadamente (por ejemplo, las direcciones IP de origen y destino y el ancho de banda del canal reservado son exactamente los mismos usados en el establecimiento de sesión SIP).
- El elemento de control de políticas previene el uso del canal portador hasta que el establecimiento de la sesión se completa y permite que el tráfico comience y termine en sincronización con los cobros de una sesión IMS.
- El elemento de control de políticas es capaz de recibir notificaciones cuando el servicio de IP-CAN modifica, suspende o rechaza el (los) portador(es) de un usuario asociado con la sesión. Esto permite a IMS rechazar una sesión porque, por ejemplo, el usuario sale del área de cobertura.

Comunicación segura. IMS provee al menos el nivel de seguridad que provee GPRS y las redes CS. Por ejemplo, IMS se asegura de que los usuarios sean autentificados antes de que puedan empezar a utilizar los servicios, y los usuarios son capaces de requerir privacidad cuando entablan una sesión.

Cobros y facturación. IMS provee la capacidad de implementar distintos modelos de cobros. Por ejemplo, puede cobrar solamente al usuario que realiza la llamada, o también puede cobrar al que la recibe, basado en los recursos utilizados a nivel de transporte.

Además se puede cobrar por el tipo de medio que compone una sesión. Es capaz de realizar distintos tipos de cobros dependiendo del tipo de medio que se transmite (voz, video, etc). Adicionalmente, permite cargo online (prepago) y offline (postpago).

[6] UE: *User Equipment*. Es el equipo o terminal de usuario, por ejemplo un teléfono móvil.

[7] La red que conecta a varios operadores de telefonía se llama red *backbone* y se caracteriza por tener un gran ancho de banda.

Soporte para roaming. El usuario puede acceder a los servicios incluso si no está ubicado geográficamente en el área de servicio de la *home network*. Existen tres tipos de *roaming*:

- **GPRS roaming**: La red *visited* provee RAN y SGSN y la *home network* provee GGSN y IMS.
- **IMS roaming**: La red *visited* entrega conectividad IP (RAN, SGSN, GGSN) y el punto de entrada IMS (por ejemplo el P-CSCF). La red *home* otorga el resto de las funcionalidades.
- **IMS circuit-switched (CS)**: Se refiere al roaming inter-dominio entre IMS y CS. Cuando un usuario no está registrado o alcanzable en algún dominio, una sesión puede ser ruteada al otro dominio. Es importante notar que estos dominios tienen sus propios servicios y no pueden ser utilizados desde otro dominio. (algunos servicios son similares y están disponibles en ambos dominios, por ejemplo VoIP en IMS y telefonía en CSCN).

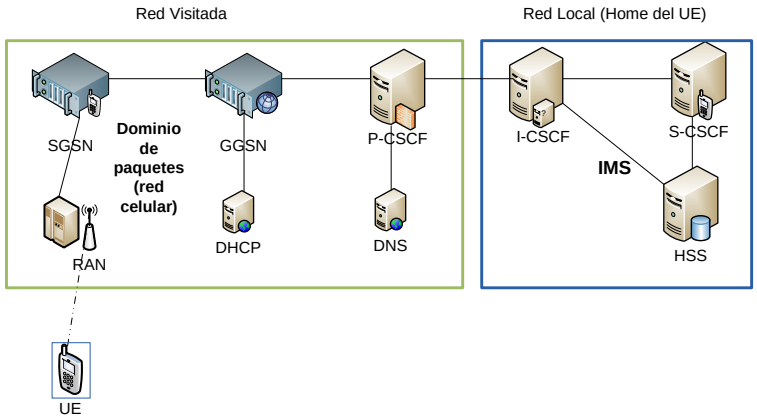

Figura 2.12: Roaming en IMS. Un equipo móvil (UE *User Equipment*) accede a los servicios provistos por su operador IMS a través de la red de paquetes 3G de un tercero.

Interworking con otras redes. IMS debe tener la facultad de ser compatible con redes las actuales. Se debe alcanzar usuarios independientemente del tipo de terminales que tengan o dónde se ubiquen. Para convertirse en una tecnología de comunicación exitosa IMS debe ser capaz de conectar la mayor cantidad de usuarios posible. IMS soporta comunicación con PSTN, ISDN, redes móviles e Internet.

Modelo de control de servicios. En redes móviles 2G se utiliza *visited service control*. Esto significa que cuando un usuario realiza roaming, una entidad en la red visitada provee servicios y controla el tráfico para el usuario. En 2G esta entidad se llama *visited mobile service switching centre*.

IMS adopta *home service control*. El nodo de red que tiene acceso a la base de datos de suscriptores e interactúa directamente con las plataformas de servicio está siempre localizada en la red *home* del cliente.

Desarrollo de servicios. La importancia de tener una plataforma de servicios escalable y la posibilidad de lanzar nuevos servicios rápidamente ha significado que la manera tradicional de estandarizar los sets completos de teleservicios, aplicaciones y servicios suplementarios no sea aceptable.

De esta manera, la organización 3GPP estandariza el soporte de servicios y no los servicios como tales. La arquitectura IMS incluye un *service framework*, que proporciona las habilidades necesarias para soportar voz, video, multimedia, mensajería, intercambio de archivos, transferencia de datos, juegos y servicios suplementarios básicos dentro de IMS.

Diseño de capas. Los servicios de transporte y bearer[8] están separados de la red de señalización IMS y de los servicios de administración de sesiones. Además los servicios corren sobre la red de señalización IMS. La figura 2.13 muestra este diseño de capas.

Este diseño aumenta la importancia de la capa de aplicación. Cuando las aplicaciones están aisladas y las funcionalidades comunes pueden ser provistas en niveles inferiores de la red IMS, las mismas aplicaciones pueden ser ejecutadas en el UE utilizando diversos tipos de acceso.

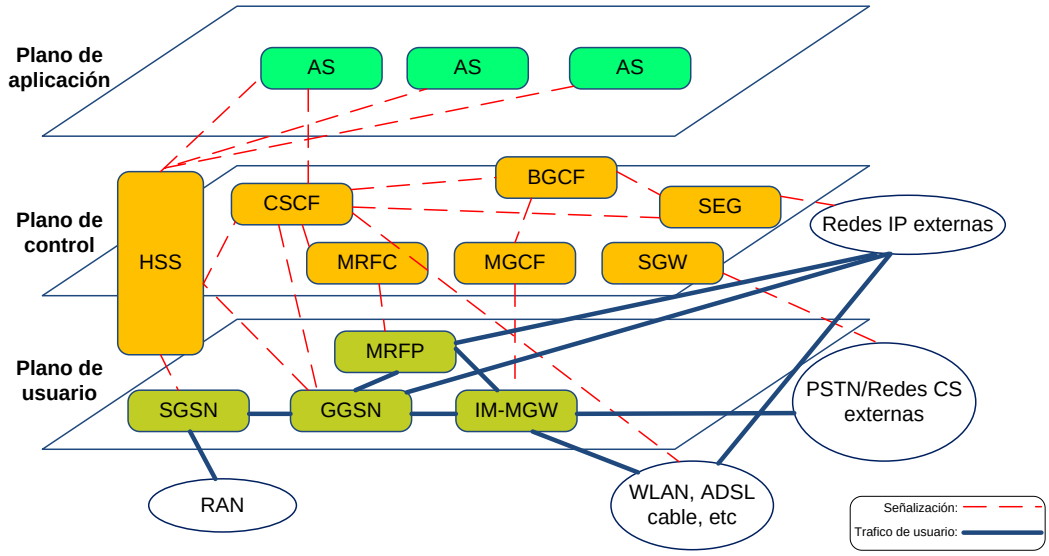

Figura 2.13: Arquitectura de capas en IMS.

2.4.3. Entidades presentes en IMS

Una entidad es un componente de la red (nodo) que realiza ciertas funciones específicas tales como señalización, control de llamadas, administración de recursos, control de usuarios, manejo de medios, etc. Se distinguen los nodos de núcleo (*Core*) que realizan tareas de conmutación, ruteo de mensajes SIP (señalización) y manejo de datos sensibles (cuentas de usuario, contraseñas, facturación), entre otros; y los nodos de borde (*Gateway*) que se encargan de ejecutar tareas de conversión de protocolos y conexión con otras redes (IMS, PSTN, Internet). En esta sección se describen los nodos relevantes del subsistema IMS.

2.4.3.1. P-CSCF *Proxy Call Session Control Function*

Este nodo es el encargado de conectar al cliente IMS con el Core. Es el primer punto de señalización hacia la red de servicios IMS. Se define en los estándares 3GPP TS 23.228 [31], TS 24.229 [32]. Entre sus principales funciones destacan:

- Direccionar la petición SIP REGISTER recibida desde el UE a un *entry point* (punto de entrada) determinado I-CSCF utilizando el nombre de dominio proporcionado por el cliente. Por ejemplo, un nombre de dominio típico es *playsip.org*.
- Direccionar los mensajes SIP recibidos desde el UE al servidor S-CSCF cuyo nombre es recibido como resultado del procedimiento de registro.

[8] Se refiere a la información del tipo relevante para el usuario (voz, video, mensajería, etc)

- Asegurarse de que los mensajes SIP recibidos enviados por el UE al SIP *server* (p.ej. S-CSCF) contienen la información correcta o al día sobre el tipo de red de acceso utilizada en ese momento por el UE.
- Direccionar las peticiones y respuestas SIP al UE.
- Detectar y manejar el establecimiento de una petición para una sesión de emergencia.
- Generación de CDR's (*Charging Data Records*). Enviar información de estado de cuenta/facturación al CCF (*Charging Collection Function*).
- Proveer protección de integridad de señalizaciones SIP y mantener una asociación de seguridad entre el UE y el P-CSCF definida en el estándar TS 33.203 [33].
- Comprimir y descomprimir mensajes SIP desde el UE.
- Suscribir un *registration event package* en el servidor de registro de usuario (S-CSCF). Este procedimiento es necesario para informar al cliente en caso de que un nodo de la red no esté disponible, en particular el nodo S-CSCF que lo sirve.
- Ejecutar política de medios. Verifica el tipo de medios a transmitir detallado por el protocolo SDP *Session Description Protocol*.
- Autorización de recursos de portador y administración de QoS. (TS 23.203 [34])
- Mantener temporizadores de sesión (*session timers*). Útil para conocer el estado de las sesiones.
- Interactuar y negociar capacidades a utilizar por el usuario con el servidor de control de políticas PDF (*Policy Decision Function*).

Antes de que el UE pueda requerir servicios, un portador apropiado IP-CAN (red de acceso) debe estar disponible para llevar las señalizaciones relativas al subsistema IMS. Para que un cliente pueda conectarse con un P-CSCF primero debe ser localizado. Este procedimiento se denomina descubrimiento de un P-CSCF y se efectúa utilizando uno de los siguientes mecanismos:

1. Como parte del establecimiento de conectividad hacia la red IP-CAN, si dicha red provee los medios.
2. Alternativamente, el descubrimiento puede ser realizado después de que la conectividad IP se ha establecido. Para esto, la IP-CAN debe proveer la opción de uso de DHCP para entregar al UE el nombre de dominio del P-CSCF y la dirección de un servidor DNS que sea capaz de resolver el nombre del P-CSCF. Esta técnica es utilizada en las pruebas que muestra este documento y es descrita en el anexo B.1.

2.4.3.2. I-CSCF *Interrogating Call Session Control Function*

Este nodo identifica los elementos de la red que sirven a determinados clientes dependiendo de los servicios que tenga contratados. Por ejemplo, asocia el servidor S-CSCF que maneja los perfiles de servicios del cliente que inicia sesión. Pueden existir múltiples I-CSCF en una red IMS de un operador. Las tareas de este servidor son:

- Contactar al HSS para obtener el nombre del S-CSCF que está sirviendo a un usuario.
- Asignar un S-CSCF basado en las capacidades informadas desde el HSS.

- Enviar respuestas y peticiones SIP al S-CSCF. Enruta los mensajes SIP recibidos desde otra red hacia el S-CSCF.
- Enviar información de estado de cuenta al CCF (*Charging Collection Function*).
- Proveer funcionalidad para esconder características. Puede contener THIG[9] que es usado para ocultar información de configuración, capacidad y topología de la red, para que no sea vista desde fuera de la red del operador.
- Traducir direcciones E.164 contenidas en todos los Request-URIs que tienen el formato de SIP URI con el parámetro `user=phone`, en el formato `Tel:URI` de IETF RFC3966[10] antes de realizar un `HSS Location Query` (consulta de ubicación).
- Basado en una configuración local, el I-CSCF puede realizar funciones de *transit routing*. Si el I-CSCF determina, basado en una consulta HSS, que el destinatario de una llamada no está dentro del dominio IMS, puede redireccionar la petición o puede retornar un respuesta de falla hacia el *end-point* originario.
- Generación de CDRs.

2.4.3.3. S-CSCF *Serving Call Session Control Function*

Se considera como el cerebro de IMS. Realiza control de sesión y servicios de registro de UEs. Cuando el UE tiene una sesión el S-CSCF la mantiene e interactúa con las plataformas de servicio y funciones tarifarias (*charging*) que el operador necesita para proveer sus servicios. Puede haber múltiples S-CSCF con diferentes funcionalidades dentro de la red del operador.

Entre las funciones realizadas por el S-CSCF durante el registro de un cliente destacan las siguientes:

- Se puede comportar como un servidor SIP *Registrar*, es decir acepta peticiones de registro y pone su información disponible a través de un servidor de ubicación (p.ej. HSS).
- Autentifica usuarios mediante el esquema IMS AKA (*Authentication and Key Agreement*). IMS AKA realiza autentificación mutua entre el UE y la *home network*.
- El S-CSCF notifica a los suscriptores sobre cambios de registro.
- Descarga información de usuario y datos relacionados con los servicios desde el HSS durante el registro o cuando se maneja una petición de un usuario no registrado.
- Maneja *timers* de registro y es capaz de de-registrar clientes cuando sea necesario.

Las funciones que cumple el S-CSCF cuando se mantiene una sesión son:

- Control de sesión para los clientes registrados.
- Puede actuar como un servidor proxy SIP. Acepta peticiones y las sirve internamente o las redirecciona.
- Se puede comportar como un UA (RFC3261), es decir puede terminar y generar transacciones SIP independientemente.
- Interactúa con plataformas de servicios (*Application Servers*). Tiene la capacidad de decidir si rutea una petición o respuesta hacia un servidor de aplicaciones para procesamiento avanzado.

[9] THIG: Topology Hiding Inter-network Gateway

- Entrega a los clientes información relacionada con servicio de eventos (por ejemplo, notificación de tonos/anuncios junto con ubicación de recursos de medios adicionales, notificación de facturación, entre otros).
- Rutea el tráfico hacia el UE destinatario por el P-CSCF respectivo y hacia el UE originario a través del I-CSCF, BGCF (*Breakout Gateway Control Function*) o el AS (*Application Server*). Cuando el cliente destinatario y originario son de la misma red/dominio del operador, redirecciona las peticiones o respuestas SIP hacia el I-CSCF dentro de la red del operador.
- Realiza traducciones de números E.164 [37] a SIP URI utilizando el mecanismo de traducción ENUM / DNS [11]. Este procedimiento es necesario porque el ruteo de señalización en IMS sólo utiliza SIP URIs.
- Ejecuta control de tipos de medios. Es capaz de verificar el contenido SDP de una sesión y validar si el cliente tiene permisos para utilizar ciertos tipos de medios o codecs. Si el contenido SDP no es válido según las políticas del operador o según el perfil del subscriptor, el S-CSCF rechaza la petición y devuelve una respuesta SIP de error al cliente respectivo.
- Envía información de facturación al CCF de los servicios utilizados por el cliente.
- Se asegura que el cliente origen/destino está suscrito al servicio de comunicación IMS utilizado.
- Redireccionar la petición/respuesta SIP al BGCF para ruteo de llamadas a los dominios PSTN o CS.

2.4.3.4. HSS *Home Suscriber Server*

Es el sistema principal de almacenamiento de datos para todos los subscriptores y para datos relacionados con el servicio de IMS. La información almacenada en el HSS incluye identidades de usuario, información de registro, parámetros de acceso e información de *service-triggering*[10].

El HSS almacena datos referentes a la funcionalidad de IMS, pero además realiza las funciones de HLR y AUC propias de los dominios CS y PS.

Los parámetros de acceso IMS almacenados en el HSS, son utilizados para establecer las sesiones. Consisten en parámetros de autentificación, autorización de roaming y nombres de S-CSCF destinados a los usuarios. Además provee los requerimientos específicos de usuario para cada S-CSCF. Esta información es utilizada por el I-CSCF para seleccionar el S-CSCF más apropiado para un usuario.

Por otra parte, la funcionalidad de HLR es requerida para proveer soporte a las entidades del dominio PS, tales como SGSN y GGSN. Esto permite al subscriptor acceder a los servicios del dominio PS. De manera similar el HLR provee soporte para las entidades del dominio CS, como MSC/MSC-servers. Con esto el suscriptor puede acceder a los servicios del dominio CS y utilizar *roaming* en las redes GSM/UMTS del dominio CS.

En el core IMS se comunica con el S-CSCF y I-CSCF mediante las interfaces Cx sobre el protocolo *Diameter*.

[10] Se refiere a las condiciones que se cumplen para gatillar un servicio de valor agregado controlado por un *Application Server*.

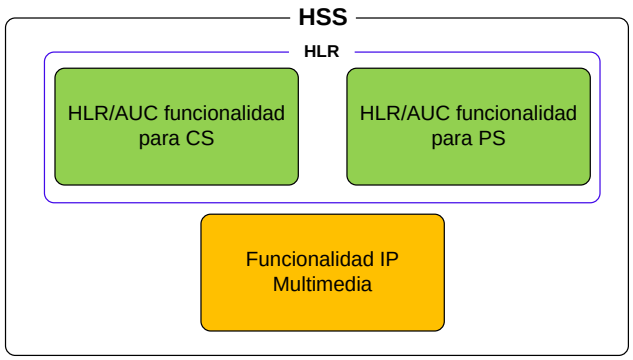

Figura 2.14: Funcionalidades del HSS.

2.4.3.5. SLF *Subscription Locator Function*

Este nodo realiza la resolución de direcciones que permite al I-CSCF, S-CSCF y al AS encontrar la dirección del HSS que mantiene la información de un subscriptor cuando existen múltiples HSS.

2.4.3.6. PDF *Policy Decision Function*

Ejecuta políticas de decisión de acuerdo al tipo de medios dentro de una sesión (esta información se obtiene desde el P-CSCF).

