ACCESO A CAPACIDADES DE IMS DESDE CLIENTES SIP IETF

FABIÁN REINALDO CUÉLLAR CALDERÓN

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELEMÁTICA
Línea de Investigación Servicios Avanzados de Telecomunicaciones
POPAYÀN, ABRIL DE 2009

ACCESO A CAPACIDADES DE IMS DESDE CLIENTES SIP IETF

FABIÁN REINALDO CUÉLLAR CALDERÓN

Trabajo de grado presentado como requisito para optar al título de Ingeniero en Electrónica y Telecomunicaciones

Director

JAVIER ALEXANDER HURTADO GUACA
Ingeniero en Electrónica y Telecomunicaciones

UNIVERSIDAD DE CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELEMÁTICA
Línea de Investigación Servicios Avanzados de Telecomunicaciones
POPAYÀN, ABRIL DE 2009

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

INTRODUCCIÓN

La fuerte penetración en el mercado de las tecnologías de acceso emergentes, como es el caso de UMTS (Universal Mobile Telecommunications System), y el afianzamiento de las tecnologías más tradicionales tales como GSM/GPRS (Global System for Mobile communications / General Packet Radio Services), hacen suponer que es necesaria la integración de los servicios provistos por las redes tradicionales con nuevos y mejores servicios. Esto, y el gran auge que ha tenido la Internet como centro de convergencia para la mayoría de los servicios multimedia en la actualidad, han llevado a los desarrolladores de tecnologías a adoptar una nueva tendencia hacia los diversos modos de acceso que se integran de forma transparente en una capa de red basada en el protocolo de Internet IP. De esta manera nace un nuevo concepto introducido por el 3GPP, denominado *All-IP* (Todo IP).

La arquitectura planteada en el Subsistema Multimedia IP (IP Multimedia Subsystem - IMS) se ha constituido como la más contundente respuesta a la tendencia *All-IP*. Esto significa que la intención del 3GPP por desarrollar una plataforma para proveer servicios convergentes está claramente definida en IMS, gracias a que esta arquitectura posibilita una integración entre los servicios 3G y la Internet multimedia, todo en tiempo real. También posibilita la creación de nuevos y mejores servicios basados en una combinación de los tradicionales servicios TCP/IP, tales como mensajería instantánea, voz sobre IP, streaming, videoconferencia, correo electrónico, Web, etc.

Entonces, IMS se establece como el punto de llegada de las múltiples tecnologías de acceso existentes, para las que se han diseñado distintos puntos de entrada a la red. Esto generalmente se ve reflejado en el desarrollo de pasarelas de medios y de señalización. Lo cual lleva a pensar que las tecnologías, protocolos y demás elementos de las redes tradicionales deben seguir en funcionamiento, y más aún, deben coexistir con los requerimientos propuestos por el 3GPP para que sean útiles en un entorno IMS. Es el caso de las PSTN (Public Switched Telephone Network), para las cuales se tiene un sistema exclusivo de adaptación dentro de IMS, que les permite entender los protocolos de señalización internos de esta arquitectura, y a su vez, proveer a los usuarios de la red telefónica tradicional un mayor número de servicios mejorados.

Pero no todas los protocolos y tecnologías han sido tenidos en cuenta dentro de la definición de IMS. Existen protocolos cuya adaptación hacia esta arquitectura requiere de un trabajo adicional, el cual generalmente está asociado con el establecimiento de nuevas pautas para la señalización y de nuevas entidades de red.

Por otro lado, el entorno en el cual se piense ubicar una red basada en la arquitectura IMS, debe cumplir con una amplia serie de requisitos regulatorios, técnicos y comerciales. Por lo tanto, es de suponer que no es fácil ejecutar una migración directa hacia esta arquitectura, sino que hace falta una previa adaptación de las tecnologías pertenecientes a dicho entorno. Es el caso de Colombia, donde un proceso regulatorio y técnico para lograr una completa migración hacia IMS por parte de los operadores de red, no ha tenido gran interés, permite pensar que el trabajo de adaptación de los protocolos de señalización existentes en el país, y por consiguiente, la adopción de la arquitectura IMS, es un trabajo que se ha puesto

plenamente al criterio de los proveedores e integradores de servicios. La forma en que estos actores del mercado de las telecomunicaciones podrían brindar una alternativa adecuada para la adopción de IMS, es la producción e implantación de herramientas Software que se integren fácilmente con los operadores de redes tradicionales, y a su vez, permitan que éstos puedan interactuar con los servicios de una red IMS.

Empieza entonces una nueva etapa hacia los servicios convergentes de IMS, correspondiente a la realización de múltiples elementos de adaptación que provean una puerta de entrada hacia estas redes. Es el caso particular del actual proyecto, donde la creación de una herramienta Software de adaptación para el tráfico de señalización basado en el Protocolo de Inicio de Sesión SIP (Session Initiation Protocol) en su especificación inicial desarrollada por la IETF (Internet Engineering Task Force), brinda la posibilidad de que una amplia cantidad de usuarios basados en esta especificación, puedan acceder a los beneficios que se han obtenido en las redes IMS.

El presente documento se desarrolla en base a la interacción entre el SIP de la IETF, y el perfil definido por el 3GPP (3rd Generation Partnership Project) para IMS. Para ello, se presenta un primer capítulo que responde a la pregunta: ¿Qué requiere el 3GPP para que SIP pueda ser utilizado dentro de IMS como protocolo base de señalización y control?. Como solución a dicha pregunta, este capítulo muestra las principales diferencias entre las dos especificaciones del protocolo, además de los requerimientos del 3GPP y las extensiones que han sido definidas por este grupo para que SIP pueda utilizarse dentro de IMS.

En el segundo capítulo, se presenta el tráfico de señalización, diseñado por el 3GPP para el flujo de mensajes SIP dentro de IMS. Esto es de suprema importancia para entender cuáles son los requerimientos de IMS en cuanto a flujo de señalización, y de esta manera plantear las consideraciones que se deberían tener en cuenta para el diseño y desarrollo de la pasarela SIP.

En el tercer capítulo se da una muestra clara de los valores de entrada y de salida (en términos de mensajes SIP) que tendría la pasarela de señalización. Con esto se da una muestra de las capacidades de la pasarela para recibir, modificar y enviar mensajes SIP adaptados para la interacción entre las dos especificaciones de SIP.

En un cuarto capítulo se describen en detalle las características del prototipo i23GW (IETF to 3GPP Gateway). Partiendo desde su arquitectura, para la cual se describen los distintos elementos que interactúan con la pasarela. Además, se brinda una descripción de los casos de uso del sistema, y el diseño de los componentes internos de i23GW. El total funcionamiento de este prototipo es validado dentro del capítulo 5, donde se da parte sobre su desempeño, usabilidad y ancho de banda requerido.