- Almacena información de sesión y medios (direcciones IP, número de puertos, ancho de banda, etc.).
- Genera datos de autorización que identifica al PDF y la sesión.
- Provee una decisión de autorización de acuerdo a la información de sesión y medios almacenados, cuando se recibe una petición de autorización de medios desde el GGSN.
- Actualiza la decisión de autorización para modificaciones de sesión y medios.
- Puede revocar la decisión de autorización en cualquier momento.
- Tiene la capacidad para permitir y denegar el uso de un portador (p.ej. Contexto PDP[11]).
- Informa al P-CSCF cuando se modifica o pierde el portador (p.ej. Contexto PDP).
- Entregar un identificador *IMS-charging* al GGSN y un identificador *GPRS-charging* al P-CSCF.

Este nodo se conecta con el resto de la red IMS utilizando las interfaces *Go* y *Gq*. La interfaz *Go* utiliza el protocolo COPS [35] y se conecta con el nodo GGSN del dominio de paquetes conmutados (GPRS) de la red core móvil. Además el PDF se conecta con el P-CSCF mediante la interfaz *Gq* usando el protocolo Diameter.

[11] Un contexto PDP es una estructura de datos utilizada en GPRS que mantiene la información de conexión del terminal móvil con la red .

2.4.3.7. MRF *Multimedia Resource Function*

Los nodos MRFC y MRFP proveen soporte para servicios relacionados con flujo de medios (*bearer*) como por ejemplo sesiones multi-partitas, anuncios al usuario o *bearer transcoding*.

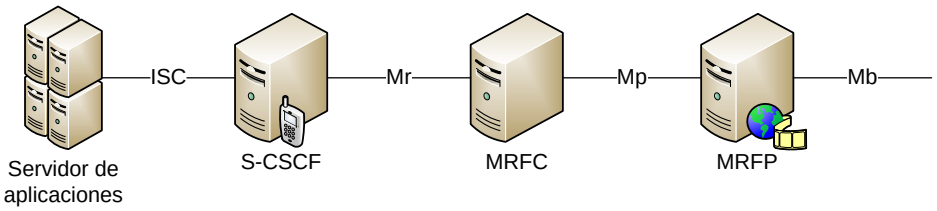

Figura 2.15: Interfaces MRFP-MRFC

MRFC - *Multimedia Resource Function Controller*. Se utiliza para servicios como conferencia, anuncios a usuarios o bearer transcoding. Interpreta la señalización SIP desde el S-CSCF y utiliza instrucciones MEGACO para controlar el MRFP. Es capaz de enviar información de facturación al CCF y al OCS (*Online Charging System*).

- Controla los recursos de media stream en el MRFP.
- Interpreta la información procedente del AS y el S-CSCF (por ejemplo, el identificador de sesión) y controla el MRFP de manera adecuada a esta interpretación.
- Genera CDR's.

MRFP – *Multimedia Resource Function Processor*. Este nodo provee recursos a nivel de usuario que son requeridos y comandados por el MRFC. Realiza las funciones siguientes:

- Mezcla de flujos (*streams*) de medios entrantes (para conferencias multi-partitas).
- Origina *media stream* (para anuncios multimedia).
- Procesa *media stream* (ej. Audio transcoding, análisis de medios).
- Controla *bearers* en la interfaz *Mb*.
- Provee recursos para ser controlados por el MRFC.
- *Floor Control*. Por ejemplo, administra derechos de acceso a recursos compartidos en un entorno de conferencia.

Punto de referencia *Mr*. Cuando el S-CSCF necesita activar servicios relativos al canal portador de media (*bearer-related*) envía señalización SIP mediante esta interfaz. Su funcionalidad no está completamente estandarizada —por ejemplo, no está especificada la manera como el S-CSCF informa al MRFC para realizar un anuncio específico— por lo tanto depende del operador implementar esta capacidad de forma propietaria. El protocolo utilizado en este punto de referencia es SIP.

Punto de referencia *Mp*. Cuando el MRFC necesita controlar media streams —por ejemplo, para crear conexiones para conferencia o para detener medios en el MRFP— se utiliza esta interfaz. Los servicios IMS eventualmente requieren algunas extensiones. La interfaz permite a un MRFC controlar recursos de *media stream* provistos por el MRFP. Es compatible con el estándar H.248/MEGACO y es de arquitectura abierta, característica necesaria para que se puedan definir extensiones en la interfaz.

2.4.3.8. AS *Application Server*

Son los nodos encargados de proveer los servicios a los subscriptores. La interfaz que conecta al plano de aplicación con el core de la red (CSCFs) se denomina ISC (*IMS Service Control*) y el protocolo de señalización seleccionado para su implementación es SIP. Las funciones principales de los servidores de aplicación son:

- Procesar una sesión SIP entrante recibida desde el IMS.
- Capacidad para originar peticiones SIP.
- Capacidad para enviar información de cuentas al CCF y al OCS.

IMS provee los métodos necesarios para invocar y proveer servicios. La lógica de operación es la siguiente:

1. Definir el posible servicio o conjunto de servicios.
2. Creación de información específica referente al usuario, cuando este requiere una subscripción o la modifica, en formato de iFC (*Initial Filter Criteria*).
3. Encaminar el requerimiento inicial hacia un servidor de aplicación.

Un servicio se inicia de acuerdo a los criterios asignados en el núcleo de red. En general cuando un cliente se registra el servidor S-CSCF descarga desde el HSS la información del suscriptor (iFC) referente a sus servicios asociados para encargarse de activarlos cuando el cliente lo solicite.

Los servicios se activan gracias a los *trigger points* (TP) asociados al iFC que indican de qué manera se gatilla el servicio. El iFC indica el servidor de aplicación asociado y los TPs. La activación se puede hacer filtrando por el método SIP, Request-URI, header SIP (por ej. `Event`), contenido SDP, entre otros.

2.4.3.9. Nodos de comunicación con otras redes

BGCF *Breakout Gateway Control Function*. Selecciona la red IMS en la cual el acceso a la red CS debe ocurrir. Puede ser la misma red donde el BGCF está ubicado o en una red externa. En el primer caso el nodo selecciona un MGCF para manejar la sesión. Para una conexión a una red externa el nodo selecciona otro BGCF de la red determinada.

MGCF *Media Gateway Control Function*. Este gateway permite habilitar la comunicación entre usuarios IMS y CS. Toda la señalización de control de llamadas proveniente de la red CS es destinada hacia el MGFC que realiza la conversión del protocolo ISUP o BICC a SIP y lo direcciona al core IMS. De la misma forma traduce la señalización desde IMS hacia CS.

IMS-MGW *IMS Media Gateway Function*. Provee el enlace entre IMS y las redes de circuitos conmutados (PSTN, GSM) para transmitir medios. Es controlado por el *Media Gateway Control Function*. Ejecuta la conversión de medios IMS/CS y realiza transcoding y procesamiento de señales cuando es necesario. Además este nodo es capaz de entregar tonos y anuncios a los usuarios de la red CS.

SGW *Signalling gateway*. Para interconectar diferentes redes de señalización a nivel de la capa de transporte. No interpreta información a nivel de aplicación (ISUP, BICC). Por ejemplo, puede convertir desde SIGTRAN SCTP/IP hacia SS7 MTP y viceversa.

2.4.4. Interfaces entre nodos IMS

La conexión entre cada entidad de una red móvil se denomina interfaz. Dos nodos se conectan mediante una interfaz utilizando un protocolo definido. La gran mayoría de las interfaces se comunican con protocolos estandarizados por la 3GPP. Sin embargo, existen conexiones no definidas en los estándares donde se permite que el protocolo sea propietario.

Dependiendo de las funciones de los nodos en la red se define un protocolo ad-hoc, por ejemplo si es necesario intercambiar información de facturación e identificación en la interfaz se utiliza *Diameter*; en el caso de que se intercambien datos de señalización el protocolo que se usa es *SIP*. La figura 2.16 muestra un esquema de las interfaces —también llamadas puntos de referencia— en el subsistema IMS. La tabla 2.1 resume la utilidad de cada interfaz y el protocolo que utiliza.

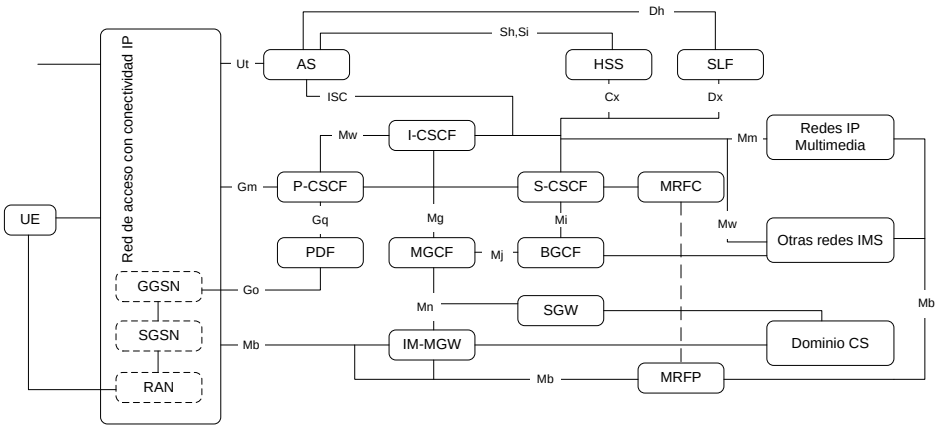

Figura 2.16: Arquitectura IMS - Puntos de referencia.

Nombre del punto de referencia	Entidades envueltas	Propósito	Protocolo
Gm	UE, P-CSCF	Se usa para intercambiar mensajes entre los UE y CSCFs	SIP
Mw	P-CSCF, I-CSCF, S-CSCF	Usado para intercambiar mensajes entre CSCFs	SIP
ISC	S-CSCF, I-CSCF, AS	Se usa para intercambiar mensajes entre CSCFs y AS	SIP
Cx	I-CSCF, S-CSCF, HSS	Comunica I-CSCF/S-CSCF con HSS	Diameter
Dx	I-CSCF, S-CSCF, SLF	Es utilizado por I-CSCF/S-CSCF para encontrar un HSS correcto en un entorno multi-HSS	Diameter
Sh	SIP AS, OSA SCS, HSS	Para intercambiar información entre SIP AS/OSA SCS y HSS	Diameter
Si	IM-SSF, HSS	Comunica al IM-SSF con HSS	MAP
Dh	SIP AS, OSA, SCF, IM-SSF, HSS	Utilizado por AS para encontrar un HSS correcto en un entorno multi-HSS	Diameter
Mm	I-CSCF, S-CSCF, red IP externa	Para intercambiar mensajes entre IMS y redes IP externas	No especificado
Mg	MGCF, I-CSCF	MGCF convierte las señalizaciones ISUP en SIP y direcciona las señalizaciones SIP al I-CSCF	SIP
Mi	S-CSCF, BGCF	Este punto de referencia es utilizado para intercambiar mensajes entre S-CSCF y BGCF	SIP
Mj	BGCF, MGCF	Para intercambiar mensajes entre BGCF y MGCF en la misma red IMS	SIP
Mk	BGCF, BGCF	Para intercambiar mensajes entre BGCFs en distintas redes IMS	SIP
Mr	S-CSCF, MRFC	Para intercambiar mensajes entre S-CSCF y MRFC	SIP
Mp	MRFC, MRFP	Para intercambiar mensajes entre MRFC y MRFP	H.248
Mn	MGCF, IM-MGW	Permite control de recursos de user-plane	H.248
Ut	UE, AS (SIP AS, OSA SCS, IM-SSF)	Habilita al UE para administrar información referente a sus servicios	HTTP
Go	PDF, GGSN	Permite a los operadores controlar QoS en un user plane e intercambiar información de correlación de tarificación entre redes IMS y GPRS	COPS
Gq	P-CSCF, PDF	Se utiliza para intercambiar información de políticas de decisiones entre P-CSCF y PDF	Diameter

Tabla 2.1: Interfaces entre los nodos IMS.

2.4.5. Extensiones SIP para IMS

La 3GPP adoptó SIP como base para IMS, el cual fue originalmente estandarizado por la IETF. En las primeras revisiones de la arquitectura IMS se comprobó que habían ciertos vacíos en el protocolo SIP original, que impedían cumplir con las características requeridas para proveer un soporte completo en redes IMS. La 3GPP generó nuevas extensiones SIP específicas para IMS. Algunos ejemplos de dichas extensiones son: control de llamadas (*call control*), presencia y mensajería instantánea, entre otras. En esta sección se detallan las extensiones más importantes presentes en los estándares IMS.

2.4.5.1. SigComp – Compresión

La extensión *SigComp* define como comprimir datos de señalización SIP textuales, los cuales pueden ser muy largos y problemáticos para transmitir, provocando retraso. *SigComp* soluciona los problemas de retraso de ida y vuelta (*round-trip*). Se utiliza para enviar mensajes entre el UE y el P-CSCF.

El estándar RFC3482 [12] define un nuevo parámetro URI `comp`, el que puede ser dispuesto por el UE o el SIP proxy (en IMS: P-CSCF) como `comp=SigComp` para expresar su deseo de rutear mensajes SIP comprimidos.

La creación de estados de compresión (llamados *compartments*) se realiza después de establecerse el Ipsec SA (*Security Agreement*) entre el UE y el P-CSCF. Cuando las entidades desean utilizar compresión no se crean dichos estados antes de este proceso. Esto es para evitar ataques de DoS[12] en contra del P-CSCF y no sobrecargarlo forzándolo a reservar memoria para un número innecesario de *compartments* SigComp.

El parámetro `comp` es utilizado dentro de las peticiones SIP en IMS:

- Por el UE en el header `Contact` de la petición REGISTER. Esto significa que el UE recibirá comprimidas las peticiones iniciales hacia él.
- Por el UE en el header `Contact` de cualquier otra petición inicial o la primera respuesta a una petición inicial. Esto significa que el UE desea recibir todas las peticiones subsecuentes dentro del diálogo de forma comprimida, ya sea las peticiones subsecuentes que son ruteadas basadas en la dirección del header `Contact` de la petición inicial (desde el lado originario) o la primera respuesta a una petición inicial (desde el lado terminal).
- Por el UE en el encabezado `Via` de cualquier petición. El UE desea recibir comprimidas todas las respuestas que contengan este parámetro en el encabezado `Via` de su mensaje.
- Por el P-CSCF en el contenido del encabezado `Record-Route` que es enviado hacia el UE. El P-CSCF desea recibir comprimidas las peticiones subsecuentes, que son ruteadas hacia los proxies SIP basados en el contenido del header `Route` (generado a partir del encabezado `Record-Route`).
- Por el P-CSCF en el header `Via` de cualquier petición. El P-CSCF desea recibir todas las respuestas a su petición comprimidas, donde las respuestas están ruteadas basadas en el encabezado `Via` relativo a la petición.

También se utiliza la opción de compresión en el momento de registro de clientes. El mensaje `REGISTER` inicial incluye la siguiente información relacionada con la compresión:

```
REGISTER sip:playsip.lab SIP/2.0
Via: SIP/2.0/UDP sip:172.16.231.185;comp=SigComp;branch=0uetb
Route: sip: 172.20.3.125;lr
Contact: <sip:172.16.231.185:1357;comp=SigComp>;expires=600000
```

[12] DoS: Denial of Service. Ataques de denegación de servicio.

Se incluye el parámetro `comp=SigComp` en el encabezado `Via` que indica que el UE desea recibir las respuestas a esta petición comprimidas. También es incluido en el encabezado `Contact`, entonces aparecerá en todas la peticiones iniciales recibidas por el UE dentro de la sesión. El S-CSCF reemplaza el *Request-URI* por la dirección de contacto registrada. Por ejemplo, sustituye el URI *javier@playsip.lab* por el valor del encabezado `Contact` de este cliente *sip:172.16.231.185;comp=SigComp*.

2.4.5.2. P-Headers

Adicionalmente a los *headers* estándar, la organización 3GPP define los *P-Headers* (RFC 3455 [14]) que son encabezados destinados a resolver problemas específicos de redes IMS, como la obtención de información acerca de la red de acceso (*cell ID*), red visitada (*roamed network*) y la determinación de la identidad del *caller* (cliente originario).

P-Associated-URI: Permite al servidor *Registrar* (S-CSCF) retornar un set de URIs asociadas para un cliente registrado. Esta extensión permite al UAC saber otras identidades públicas que el proveedor de servicios ha asociado a una identidad registrada. El S-CSCF inserta el header en la respuesta `200 OK` a una petición `REGISTER`.

Las URIs asociadas son identidades públicas que el proveedor de servicios ha destinado a un usuario para su uso propio. Por ejemplo, un cliente puede tener asociada la identidad *javier@work.playsip.lab* para realizar llamadas de su trabajo y *javier@home.playsip.lab* para asociar las llamadas privadas. El S-CSCF contiene la información que permite que una identidad registrada sea asociada con varias URIs.

Sólo el URI presente en el encabezado `To` del mensaje `REGISTER` es registrado. El resto de los URIs asociados no necesariamente están registrados.

P-Called-Party-ID: Un proxy inserta este header típicamente en una petición `INVITE`. El header es llenado con el *Request-URI* recibido por el proxy en la petición. Esto se hace porque el servidor que atiende al cliente destino altera el *Request URI* con el valor de `Contact` proporcionado por él al registrarse (típicamente una dirección IP). Por lo tanto, para que la identidad del cliente destino no se pierda se copia en el header `P-Called-Party-ID` antes de ser reemplazada. El UA puede utilizar la información contenida en este encabezado para ejecutar distintas tareas dependiendo de la URI (identidad pública) que fue invitada, por ejemplo, hacer sonar un tono de alerta distintivo.

```
INVITE sip:javier@192.0.2.4 SIP/2.0
Via: SIP/2.0/UDP 192.0.2.10:5060;branch=z9hG4bKg48sh128
Via: SIP/2.0/UDP 192.0.2.20:5060;branch=z9hG4bK03djaoe1
To: sip:javier@playsip.lab
From: sip:jesus@santiago.lab;tag=938s0
Call-ID: 843817637684230998sdasdh09
P-Called-Party-ID: sip:javier-office@playsip.org
CSeq: 101 INVITE
```

P-Visited-Network-ID: Las redes 3GPP están compuestas por redes locales (*home networks*), redes visitadas (*visited networks*) y suscriptores. Una *home network* puede tener acuerdos de *roaming* con una o más redes visitadas. Esto tiene el efecto de que cuando un terminal móvil está haciendo *roaming*, puede utilizar recursos de la *visited network* de forma transparente.

Existe una necesidad para indicar a la red local cuál es la red visitada que está otorgando servicios al terminal que utiliza *roaming*.

Los UAs 3GPP siempre se registran en su red *home*. La petición `REGISTER` es enviada a través de uno o más proxies localizados en la *visited network*. La red puede autorizar el registro si tiene un acuerdo de *roaming* con la red externa o denegarlo en caso contrario. Los UAs no agregan este *header*

en ningún mensaje SIP. El encargado de insertar el encabezado `P-Visited-Network-ID` es algún proxy localizado en la red *visited*.

`P-Access-Network-Info:` Este *header* es útil en redes basadas en SIP que también proveen conectividad de capa 2/capa 3 a través de diferentes tecnologías de acceso. Los UAs pueden usar este *header* para informar a los servidores que proveen los servicios IMS con el fin de optimizarlos de acuerdo al medio de acceso.

`P-Charging-Function-Addresses:` La 3GPP ha definido una arquitectura distribuida que resulta en múltiples entidades de red encargadas de proveer servicios y acceso. Existe una necesidad de informar a cada proxy SIP involucrado en una transacción acerca de las entidades encargadas de la facturación para recibir los registros de cobros generados o los eventos de cobros.

La solución que provee 3GPP es definir 2 tipos de entidades funcionales de cobros: *Charging Collection Function* (CCF) y *Event Charging Function* (ECF). CCF es usado para cobro off-line (postpago). ECF se utiliza para cobro on-line (por ejemplo, para un servicio de prepago).

Un SIP proxy que soporta esta extensión y recibe una petición o respuesta sin el *header* debiera insertarlo antes de reenviarlo. Dicho encabezado es poblado con una lista de direcciones de uno o más nodos de cobro donde el proxy debiese enviar información relacionada con facturación de servicios.

`P-Charging-Vector:` Los operadores necesitan la habilidad y flexibilidad de cobrar por el acceso y el servicio que proveen. Esto requiere coordinación entre las entidades de red (por ejemplo los proxies), que incluyen registros de cobros correlacionados generados desde diferentes entidades para una sesión de usuario. La información de correlación incluye, un único identificador global que facilita la labor de facturación conocido como *IMS Charging Identity* (ICID).

Un proxy que soporta esta extensión debe insertar el *header* previamente al reenvío de una petición o respuesta que no lo contenga. Si la dirección a reenviar el mensaje no es parte de la red confiable, el *header* es removido.

2.4.5.3. Security Agreement

Esta extensión especifica como negociar las capacidades de seguridad para múltiples tipos de terminales *end-points*.

La especificación RFC 3329 [15] describe los procedimientos necesarios para agregar seguridad en las transacciones SIP. El mecanismo de seguridad definido es aplicado entre el UA y el nodo adyacente (por ejemplo el *outbound proxy*).

Si el cliente utiliza TLS[13] para contactar al servidor, no debe utilizar los procedimientos de seguridad de esta especificación. En caso contrario debiese ocuparlos para detectar *DNS spoofing*, o para negociar otro tipo de seguridad distinto a TLS.

El servidor que recibe una petición desde la interfaz de red configurada para utilizar los mecanismos de seguridad, debe verificar que la petición tenga sólo un campo `Via`. En caso contrario el servidor no es el primer nodo en el diálogo, por lo que no debe utilizar este mecanismo y debe retornar una respuesta `502 Bad Gateway`. El mecanismo se describe a continuación.

```
1. Client ----------client list---------> Server
2. Client <---------server list---------- Server
3. Client ------(turn on security)------- Server
4. Client ----------server list---------> Server
5. Client <---------ok or error---------- Server
```

[13]TLS: Transport Layer Security (RFC 2246 [16])

1. Los clientes que desean utilizar los métodos de seguridad provistos por este estándar envían una lista de sus mecanismos de seguridad soportados dentro de la primera petición al servidor.
2. El servidor requerido envía una respuesta al cliente con los mecanismos de seguridad que soporta.
3. El cliente selecciona el mecanismo seguridad de su preferencia que tiene en común con el servidor.
4. El cliente contacta al servidor utilizando el mecanismo de seguridad seleccionado.
5. El servidor verifica su propia lista de mecanismos de seguridad para asegurarse que la lista original no fue cambiada.

Los servidores involucrados no guardan estados (*Stateless Server*), por lo tanto el procedimiento anterior debe realizarse cada vez que se inicie una conexión, a menos que el método de seguridad escogido requiera lo contrario.

Los encabezados SIP definidos en el estándar son `Security-Client`, `Security-Server` y `Security-Verify`. Para ser utilizados el cliente debe agregar la opción `sec-agree` en el *header* `Require` y `Proxy-Require`. Un ejemplo del contenido de un mensaje SIP se muestra en el cuadro siguiente.

```
INVITE sip:proxy.ejemplo.com SIP/2.0
       Security-Verify: ipsec-ike;q=0.1
       Security-Verify: tls;q=0.2
       Route: sip:usuario@dominio.com
       Require: sec-agree
       Proxy-Require: sec-agree
```

2.4.5.4. AKA-MD5

Esta extensión [17] determina cómo los terminales y las redes son autentificadas utilizando un mecanismo ya definido (por ejemplo ISIM), además de un intercambio de llaves específico. Puesto que el *framework* de autentificación de SIP sigue cercanamente al de HTTP, Digest AKA es aplicable directamente al protocolo SIP. La figura 2.17 muestra un flujo de mensajes de un proceso Digest AKA de autentificación en un diálogo SIP.

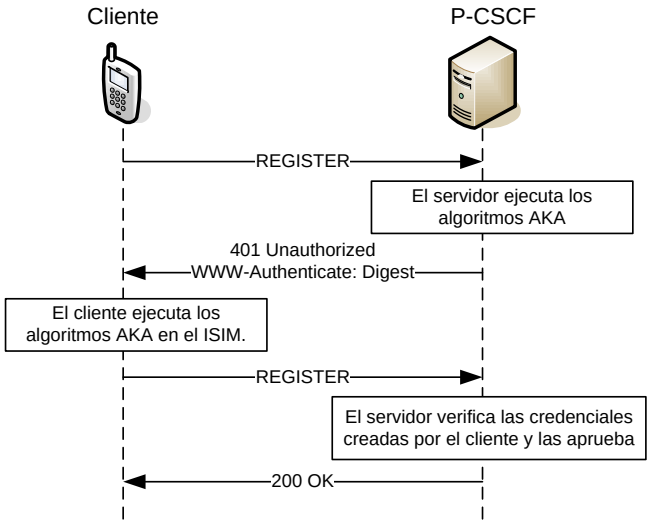

Figura 2.17: Flujo de mensajes de una autentificación exitosa.

1. Petición inicial (registro)

```
REGISTER sip:playsip.lab SIP/2.0
```

2. Respuesta

```
SIP/2.0 401 Unauthorized - Challenging the UE
WWW-Authenticate: Digest
    realm="playsip.lab",
    nonce="j/ZC0TTu2RPMeAad+GTRjFsbkHDM6wAAEPmCcXYEFK8=",
    algorithm=AKAv1-MD5
```

3. Petición con credenciales

```
REGISTER sip:playsip.lab SIP/2.0
    Authorization: Digest
    username="javier@playsip.lab",
    realm="playsip.lab",
    nonce="j/ZC0TTu2RPMeAad+GTRjFsbkHDM6wAAEPmCcXYEFK8=",
    uri="sip:playsip.lab",
    response="aa5ec494b84fe556aba2e3c2a86bf9a9",
    algorithm=AKAv1-MD5
```

4. Respuesta exitosa

```
SIP/2.0 200 OK - SAR succesful and registrar saved
```

2.4.5.5. Otras Extensiones

Mobile Registration: En redes IMS, el proceso de registro de terminal es más complicado, ya que incluye varias extensiones de seguridad y debe tratar con registros desde una red *visited*. La organización de estandarización IETF [24, 25] define la sintáxis y el uso de las entidades SIP de los encabezados `Service-route` y `Path`.

Reg-event Package: Utilizado por el terminal y el P-CSCF para saber el estado del registro del terminal en una red (IETF RFC3680 [29]).

Preconditions: Especifica métodos para negociar QoS, seguridad y otros comportamientos de llamadas requeridos entre dos terminales. Define cómo hacer reservas de recursos para llamadas o sesiones (RFC 3312 [26]).

Media Authorization: Esta extensión (RFC 3313 [27]) es utilizada para intregrar control de admisión con calidad de servicio con señalización de llamadas y ayudar a prevenir ataques de denegación de servicio. Se asegura de que solamente los recursos de medios autorizados sean utilizados.

SDP Session Description Protocol: IMS extiende SDP con incluso más extensiones, tales como *grouping media lines* [18], *QoS* y *preconditions attributes* [19], soporte para *codec supplemental*, y modificadores de ancho de banda.

IPSec IPSec (RFC 2401 [20]:) es utilizado en varias interfaces IMS y entre diferentes redes IMS. IMS utiliza IPSec en el modo de transporte, a diferencia del estándar utilizado en servicios VPN.

Uso extensivo de XML: La señalización IMS SIP usa protocolos XML extensivamente, incluyendo XCAP [23], para implementar varios tipos de contenido en mensajes SIP y permitir interfaces de funcionalidad completa entre entidades IMS.

IMS Simple Extensions: El grupo SIMPLE [22] forma parte de la IETF y define los requerimientos de presencia y mensajería instantánea. Las definiciones básicas de SIMPLE fueron inadecuadas para las aplicaciones IMS porque no eran suficientemente eficientes para su uso con enlaces aéreos. IMS SIP extiende este estándar con: *Partial Notifications/Publications*, *Notifications filtering*, *Resource list/SIP exploders* y *Message Session Relay Protocol* (MSRP), entre otros.

Capítulo 3

Construcción de un laboratorio IMS

Este capítulo se divide en dos partes. La primera muestra los procedimientos necesarios para elaborar los módulos de práctica de un curso de laboratorio basado en la arquitectura IMS. La segunda parte señala las actividades a realizar para construir e integrar un core IMS, junto con las pruebas de funcionalidad básica a aplicar sobre la plataforma.

3.1. Laboratorios docentes

En esta sección se describe el proceso de elaboración de un curso de laboratorio. Como se trata de un curso práctico, es necesario definir de manera precisa la base teórica de tal forma de tener una referencia bibliográfica completa que ayude al alumno a complementar los conocimientos adquiridos en una experiencia práctica.

El proceso se divide en tres etapas que conforman la creación del curso. La etapa de planificación entrega la base teórica para lograr diseñar cada experiencia de laboratorio. El diseño de experiencias muestra como se estructura cada una de las experiencias del curso. La etapa de práctica consiste en diseñar la forma en que se aplican las experiencias a un grupo de alumnos con conocimientos básicos en telecomunicaciones.

3.1.1. Planificación del curso de laboratorio

El curso de laboratorio consiste, en principio, en una serie de experiencias desarrolladas en cada sesión. Se estima que el curso debe componerse de 8 a 10 sesiones, de 90 minutos cada una. De acuerdo a esto se diseñan experiencias prácticas que se adecúan a este límite de tiempo. Por lo tanto, el número de experiencias es a lo más igual al número de sesiones del curso, o menor si se trata de experiencias de mayor extensión de tiempo.

A continuación se presenta la metodología de desarrollo del laboratorio, que consiste en las etapas a realizar para la construcción de cada experiencia, partiendo por la revisión de antecedentes, y terminando con el diseño de cada actividad.

Recopilación de información. Corresponde a:

- Revisión de antecedentes y listado de tópicos más importantes. Corresponde a un estudio acabado de la arquitectura IMS y la identificación de sus características más importantes.
- Revisión de pruebas realizadas en la construcción del Core IMS. Se buscan herramientas de software que cumplen con los estándares IMS y se aplican pruebas de conectividad, capacidad,

interoperabilidad y servicios, donde finalmente se realiza una selección de pruebas relevantes a ser estudiadas en una sesión de laboratorio.

- Factores que condicionan las características del curso. Se identifican las restricciones bajo las cuales es aplicado el curso: disponibilidad de herramientas (hardware, software), duración del período académico y tiempo máximo de cada clase, cantidad de alumnos con los que contará el curso y conocimientos previos necesarios para participar en el curso.

Formulación de objetivos del curso. Una vez obtenidos los antecedentes bibliográficos, se plantea los conocimientos que deberán adquirir los alumnos luego de finalizado el curso. Es importante hacer compatible dichos conocimientos con los objetivos y lineamientos del departamento o institución que impartirá el curso.

Generación del programa de estudios. Se detallan los objetivos generales, haciendo específicas las materias a tratar en las experiencias. Con esto es posible plantear las experiencias que se realizarán, y sus contenidos de acuerdo a los objetivos planteados anteriormente.

Construcción de matriz de contenidos y experiencias. Con las experiencias ya planificadas se distribuyen los contenidos en cada una de ellas. Con esto se logra que las experiencias vayan teniendo un grado de dificultad creciente con el correr del tiempo.

Diseño de experiencias. Se crean las actividades y preguntas que el estudiante responderá en las experiencias.

3.1.2. Diseño de Experiencias

Los tópicos incluidos en cada experiencia se describen a continuación:

- Resumen de experiencia: Introducción y descripción general de la guía de laboratorio.
- Objetivos: Se listan los objetivos de la experiencia. Fija un lineamiento de las actividades que se realizan.
- Red de referencia: Se incluye en cada experiencia un diagrama de la topología de la red utilizada para la ejecución de pruebas. Se incluyen los nombres de servidores, hosts, IPs de los computadores, tablas de rutas si son necesarias, etc.
- Temas cubiertos por la experiencia: Indica los elementos teóricos que cubre la guía de laboratorio. Se basa en la matriz de cruce de contenidos y experiencias planteada más adelante.
- Contenidos necesarios: Corresponde al listado de conocimientos teóricos previos necesarios para desarrollar las actividades presentes en la guía.
- Materiales: Lista de todos los materiales de software y hardware necesarios para montar la red de referencia y realizar las pruebas.
- Actividades de la experiencia: Corresponde a las instrucciones paso a paso para obtener los resultados esperados. Se detalla la utilización de las herramientas para lograr un correcto funcionamiento de la plataforma y obtener apropiadamente los resultados de cada prueba.
- Evaluación: Set de preguntas ligadas a las actividades que evalúan el conocimiento obtenido de ellas.
- Conclusiones: Cierre de la guía donde el alumno debe resumir lo aprendido en la experiencia comentando cada una de las actividades realizadas.

3.1.3. Experiencias y contenidos

Las experiencias a realizar se describen a continuación.

Experiencia 00 – *Instalación de red de referencia.* Se detallan los procedimientos para instalar toda la plataforma de pruebas. Incluye la instalación de los servidores DNS, SIP proxy, CSCF, HSS, PCEF-PCRF y los clientes SIP e IMS a utilizar. Además se indican las herramientas usadas para obtener resultados.

Experiencia 01 – *Servidores SIP Proxy.* Corresponde a la experiencia introductoria al protocolo SIP. Se efectúan pruebas sobre un servidor proxy. El análisis de señalización esta enfocado en el registro de los clientes y la sesión SIP estándar. El ruteo y la manipulación de mensajes SIP (INVITE, REGISTER) es el foco de esta experiencia.

Experiencia 02 – *Red SIP - Detalle de Señalización.* En esta experiencia se ejemplifican mensajes SIP más complejos utilizando una red de servidores SIP cada uno con distintas funcionalidades.

Se ejecutan pruebas de funcionamiento en un servidor SIP *proxy*. Este servidor se conecta a un servidor SIP *registrar* que sirve a los usuarios registrados, entregando la funcionalidad de autentificación. Adicionalmente se necesita una base de datos donde se almacena la información de los clientes SIP.

Experiencia 03 – *Introducción al Core IMS: P-CSCF.* Esta experiencia introduce la interacción entre un cliente IMS y el elemento de entrada al core, el servidor P-CSCF. Se plantean las diferencias con un servidor SIP proxy convencional y los procedimientos necesarios para utilizar la red de un operador IMS. La red de acceso utilizada es WiFi o conexión Ethernet.

Experiencia 04 – *Elementos principales de un core IMS.* Esta experiencia muestra el detalle de señalización dentro del Core. Se analiza en detalle la manipulación de los mensajes por parte de los servidores IMS. El estudio se enfoca en el registro de terminales IMS y en el establecimiento de llamadas de voz y mensajería.

Experiencia 05 – *Compatibilidad redes SIP-IMS.* En esta experiencia se combina una red SIP convencional con una red IMS. Utilizando lo aprendido en las experiencias anteriores se monta una red más compleja que permite a los usuarios de un servicio de voz IP básico basado puramente en SIP comunicarse con usuarios del core IMS. Se analizan las deficiencias que presenta esta interoperabilidad y los detalles de señalización que realizan estas plataformas para poder interactuar.

Experiencia 06 – *IMS: Servicios de valor agregado.* En esta experiencia se estudia el flujo de mensajes en un escenario compuesto por el core IMS y un servidor de aplicaciones. En general, el cliente es capaz de gatillar servicios de valor agregado de acuerdo al perfil de su subscripción en la red IMS a la que pertenece. Una característica importante es que el cliente independientemente de donde esté puede utilizar sus servicios, incluso si está conectado a la red de otro operador.

Experiencia 07 – *Calidad de Servicio en IMS - Roaming.* Las pruebas realizadas en esta experiencia muestran la interacción de un servidor P-CSCF con la plataforma de políticas de QoS conformada por los servidores PCRF y PCEF. Se realizan pruebas de funcionamiento y ruteo de mensajes en escenarios en que las condiciones de calidad de servicio se alteran provocando la denegación de servicio al cliente y la generación de alarmas. Se plantea adicionalmente la interacción entre dos dominios IMS para probar la característica de *roaming* y la sesión inter-dominios.

3.1.3.1. Matriz de contenidos

El cruce de contenidos con cada experiencia se muestra en la tabla 3.1

Materias	Nombre Experiencia	Instalación de red de referencia 00	Servidor SIP proxy 01	Red SIP - Detalle de Señalización 02	P-CSCF 03	Elementos de un Core IMS 04	Roaming - compatibilidad redes SIP-IMS 05	Servicios de valor agregado 06	Calidad de servicio - Roaming 07
Redes locales		x							
DNS		x							
NAT		x							
Sesión SIP			x	x					
Diálogo SIP			x	x					
Componentes de un mensaje SIP			x	x					
Comportamiento de UA en diálogos SIP			x	x					
Ruteo de mensajes				x					
Servidores SIP		x	x	x				x	
Proxy			x	x					
Registrar									
Location Register									
Cliente SIP		x							
Servidores IMS		x			x	x	x		
Extensiones SIP en IMS					x	x	x		
Ruteo de mensajes IMS					x	x	x		
Descubrimiento de punto de entrada						x	x		x
Registro						x	x		
Asignación de Serving CSCF						x			
Autentificación IMS						x			
Mecanismos de seguridad						x	x		x
Sesión IMS					x	x	x		
Identidades de UA					x				
Ruteo de peticiones					x	x			
Compresión								x	
Medios								x	
Reserva de recursos									x
Control de medios									x
Cobros									
Finalización de sesión					x	x	x		

Tabla 3.1: Matriz de contenidos del curso.