1. COMPARACIÓN DE LAS ESPECIFICACIONES IETF Y 3GPP PARA EL PROTOCOLO SIP

1.1 Generalidades del protocolo SIP especificado por la IETF

SIP[1] es un protocolo definido inicialmente por la IETF y ha sido escogido por el 3GPP como protocolo base en los procesos de señalización dentro de la arquitectura IMS. SIP es un protocolo perteneciente a la capa de aplicación del sistema OSI (Open System Interconection), diseñado principalmente para tratar el establecimiento, la modificación y terminación de sesiones multimedia.

SIP funciona de manera conjunta con una serie de protocolos definidos también por la IETF para lograr una comunicación verticalmente integrada. Algunos de ellos son RTP (Real Time Protocol) para el transporte de información en tiempo real, RTCP (Real Time Control Protocol) para proveer Calidad de Servicio en comunicaciones de tiempo real, y el Protocolo utilizado para la Descripción de las Sesiones SDP (Session Description Protocol).

SIP reutiliza características de otros protocolos de Internet tales como el HTTP (HiperText Transfer Protocol)[2] utilizado en la distribución y manejo de contenidos a través de Internet, y SMTP (Simple Mail Transfer Protocol)[3] utilizado en la transferencia de correo electrónico. SIP está definido como un protocolo de texto codificado de alta extensibilidad. Esta capacidad se ve reflejada en las diferentes modificaciones o extensiones que se han realizado sobre las características y servicios básicos propios de la definición original del protocolo. Lo anterior es posible, gracias a que dentro de la estructura de SIP se pueden adicionar nuevos métodos y cabeceras, de tal manera que este protocolo pueda soportar los múltiples requisitos de las distintas redes, como por ejemplo, los servicios de control de llamada, movilidad e interacción con sistemas de telefonía existentes. Es el caso de SIP-T [4], definido para trabajar en la interconexión entre las PSTN (Public Switched Telephone Network) y las redes SIP, especialmente, como un conjunto de prácticas que puedan optimizar el uso de pasarelas entre estas dos tecnologías.

En los procesos relacionados con el manejo de las sesiones multimedia, incluyendo las labores necesarias para invitar nuevos participantes a una conversación (conferencia), SIP soporta cinco aspectos básicos:

- Localización de usuario.
- Disponibilidad de usuario.
- Capacidades de usuario.
- Negociación de sesión.
- Gestión de sesión.

Estos aspectos básicos, al igual que los detalles del protocolo, son descritos de manera específica en el Anexo A.

Gracias a su extensibilidad, SIP ha sido adoptado como el corazón en las tareas de señalización dentro de la plataforma de servicios de nueva generación propuesta por el 3GPP, IMS. Entender lo que significa IMS dentro del mercado de las telecomunicaciones resulta muy importante, y en especial, para el desarrollo del presente proyecto, la relación que las capacidades de IMS puedan tener con el protocolo SIP. A continuación se da una descripción de dichas capacidades y características de IMS.

1.2 Subsistema Multimedia IP (IP Multimedia Subsystem - IMS)

IMS es una arquitectura para el despliegue de servicios avanzados multimedia IP en redes móviles y fijas. El *core (núcleo)* de una red IMS incluye una plataforma de servicios que soporta terminales IP, servicios idénticos a los entregados por los proveedores tradicionales, ya sea que el destino se encuentre dentro de una red IP o una red de conmutación de circuitos. Los servicios IMS habilitan comunicaciones en una amplia variedad de modos, incluyendo texto, voz, localización, imágenes y video, o cualquier combinación de ellos, dentro de un entorno altamente seguro y personalizado. IMS brinda capacidades importantes y de alta demanda, tales como Calidad de Servicio (QoS), gestión de los recursos de la red, y la habilidad de mezclar o integrar servicios de distintos proveedores [6][7]. Como consecuencia, IMS es visto como el punto de llegada entre las estrategias de convergencia de los operadores de telecomunicaciones móviles y fijas. [5]

La arquitectura IMS está dividida en tres capas principales:

La Capa de Aplicación, que contiene una serie de distintos tipos de servidores de aplicaciones, dotados con todas las características SIP necesarias para ofrecer servicios en el entorno de IMS.

La capa de Control es el centro de IMS en labores de señalización. Abarca un número de distintas funciones útiles en los procesos de flujo de tráfico de señalización, por ejemplo, la Función de Control de Sesión de Llamada (Call Session Control Function - CSCF), el Servidor Local de Subscriptor (Home Subscriber Server - HSS), la Función de Control de la Pasarela Multimedia (Media Gateway Control Function - MGCF) y la Función Controladora de Recursos Multimedia (Media Resource Function Controller - MRFC). Los detalles acerca de estas entidades se pueden consultar en el Anexo B.

Una tercera capa es la de **Transporte Multimedia**, que tiene como función principal el transporte de información multimedia directamente entre distintos subscriptores, y también, entre los subscriptores y una función generadora de medios de IMS. [6] [7]

Además, dentro de estas capas de la arquitectura IMS, es frecuente encontrar la implementación de distintos módulos, los cuales actúan de manera directa con los servicios y/o con los clientes, o también integrados como recursos compartidos entre las distintas capas generales de la arquitectura. Por ejemplo, el repositorio de datos de usuario referido en el denominado HSS, las pasarelas de medios (Media Gateways) y de señalización (Signalling Gateways), brindan parte de la funcionalidad necesaria para que la arquitectura IMS pueda interactuar con un ambiente externo y proveer servicios convergentes a los usuarios de distintos proveedores. Una explicación más detallada de estos módulos pertenecientes a la arquitectura de IMS se encuentra en el Anexo B.

Alrededor de todo lo referente con IMS, el centro del estudio del presente proyecto se ubica en la capa de Control, específicamente en el CSCF. El CSCF está definido como un servidor SIP, encargado de procesar todo el tráfico de señalización IMS en pro de controlar las sesiones multimedia. Actualmente se encuentran definidos tres tipos de CSCF: [9][5]

- Proxy CSCF (P-CSCF): Como la puerta de entrada del tráfico de señalización ante las redes IMS, en especial, definida para los clientes IP basados en SIP.
- Serving CSCF (S-CSCF): Provee de un servicio de lógica de coordinación, útil en el registro de usuarios y el control de sesiones.
- Interrogating CSCF (I-CSCF): Actúa como un proxy SIP que proporciona una pasarela para otros dominios o para otras redes IMS.

A lo largo de este documento se dará una referencia mucho más precisa de la participación que tiene cada una de estas tres funciones dentro del flujo de señalización en IMS, especialmente, en los procesos de señalización relacionados con el protocolo SIP y su vínculo con la Gateway SIP. Por lo pronto, se describen los requisitos que el 3GPP ha propuesto sobre el protocolo SIP, para que éste pueda ser utilizado dentro de IMS como protocolo base.