3.2. Laboratorio de pruebas de un Core IMS

El objetivo es construir un core IMS. La construcción se realiza de manera modular, es decir, se agrupan las componentes básicas que le dan funcionalidad al core según los estándares. Los componentes del core se integran de forma progresiva. En primer lugar se pone en funcionamiento una red de servidores SIP, a modo de referencia para la implementación posterior del core IMS. Las etapas a seguir se describen a continuación.

Diseño: Se describe el diseño de red y los procesos a realizar para la construcción del core IMS y la creación

de un laboratorio docente. Se define la topología de red y sus componentes.

Búsqueda de herramientas: Componentes de hardware y software necesarios para montar la plataforma, de acuerdo al diseño previo.

Construcción: Instalación, configuración e integración del Core. Se entiende por integración como la comunicación entre todos los componentes del sistema.

Pruebas: Descripción de las actividades para verificar el funcionamiento. Utilización de herramientas de software.

3.2.1. Diseño de red de referencia

En la red base (figura 3.1) se instalan los servidores SIP e IMS donde se realizan las pruebas. Está compuesta por dos segmentos de red. En el segmento 1 se encuentran las máquinas clientes, es decir, donde alojan por ejemplo los softphones. Además estas máquinas operan como terminales de acceso y mantención a los servidores remotos. También en este segmento está ubicado el servidor de pruebas llamado *IMSlab01*, que es el componente principal del laboratorio de pruebas. El segmento 2 está compuesto por los servidores DNS, SIP, IMS y de bases de datos.

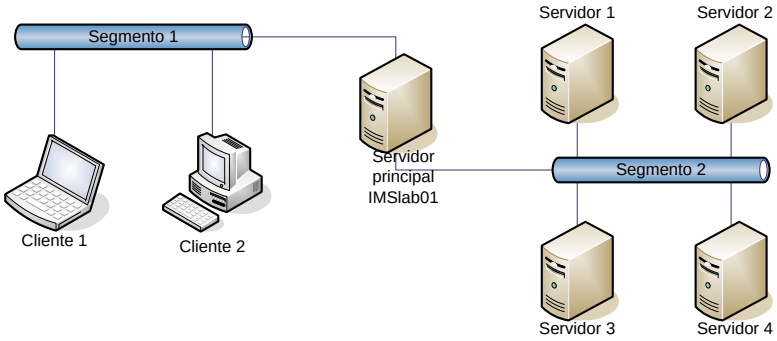

Figura 3.1: Esquema de red de referencia.

Debido a que no se cuenta con una cantidad suficiente de máquinas se opta por construir una red virtual para integrar el segmento 2. Se proponen dos alternativas para implementar este segmento. La primera es utilizando máquinas virtuales y la segunda es integrando en un computador único toda la plataforma. La topología de red es distinta entre los dos escenarios pero el comportamiento de los servidores SIP es idéntico en términos de la lógica de ruteo.

En el caso de utilización de máquinas virtuales (fig. 3.2) el host *IMSlab01* actúa como un proxy y accede a la red 172.16.231.213 a través la interfaz física *eth0* y a la red 10.111.111.0 mediante la interfaz virtual *qtap0*. En esta red virtual se disponen cuatro máquinas, o más si es necesario, las cuales son utilizadas para instalar los servidores *registrar*, *location register*, S-CSCF, I-CSCF, entre otros, de acuerdo a la configuración que se necesite.

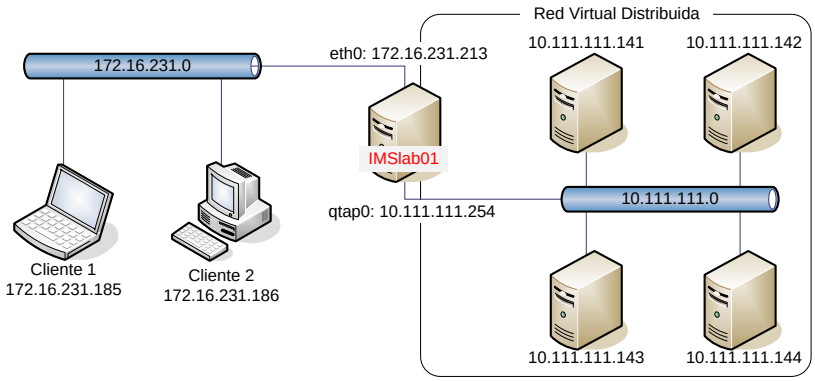

Figura 3.2: Primera opción de implementación de la red de referencia. Se utilizan máquinas virtuales para disponer un escenario de red distribuida.

Para la segunda opción, se dispone de una red de pruebas integrada. La máquina *IMSlab01* aloja cada uno de los servidores, diferenciados por el puerto de acceso. La figura 3.3 muestra esta configuración con un segmento de red único. De esta forma es posible ejecutar múltiples instancias de un servidor SIP o IMS siempre y cuando se configuren para que utilicen distintos puertos de comunicación UDP o TCP. La ventaja de esta alternativa es que al estar todo en una misma máquina, la plataforma adquiere portabilidad permitiendo instalarla en otros sistemas.

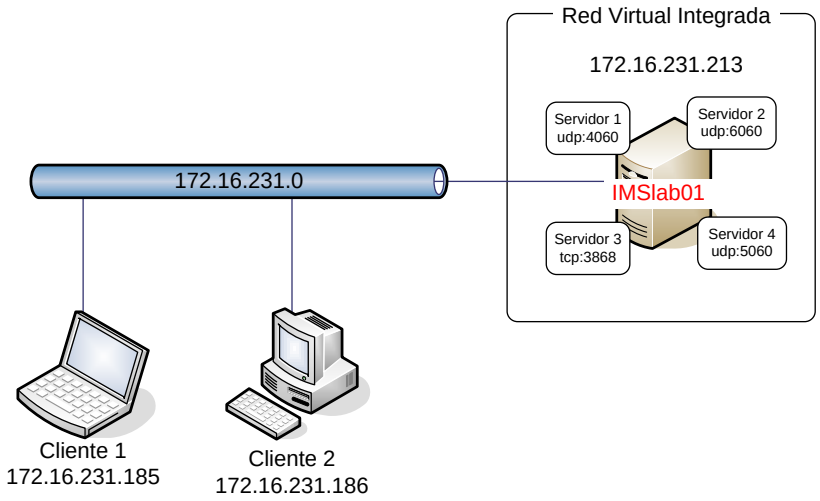

Figura 3.3: Segunda opción de implementación de la red de referencia. Los servidores se integran en un mismo computador diferenciados por el puerto de comunicación.

3.2.1.1. Servidores SIP

En esta etapa se realiza un montaje de servidores SIP basados en *OpenSer*. El montaje se ejecuta secuencialmente, partiendo por la configuración por defecto hasta llegar a una configuración más compleja. La figura 3.4 muestra el esquema de red utilizado.

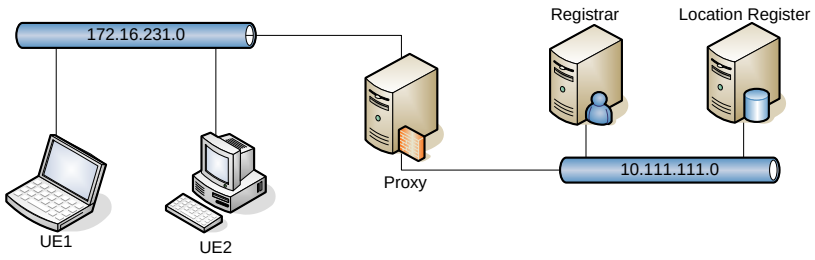

Figura 3.4: Esquema de red servidores SIP.

3.2.1.2. Servidores IMS

Los componentes (entidades) básicos que conforman la plataforma IMS se muestran en la figura 3.5. Se utilizan 4 nodos donde corren los servidores CSCF y HSS.

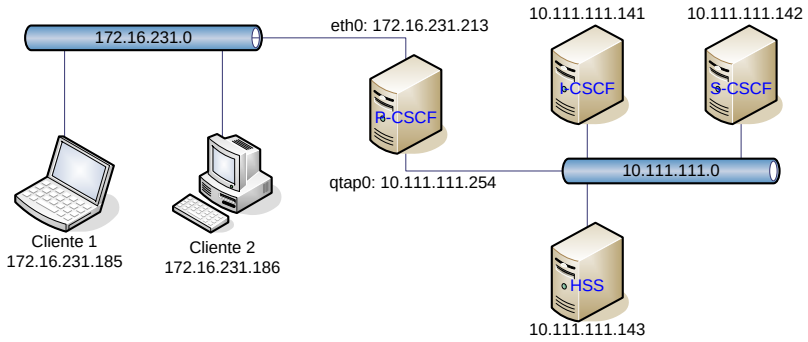

Figura 3.5: Diseño de red del Core IMS.

3.2.2. Materiales y herramientas

Se presenta en este apartado las herramientas a utilizar tanto en la construcción del core como en la obtención de resultados en la etapa de pruebas.

1. **Herramientas de Hardware**

   - 3-4 Computadores de escritorio
   - Conexión de red alámbrico/inalámbrico
   - Router
   - Teléfonos SIP inalámbricos
   - Red de alimentación de 220V

2. **Herramientas de Software**

   - Sistemas Operativos. Linux (Ubuntu), Windows XP.
   - Virtualización Qemu. Soporte para generar una red de clientes y servidores mas amplia.
   - Compiladores C: Gcc, Java: JDK 1.5, ant.
   - Servidores SIP. Openser.
   - Core IMS. OpenIMSCore.

- Administración
  - Mysql
  - Apache
  - PHPMyAdmin
- Clientes SIP. X-lite, OpenWengo, BolSIP.
- Clientes IMS. UCT IMS Client, OpenICLite, IMSCommunicator.
- Análisis - Pruebas.
  - Wireshark
  - tcpdump.
  - Herramientas Linux para despliegue de red: ssh, dnslookup, ping, etc.
  - SIP Scenario

3.2.3. Instalación y configuración servidores SIP

Un servidor SIP puede comportarse de distintas formas dependiendo de como esté configurado. En esta etapa se configura un servidor SIP actuando como Proxy. Luego se configura un servidor Registrar. El objetivo es lograr que los usuarios puedan comunicarse a través de ellos. Para simplificar la implementación los servidores y los usuarios están ubicados dentro de una misma red local.

Con esta implementación se logra poner en marcha una plataforma de comunicación de telefonía IP básica, además de mensajería instantánea y video llamadas. Finalmente, se incluye un servidor de bases de datos que permite autentificar a los usuarios con el servicio de telefonía IP. La figura 3.4 muestra el diseño de referencia de la red.

Configuración Global: Para esta etapa se utiliza el software *OpenSer* que provee las funcionalidades de un servidor SIP. Este servidor está compuesto por un núcleo que otorga las capacidades básicas para el manejo de mensajes SIP, y por módulos que agregan otras características al núcleo. Para integrar los módulos con el núcleo, además de definir el comportamiento del servidor SIP en base a estos módulos, se utiliza un archivo de configuración llamado `openser.cfg`.

La estructura de dicho archivo de configuración se describe a continuación:

1. Sección de definiciones globales.
2. Sección de módulos
3. Sección de configuración de módulos.
4. Bloque principal de ruteo.
5. Bloques secundarios de ruteo.
6. Bloque de ruteo de respuestas
7. Bloque de ruteo de fallas.

3.2.4. Instalación del Core

Se procede con la integración del core IMS. Las etapas se muestran a continuación. El detalle de la instalación se muestra en el anexo **??**.

Red virtual: En el caso del escenario distribuido se utiliza la herramienta *qemu* para instalar las máquinas virtuales. Se requieren recursos de disco y memoria en el computador principal. Utilizando *vdeqemu* se levanta un switch virtual para agregar conectividad IP sobre Ethernet a las nuevas máquinas.

Lo anterior no es necesario realizar si se opta por utilizar el escenario de red de pruebas integrada (fig. 3.3).

Servidor DNS: Mediante el software *Bind* se instala un servidor DNS en la máquina principal *IMSlab01*. El dominio definido para la red virtual es *playsip.lab* y el nombre de las máquinas es *pcscf.playsip.lab* (172.16.231.213), *icscf.playsip.lab* (10.111.111.141), *scscf.playsip.lab* (10.111.111.142) y *hss.playsip.lab* (10.111.111.143). Estas direcciones IP pueden variar si se utiliza el escenario integrado en una sola máquina. En ese caso la única dirección que se utiliza para todos los servidores es 172.16.231.213 (se distinguen por el puerto UDP que ocupan).

CSCF Se realiza la instalación del software OpenIMSCore. Es necesario compilar dicho software con gcc. Dependiendo de la configuración el servidor CSCF funcionará como Proxy, Interrogating o Serving CSCF. Se hace una copia de cada módulo en cada una de las máquinas asignadas.

Base de Datos: Tanto el I-CSCF como el HSS necesitan acceder a una base de datos. Se instala MySQL en el computador principal. Con esto se pretende mantener un único servidor de base de datos, así es más fácil administrar los datos de manera centralizada. Como existe completa conectividad es trivial realizar la conexión desde los hosts corriendo el core hacia el servidor de base de datos.

HSS: La suite FHoSS (parte de OpenIMSCore) se copia en la máquina virtual asignada y se compila con Java. Luego se define en los archivos de configuración la ubicación de la base de datos donde se almacenan los suscriptores, entre otras cosas.

Una vez finalizadas estas actividades el core IMS se encuentra listo para funcionar. El detalle de ejecución de cada uno de los componentes aparece en el anexo **??**.

3.2.5. Planificación de pruebas

Luego de tener el core IMS y los servidores SIP operativos se realizan las pruebas de funcionamiento. En primer lugar se analizan actividades básicas de señalización SIP. Luego se verifica el comportamiento de los servidores y clientes frente a las sesiones multimedia a entablar (flujo de datos, intercambio de codecs, compatibilidad). Además se aplican pruebas de mensajes SIP a los servidores, para analizar el tipo de respuestas.

3.2.5.1. Pruebas SIP

Prueba	Nombre	Objetivo	Resultado Esperado
1	Registro	Estudiar los mensajes de registro. Revisión de headers SIP en REGISTER y sus respuestas.	Flujo de mensajes de acuerdo al estándar
2	Invitación	Realizar llamadas entre clientes. Mensajes INVITE, 180, 200, entre otros.	Flujo de mensajes de acuerdo al estándar.
3	Re-registro	Cliente actualiza su registro contra el servidor.	Análisis de re-registro cuando se cursa una llamada. Comportamiento del cliente y servidor.
4	Flujo de media	Transmitir datos multimedia	Entablar una conversación dentro de una llamada.
5	Mensajería	Transmisión de mensajería de texto. Verificar medios de transmisión.	Mensajes sobre protocolo.

Tabla 3.2: Pruebas SIP.

3.2.5.2. Pruebas en Core IMS

Prueba	Nombre	Objetivo	Resultado Esperado
1	Registro	Estudiar los mensajes de registro. Revisión de headers SIP e IMS en REGISTER, SUBSCRIBE 401 y 200.	Flujo de mensajes de acuerdo al estándar.
2	Invitación	Realizar llamadas entre clientes. Mensajes INVITE, UPDATE, PRACK.	Flujo de mensajes de acuerdo al estándar.
3	Flujo de media	Transmitir datos multimedia.	Entablar una conversación dentro de una llamada.
4	Mensajería	Transmisión de mensajeria de texto. Verificar medios de transmisión.	Mensajes sobre protocolo.
5	SIP-IMS	Establecer comunicación entre cliente SIP e IMS.	Obtener llamadas exitosas. Analizar comportamiento de servidores proxy.
6	IMS-SIP	Establecer comunicación entre cliente SIP e IMS.	Obtener llamadas exitosas. Analizar comportamiento de servidores proxy.
7	Roaming	Registro de un cliente fuera de la red home.	Obtener registro exitoso. Cambios en header respecto del registro local.

Tabla 3.3: Pruebas IMS.

Capítulo 4

Resultados

En este capítulo se pone en evidencia el resultado de las pruebas realizadas, descritas en el capítulo anterior. Primero aparecen las pruebas enfectuadas a los servidores SIP. Luego se muestra el resultado y análisis de las pruebas en el core IMS. Finalmente se dispone de una guía docente que forma parte del set de experiencias elaborado para el curso de laboratorio.

4.1. Red de pruebas

La instalación de la red de pruebas se realizó siguiendo la metodología planteada. Fue posible montar la red objetivo incluyendo todas sus componentes. No obstante, para efectos de obtención de resultados en la plataforma se optó por utilizar un esquema integrado en desmedro del sistema distribuido. La razón de esto fue la pérdida de rendimiento al ejecutar máquinas virtuales todas en un mismo sistema. Además hubo problemas de estabilidad en los servidores CSCF, especialmente en el S-CSCF que paraba su funcionamiento sin motivos aparentes. Por otra parte, en la pruebas de *roaming* es necesario comunicar los CSCF de dos dominios distintos alojados en máquinas independientes. Por ejemplo, la comunicación entre el servidor S-CSCF del dominio *playsip.lab* y el I-CSCF de *santiago.lab* debe ser directa y como en la configuración de máquinas virtuales el único punto de contacto es el P-CSCF, el resto de los CSCF permanecen escondidos entre sí por estar en segmentos de red distintos (figura 4.1). La solución es entonces distinguir cada uno de los servidores del Core por los puertos UDP de las máquinas estando todos en el mismo segmento (figura 4.2). Esto genera problemas de seguridad en un ambiente real puesto que todos los servidores están visibles en la red. No obstante, una configuración de NAT (inclusión de routers) torna más compleja la administración del sistema, que para efectos docentes no resulta realmente útil.

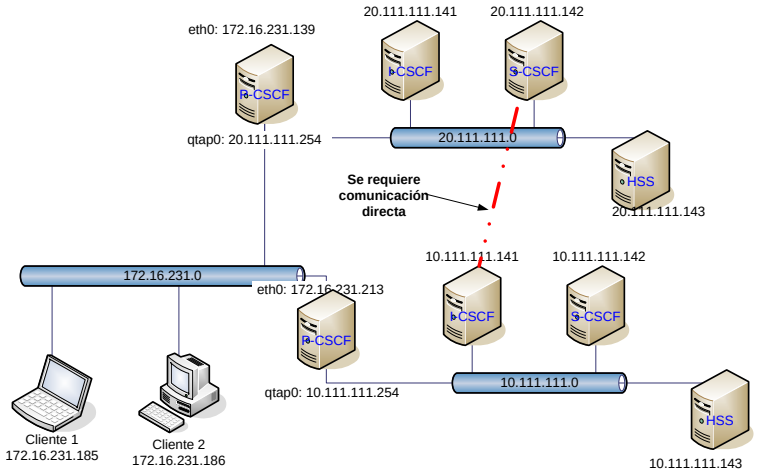

Figura 4.1: Red objetivo inicial. No cumple con los requerimientos de funcionamiento.

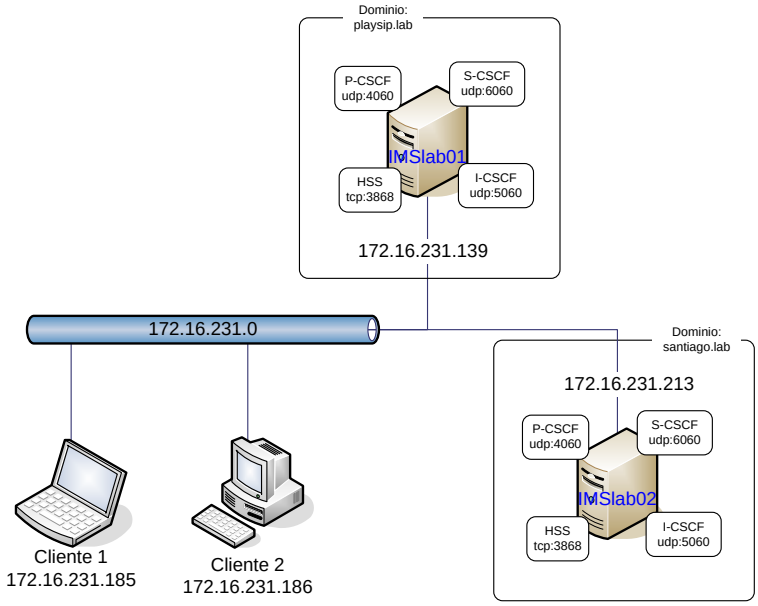

Figura 4.2: Red objetivo final. Utilizada para las pruebas.

4.2. Pruebas SIP

En esta sección se muestrán los resultados de señalización SIP en el registro e inicio de sesión, junto con el análisis de flujo multimedia y mensajería instantánea.

4.2.1. Registro de un cliente

El cliente SIP se registra contra el servidor. La figura 4.3 muestra el registro del cliente utilizando autentificación. A continuación se muestran los 4 mensajes de registro que intercambian el cliente y el proxy.

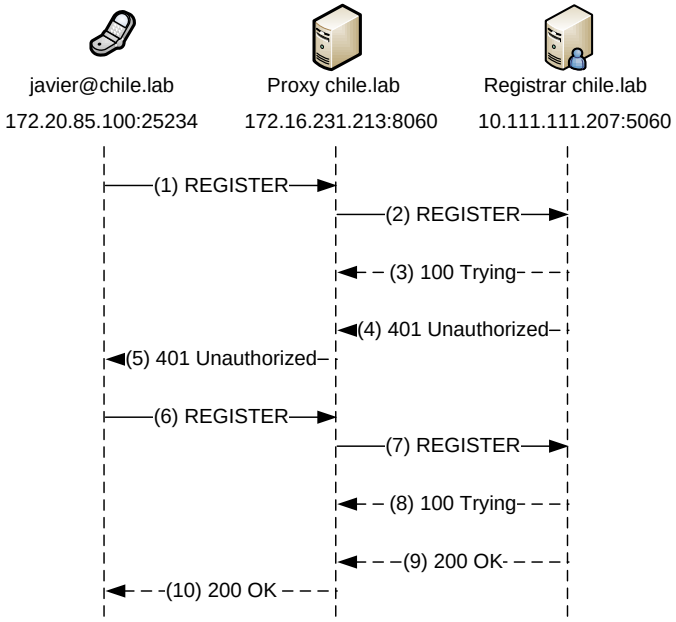

Figura 4.3: Registro SIP con autentificación.

```
REGISTER sip:chile.lab SIP/2.0
Via: SIP/2.0/UDP 172.20.85.100:65232;
    branch=z9hG4bK-d87543-0746bb3c7b390a52-1--d87543-
Max-Forwards: 70
Contact: <sip:javier@172.20.85.100:65232;rinstance=0a1ea3d7187617bd>
To: "javier"<sip:javier@chile.lab>
From: "javier"<sip:javier@chile.lab>;tag=f061bc12
Call-ID: N2U1ZmFhNDQ2ZWEwZDNlMTRiNTBiOTJhYWFjYWQ0Yjc.
CSeq: 1 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 0
```

El cliente se registra con el servidor proxy *chile.lab* indicado en el *Request-URI*. En la configuración del cliente se indica explícitamente la dirección IP del servidor, por lo que no es necesario utilizar un mecanismo DNS para encontrar el dominio.

Se incluye el encabezado `Via`, que indica la dirección donde debe ser respondida esta petición (IP y puerto del cliente). Además el cliente incluye su dirección de contacto para ser localizado en futuras peticiones (por ejemplo si otro cliente quiere establecer una sesión con él) en el header `Contact`.

En los encabezados `To` y `From` se indica la identidad pública del cliente. Esta información la utiliza el proxy para identificar a los usuarios ante una llamada entrante.

El campo `Call-ID` corresponde a un identificador de llamada. Junto con el header `CSeq` y el parámetro `tag` definen el diálogo.

Adicionalmente el cliente indica el tiempo por el cual el URI registrado es válido con el header `Expires`. `Allow` indica los métodos soportados por el cliente y `User-Agent` el nombre del cliente (típicamente el nombre del software).

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 172.20.85.100:65232;
    branch=z9hG4bK-d87543-0746bb3c7b390a52-1--d87543-
To: "javier"<sip:javier@chile.lab>;tag=f5e6af3db662f272dd3336f571144ca8.ac67
```

```
From: "javier"<sip:javier@chile.lab>;tag=f061bc12
Call-ID: N2U1ZmFhNDQ2ZWEwZDNlMTRiNTBiOTJhYWFjYWQ0Yjc.
CSeq: 1 REGISTER
WWW-Authenticate: Digest realm="chile.lab",
    nonce="48a35676e484024f53b12ac8ec05075c3c5cc41f"
Server: OpenSER (1.2.2-notls (i386/linux))
Content-Length: 0
```

Luego de que el proxy reenvía la petición de registro al servidor dedicado para esta tarea (el servidor *Registrar*) responde denegando el registro adjuntando las credenciales de autentificación necesarias. En este caso el registrar autentifica a los clientes utilizando el método Digest MD5.

```
REGISTER sip:chile.lab SIP/2.0
Via: SIP/2.0/UDP 172.20.85.100:65232;
    branch=z9hG4bK-d87543-7a069a40442fc869-1--d87543-
Max-Forwards: 70
Contact: <sip:javier@172.20.85.100:65232;rinstance=0a1ea3d7187617bd>
To: "javier"<sip:javier@chile.lab>
From: "javier"<sip:javier@chile.lab>;tag=f061bc12
Call-ID: N2U1ZmFhNDQ2ZWEwZDNlMTRiNTBiOTJhYWFjYWQ0Yjc.
CSeq: 2 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
User-Agent: X-Lite release 1011s stamp 41150
Authorization: Digest username="javier",realm="chile.lab",
    nonce="48a35676e484024f53b12ac8ec05075c3c5cc41f",
    uri="sip:chile.lab",response="293e492d591cdc76fed1eb2125d42264",
    algorithm=MD5
Content-Length: 0
```

Ante esta petición el cliente vuelve a intentar el registro con las credenciales de seguridad requeridas (*username*, *password*, *realm*). Como se trata de una nueva petición el contador *Cseq* es incrementado.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.20.85.100:65232;
    branch=z9hG4bK-d87543-7a069a40442fc869-1--d87543-
To: "javier"<sip:javier@chile.lab>;tag=f5e6af3db662f272dd3336f571144ca8.8789
From: "javier"<sip:javier@chile.lab>;tag=f061bc12
Call-ID: N2U1ZmFhNDQ2ZWEwZDNlMTRiNTBiOTJhYWFjYWQ0Yjc.
CSeq: 2 REGISTER
Contact: <sip:javier@172.20.85.100:65232;rinstance=0a1ea3d7187617bd>;expires=3600
Server: OpenSER (1.2.2-notls (i386/linux))
Content-Length: 0
```

Esta vez el cliente es aceptado por el *Registrar* enviando la respuesta `200 OK`. En ese momento el cliente está registrado.

4.2.2. Inicio de sesión (llamada)

La figura 4.4 ilustra el flujo de mensajes en el establecimiento de una sesión SIP. Dos usuarios de distintos dominios se comunican a través de sus respectivos servidores proxy.

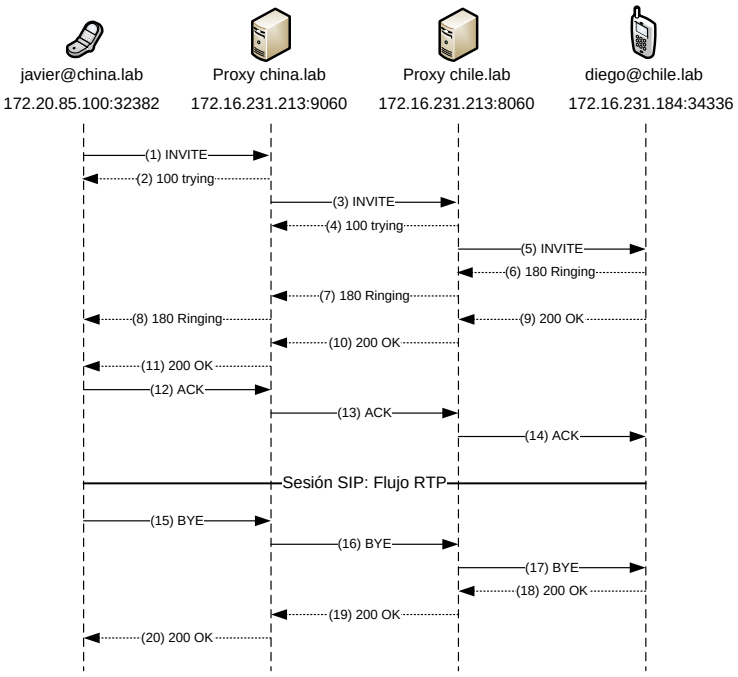

Figura 4.4: Sesión SIP.

```
INVITE sip:diego@chile.lab SIP/2.0
Via: SIP/2.0/UDP 172.20.85.100:32382;
    branch=z9hG4bK-d87543-5e636c6edf52e653-1--d87543-
Max-Forwards: 70
Contact: <sip:javier@172.20.85.100:32382>
To: "diego@chile.lab"<sip:diego@chile.lab>
From: "javier"<sip:javier@china.lab>;tag=9555100d
Call-ID: OWQ5YzI1ZTg1MDk5MDZiYTQwMDA4YjFkNmRjMGVjNzY.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Content-Type: application/sdp
User-Agent: X-Lite release 1011s stamp 41150
```

El cliente *javier@china.lab* invita a una sesión de voz a *diego@chile.lab* (mensaje (1)) . El campo `Max-Forwards` indica el número máximo de nodos que puede atravesar el mensaje; se utiliza para evitar que el mensaje permanezca en la red indefinidamente en caso de loops.

```
INVITE sip:diego@chile.lab SIP/2.0
Record-Route: <sip:172.16.231.213:9060;lr=on;ftag=9555100d>
Via: SIP/2.0/UDP 172.16.231.213:9060;
    branch=z9hG4bK699a.5a87ddc5.0
Via: SIP/2.0/UDP 172.20.85.100:32382;
    branch=z9hG4bK-d87543-5e636c6edf52e653-1--d87543-
Max-Forwards: 69
Contact: <sip:javier@172.20.85.100:32382>
To: "diego@chile.lab"<sip:diego@chile.lab>
From: "javier"<sip:javier@china.lab>;tag=9555100d
Call-ID: OWQ5YzI1ZTg1MDk5MDZiYTQwMDA4YjFkNmRjMGVjNzY.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Content-Type: application/sdp
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 372
P-hint: outbound
```

El proxy *china.lab* direcciona el mensaje (2) hacia el servidor *chile.lab* luego de buscar este dominio utilizando DNS. Agrega el campo `Record-Route` indicando que las futuras peticiones para esta sesión

deben pasar obligatoriamente por este proxy (el campo `Via` es usado solamente para las respuestas a la petición actual).

```
INVITE sip:diego@172.16.231.184:34336;rinstance=3aa4598645df2824 SIP/2.0
Record-Route: <sip:172.16.231.213:8060;lr=on;ftag=9555100d>
Record-Route: <sip:172.16.231.213:9060;lr=on;ftag=9555100d>
Via: SIP/2.0/UDP 172.16.231.213:8060;branch=z9hG4bK699a.65581493.0
Via: SIP/2.0/UDP 172.16.231.213:9060;branch=z9hG4bK699a.5a87ddc5.0
Via: SIP/2.0/UDP 172.20.85.100:32382;
    branch=z9hG4bK-d87543-5e636c6edf52e653-1--d87543-
Max-Forwards: 68
Contact: <sip:javier@172.20.85.100:32382>
To: "diego@chile.lab"<sip:diego@chile.lab>
From: "javier"<sip:javier@china.lab>;tag=9555100d
Call-ID: OWQ5YzI1ZTg1MDk5MDZiYTQwMDA4YjFkNmRjMGVjNzY.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Content-Type: application/sdp
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 372
P-hint: outbound
P-hint: usrloc applied
```

El Request-URI cambia de `INVITE sip:diego@chile.lab` a `INVITE sip:diego@172.16.231.184:34336` en el mensaje (3). Esto ocurre porque el proxy traduce el dominio de Diego a la dirección IP que él indicó en el header `Contact` al momento de registrarse. De la misma forma el proxy *chile.lab* agrega el header `Record-Route` para permanecer en la ruta de la sesión entre Javier y Diego.

Despúes de recibir el INVITE el UA envía la respuesta 180 Ringing (mensaje (4)) a la espera de que el cliente conteste la llamada.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.231.213:8060;branch=z9hG4bK699a.65581493.0
Via: SIP/2.0/UDP 172.16.231.213:9060;branch=z9hG4bK699a.5a87ddc5.0
Via: SIP/2.0/UDP 172.20.85.100:32382;
    branch=z9hG4bK-d87543-5e636c6edf52e653-1--d87543-
Record-Route: <sip:172.16.231.213:8060;lr=on;ftag=9555100d>
Record-Route: <sip:172.16.231.213:9060;lr;ftag=9555100d>
Contact: <sip:diego@172.16.231.184:34336;rinstance=3aa4598645df2824>
To: "diego@chile.lab"<sip:diego@chile.lab>;tag=75158706
From: "javier"<sip:javier@china.lab>;tag=9555100d
Call-ID: OWQ5YzI1ZTg1MDk5MDZiYTQwMDA4YjFkNmRjMGVjNzY.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Content-Type: application/sdp
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 374
```

El cliente contesta la llamada y envía `200 OK`. Este mensaje es ruteado hasta alcanzar el UE originante. Posteriormente el UA de Javier envía el acuso de recibo `ACK` (mensaje (12)) lo que determina el inicio de la sesión.

Se observa la aparición del campo *Route* que contiene la información indicada en *Record-Route* de los mensajes previos. Esto permite que el mensaje sea conducido por una ruta ya conocida.

```
ACK sip:diego@172.16.231.184:34336;rinstance=3aa4598645df2824 SIP/2.0
Via: SIP/2.0/UDP 172.20.85.100:32382;branch=z9hG4bK-d87543-4a4b6b72431ec407-1--d87543-
Max-Forwards: 70
Route: <sip:172.16.231.213:9060;lr;ftag=9555100d>
Route: <sip:172.16.231.213:8060;lr=on;ftag=9555100d>
Contact: <sip:javier@172.20.85.100:32382>
To: "diego@chile.lab"<sip:diego@chile.lab>;tag=75158706
```

```
From: "javier"<sip:javier@china.lab>;tag=9555100d
Call-ID: OWQ5YzI1ZTg1MDk5MDZiYTQwMDA4YjFkNmRjMGVjNzY.
CSeq: 1 ACK
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 0
```

Cuando los usuarios terminan la conversación uno de ellos envía un `BYE` (mensaje (15)) indicando el fin de la sesión. Este mensaje es respondido con un `200 OK` y la sesión se termina.

```
BYE sip:diego@172.16.231.184:34336;rinstance=3aa4598645df2824 SIP/2.0
Via: SIP/2.0/UDP 172.20.85.100:32382;branch=z9hG4bK-d87543-6562fe0c3e44d743-1--d87543-
Max-Forwards: 70
Route: <sip:172.16.231.213:9060;lr;ftag=9555100d>
Route: <sip:172.16.231.213:8060;lr=on;ftag=9555100d>
Contact: <sip:javier@172.20.85.100:32382>
To: "diego@chile.lab"<sip:diego@chile.lab>;tag=75158706
From: "javier"<sip:javier@china.lab>;tag=9555100d
Call-ID: OWQ5YzI1ZTg1MDk5MDZiYTQwMDA4YjFkNmRjMGVjNzY.
CSeq: 2 BYE
User-Agent: X-Lite release 1011s stamp 41150
Reason: SIP;description="User Hung Up"
Content-Length: 0
```

4.2.2.1. Intercambio de multimedia

En el cuerpo de los mensajes SIP `INVITE` y `200 OK` se envían los descriptores de la sesión multimedia con el fin de acordar las direcciones donde se envía el flujo de voz y los codecs utilizados. El SDP que envía el cliente originario (*javier@china.lab*) es el siguiente.

```
v=0 r
o=- 5 2 IN IP4 172.20.85.100
s=CounterPath X-Lite 3.0
c=IN IP4 172.20.85.100
t=0 0
m=audio 26724 RTP/AVP 107 119 100 106 0 105 98 8 101
a=fmtp:101 0-15
a=rtpmap:107 BV32/16000
a=rtpmap:119 BV32-FEC/16000
a=rtpmap:100 SPEEX/16000
a=rtpmap:106 SPEEX-FEC/16000
a=rtpmap:105 SPEEX-FEC/8000
a=rtpmap:98 iLBC/8000
a=rtpmap:101 telephone-event/8000
a=sendrecv
```

El flujo a transmitir se indica con *m=audio*. Los codecs se describen con la opción *a=rtpmap*. Por su parte, el cliente llamado (*diego@chile.lab*) responde con el SDP de más abajo. Ambos clientes utilizan un orden de prioridad de los codecs indicado en el campo *m=audio* y acuerdan transmitir con el codec 107 BV32/16000.

```
v=0
o=- 5 2 IN IP4 172.16.231.184
s=CounterPath X-Lite 3.0
c=IN IP4 172.16.231.184
t=0 0
m=audio 39462 RTP/AVP 107 119 100 106 0 105 98 8 101
a=fmtp:101 0-15
a=rtpmap:107 BV32/16000
a=rtpmap:119 BV32-FEC/16000
```

```
a=rtpmap:100 SPEEX/16000
a=rtpmap:106 SPEEX-FEC/16000
a=rtpmap:105 SPEEX-FEC/8000
a=rtpmap:98 iLBC/8000
a=rtpmap:101 telephone-event/8000
a=sendrecv
```

El contenido de un paquete RTP es el siguiente. En él se indican los números de secuencia, el tipo de datos (*ITU-T G.711 PCMU* en este caso) y el medio codificado (*Payload*).