1.3 Requisitos de IMS para el protocolo SIP

Al tratar de implementar una arquitectura convergente como IMS, el 3GPP ha encontrado una amplia lista de requisitos relacionados con las exigencias ya existentes de manera individual para cada una de las redes tradicionales, y a su vez, con la necesidad de lograr un alto nivel de interacción entre estas redes. Además, una de las principales razones abordadas, ha sido la especial ubicación de IMS dentro de un entorno móvil, con implicaciones sobre SIP relacionadas con la red de acceso y los parámetros de radio comunicaciones, las cuales no han sido consideradas en las definiciones previas del protocolo.

A continuación se muestra una lista de los requisitos, y su implicación en los procesos de señalización basados en el protocolo SIP. [10]

1.3.1 Requisitos Generales

- Uso eficiente de la interfaz de radio: El tráfico de señalización se debe ver notablemente reducido, debido a la escasez en los recursos de radio, tales como potencia, ancho de banda, seguridad, etc.

- Mínimo tiempo de establecimiento de la comunicación: se deben dedicar recursos suficientes al establecer la sesión, de tal manera que el usuario perciba un tiempo mínimo en el inicio de la comunicación.

- Mínimo soporte requerido en el terminal: teniendo en cuenta todas las limitantes de los terminales, en especial de los dispositivos móviles, tales como memoria, procesador, potencia, etc. Se determina que las labores de señalización deben exigir

al mínimo a los terminales involucrados, y se debe hacer transparente para éstos la generación de un nuevo y complejo tráfico de señalización.

- Soporte para escenarios Roaming y no-Roaming: No deben existir cambios significantes en el tráfico de señalización entre estos dos escenarios.

- Gestión de Usuarios Móviles: Esta gestión corresponde a la capa de Acceso, por lo tanto no deben existir variantes en SIP que se afecten por la gestión de usuarios móviles.

- SIP debe soportar direcciones IPv6.

1.3.2 Requisitos en el Registro

- Los usuarios se deben registrar previo al establecimiento de una sesión: El proxy SIP debe estar en capacidad de reconocer la ubicación y la disponibilidad de los usuarios que intervienen en la comunicación. Además, el SIP proxy debe poder perfilar a los usuarios, de tal manera que le asigne a los mismos solamente determinados servicios orientados a su perfil. Lo anterior se puede lograr únicamente con un registro previo de los usuarios en el proxy SIP.

- Registro Eficiente: Un simple mensaje REGISTER debe ser útil para realizar la labor completa de registro, debido al requisito de bajas exigencias para la interfaz de radio.

- Los usuarios pueden iniciar el proceso de eliminación de su registro en la red, o lo que se podría denominar "*des-registro*" (según una traducción literal del inglés) del Equipo de Usuario (User Equipment - UE): En el momento en que el usuario desactive su terminal, éste debe enviar un mensaje al proxy para que lo *des-registre*. De la misma manera, se puede iniciar un des-registro desde la S-CSCF.

- La red tiene la capacidad de des-registrar o volver a registrar a un usuario: En IMS la red debe cumplir algunas labores sobre las sesiones que generalmente no se realizan en una comunicación basada en SIP, tales como eliminar el registro de un usuario o volver a registrarlo. Esto, con el fin de soportar algunas de las exigencias de la integración de servicios.

1.3.3 Requisitos de compresión de mensajes SIP

- Debido a la escasez en los recursos de radio y al bajo ancho de banda que esta interfaz representa, se deben comprimir los mensajes SIP que viajan por medio del aire, para reducir el número de bytes enviados desde el Agente de Usuario (User Agent - UA) hacia el proxy SIP.

- El mecanismo de compresión debe ser independiente del algoritmo escogido.

- El impacto de la compresión de SIP debe ser mínimo para la red.

- Las especificaciones de compresión en la estructura de SIP debe ser extensible, para soportar nuevos algoritmos de compresión.

1.3.4 Requisitos de Calidad de Servicio relacionados con SIP

- Los parámetros de Calidad de Servicio destinados para las labores de señalización, y la selección de los esquemas de asignación de recursos, deben ser independientes de los protocolos de control de sesiones escogidos.

- Debe existir una coordinación entre SIP y la asignación de parámetros de Calidad de Servicio y Recursos a las sesiones establecidas.

1.3.5 Prevención de uso indebido de los servicios SIP

- Los usuarios en una red IMS deben estar limitados para que no hagan un mal uso de la misma, como por ejemplo, no cumplir con los procedimientos completos de enrutamiento. Además, un usuario que no está pagando por determinado servicio, no debe poder consumirlo, y tampoco debe poder consumir determinados recursos de Calidad de Servicio por los cuales no está facturando. La red debe estar en capacidad de lograr dicha limitación, basándose en las labores de señalización y establecimiento de las sesiones.

1.3.6 Identificación de Usuarios

- SIP debe soportar las Identidades Privadas de Usuario. Estas identidades son asignadas a usuarios desde la red local para manejar una perspectiva propia desde la red para estos usuarios. Las Identidades Privadas son usadas generalmente para autenticación, autorización, administración e incluso en algunos casos para tarificación.

- Los usuarios hacen uso también de una o varias identidades públicas. Estas identidades son utilizadas cuando se solicita una comunicación con otros usuarios. SIP debe soportar el uso extendido de múltiples identidades públicas dentro de su estructura.

1.3.7 Identificadores utilizados en Enrutamiento

- En IMS, los identificadores utilizados en capa de enrutamiento son reflejados dentro de SIP como URIs. Por lo tanto, cuando el terminal pertenece a una red cuyo formato de identificadores está basado en E.164 [11], se debe hacer una conversión a las URI de SIP para manejo interno dentro de una red IMS.

1.3.8 Enrutamiento de Mensajes SIP

- Debe existir un Proxy de salida (outbound proxy) localizado generalmente en la red externa, el cual realiza tareas de compresión de los mensajes SIP y funciones de seguridad. Además, debe estar en capacidad de interactuar con los mecanismos utilizados por la red para autenticación y autorización en la reservación de medios.

- La determinación de qué servicios van dirigidos a qué usuarios se realiza por medio de un proxy de servicios SIP (SIP Serving Proxy).

1.3.9 Tarificación

- Las sesiones deben tener soporte para los dos modelos más típicos de tarificación: prepago y postpago. Por lo tanto, SIP deberá estar en capacidad de ser útil en el establecimiento de sesiones embarcadas en estos dos modelos. Esto, debido a que la red deberá tener algunos privilegios en línea sobre las sesiones, en el caso de las comunicaciones tarificadas en un modelo prepago, donde las labores de tarificación se realizan en tiempo real. En el caso de las comunicaciones postpago, los procesos de tarificación no afectan las comunicaciones en tiempo real, pero sí periódicamente, y esto se constituye en una responsabilidad adicional para el protocolo SIP.

- Uno de los principales objetivos abordados al plantear la arquitectura de IMS ha sido el de la diferenciación de servicios. Esta diferenciación supone el uso de nuevos métodos de tarificación en comunicaciones de voz, video y datos, distintos a los métodos habituales basados en el tiempo o la tasa de transferencia en una comunicación. Tales métodos podrían ser, por ejemplo, los relacionados con el número de recursos multimedia que la comunicación exija, o con el tipo de recursos multimedia consumidos en una misma sesión. SIP debe portar en su contenido determinados identificadores del tipo de tarificación IMS que se está utilizando para cierta sesión.

1.3.10 Soporte SIP para los servicios y capacidades IMS adicionales

- Gracias a la extensibilidad del protocolo SIP, el 3GPP ha visto en él una alternativa óptima para suplir las necesidades de señalización dentro de la arquitectura de IMS tanto para servicios tradicionales, como para nuevos y mejores servicios basados en las capacidades adicionales de convergencia propuestas en IMS.

- SIP debe soportar las exigencias que surgen con relación a los servicios y protocolos tradicionales, debido a que estos deben prestarse por lo menos con la misma calidad que en un sistema anterior a la implantación de IMS.

1.3.11 Modelo de seguridad

- Los parámetros de seguridad en IMS tienen una relación muy directa con los mensajes SIP entre cada una de las entidades que lo utilizan. Básicamente se considera que el requerimiento de seguridad sobre SIP se ve reflejado en la implementación de nuevas extensiones que permitan adaptar métodos de seguridad a las sesiones.

- Los escenarios donde SIP debería soportar los parámetros de seguridad exigidos son: entre el dispositivo del usuario y la red externa, y entre la red externa y la red local, o dentro de la misma red local.

Todos estos requisitos tienen una representación práctica dentro de la estructura del protocolo SIP, y dentro del flujo de señalización producido con un nuevo perfil de este protocolo, definido en conjunto por el 3GPP y la IETF. A continuación se brinda una descripción de este protocolo, y su relación con IMS.

1.4 Generalidades del protocolo SIP adaptado para la arquitectura de IMS

Uno de los principales objetivos planteados al definir la arquitectura de IMS ha sido la integración de la mayor parte de servicios de telecomunicaciones tradicionalmente desplegados por los distintos operadores. En la búsqueda de este objetivo, una de las tareas que surgió fue la definición de un lenguaje o protocolo común entre los servicios que se desean integrar, convirtiéndose esto en la base del fenómeno de la convergencia de servicios actual. Por lo tanto, la escogencia de un protocolo debería orientarse a la capacidad que éste tenga para adaptarse a las características de los servicios y las redes existentes, además, adaptarse a las necesidades de mejoramiento que proponen las redes emergentes.

Durante la definición de la arquitectura IMS se evidenciaron amplias ventajas del protocolo SIP, definido por la IETF, frente a otros protocolos de señalización tales como Señalización Número Siete (Signaling System #7 - SS7) o la familia de protocolos H.323, para ser utilizado como base en la definición de un nuevo perfil de protocolo que cumpliera con la mayor parte de los requisitos de señalización en una red IP como lo es IMS. De esta manera surge una nueva definición para SIP, considerada como un nuevo perfil de este protocolo, desarrollada por el 3GPP y que cuenta con la adición de las características necesarias para su uso dentro de IMS. [5]

La manera en que el 3GPP ha adoptado al protocolo SIP en su arquitectura IMS, ha sido mediante la adición de múltiples extensiones, ya que por definición, SIP no es un protocolo destinado a un tipo de red o aplicación en especial. Dichas extensiones se describen a continuación [5][6][12]:

- SigComp: Mecanismo utilizado en la compresión de mensajes SIP.[13]
- P-headers: Cabeceras adicionadas a SIP para requerimientos exclusivos de IMS.[14]
- Acuerdo de Seguridad: Define la negociación de parámetros de seguridad según el tipo de usuario que acceda a la red.
- AKA-MD5: Determina cómo los terminales y las redes son autenticados, y define claves criptográficas a utilizar en IPsec. [16]

- IPsec: Es un conjunto de protocolos que define parámetros de seguridad en distintos puntos de la red. [17]
- Media Authorization: Determina qué medios están autorizados para utilizarse.[12]
- Mobile Registration: Útil en la determinación de rutas entre la red y los terminales.
- Reg-Event Package: Visualiza el estado de registro de un usuario en la red.[18]
- IPv6: Para el manejo de las diferentes variaciones propuestas por el protocolo IPv6.
- Preconditions: Para la negociación de Calidad de Servicio y otros requerimientos antes de iniciar una comunicación entre dos terminales.
- IMS Resource Reservation: Define cómo hacer reservación de recursos para los clientes que se comuniquen o las sesiones que se establecen.
- Session Description Protocol (SDP): Incluye las características tradicionales del protocolo SDP y las adicionales para IMS.[19]
- Uso de XML: para los protocolos XML altamente usados en señalización SIP-3GPP.
- Extensiones SIMPLE de IMS: Abordan información sobre presencia y requerimientos de señalización en mensajes instantáneos.

Algo que se puede notar en esta lista de extensiones, es que gran parte de ellas están destinadas al uso exclusivo dentro de la arquitectura IMS, y por lo tanto, clientes basados en el protocolo SIP de la IETF no estarían en posibilidad de acceder a determinadas capacidades y/o servicios de estas Redes de Próxima Generación. Esto muestra la importancia del desarrollo de una pasarela de señalización como la que se presenta en el actual proyecto (ver capítulo 4 de este documento), la cual está en capacidad de brindar acceso a determinadas características y servicios de una red IMS desde clientes SIP-IETF, haciendo uso de herramientas Software para el manejo de las extensiones anteriormente descritas.

Uno de los principales subproductos predecesores al diseño y desarrollo de una pasarela de señalización SIP, es el establecimiento de las diferencias existentes entre el protocolo SIP-IETF y el perfil diseñado por el 3GPP para IMS, SIP-3GPP. En el siguiente apartado se muestra una lista de dichas diferencias, y en un sentido más específico, una lista de las adiciones y modificaciones que se deberían hacer al protocolo SIP para permitirle ser útil dentro de la arquitectura IMS.