```
Real-Time Transport Protocol
    [Stream setup by SDP (frame 100)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    1... .... = Marker: True
    Payload type: ITU-T G.711 PCMU (0)
    Sequence number: 2613
    [Extended sequence number: 68149]
    Timestamp: 1230400
    Synchronization Source identifier: 0x3ddb67f0 (1037789168)
    Payload: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF...
```

4.2.3. Mensajería

La mensajería instantánea se transmite utilizando el método MESSAGE siempre y cuando el cliente lo soporte (como en esta prueba). Los eventos de mensajería se indican en el cuerpo del mensaje SIP utilizando XML. El cuadro siguiente muestra un mensaje de aviso indicando que el cliente Javier está escribiéndole a Diego. El cliente SIP muestra esta información al usuario siempre y cuando soporte el mecanismo; en caso contrario no realiza ninguna acción. El ruteo de los mensajes es similar al de un INVITE. De la misma forma la respuesta a cada mensaje es un 200 OK.

Este método no inicia un diálogo. Cada mensaje es independiente del otro, es decir no tienen una relación en el contexto de un diálogo. Los clientes diferencian cada mensaje que envían con el header `Cseq`. El encabezado `Call-ID` se mantiene constante pero son distintos entre clientes. El header `Contact` no aparece en el mensaje y por lo tanto en el Request-URI no se reemplaza el URI del dominio por la dirección IP del terminal destino.

```
MESSAGE sip:diego@chile.lab SIP/2.0
Via: SIP/2.0/UDP 172.20.85.100:32382;
    branch=z9hG4bK-d87543-da648d364c249051-1--d87543-
Max-Forwards: 70
To: "diego@chile.lab"<sip:diego@chile.lab>
From: "javier"<sip:javier@china.lab>;tag=f729fa31
Call-ID: NmQ1ZjQ2NTc4NmJjZWI5OGMxNWUyMjZkMjhlMDA1ZGM.
CSeq: 2 MESSAGE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Content-Type: application/im-iscomposing+xml
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 263

<?xml version='1.0' encoding='UTF-8'?>
<isComposing xmlns='urn:ietf:params:xml:ns:im-iscomposing'
  xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'>
    <state>active</state>
    <contenttype>text/plain</contenttype>
    <refresh>60</refresh>
</isComposing>
```

El mensaje instantáneo que el cliente envía va en el cuerpo de MESSAGE en texto plano.

```
MESSAGE sip:diego@chile.lab SIP/2.0
Via: SIP/2.0/UDP 172.20.85.100:32382;
    branch=z9hG4bK-d87543-104275228f03695d-1--d87543-
Max-Forwards: 70
To: "diego@chile.lab"<sip:diego@chile.lab>
From: "javier"<sip:javier@china.lab>;tag=f729fa31
Call-ID: NmQ1ZjQ2NTc4NmJjZWI5OGMxNWUyMjZkMjhlMDA1ZGM.
CSeq: 3 MESSAGE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Content-Type: text/plain
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 6

hola
```

4.3. Pruebas en el Core

Se describe el resultado de las pruebas de señalización en el core IMS. Se hace análisis al registro en la plataforma, inicio de una sesión multimedia, intercambio de medios, modos de operación de mensajería instantánea, subscripción a eventos y transacciones Diameter. Se muestra también la interoperabilidad entre clientes SIP e IMS, servidores de aplicación y calidad de servicio.

4.4. Curso de Laboratorio

Como resultado de las pruebas anteriores y de la metodología elaborada en el capítulo 3 se obtiene el material para crear las actividades presentes en las guías del curso. En esta sección se muestra resuelta la experiencia 04: *Elementos principales de un core IMS*. El resto del material docente aparece en el anexo A.

Capítulo 5

Conclusiones

En este capítulo se muestran las conclusiones del trabajo realizado. Se comenta sobre el alcance de los objetivos, el desarrollo del proyecto, la obtención de resultados en el marco de pruebas y desarrollo del curso de laboratorio y por último algunos comentarios finales y mención sobre trabajos futuros ligados a este proyecto.

5.1. Objetivos

El trabajo realizado demuestra el cumplimiento de los objetivos en su totalidad. A continuación se comenta sobre los objetivos general y específicos planteados y el cumplimiento de cada uno de ellos.

5.1.1. Objetivo general

El proyecto realizado fue fundamentado sobre la plataforma de redes convergentes IMS para telefonía móvil. El objetivo principal fue crear la base de un curso de laboratorio que tuviera como eje dicha plataforma. Para tal efecto fue necesario, en primer lugar, recopilar y estudiar la información disponible en los organismos de estandarización y algunos trabajos disponibles casi en su totalidad en Internet. Como el enfoque del trabajo está en una arquitectura para redes móviles se hizo una breve introducción a la evolución de la red celular desde la primera generación hasta 3G. Cabe destacar que dicha evolución está constantemente en desarrollo y presenta actualizaciones periódicamente, por lo que fue necesario definir previamente los límites del estudio. A la fecha de edición de este documento la red 3G está en funcionamiento basado en la cuarta iteración del estándar 3GPP (conocido como *3G UMTS Release 4*) en prácticamente todo el mundo. IMS hace su aparición en *Release 5* y por lo tanto el trabajo se enfoca en este conjunto de estándares en adelante.

5.1.2. Objetivos específicos

Los antecedentes necesarios para la investigación se obtuvieron oportunamente quedando en evidencia los temas más importantes en el capítulo 2 de este documento. Con esta base teórica se facilitó el desarrollo de las pruebas y experiencias prácticas que condujeron a la creación del curso.

La integración del core IMS se logró luego de una serie de pruebas de instalación que revelaron las falencias y ventajas del modelo propuesto en el capítulo 3. Se desechó la opción de virtualización de la red de pruebas puesto que hacia el sistema innecesariamente complejo. Se optó por una solución integrada en una misma máquina de forma de facilitar la portabilidad del sistema y la obtención de los flujos de llamadas en las capturas de paquetes.

El plan de pruebas desarrollado fue basado en el marco teórico planteado. Gracias a este plan fue posible estimar la complejidad de las pruebas a realizar y a la vez obtener la mayor cantidad de resultados relevantes posible.

Por último se logro efectuar la conexión entre usuarios utilizando los servicios que provee el core IMS y las plataformas de aplicación integradas a él.

Con todo lo anterior logrado con éxito se consiguió el material necesario para crear las experiencias del curso IMS. Los procedimientos para generar guías de trabajo se realizaron exitósamente generando como resultado un set de 7 experiencias prácticas con el core IMS como materia de estudio más una experiencia de instalación de la plataforma de pruebas.

5.2. Desarrollo del trabajo

El trabajo esta enfocado en el protocolo de señalización SIP, elemento eje de IMS. Puesto que gran parte de las componentes del Core IMS se comunican mediante SIP fue imperante dar a conocer sus características principales. Es así como se mostró el conjunto de nodos de red que hacen posible la comunicación además de los diálogos y sesiones SIP junto con la lógica de ruteo de mensajes.

El elemento teórico con el que se concluyó el estudio es la arquitectura IMS. Se mostró principalmente los fundamentos de por qué es necesaria la creación de una arquitectura convergente y los requerimientos que requiere el sistema relacionados con la provisión de servicios, los medios de acceso, la seguridad y la calidad de servicio. Para cumplir todos los requerimientos es necesario incluir nuevas características que enriquecen la funcionalidad de SIP, lo que se ve reflejado en la aparición de nuevos estándares.

El proceso siguiente a la documentación fue la planificación del proyecto. En el marco del curso de laboratorio se definieron la materias que serían tratadas y en base a esto se creó un plan de pruebas enfocado el el funcionamiento de los servidores SIP y el core IMS conformado por los CSCFs y HSS. Se definieron las herramientas de hardware y software necesarios en primera instancia y en el transcurso del trabajo fueron apareciendo algunas otras que complementaron el desarrollo tanto de las pruebas de plataforma como el desarrollo del curso.

Se construyó la red de pruebas basada principalmente en un segmento de red y dos máquinas servidor más dos computadores actuando como clientes del sistema. En una primera aproximación se utilizó una red de máquinas virtuales de tal forma de lograr un escenario más completo y distribuido. El objetivo de está configuración de virtualización era tener en cada una de las máquinas un nodo de red (CSCFs, HSS, Cliente) para lograr un sistema escalable. El resultado a nivel de topología de red fue satisfactorio, pero sin embargo se optó por unificar el sistema en a lo más dos máquinas para permitir una mayor versatilidad en la obtención de resultados, con lo que la solución de máquinas virtuales se desechó en la etapa final de pruebas.

Luego se dió paso a la ejecución de pruebas de señalización SIP y ruteo de mensajes en un entorno de servidores SIP convencionales. En esta etapa se reflejarían las primeras experiencias de laboratorio introductorias al curso IMS. Se hizo un análisis de los mensajes básicos del protocolo y se determinó el comportamiento de los servidores y clientes utilizando distintos escenarios. Se probó registro de clientes, inicio de sesión, autentificación de usuarios, mensajería y flujo de medios.

Una vez completadas las pruebas SIP, se efectuaron las actividades sobre el core IMS montado en la red de pruebas. Las pruebas realizadas consistieron en el registro de clientes, inicialización de sesiones de voz y mensajería. Además se analizó la interacción entre un cliente registrado en una red SIP covencional y un cliente IMS. Se efectuaron pruebas de roaming, e interacción entre dos dominios distintos, por lo que fue necesario integrar dos core IMS en la red de pruebas. Finalmente se dio paso a la provisión de servicios de valor agregado y la ejecución de servidores de políticas de QoS. Con la extensión de estas pruebas fue posible ir generando las experiencias de laboratorio del curso.

En paralelo a las pruebas sobre la plataforma se fueron creando cada una de las experiencias del curso del laboratorio. El curso se compuso finalmente de 7 experiencias que van desde los aspectos básicos del protocolo SIP, pasando por los componentes principales del core IMS, y terminando con servicios de valor agregado y QoS.

5.3. Pruebas de señalización SIP

Esta etapa muestra la integración de una red SIP. Se logró en plenitud realizar el proceso de registro de clientes contra los servidores SIP Proxy y Registrar autentificando mediante *Digest MD5*. Los mensajes SIP analizados fueron *REGISTER*, *200 OK*, *100 Trying* y *401 Unauthorized*. Este mecanismo de registro permite a los servidores de dominio conocer la ubicación de sus clientes para poder contactarlos en el caso de un inicio de sesión.

De la misma forma se concretó una sesión SIP entre dos clientes registrados en distintos dominios. En esta parte se estudió el mecanismo con que se rutean los mensajes de inicio de sesión tales como *INVITE*, *180 Ringing*, *200 OK* y *ACK* y los de término de sesión *BYE* y *200 OK*.

Una funcionalidad importante para poder lograr la comunicación entre los dos dominios fue la implementación de un servidor DNS que permite localizar de manera sencilla a los clientes utilizando simplemente la dirección URI de cada uno. Se decidió no incluir el resultado del descubrimiento DNS de los dominios ya que se aleja del marco de estudio.

También se incluye un análisis sobre el tipo de medios que trafican los clientes una vez entablada la sesión. Un alcance importante de este proceso es que los servidores SIP no intervienen en él, tratándose netamente de una comunicación entre clientes (*peer to peer*). Para lograr esta comunicación se hace uso del protocolo SDP que aparece en el cuerpo de los mensajes SIP, de una forma similar a un mensaje de correo electrónico.

5.4. Pruebas en el core IMS

El resultado de esta etapa fue satisfactorio donde se recrearon los escenarios estándar de inicio de sesión y registro de usuarios. En el caso del registro se verificó la lógica estándar cursada para autentificar a los clientes incluyendo el comportamiento de cada uno de los servidores al rutear mensajes SIP y Diameter. En esta etapa también se verificó la subscripción del cliente al evento de registro.

La sesión multimedia mostrada corresponde al escenario más complejo en términos de nodos involucrados. Ambos clientes se encuentran haciendo roaming habiendo un total de cuatro dominios distintos en la prueba. Se realizó un análisis de ruteo de mensajes poniendo atención en cada uno de los encabezados involucrados y las modificaciones realizadas por cada uno de los nodos. El uso de la extensión *preconditions* fue una diferencia notable respecto de una sesión SIP convencional. Se observó el intercambio de multimedia sobre el protocolo RTP para el caso de voz y video y sobre MSRP para mensajería instantánea, todos ellos definidos con los descriptores SDP en el inicio de la sesión. Adicionalmente, se ejecutó una prueba de interoperabilidad entre un cliente SIP e IMS, los resultados arrojados demostraron un comportamiento similar a una sesión SIP estándar.

Se probaron varios clientes IMS y se optó finalmente por realizar las pruebas con *UCT IMS Client* que fue el que se desempeñó de mejor manera en términos de estabilidad, apego al estándar 3GPP y funcionalidades multimedia.

Luego se continuó con pruebas en servidores de aplicaciones conectados al core. Se proporcionó los servicios de *video streaming* y presencia para mensajería instantánea. El estudio de resultados se enfocó en la subscripción de servicios, el ruteo de mensajes SIP/XML y flujo multimedia.

Finalmente, se analizó la inclusión al sistema de una plataforma de control de calidad de servicio poniendo enfásis en el comportamiento general del core IMS frente a sucesos relacionados con la reserva de recursos multimedia y pérdida de comunicación. Dicha plataforma de control de políticas QoS interactúa con el servidor P-CSCF de manera similar como lo hacen los nodos CSCF y HSS usando el protocolo Diameter.

5.5. Experiencias del laboratorio docente

Los contenidos de las experiencias de laboratorio creadas están basados plenamente en los resultados recogidos. La metodología de enseñanza parte con los conceptos básicos de señalización SIP para luego ir aumentando la dificultad hasta llegar al estudio del core IMS. El nivel de complejidad del core es notablemente mayor comparado con una red SIP convencional ya que participan varios nodos, cada uno con características bien definidas.

En cada una de las experiencias se otorga un fuerte enfoque en la señalización SIP y sus extensiones para IMS según el estándar. Se plantea la recreación de flujos de llamada y ruteo de mensajes que entregan un conocimiento acabado de los mecanismos que logran comunicar a los clientes. Adicionalmente, el contenido del curso aborda las transacciones entre algunos nodos del core IMS con el protocolo Diameter que permite identificar los procesos de autentificación, ubicación y capacidad multimedia de los clientes. Cada experiencia también incluye el análisis multimedia de tal forma de entender como se transmite la voz, video y mensajería instantánea.

5.6. Comentarios finales

Casi en su totalidad los resultados fueron satisfactorios desde el punto de vista docente, es decir se logró un buen aprendizaje de la tecnología y las experiencias reflejan de manera completa los contenidos teóricos y prácticos estudiados previamente.

El enfoque que se le dió al trabajo casi en su totalidad fue analizar la señalización SIP en el core IMS. Con esto se entendió el modo de funcionamiento en el registro y establecimiento de sesiones de clientes. Además se analizó las interacciones Diameter principalmente entre los servidores CSCF y HSS en el escenario de registro. Con esto se apreció la lógica de ruteo que aplican los nodos del core IMS. Por supuesto que el core IMS es mucho más complejo que esto, sin embargo analizar cada uno de los componentes en detalle es una tarea inviable y se aleja del propósito de este proyecto.

5.6.1. Nuevas áreas de investigación

Establecido lo anterior, es importante señalar que este trabajo abre una puerta a la investigación en detalle de las otras componentes del subsistema IMS. Es posible profundizar en el manejo de calidad de servicio, facturación, políticas AAA (*Autentification, Authorization, Accounting*), métodos de seguridad, protocolos de transporte, codificación y administración de multimedios, entre otros.

Se propone de esta forma, para trabajos futuros relacionados con la arquitectura de redes convergentes IMS, continuar con la investigación de los elementos que no forman parte del core pero que cumplen tareas importantísimas en lo que se refiere a la interacción con otras redes. En efecto, a la fecha de la edición de este documento se realiza un trabajo de sobre los componentes de tasación y facturación del core IMS enfocado en los protocolos que comunican las plataformas involucradas. De esta forma se pretende abarcar todo el espectro de posibilidades que el paradigma de convergencia en telecomunicaciones ofrece.

Acrónimos

3GPP	Third Generation Partnership Project
AKA	Authentication and Key Agreement
AMPS	Advanced Mobile Phone System
AS	Application Server
AUC	Authentication Centre
BGCF	Breakout Gateway Control Function
BICC	Bearer Independent Call Control
BNF	Backus-Naur Form
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CCF	Call Control Function
CDR	Charging Data Record
CN	Core Network
CS	Circuit Switched
CSCN	Circuit Switched Core Network
CS-MGW	Circuit Switched Media Gateway
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNS SRV	DNS Service Record
EDGE	Enhanced Data Rate for GSM Evolution
EIR	Equipment Identity Register
FQDN	Full Qualified Domain Name
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobil Switching Centre
GPRS	General Packet Radio Service
GSM	Global System for Mobil communications
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hipertext Transfer Protocol
I-CSCF	Interrogating Call Session Control Function
IETF	Internet Engineering Task Force
iFC	Initial Filter Criteria
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem

IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
ISDN	Integrated Services Digital Network
ISIM	IP Multimedia Services Identity Module
ISUP	ISDN user part signaling
MEGACO	Media Gateway Control
MGCF	Media Gateway Control Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MSC	Mobile Service Switching Centre
NMS	Network Management Subsystem
NSS	Network Switching Subsystem
OCS	Online Charging System
PCEF	Policy and Charging Enforcement Point
PCRF	Policy and Charging Rule Function
P-CSCF	Proxy Call Session Control Function
PDF	Policy Decision Function
PS	Packet Switched
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAN	Radio Access Network
RNC	Radio Network Controller
RTP	Real Time Protocol
S-CSCF	Servig Call Session Control Function
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
SGW	Signalling Gateway
SIGTRAN	Signalling Transport
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SMTP	Simple Mail Transfer Protocol
TACS	Total Access Communication System
TCP	Transfer Control Protocol
TDMA	Time division Multiple Access
THIG	Topology Hiding Inter-Network Gateway
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
TP	Trigger Point
TRAU	Transcoder Rate Adaptation Unit
TU	Transaction User
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UMTS	Universal Mobil Telecommunications System
URI	Uniform Resource Identifier
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visitor Location Register

VoIP	Voicer over IP
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WLAN	Wireless Local Area Network
xDSL	Digital Subscriber Line

Bibliografía

[1] JOHNSTON, A.B. *SIP : Understanding the Session Initiation Protocol*. Artech House, Boston, MA :, 2° edición, 2003. ISBN 1580536557.

[2] CAMARILLO, G. y GARCIA-MARTIN, M.A. *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds*. John Wiley & Sons, 2° edición, 2006. ISBN 0470018186.

[3] POIKSELKÄ, M., MAYER, G., KHARTABIL, H., y NIEMI, A. *The IMS IP Multimedia Concepts and Services in the Mobile Domain*. John Wiley & Sons, 2004. ISBN 047087113X.

[4] SAAVEDRA, D. *Arquitectura de Aplicaciones para Redes Convergentes*. Memoria para optar al Título de Ingeniero Civil Electricista, Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, 2008.

[5] MANZO, C. *Docencia en Seguridad en Redes de Computadores*. Memoria para optar al Título de Ingeniero Civil Electricista, Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, 2004.

[6] PEÑA, P. *Estudio de Arquitecturas para la Convergencia de Telefonía Fija-Móvil*. Memoria para optar al Título de Ingeniero Civil Electricista, Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, 2007.

[7] ROSENBERG, J., SCHULZRINNE, H., CAMARILLO, G., JOHNSTON, A., PETERSON, J., SPARKS, R., HANDLEY, M., y SCHOOLER, E. *RFC 3261, SIP: Session Initiation Protocol*. IETF, 2002. `http://www.ietf.org`.

[8] D. CROCKER, E. y OVERELL, P. *RFC 4234, Augmented BNF for Syntax Specifications: ABNF*. IETF, 2005. `http://www.ietf.org`.

[9] HANDLEY, M., JACOBSON, V., y PERKINS, C. *RFC 4566, SDP: Session Description Protocol*. IETF, 2006. `http://www.ietf.org`.

[10] SCHULZRINNE, H. *RFC 3966, The tel URI for Telephone Numbers*. IETF, 2004. `http://www.ietf.org`.

[11] FALTSTROM, P. *RFC 2916, E.164 number and DNS*. IETF, 2000. `http://www.ietf.org`.

[12] FOSTER, M., MCGARRY, T., y YU, J. *RFC 3482, Number Portability in the Global Switched Telephone Network (GSTN): An Overview*. IETF, 2003. `http://www.ietf.org`.

[13] NEUFELD, G. y BAER, J. *RFC 2369, The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields*. IETF, 1998. `http://www.ietf.org`.

[14] GARCIA-MARTIN, M., HENRIKSON, E., y MILLS, D. *RFC 3455, Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)*. IETF, 2003. `http://www.ietf.org`.

[15] ARKKO, J., TORVINEN, V., CAMARILLO, G., NIEMI, A., y HAUKKA, T. *RFC 3329, Security Mechanism Agreement for the Session Initiation Protocol (SIP)*. IETF, 2003. http://www.ietf.org.

[16] DIERKS, T. y ALLEN, C. *RFC 2246,The TLS Protocol Version 1.0*. IETF, 1999. http://www.ietf.org.

[17] NIEMI, A., ARKKO, J., y TORVINEN, V. *RFC 3310,Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)*. IETF, 2002. http://www.ietf.org.

[18] CAMARILLO, G., ERIKSSON, G., HOLLER, J., y SCHULZRINNE, H. *RFC 3388, Grouping of Media Lines in the Session Description Protocol (SDP)*. IETF, 2002. http://www.ietf.org.

[19] ANDREASEN, F. y WING, D. *RFC 5027, Security Preconditions for Session Description Protocol (SDP) Media Streams*. IETF, 2007. http://www.ietf.org.

[20] KENT, S. y ATKINSON, R. *RFC 5027, Security Architecture for the Internet Protocol*. IETF, 1998. http://www.ietf.org.

[21] DRAGE, K. *Internet-Draft, A Session Initiation Protocol (SIP) Extension for the Identification of Services*. IETF, 2007. http://www.ietf.org.

[22] IETF. *SIP for Instant Messaging and Presence Leveraging Extensions (simple)*. http://www.ietf.org/html.charters/simple-charter.html.

[23] ROSENBERG, J. *RFC 4825, The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)*. IETF, 2007. http://www.ietf.org.

[24] WILLIS, D. y HOENEISEN, B. *RFC 3327, Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts*. IETF, 2002. http://www.ietf.org.

[25] WILLIS, D. y HOENEISEN, B. *RFC 3608, Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration*. IETF, 2003. http://www.ietf.org.

[26] CAMARILLO, G., MARSHALL, W., y ROSENBERG, J. *RFC 3312, Integration of Resource Management and Session Initiation Protocol (SIP)*. IETF, 2002. http://www.ietf.org.

[27] MARSHALL, W. *RFC 3313, Private Session Initiation Protocol (SIP) Extensions for Media Authorization*. IETF, 2003. http://www.ietf.org.

[28] GULBRANDSEN, A., VIXIE, P., y ESIBOV, L. *RFC 2782, A DNS RR for specifying the location of services (DNS SRV)*. IETF, 2000. http://www.ietf.org.

[29] ROSENBERG, J. *RFC 3680, A Session Initiation Protocol (SIP) Event Package for Registrations*. IETF, 2004. http://www.ietf.org.

[30] 3GPP. *TS 22.228, Service Requirements for the IP Multimedia Core Network (IM CN) Subsystem - Stage 1*. http://www.3gpp.org/.

[31] 3GPP. *TS 23.228, IP Multimedia Subsystem (IMS) - Stage 2*. http://www.3gpp.org/.

[32] 3GPP. *TS 24.229, IP Multimedia Call Control Protocol based on SIP and SDP - Stage 3*. http://www.3gpp.org/.

[33] 3GPP. *TS 33.203, Access Security for IP-based Services*. http://www.3gpp.org/.

[34] 3GPP. *TS 23.203, Policy and Charging Control Architecture*. http://www.3gpp.org/.

[35] 3GPP. *TS 29.207, Policy Control over Go Interface*. http://www.3gpp.org/.

[36] ETSI. *TR 180 001, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1*. http://www.etsi.org.

[37] International Telecommunication Union. *E.164 : The international public telecommunication numbering plan*. http://www.itu.int/rec/T-REC-E.164/en.

[38] Shenzhen Billion Online Technology Co., Ltd. China. *BOL SIPPhone*. http://www.bol2000.com.

[39] IPC Information Systems Inc. *SIPScenario*, 2004. http://www.iptel.org/~sipsc/.

[40] Virtualsquare. *VDE - Virtual Distributed Ethernet*. http://wiki.virtualsquare.org/index.php/Main_Page.

[41] Kamailio. *Kamailio, ex-OpenSER*. http://www.kamailio.net.

[42] OpenSIPS. *OpenSER*. http://www.opensips.org.

[43] Fraunhofer FOKUS NGNI. *OpenIMSCore*. http://www.openimscore.org.

Apéndice A

Experiencias laboratorio IMS

Apéndice B

Antecendentes

Esta sección muestra algunos temas específicos que es necesario conocer para un mejor entendimiento de los conceptos IMS.

B.1. DNS

Procedimiento DHCP/DNS:

1. Se establece un portador IP-CAN si aún no se ha hecho, mediante los procedimientos disponibles en la IP-CAN.
2. El UE requiere un servidor DHCP y adicionalmente requiere el nombre de dominio del P-CSCF y la dirección IP de los servidores DNS.
3. El UE realiza una petición DNS para obtener una lista de direcciones de P-CSCF(s) donde se selecciona una. Si la respuesta no contiene las direcciones IP, una petición DNS adicional se necesita para resolver un FQDN a una dirección IP. Luego de que el UE recibe la IP del proxy, puede iniciar la comunicación con IMS.

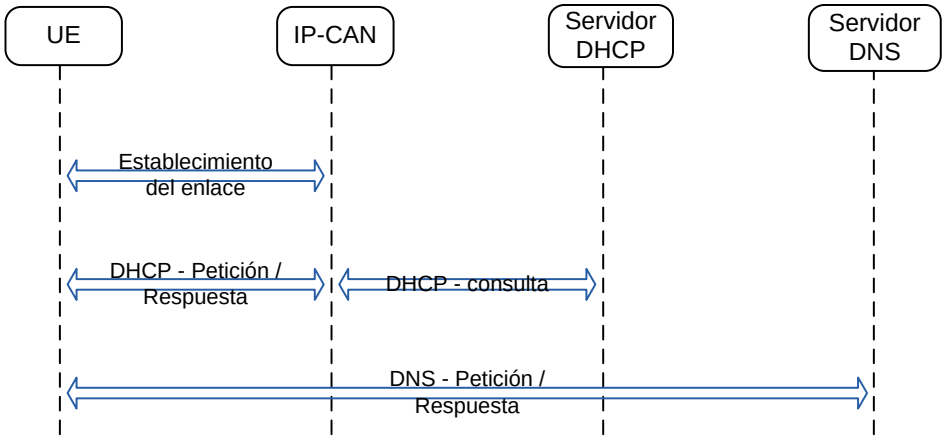

Figura B.1: Descubrimiento DHCP-DNS

DNS provee dos *record types* relevantes para peticiones SIP: SRV y NAPTR. Algunas implementaciones utilizan solamente SRV.

B.1.1. SRV Records

Proveen un mecanismo para direccionar peticiones a servidores proxies. Utilizan prioridad, que es útil cuando hay varios servidores proxies en un dominio (*backup*).

Son de la forma:

```
"_Service._Proto.Name TTL Class SRV Priority Weight Port Target"
```

Ejemplo:

```
"_sip._udp.bigu.edu 43200 IN SRV 10 10 5060 sipserver.bigu.edu."
```

- El servicio es SIP.
- El transporte es UDP. También puede ser TCP, SCTP o TLS.
- El tiempo de vida del caché es 12 horas (43200 segundos).
- La clase es IN (obligatorio).
- El record type es SRV.
- La prioridad es 10. Con múltiples SRV records la prioridad determina el orden de consulta de los proxies. Valores inferiores son consultados primero.
- El peso es 10. Con múltiples SRV records de prioridad similar, el peso determina proporcionalmente cuan seguido un proxy es consultado. Valores altos son consultados más seguido. Por ejemplo, un peso de 20 es consultado el doble de veces que un peso de 10. Un peso de 30, tres veces uno de 10.
- El puerto es 5060.
- El FQDN del servidor proxy es *sipserver.bigu.edu* y como es requerido en DNS el FQDN es terminado con un punto.

B.1.2. NAPTR Records

Proveen un mecanismo para que el dominio de entrada (*inbound*) especifique los protocolos de transporte que prefiere usar en una petición SIP.

Un record NAPTR tiene la siguiente forma:

```
"domain-name TTL Class NAPTR order preference flags service
regexp target"
```

Ejemplo,

```
"bigu.edu. IN NAPTR 60 50 "s" "SIP+D2U" "" _sip._udp.bigu.edu."
```

- El nombre de dominio a consultar (el lado derecho de sip:alice.smith@bigu.edu.).
- El tiempo de vida del caché es 12 horas.
- La clase es IN (obligatorio).
- El record type: NAPTR.

- `Order` es 60. `Preference` es 50. Valores menores son prioritarios. `Order` especifica el orden en que los records son leídos. Si las capacidades entre el *calling party* y el *called party* coinciden, el protocolo correspondiente debe ser utilizado y los otros se desechan. Si todos los records tienen el mismo valor para `order`, el campo `preference` es examinado. Valores bajos tienen mayor precedencia pero el *calling party* puede seleccionar un valor más alto de `preference` que el que tiene el *called party*.
- El valor de `flag` es s. Flags son específicos para aplicaciones.
- `service` es SIP+D2U. Especifica que se utiliza UDP. Otros valores posibles son SIP+D2T para SIP sobre TCP, SIP+D2S para SIP sobre SCTP y SIPS+D2T para SIP sobre TLS+TCP. TLS sobre UDP no esta definido.
- `regexp` es vacío. Target es `_sip._udp.bigu.edu.`

B.2. Protocolos de transporte SIP

El estándar IETF *RFC 3261* define 3 protocolos de transporte. Ellos son TCP, UDP y TLS. A continuación se entrega una breve descripción de cómo SIP utiliza dichos protocolos para transportar mensajes.

B.2.1. UDP

Cada mensaje (petición o respuesta) es transportado en un datagrama o paquete single. El puerto de origen es escogido por sobre el valor 49172. En algunos casos se utiliza el puerto SIP por defecto 5060. Dada la característica de UDP los datagramas eventualmente pueden perderse.

La capacidad de checksum permite descartar datagramas con errores, logrando que SIP asuma que el mensaje recibido tiene errores.

UDP pude ser usado sin problemas cuando se tiene conocimiento de que el mensaje es de menor tamaño que el MTU definido en la red IP (en el caso de mensajes SIP simples sin grandes cabeceras ni cuerpos de mensaje múltiples).

B.2.2. TCP

Provee una capa de transporte confiable pero compleja y con retrasos en la transmisión sobre la red. Provee control de congestión. Soporta mensajes de tamaño arbitrario.

Se debe abrir una conexión entre dos terminales antes de ser enviados los mensajes SIP. El header `Content-Lenght` es necesario para encontrar el final de un mensaje y el comienzo de otro.

Entre sus desventajas se cuentan el retraso en establecer la conexión la necesidad de los servidores de mantener el estado de conexión en la capa de transporte.

B.2.3. TLS

SIP puede utilizar TLS sobre TCP para transporte cifrado con capacidades adicionales de autentificación. El puerto por defecto para el uso de TLS es el 5061. Si se usa entre dos proxies, cada uno de ellos debe tener un certificado para autentificarse mutuamente.

B.2.4. SCTP

Es similar a TCP en lo que se refiere al transporte confiable. Tiene algunas ventajas sobre TCP para protocolos basados en el transporte de mensajes. Tiene incorporado segmentación de mensajes, es decir los mensajes individuales son separados en la capa de transporte. Sus características principales se describen a continuación.

Evita el problema *head of line blocking*. Con TCP un segmento perdido con una ventana muy larga provoca que todas las ventanas de mensajes esperen en un buffer, por lo tanto se bloquean hasta que el segmento es retransmitido. Sobre SCTP se sigue enviando paquetes a pesar de que alguno se pierda.

Soporta multihoming. Si uno de los servidores (que conforman un par con carga balanceada) falla, el otro puede recibir inmediatamente los mensajes sin requerir un DNS o una búsqueda en una base de datos. Permite múltiples interfaces de los end-points. De esta forma permite alternar direcciones cuando ocurre un fallo en alguna interfaz.

Requiere soporte de sistema operativo. Si la red no presenta perdidas de paquetes, el rendimiento de SCTP es idéntico a TCP.

Message Orientation. Se de adecúa al framing de mensajes. El mensaje se recibe en una sola lectura (como UDP pero agrega confiabilidad).

Un-Ordered Service. Permite el envío de mensajes desordenados.

Extensible. Utiliza TLV (Tag Lenght Value) que permite agregar opciones dentro de los paquetes. Permite compatibilidad con implementaciones previas de SCTP.

Message time to live. Permite descartar paquetes que no han sido recibidos dentro de un período de tiempo.

Syn Cookies. Previene IP Spoofing. Implementa *four way handshake*.

Checksum de 32 bit. Control de redundancia más fuerte que TCP (16 bit) para verificar que los datos no están corruptos.

Apéndice C

Detalle resultados

Se describe el contenido de los mensajes capturados en las pruebas de funcionamiento.

C.1. IMS: Registro

Petición REGISTER:

```
SIP MESSAGE 1        172.16.231.139:5060() -> 172.16.231.213:4060()
UDP Frame 465      3/Jun/08 16:23:36.0401 TimeFromPreviousSipFrame=22.2940 TimeFromStart=22.2940
REGISTER sip:playsip.lab SIP/2.0
Via: SIP/2.0/UDP 172.16.231.139:5060;rport;branch=z9hG4bK1722419167
From: <sip:javier@playsip.lab>;tag=68687288
To: <sip:javier@playsip.lab>
Call-ID: 896910588
CSeq: 1 REGISTER
Contact: <sip:javier@172.16.231.139:5060;line=36020458036904f>
Authorization: Digest username="javier@playsip.lab", realm="playsip.lab",
    nonce=" ", uri="sip:playsip.lab", response=" "
Max-Forwards: 70
User-Agent: UCT IMS Client
Expires: 600000
Supported: path
Content-Length: 0


SIP MESSAGE 2        172.16.231.213:4060() -> 10.111.111.141:5060()
UDP Frame 466      3/Jun/08 16:23:36.0738 TimeFromPreviousSipFrame=0.0337 TimeFromStart=22.3277
REGISTER sip:playsip.lab SIP/2.0
Via: SIP/2.0/UDP 172.16.231.213:4060;branch=z9hG4bK923c.b85e2047.0
Via: SIP/2.0/UDP 172.16.231.139:5060;rport=5060;branch=z9hG4bK1722419167
From: <sip:javier@playsip.lab>;tag=68687288
To: <sip:javier@playsip.lab>
Call-ID: 896910588
CSeq: 1 REGISTER
Contact: <sip:javier@172.16.231.139:5060;line=36020458036904f>
Max-Forwards: 16
User-Agent: UCT IMS Client
Expires: 600000
Supported: path
Content-Length: 0
Authorization: Digest username="javier@playsip.lab", realm="playsip.lab",
    nonce=" ", uri="sip:playsip.lab", response=" ", integrity-protected="no"
Path: <sip:term@pcscf.playsip.lab:4060;lr>
Require: path
P-Charging-Vector: icid-value="P-CSCFabcd4845a848000002c6";
    icid-generated-at=172.16.231.213;orig-ioi="playsip.lab"
P-Visited-Network-ID: playsip.lab
```

```
SIP MESSAGE 1        10.111.111.141:5060() -> 10.111.111.142:6060()
UDP Frame 334      3/Jun/08 16:23:36.3411 TimeFromPreviousSipFrame=23.9486 TimeFromStart=23.9486
REGISTER sip:scscf.playsip.lab:6060 SIP/2.0
Via: SIP/2.0/UDP 10.111.111.141;branch=z9hG4bK923c.0bdf6d41.0
Via: SIP/2.0/UDP 172.16.231.213:4060;branch=z9hG4bK923c.b85e2047.0
Via: SIP/2.0/UDP 172.16.231.139:5060;rport=5060;branch=z9hG4bK1722419167
From: <sip:javier@playsip.lab>;tag=68687288
To: <sip:javier@playsip.lab>
Call-ID: 896910588
CSeq: 1 REGISTER
Contact: <sip:javier@172.16.231.139:5060;line=36020458036904f>
Max-Forwards: 15
User-Agent: UCT IMS Client
Expires: 600000
Supported: path
Content-Length: 0
Authorization: Digest username="javier@playsip.lab", realm="playsip.lab",
    nonce=" ", uri="sip:playsip.lab", response=" ", integrity-protected="no"
Path: <sip:term@pcscf.playsip.lab:4060;lr>
Require: path
P-Charging-Vector: icid-value="P-CSCFabcd4845a848000002c6";
    icid-generated-at=172.16.231.213;orig-ioi="playsip.lab"
P-Visited-Network-ID: playsip.lab
```

Respuesta 401:

```
SIP MESSAGE 2        10.111.111.142:6060() -> 10.111.111.141:5060()
UDP Frame 349      3/Jun/08 16:23:36.7081 TimeFromPreviousSipFrame=0.3671 TimeFromStart=24.3157
SIP/2.0 401 Unauthorized - Challenging the UE
Via: SIP/2.0/UDP 10.111.111.141;branch=z9hG4bK923c.0bdf6d41.0
Via: SIP/2.0/UDP 172.16.231.213:4060;branch=z9hG4bK923c.b85e2047.0
Via: SIP/2.0/UDP 172.16.231.139:5060;rport=5060;branch=z9hG4bK1722419167
From: <sip:javier@playsip.lab>;tag=68687288
To: <sip:javier@playsip.lab>;tag=71f77aaa2a5267725ec308ae04f1e3fc-d433
Call-ID: 896910588
CSeq: 1 REGISTER
WWW-Authenticate: Digest realm="playsip.lab",
    nonce="OpT8jcuVzTkd5aeE0mL85rlcOskg5QAAIvrMJiGB6p4=",
    algorithm=AKAv1-MD5, ck="c4a372d3edd9e6f8ff54fdbf64403597",
    ik="e7f99fc784cecf4014484d6fd024714b"
Path: <sip:term@pcscf.playsip.lab:4060;lr>
Service-Route: <sip:orig@scscf.playsip.lab:6060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, MESSAGE, INFO
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0
Warning: 392 10.111.111.142:6060 "Noisy feedback tells:
    pid=5905 req_src_ip=10.111.111.141 req_src_port=5060
    in_uri=sip:scscf.playsip.lab:6060 out_uri=sip:scscf.playsip.lab:6060 via_cnt==3"


SIP MESSAGE 5        10.111.111.141:5060() -> 172.16.231.213:4060()
UDP Frame 691      3/Jun/08 16:23:36.6837 TimeFromPreviousSipFrame=0.0446 TimeFromStart=22.9377
SIP/2.0 401 Unauthorized - Challenging the UE
Via: SIP/2.0/UDP 172.16.231.213:4060;branch=z9hG4bK923c.b85e2047.0
Via: SIP/2.0/UDP 172.16.231.139:5060;rport=5060;branch=z9hG4bK1722419167
From: <sip:javier@playsip.lab>;tag=68687288
To: <sip:javier@playsip.lab>;tag=71f77aaa2a5267725ec308ae04f1e3fc-d433
Call-ID: 896910588
CSeq: 1 REGISTER
WWW-Authenticate: Digest realm="playsip.lab",
    nonce="OpT8jcuVzTkd5aeE0mL85rlcOskg5QAAIvrMJiGB6p4=",
    algorithm=AKAv1-MD5, ck="c4a372d3edd9e6f8ff54fdbf64403597",
    ik="e7f99fc784cecf4014484d6fd024714b"
Path: <sip:term@pcscf.playsip.lab:4060;lr>
Service-Route: <sip:orig@scscf.playsip.lab:6060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, MESSAGE, INFO
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0
Warning: 392 10.111.111.142:6060 "Noisy feedback tells:
    pid=5905 req_src_ip=10.111.111.141 req_src_port=5060
```

```
    in_uri=sip:scscf.playsip.lab:6060 out_uri=sip:scscf.playsip.lab:6060 via_cnt==3"


SIP MESSAGE 6        172.16.231.213:4060() -> 172.16.231.139:5060()
UDP Frame 692      3/Jun/08 16:23:36.6841 TimeFromPreviousSipFrame=0.0003 TimeFromStart=22.9380
SIP/2.0 401 Unauthorized - Challenging the UE
Via: SIP/2.0/UDP 172.16.231.139:5060;rport=5060;branch=z9hG4bK1722419167
From: <sip:javier@playsip.lab>;tag=68687288
To: <sip:javier@playsip.lab>;tag=71f77aaa2a5267725ec308ae04f1e3fc-d433
Call-ID: 896910588
CSeq: 1 REGISTER
Path: <sip:term@pcscf.playsip.lab:4060;lr>
Service-Route: <sip:orig@scscf.playsip.lab:6060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, MESSAGE, INFO
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0
Warning: 392 10.111.111.142:6060 "Noisy feedback tells:
    pid=5905 req_src_ip=10.111.111.141 req_src_port=5060
    in_uri=sip:scscf.playsip.lab:6060 out_uri=sip:scscf.playsip.lab:6060 via_cnt==3"
WWW-Authenticate: Digest realm="playsip.lab",
    nonce="OpT8jcuVzTkd5aeE0mL85rlcOskg5QAAIvrMJiGB6p4=",
    algorithm=AKAv1-MD5
```

C.2. IMS: inicio de sesión

Se muestran los mensajes obtenidos de la prueba de sesión. Por simplificación se muestra un mensaje por método.

```
     SIP MESSAGE 1        172.16.231.139:5061() -> 172.16.231.213:4065()
     UDP Frame 31       26/Jun/08 13:14:29.0329 TimeFromPreviousSipFrame=3.7966
     TimeFromStart=3.7966
INVITE sip:javier@playsip.lab SIP/2.0
Via: SIP/2.0/UDP 172.16.231.139:5061;rport;branch=z9hG4bK301682348
Route: <sip:orig@scscf.santiago.lab:6060;lr>
From: "Jesus" <sip:jesus@santiago.lab>;tag=124864303
To: <sip:javier@playsip.lab>
Call-ID: 1985868597
CSeq: 20 INVITE
Contact: <sip:jesus@172.16.231.139:5061>
Content-Type: application/sdp
Max-Forwards: 70
User-Agent: UCT IMS Client
Subject: IMS Call
Expires: 120
P-Preferred-Identity: "Jesus" <sip:jesus@santiago.lab>
Privacy: none
P-Access-Network-Info: IEEE-802.11a
Require: precondition
Require: sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Content-Length:   335

v=0
o=- 0 0 IN IP4 172.16.231.139
s=IMS Call
c=IN IP4 172.16.231.139
t=0 0
m=audio 38246 RTP/AVP 3 0 101
b=AS:64
a=rtpmap:3 GSM/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
a=curr:qos local none
a=curr:qos remote none
```

```
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv

     SIP MESSAGE 2        172.16.231.213:4065() -> 172.16.231.139:5061()
     UDP Frame 32       26/Jun/08 13:14:29.0334 TimeFromPreviousSipFrame=0.0005
     TimeFromStart=3.7971
SIP/2.0 100 trying -- your call is important to us
Via: SIP/2.0/UDP 172.16.231.139:5061;rport=5061;branch=z9hG4bK301682348
From: "Jesus" <sip:jesus@santiago.lab>;tag=124864303
To: <sip:javier@playsip.lab>
Call-ID: 1985868597
CSeq: 20 INVITE
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0
Warning: 392 172.16.231.213:4065 "Noisy feedback tells:
    pid=10357 req_src_ip=172.16.231.139 req_src_port=5061
    in_uri=sip:javier@playsip.lab out_uri=sip:javier@playsip.lab via_cnt==1"


     SIP MESSAGE 19       172.16.231.213:5061() -> 172.16.231.139:4068()
     UDP Frame 87       26/Jun/08 13:14:29.1586 TimeFromPreviousSipFrame=0.1084
     TimeFromStart=3.9223
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 172.16.231.139:4068;branch=z9hG4bK74e.0f2eddc5.0
Via: SIP/2.0/UDP 172.16.231.213:6060;received=172.16.231.213;rport=6060;
    branch=z9hG4bK74e.8f9ae231.0
Via: SIP/2.0/UDP 172.16.231.213;branch=z9hG4bK74e.a7e85b41.0
Via: SIP/2.0/UDP 172.16.231.139:6060;branch=z9hG4bK74e.4952c344.0
Via: SIP/2.0/UDP 172.16.231.213:4065;branch=z9hG4bK74e.5ca37f3.0
Via: SIP/2.0/UDP 172.16.231.139:5061;rport=5061;branch=z9hG4bK301682348
Record-Route: <sip:mt@pcscf.temuco.lab:4068;lr>
Record-Route: <sip:mt@scscf.playsip.lab:6060;lr>
Record-Route: <sip:mo@scscf.santiago.lab:6060;lr>
Record-Route: <sip:mo@pcscf.arica.lab:4065;lr>
From: "Jesus" <sip:jesus@santiago.lab>;tag=124864303
To: <sip:javier@playsip.lab>;tag=1659125644
Call-ID: 1985868597
CSeq: 20 INVITE
Contact: <sip:javier@172.16.231.213:5061>
Content-Type: application/sdp
User-Agent: UCT IMS Client
Require: 100rel
Require: precondition
RSeq: 1
P-Access-Network-Info: IEEE-802.11a
Content-Length:   364

v=0
o=- 0 0 IN IP4 172.16.231.213
s=IMS_Call
c=IN IP4 172.16.231.213
t=0 0
m=audio 36570 RTP/AVP 3 0 101
b=AS:64
a=curr:qos remote none
a=curr:qos local none
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000


     SIP MESSAGE 25       172.16.231.139:5061() -> 172.16.231.213:4065()
     UDP Frame 100      26/Jun/08 13:14:29.6804 TimeFromPreviousSipFrame=0.5130
     TimeFromStart=4.4440
PRACK sip:javier@172.16.231.213:5061 SIP/2.0
Via: SIP/2.0/UDP 172.16.231.139:5061;rport;branch=z9hG4bK1496069389
Route: <sip:mo@pcscf.arica.lab:4065;lr>
```

```
Route: <sip:mo@scscf.santiago.lab:6060;lr>
Route: <sip:mt@scscf.playsip.lab:6060;lr>
Route: <sip:mt@pcscf.temuco.lab:4068;lr>
From: "Jesus" <sip:jesus@santiago.lab>;tag=124864303
To: <sip:javier@playsip.lab>;tag=1659125644
Call-ID: 1985868597
CSeq: 21 PRACK
Contact: <sip:jesus@172.16.231.139:5061>
Content-Type: application/sdp
Max-Forwards: 70
User-Agent: UCT IMS Client
RAck: 1 20 INVITE
Require: precondition
Require: sec-agree
P-Access-Network-Info: IEEE-802.11a
Content-Length:   364

v=0
o=- 0 0 IN IP4 172.16.231.139
s=IMS_Call
c=IN IP4 172.16.231.139
t=0 0
m=audio 38246 RTP/AVP 3 0 101
b=AS:64
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000

     SIP MESSAGE 30       172.16.231.213:5061() -> 172.16.231.139:4068()
     UDP Frame 105      26/Jun/08 13:14:29.6839 TimeFromPreviousSipFrame=0.0004
     TimeFromStart=4.4476
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.231.139:4068;branch=z9hG4bK84e.1a555e7.0
Via: SIP/2.0/UDP 172.16.231.213:6060;received=172.16.231.213;rport=6060;
    branch=z9hG4bK84e.fd520a45.0
Via: SIP/2.0/UDP 172.16.231.139:6060;branch=z9hG4bK84e.fee54916.0
Via: SIP/2.0/UDP 172.16.231.213:4065;branch=z9hG4bK84e.7a33a5a7.0
Via: SIP/2.0/UDP 172.16.231.139:5061;rport=5061;branch=z9hG4bK1496069389
From: "Jesus" <sip:jesus@santiago.lab>;tag=124864303
To: <sip:javier@playsip.lab>;tag=1659125644
Call-ID: 1985868597
CSeq: 21 PRACK
User-Agent: UCT IMS Client
Content-Length: 0


     SIP MESSAGE 35       172.16.231.139:5061() -> 172.16.231.213:4065()
     UDP Frame 110      26/Jun/08 13:14:29.8788 TimeFromPreviousSipFrame=0.1928
     TimeFromStart=4.6425
UPDATE sip:javier@172.16.231.213:5061 SIP/2.0
Via: SIP/2.0/UDP 172.16.231.139:5061;rport;branch=z9hG4bK615301653
Route: <sip:mo@pcscf.arica.lab:4065;lr>
Route: <sip:mo@scscf.santiago.lab:6060;lr>
Route: <sip:mt@scscf.playsip.lab:6060;lr>
Route: <sip:mt@pcscf.temuco.lab:4068;lr>
From: "Jesus" <sip:jesus@santiago.lab>;tag=124864303
To: <sip:javier@playsip.lab>;tag=1659125644
Call-ID: 1985868597
CSeq: 22 UPDATE
Contact: <sip:jesus@172.16.231.139:5061>
Content-Type: application/sdp
Max-Forwards: 70
User-Agent: UCT IMS Client
Content-Length:   368
```

```
v=0
o=- 0 0 IN IP4 172.16.231.139
s=IMS_Call
c=IN IP4 172.16.231.139
t=0 0
m=audio 38246 RTP/AVP 3 0 101
b=AS:64
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000

     SIP MESSAGE 40       172.16.231.213:5061() -> 172.16.231.139:4068()
     UDP Frame 118      26/Jun/08 13:14:29.9662 TimeFromPreviousSipFrame=0.0833
     TimeFromStart=4.7298
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 172.16.231.139:4068;branch=z9hG4bK74e.0f2eddc5.0
Via: SIP/2.0/UDP 172.16.231.213:6060;received=172.16.231.213;rport=6060;
    branch=z9hG4bK74e.8f9ae231.0
Via: SIP/2.0/UDP 172.16.231.213;branch=z9hG4bK74e.a7e85b41.0
Via: SIP/2.0/UDP 172.16.231.139:6060;branch=z9hG4bK74e.4952c344.0
Via: SIP/2.0/UDP 172.16.231.213:4065;branch=z9hG4bK74e.5ca37f3.0
Via: SIP/2.0/UDP 172.16.231.139:5061;rport=5061;branch=z9hG4bK301682348
Record-Route: <sip:mt@pcscf.temuco.lab:4068;lr>
Record-Route: <sip:mt@scscf.playsip.lab:6060;lr>
Record-Route: <sip:mo@scscf.santiago.lab:6060;lr>
Record-Route: <sip:mo@pcscf.arica.lab:4065;lr>
From: "Jesus" <sip:jesus@santiago.lab>;tag=124864303
To: <sip:javier@playsip.lab>;tag=1659125644
Call-ID: 1985868597
CSeq: 20 INVITE
Contact: <sip:javier@172.16.231.213:5061>
Content-Type: application/sdp
User-Agent: UCT IMS Client
Require: 100rel
RSeq: 2
Content-Length:   372

v=0
o=- 0 0 IN IP4 172.16.231.213
s=IMS_Call
c=IN IP4 172.16.231.213
t=0 0
m=audio 36570 RTP/AVP 3 0 101
b=AS:64
a=curr:qos remote sendrecv
a=curr:qos local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000

     SIP MESSAGE 41       172.16.231.213:5061() -> 172.16.231.139:4068()
     UDP Frame 119      26/Jun/08 13:14:29.9662 TimeFromPreviousSipFrame=0.0001
     TimeFromStart=4.7299
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.231.139:4068;branch=z9hG4bK54e.5061c885.0
Via: SIP/2.0/UDP 172.16.231.213:6060;received=172.16.231.213;rport=6060;
    branch=z9hG4bK54e.5f913c25.0
Via: SIP/2.0/UDP 172.16.231.139:6060;branch=z9hG4bK54e.973a0b55.0
Via: SIP/2.0/UDP 172.16.231.213:4065;branch=z9hG4bK54e.5350ce65.0
Via: SIP/2.0/UDP 172.16.231.139:5061;rport=5061;branch=z9hG4bK615301653
From: "Jesus" <sip:jesus@santiago.lab>;tag=124864303
```

```
To: <sip:javier@playsip.lab>;tag=1659125644
Call-ID: 1985868597
CSeq: 22 UPDATE
Contact: <sip:javier@172.16.231.213:5061>
Content-Type: application/sdp
User-Agent: UCT IMS Client
Require: pre-condition, sec-agree
Proxy-Require: sec-agree
Content-Length:   372

v=0
o=- 0 0 IN IP4 172.16.231.213
s=IMS_Call
c=IN IP4 172.16.231.213
t=0 0
m=audio 36570 RTP/AVP 3 0 101
b=AS:64
a=curr:qos remote sendrecv
a=curr:qos local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
```

C.3. IMS: Servicios

C.3.1. (Perfiles de usuario Diameter)

Contenido mensaje XML Server-Assignment

```
<?xml version="1.0" encoding="UTF-8"?>
<IMSSubscription>
  <PrivateID>javier@playsip.lab</PrivateID>
  <ServiceProfile>
    <PublicIdentity>
      <Identity>sip:javier@playsip.lab</Identity>
      <Extension>
        <IdentityType>0</IdentityType>
      </Extension>
    </PublicIdentity>
    <InitialFilterCriteria>
      <Priority>0</Priority>
      <TriggerPoint>
        <ConditionTypeCNF>1</ConditionTypeCNF>
        <SPT>
          <ConditionNegated>0</ConditionNegated>
          <Group>0</Group>
          <Method>PUBLISH</Method>
          <Extension></Extension>
        </SPT>
        <SPT>
          <ConditionNegated>0</ConditionNegated>
          <Group>0</Group>
          <Method>SUBSCRIBE</Method>
          <Extension></Extension>
        </SPT>
        <SPT>
          <ConditionNegated>0</ConditionNegated>
          <Group>1</Group>
          <SIPHeader>
            <Header>Event</Header>
            <Content>.*presence.*</Content>
          </SIPHeader>
```

```
          <Extension></Extension>
        </SPT>
      </TriggerPoint>
      <ApplicationServer>
        <ServerName>sip:172.16.231.213:5065</ServerName>
        <DefaultHandling>0</DefaultHandling>
      </ApplicationServer>
    </InitialFilterCriteria>

    <InitialFilterCriteria>
      <Priority>1</Priority>
      <TriggerPoint>
        <ConditionTypeCNF>1</ConditionTypeCNF>
        <SPT>
          <ConditionNegated>0</ConditionNegated>
          <Group>0</Group>
          <Method>INVITE</Method>
          <Extension></Extension>
        </SPT>
        <SPT>
          <ConditionNegated>0</ConditionNegated>
          <Group>1</Group>
          <SIPHeader>
            <Header>To</Header>
            <Content>.*iptv.playsip.lab.*</Content>
          </SIPHeader>
          <Extension></Extension>
        </SPT>
      </TriggerPoint>
      <ApplicationServer>
        <ServerName>sip:172.16.231.213:7070</ServerName>
        <DefaultHandling>0</DefaultHandling>
      </ApplicationServer>
    </InitialFilterCriteria>
  </ServiceProfile>
</IMSSubscription>
```