1.5 Paralelo entre las definiciones IETF y 3GPP para el protocolo SIP

1.5.1 Extensiones 3GPP para el protocolo SIP

Como se ha mencionado anteriormente, SIP es un protocolo altamente extensible, y por eso, el 3GPP junto con la IETF han emprendido la búsqueda de una definición renovada del protocolo SIP que satisfaga completamente las necesidades impuestas en la arquitectura de IMS. Según el apartado anterior, al definir las características principales de una red convergente como IMS, se debe contar también con ciertas implicaciones y requerimientos de señalización que los avances propuestos por esta especificación conllevan. Básicamente, la solución para estos requerimientos se ha constituido por una serie de modificaciones y adiciones a la estructura del protocolo SIP. Éstas, se ven reflejadas en el uso de nuevas extensiones especialmente definidas por el 3GPP y la IETF para SIP, las cuales se pueden agrupar en 5 categorías: extensiones generales, de operación de la sesión, de calidad de servicio, AAAC y seguridad. Estas categorías se describen a continuación: [12]

1.5.1.1 Extensiones Generales

En IMS se requiere transparencia para el usuario en la ejecución del *roaming*. Además, los procesos de señalización se hacen más complejos debido a que el número de los proxy CSCF necesarios para el establecimiento de las sesiones entre distintas redes es bastante alto. Los recursos de ancho de banda también se reducen para un ambiente móvil, donde la interfaz de radio impone algunas limitantes, haciendo necesario el uso de compresión de mensajes SIP. Todos estos requerimientos se manifiestan en algunas extensiones agregadas a la estructura básica del protocolo SIP, que contienen información sobre la red de acceso y en especial, sobre las características del dispositivo y la interfaz de radio utilizada. Estas extensiones podrían ser: la cabecera Path, y el mecanismo básico de SIP, record-route, para el reconocimiento de múltiples proxy CSCF involucrados en la transmisión de un mensaje SIP. Además, para le compresión de mensajes se utiliza la extensión Sig-Comp [13] entre el Equipo de Usuario y la P-CSCF.

1.5.1.2 Extensiones relacionadas con la operación de las sesiones.

En el establecimiento de las sesiones se han adicionado nuevas funcionalidades, tales como localización de usuarios en un ambiente móvil, identificación de perfiles de usuario, solicitudes de privacidad en la sesión y demás servicios y capacidades sobre la sesión que se han atribuido al uso exclusivo de una red IMS. Estas nuevas capacidades referidas estrictamente al manejo general de las sesiones, son abordadas mediante el uso de las Cabeceras Privadas [14]. Un par de ejemplos de estas cabeceras serían: P-Access-Network-Info, para la localización de la identidad y posición de usuarios en interfaces móviles, y P-Asserted-Identity, para la identificación de usuario y sus capacidades durante el establecimiento de la sesión.

1.5.1.3 Extensiones relacionadas con Calidad de Servicio (QoS)

El protocolo para la descripción de las sesiones SDP tiene una gran responsabilidad a la hora de negociar los parámetros de Calidad de Servicio relacionados con las capacidades disponibles en terminales participantes en una comunicación SIP. Esto se realiza mediante el modelo característico en SIP de oferta/respuesta. Además, se deben considerar las capacidades adicionales de IMS relacionadas con diferenciación de servicios y localización de parámetros de Calidad de Servicio.

1.5.1.4 Extensiones relacionadas con AAAC (Authentication, Authorization, Accounting and Charging)

En la interconexión de distintas redes IMS, una red visitada debe pasar a la red local algunos parámetros referentes al usuario que desea establecer la comunicación, para que la red local lo pueda identificar, o dado el caso, registrar. Además, las entidades de IMS se han definido

con nuevas capacidades sobre las sesiones, como por ejemplo, eliminar del registro o volver a registrar a un usuario, con el ánimo de actualizar o modificar algunos de sus datos o gestionar sus capacidades. Todos estos requerimientos deben ser soportados por SIP, y es mediante el uso de las P-headers [14] que logra satisfacer dichas necesidades. En el caso particular del envío de los datos de usuario para su propio registro, se utiliza la P-Visited-Netwok-ID, cuyo valor sirve como identificador de un usuario perteneciente a una red externa, generalmente denominada Red Visitada. Además, se debe implementar el uso de notificaciones de eventos SIP, para darle capacidades, sobre las sesiones, a las entidades IMS, específicamente, al S-CSCF. Dichas notificaciones se basan en el mensaje SIP NOTIFY, enviado por la S-CSCF hacia los Equipos de Usuario, con el objetivo de informarles sobre cambios en el registro.

Otra P-header que actúa en labores de AAAC, es la P-Media-Authorization. Esta cabecera es utilizada para brindar un control de recursos multimedia entre el terminal y el P-CSCF, evitando que los usuarios consuman servicios y capacidades multimedia de IMS a las cuales no tienen permiso.

En cuanto a la tarificación, se deben implementar las cabeceras SIP P-Charging-Vector para transportar información de la tarificación sobre determinado usuario, y la P-Charging-Function-Address, para distribuir direcciones de los elementos de tarificación por entre los distintos nodos IMS. [20]

1.5.1.5 Extensiones de Seguridad

Uno de los principales objetivos en la definición de IMS, ha sido adicionar características más completas de seguridad a redes que tradicionalmente no han tenido un alto nivel de confiabilidad, como son las redes IP. Esta responsabilidad se ha asignado al uso del protocolo IPSec Encapsulated Segurity Payload (ESP) [17]. Éste, se comporta naturalmente como un protocolo de capa de aplicación, lo cual reduce completamente los traumatismos sobre las tareas de señalización que debe cumplir SIP.

Además de IPSec, se implementa un mecanismo para ocultación de topologías (THIG) [9][21]. Esta labor se realiza dentro del I-CSCF, el cual entraría a actuar como un proxy SIP de ocultación (Hiding Proxy), dándole seguridad a la información privada que se involucra en el establecimiento y manejo de las sesiones.

Gracias a la definición de las extensiones agregadas por el 3GPP al protocolo SIP, es posible proceder al establecimiento de las diferencias más relevantes que aparecen entre la especificación inicial de SIP, y el perfil desarrollado por el 3GPP para este protocolo.

1.5.2 Diferencias Teóricas entre las Especificaciones IETF y 3GPP para el protocolo SIP

En una comunicación basada en el protocolo SIP definido por la IETF, actúan generalmente dos o más UAs, los cuales dan inicio prácticamente a todas las labores de señalización SIP para el establecimiento, modificación y terminación de las sesiones [1]. Los demás elementos que actúan en este tipo de comunicación son, principalmente, los proxy

pertenecientes a cada una de las redes participantes. Estos proxy no tienen capacidades de manejo sobre las sesiones, sino que responden (con registro y búsqueda de usuarios, localización, etc.) a las solicitudes realizadas por los UAs involucrados en la comunicación. En IMS, una de las características más importantes hace referencia a las capacidades que adquieren algunas entidades del núcleo de la capa de control sobre las sesiones. Dichas entidades actúan regularmente como proxy, específicamente el CSCF y sus derivaciones: P-CSCF, I-CSCF y S-CSCF.

Las capacidades sobre las sesiones que poseen las funciones de la capa de control de IMS, hacen necesario el uso de una serie de extensiones y modificaciones a la especificación básica del protocolo SIP, cuya clasificación ha sido descrita en la sección 1.5.1. A continuación se muestra una lista de las implicaciones que dichas extensiones han tenido sobre las características generales de los procesos de señalización SIP, con relación a las distintas entidades (UA, Proxy) y métodos involucrados en estos procesos (Registro, Establecimiento, Terminación, Modificación, etc.) [12]

1.5.2.1 Características Generales

SIP – IETF	SIP – 3GPP
Las cabeceras SIP pueden usar cifrado S/MIME (Secure / Multipurpose Internet Mail Extensions) utilizado para criptografía y firmas digitales de correo electrónico. Esto se puede llevar a cabo gracias a que simplemente dos proxy, uno inicial y otro final, deberán entender el cifrado S/MIME, lo cual no representa una labor mayormente compleja. De la misma manera sucedería para el cifrado del cuerpo (body) en los mensajes SIP.	Debido a la implementación de múltiples proxy intermedios para el establecimiento de una comunicación entre redes basadas en la arquitectura IMS, las cabeceras SIP no pueden ser cifradas utilizando S/MIME. Esto, debido a que esa información no sería entendible por parte de los proxy intermedios. De la misma manera sucedería para el cuerpo (body) de los mensajes SIP.
Las cabeceras en SIP – IETF son cifradas bajo la utilización de S/MIME.	Utilización de THIG para ocultación de las cabeceras SIP.
La Autenticación de agente de usuario (UA) es opcional en el proxy.	La Autenticación de UAs en los proxy es prohibida.

Tabla 1. Diferencias en las Características Generales entre SIP-IETF y SIP-3GPP

1.5.2.2 Características relacionadas con transacciones SIP

SIP – IETF	SIP – 3GPP
El denominado Registro de Enrutamiento en SIP (SIP Record-Route), hace referencia a la obligación que tienen los proxy de filtrar determinadas cabeceras de enrutamiento pertenecientes a los mensajes SIP y actuar consecuentemente, haciendo un enrutamiento de las mismas hacia los Equipos de Usuario (UE). Este procedimiento es opcional en el uso de SIP-IETF.	El CSCF posee ciertas capacidades sobre las características de las sesiones, como por ejemplo la de filtrar determinadas cabeceras SIP para enrutamiento con el objetivo de ocultar detalles de la topología de red de los usuarios. Entonces, el P-CSCF debe estar en capacidad de filtrar las cabeceras de enrutamiento de los mensajes SIP, lo que hace que el Registro de Enrutamiento sea obligatorio en SIP-3GPP.
Las cabeceras que contienen el tamaño del cuerpo del mensaje SIP (SIP Content Length) no son siempre obligatorias. La aparición de estas depende del uso que se les pueda dar en capa de transporte.[1]	Las cabeceras Content-Length de SIP son obligatorias en SIP-3GPP.
Solamente las transacciones del REGISTER de SIP pueden llevar la dirección del UA en su cabecera TO.	La dirección del UE va en las cabeceras de los mensajes para subscripción de paquetes de eventos, es decir, en los mensajes SUBSCRIBE de SIP.[21]
Las cabeceras REQUIRE son utilizadas por los clientes para anunciarle a los servidores de UA sobre las opciones que él espera que el servidor soporte, con el objetivo de procesar las solicitudes apropiadamente [1]. En SIP-IETF estas cabeceras se hacen estrictamente necesarias, debido a que en ellas se definen las extensiones requeridas para el establecimiento de las sesiones.	Las extensiones obligatorias 100Rel [22] se refieren al uso del método PRACK (Provisional Aknowledgment) para brindar fiabilidad a los métodos provisionales de SIP (1XXX)[1]. Estas extensiones no hacen parte de las cabeceras Require de SIP-3GPP.
Los proxy que actúan en una comunicación SIP-IETF no pueden iniciar procedimientos para la liberación de las sesiones.	Además del procedimiento para la liberación de sesiones, la S-CSCF y P-CSCF están en capacidad de maniobrar sobre distintas capacidades de las mismas.

Tabla 2. Diferencias en las Transacciones SIP entre SIP-IETF y SIP-3GPP

1.5.2.3 Extensiones SIP soportadas en IMS

SIP – IETF	SIP – 3GPP
Las cabeceras privadas (P-Headers) no son necesarias.	En la definición de IMS, uno de los principales avances fue la definición de cabeceras SIP exclusivas de IMS, destinadas al cumplimiento de los objetivos de convergencia, calidad de servicio, seguridad y diferenciación de servicios propuestos por el 3GPP. Estas cabeceras están definidas en el RFC-3455 [14], denominadas como P-Headers, útiles en la localización, tarificación, autenticación, etc., dentro de IMS.
Se define un Mecanismo de Privacidad descrito en el RFC-3323 [23]	La privacidad en la información de los usuarios se hace estrictamente necesaria en IMS. Por lo tanto, la implementación del Mecanismo de Privacidad para SIP definido en el RFC-3323 [23] es obligatoria.

Tabla 3. Diferencias en las Extensiones Generales SIP entre SIP-IETF y SIP 3GPP

1.5.2.4 Extensiones SIP soportadas en el UA

SIP – IETF	SIP – 3GPP
Para el UA en el establecimiento de una sesión basada en SIP-IETF son opcionales las siguientes cabeceras: - Fiabilidad en Respuestas Provisionales. (RFC 3262) [22]. - Integración de Recursos de Gestión (RFC 3312) [24]	Para el UA en el establecimiento de una sesión basada en SIP-3GPP son obligatorias las siguientes cabeceras: - Fiabilidad en Respuestas Provisionales. (RFC 3262) [22]. - Integración de Recursos de Gestión (RFC 3312) [24]
Las cabeceras para notificación de eventos (Event Notification) (RFC 3265) [25] son opcionales.	La S-CSCF se comporta siempre como un notificador. Por lo tanto, las cabeceras para notificación de eventos son obligatorias en SIP-3GPP. Además, los roles de notificador y subscriptor de usuarios SIP, son obligatorios para algunas entidades de IMS, y por tanto las cabeceras referidas a ellos también lo son.
Las siguientes cabeceras SIP de UA son opcionales: - Cabecera para el registro de contactos no adyacentes (RFC 3327)[26] - Cabeceras para descubrimiento de ruta en tiempo de registro (RFC 2608)[27]	Las siguientes cabeceras SIP de UA son obligatorias para la S-CSCF y el UE: - Cabecera para el registro de contactos no adyacentes (RFC 3327)[26] - Cabeceras para descubrimiento de ruta en tiempo de registro (RFC 2608)[27]

SIP messaging (RFC 3428)[28] es opcional.	SIP messaging (RFC 3428) [28] es obligatorio para la S-CSCF.
SIP compression (RFC 3320) [13] es opcional.	SIP compression (RFC 3320) [13] es obligatorio para el UE, debido a la escasez de recursos en la interfaz de radio, para un ambiente móvil.
Acuerdo de Mecanismo de Seguridad (RFC 3329) [15] es opcional.	Acuerdo de Mecanismo de Seguridad (RFC 3329) [15] es obligatorio para el UE.

Tabla 4 Diferencias en las Extensiones soportadas por UA entre SIP-IETF y SIP-3GPP

1.5.2.5 Extensiones SIP soportadas en el Proxy

SIP – IETF	SIP – 3GPP
Las siguientes cabeceras son opcionales para el Proxy SIP-IETF: - Cabecera para registro de contactos no adyacentes. (RFC 3327) [26]. - Cabecera para descubrimiento de servicios durante registro (RFC 2608)[27]. - SIP Messaging (RFC 3428)[28]. - SIP Compression (RFC 3320)[13]. - Acuerdo de mecanismo de seguridad (RFC 3329)[3329]	Las siguientes cabeceras son obligatorias para el P-CSCF de SIP: - Cabecera para registro de contactos no adyacentes. (RFC 3327) [26]. - Cabecera para descubrimiento de servicios durante registro (RFC 2608)[27]. - SIP Messaging (RFC 3428)[28]. - SIP Compression (RFC 3320)[13]. - Acuerdo de mecanismo de seguridad (RFC 3329)[3329]

Tabla 5. Diferencias en las Extensiones para Proxy soportadas por SIP-IETF y SIP-3GPP

Uno de los aspectos más relevantes por resaltar en la anterior comparación, es que las entidades pertenecientes a la capa de control de IMS pueden asumir el rol que generalmente es afrontado por los UA o Proxy, en determinados estados del flujo de señalización de las sesiones. Por ejemplo, en la terminación de un registro, la entidad IMS donde ocurrió el evento de des-registro (generalmente la S-CSCF), actúa como un UA, para enviar la notificación de dicho des-registro a la red.

Además, en el contenido de las tablas anteriores, se hace evidente que existen determinadas características obligatorias dentro de una especificación de SIP, pero que pueden ser prescindibles dentro de una comunicación basada en la otra especificación del protocolo. Por ejemplo, el uso de las P-headers, los métodos de ocultación, mecanismos de seguridad, cabeceras de notificación, entre otros aspectos de la definición del 3GPP para SIP, resulta de carácter obligatorio dentro de las funciones de la señalización en IMS.

2. PROCESOS DE SEÑALIZACIÓN DENTRO DE UN ENTORNO BASADO EN LA ARQUITECTURA IMS

Las tareas de señalización requeridas para establecer una comunicación convergente en una red IMS han tenido especial atención durante el desarrollo de esta arquitectura, teniendo en cuenta que dentro de los procesos de señalización se deben encauzar algunos requerimientos que hacen referencia a las capacidades adicionales encontradas en una red IMS, tales como Calidad de Servicio, seguridad, diferenciación de servicios y convergencia, entre otras.

La necesidad de asignar nuevas responsabilidades al protocolo de señalización, hace suponer la utilización de un protocolo altamente extensible, tanto para hacerlo adaptable a las capacidades internas (control, registro, autenticación y acceso a servicios) de una red IMS, como para el manejo de información adicional sobre la red visitada, en capa de acceso y con relación a las características y capacidades del Equipo de Usuario (UE).

Para el flujo de señalización se deben tener en cuenta consideraciones tanto de capa de aplicación relacionadas con los mensajes, cabeceras y cifrados utilizados en el manejo comunicaciones SIP, como en elementos necesarios para generar una conectividad con las redes IP[29].En este documento se tendrán en cuenta solamente las implicaciones de señalización que hacen referencia estrictamente al protocolo SIP, debido a que éste corresponde al centro de estudio del proyecto, y las características de conectividad IP deben ser indiferentes en el manejo de servicios con protocolo de capa de aplicación como SIP.

Cada función de la arquitectura IMS asigna nuevas responsabilidades al protocolo de señalización SIP, las cuales tienen que ver con labores de registro, AAAC, acceso a servicios SIP, gestión de sesiones con usuario final, etc. En el siguiente apartado se explica de manera detallada cuáles son los efectos y requerimientos que tiene cada función y entidad perteneciente a la arquitectura IMS sobre el flujo de señalización SIP y los demás protocolos de señalización involucrados en una comunicación.

2.1 Protocolos de Señalización utilizados en la arquitectura IMS

Una red basada en la arquitectura IMS está conformada por distintas funciones, en lugar de módulos (Ver Anexo B), cuya interacción está basada en la utilización de diversos protocolos de comunicación que han sido escogidos para actuar dentro de la arquitectura IMS según sus características de seguridad, simplicidad, y efectividad en el desempeño para comunicar cada par de funciones. Además, existen protocolos dentro de la arquitectura destinados a proveer acceso a elementos externos a la misma, tales como los clientes u otras redes IMS o no IMS, de manera independiente al tipo de acceso de red utilizado.[9]

En la figura 1 se muestra la ubicación de cada protocolo de señalización dentro de la arquitectura de IMS.[29][30]

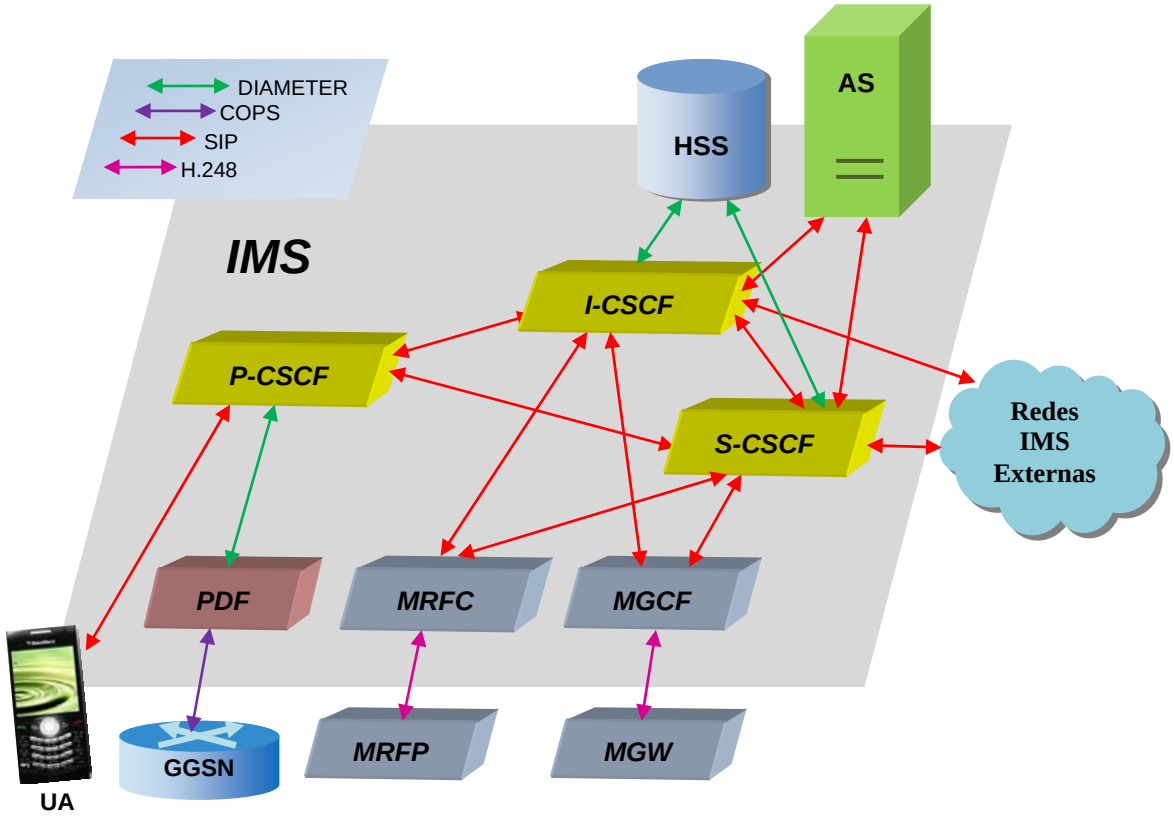


Figura 1. Arquitectura IMS y sus Protocolos de Señalización

2.1.1 SIP

SIP es utilizado dentro de la arquitectura IMS como protocolo de señalización para el control de sesiones y el control de servicio, permitiendo la negociación de recursos multimedia. SIP hereda de ciertas funcionalidades del protocolo de Transporte de Hipertexto (Hyper Text Transport Protocol - HTTP) utilizado para navegar sobre la web, y del Protocolo de Transporte Simple de Correo (Simple Mail Transport Protocol - SMTP) usados para la transmisión de mensajes electrónicos (e-mails).[30]

En la sección 2.2 se brinda una descripción más completa de la utilización de SIP como protocolo base en la señalización y control de sesiones en IMS. Las características generales del protocolo SIP están descritas en el Anexo B.

En el capítulo 3, se presenta el funcionamiento del protocolo SIP y sus requerimientos en el despliegue completo de un servicio IMS, haciendo referencia no solamente a las características de los mensajes SIP entre el cliente, la red visitada y la red local, sino también entre las distintas funciones pertenecientes a las tres capas básicas de la arquitectura IMS; y las implicaciones que tendrían dichas características sobre el proyecto presentado en este documento.

2.1.2 DIAMETER

Diameter [31] ha sido escogido para ser utilizado en redes basadas en la arquitectura IMS con el objetivo de realizar tareas de AAAC. Es una evolución del protocolo RADIUS[32]. Diameter funciona a la par con la aplicación que lleva su mismo nombre, la cual provee ciertas extensiones definidas dentro de las especificaciones de IMS.[30]

Diameter actúa dentro de IMS entre la I-CSCF y el HSS, en secuencia con los mensajes SIP utilizados para registro y establecimiento de sesiones, específicamente, aquellas tareas de señalización que requieren consultas en los registros de usuarios alojados en el HSS.

2.1.3 H.248 MEGACO

MEGACO [33] es utilizado entre la Media Gateway (MGW) y el Media Gateway Controller para manejar las tareas de señalización y gestión de sesiones durante una comunicación multimedia, entre dos o más clientes. Entre el MGW y el Media Gateway Controller se comparte una relación maestro/esclavo. De la misma manera que el 3GPP ha adicionado ciertas extensiones para el protocolo SIP con el objetivo de hacerlo funcional dentro de la arquitectura IMS, también se han añadido algunas extensiones al H.248, con el fin de que pueda ser interpretado en el manejo de conferencias multimedia por parte de la función IMS MGCF (Media Gateway Control Function).

2.1.4 COMMON OPEN POLICY SERVICE

Common Open Policy Service (COPS) [34], es un protocolo utilizado dentro de la arquitectura IMS para el transporte de políticas entre los puntos de decisión, denominados PDP (Policy Decision Points) y los puntos de políticas de ejecución, o PEP (Policy Enforcement Points). COPS es un protocolo utilizado generalmente para la administración, configuración y ejecución de políticas entre el PDP y el PEP. Estas dos entidades se alojan generalmente cada una en el servidor y el cliente respectivamente, con el objetivo de que la información de las políticas sea negociada entre estos dos elementos.

2.1.5 IPSec

Internet Protocol Security (IPSec) [17] provee protección a la integridad y confidencialidad de la información en la capa de red. Este protocolo funciona agregando seguridad a los protocolos de capas superiores y es generalmente utilizado para comunicaciones seguras entre nodos y pasarelas de seguridad. Según el tipo de protocolo que se va a proteger mediante el uso de IPSec, este actúa en dos modos distintos, modo tráfico o modo túnel. En modo tráfico generalmente provee servicios para la protección de protocolos de capas superiores, y en modo túnel para proteger el tráfico IP, abarcando por completo los datagramas transportados.

IPSec es utilizado en varias interfaces IMS: En modo tráfico es utilizado entre el terminal y la red, y en modo túnel es utilizado entre dos redes IMS distintas. Esto denota que IPSec es utilizado en el medio de prácticamente todas las entidades importantes de la arquitectura IMS, por lo tanto resulta de suma importancia su implementación dentro de la misma.

2.2 Procesos de señalización SIP dentro de una arquitectura IMS

Los módulos de la arquitectura de IMS que actúan dentro de los procesos de señalización en las comunicaciones y registro de usuarios son: CSCF y sus derivaciones P-CSCF, I- CSCF, S-CSCF; este módulo actúa como un proxy SIP, útil en el registro de usuarios y redirección de mensajes SIP. El módulo HSS, se introduce en los procesos de señalización como un repositorio útil en el registro, subscripción y determinación de características y capacidades de los usuarios SIP. El flujo completo de señalización SIP se basa en la especificación inicial del protocolo, utilizando la estructura SIP para el proceso de solicitudes y respuestas [29]. Se presenta a continuación una visión general del proceso de señalización en el contexto de una red IMS. [29][35]

2.2.1 Registro de un usuario no registrado en IMS utilizando el método SIP REGISTER

El proceso de registro de un usuario SIP dentro de una arquitectura IMS corresponde a un flujo muy similar al generalmente encontrado en el registro de usuarios SIP en cualquier SIP Registrar de un servidor SIP convencional. El SIP Registrar hace referencia a un proxy SIP encargado del registro de los datos de usuario, gestionando su estado de conexión y de disponibilidad dentro de la red.

Se inicia por una solicitud de registro por parte de un Agente de Usuario (UA), en el caso de IMS un Equipo de Usuario (UE), la cuál envía un mensaje SIP Register hacia el proxy SIP, que a su vez devuelve un desafío de autenticación al UE reflejado en un código desarrollado mediante el uso del tipo de cifrado acordado entre el UE y el servidor SIP. El UE debe reenviar un REGISTER, conteniendo una respuesta al desafío propuesto por el servidor SIP. Dicha respuesta corresponde a un código desarrollado en el mismo tipo de cifrado previamente acordado, y está implementada en función de los valores de nombre y contraseña de usuario, y dominio del SIP Proxy. De ser correcta esta respuesta, el servidos SIP emprende la labor final de registro del usuario en su base de datos, y devuelve una respuesta satisfactoria al UE (respuesta SIP 200 Ok). [29]

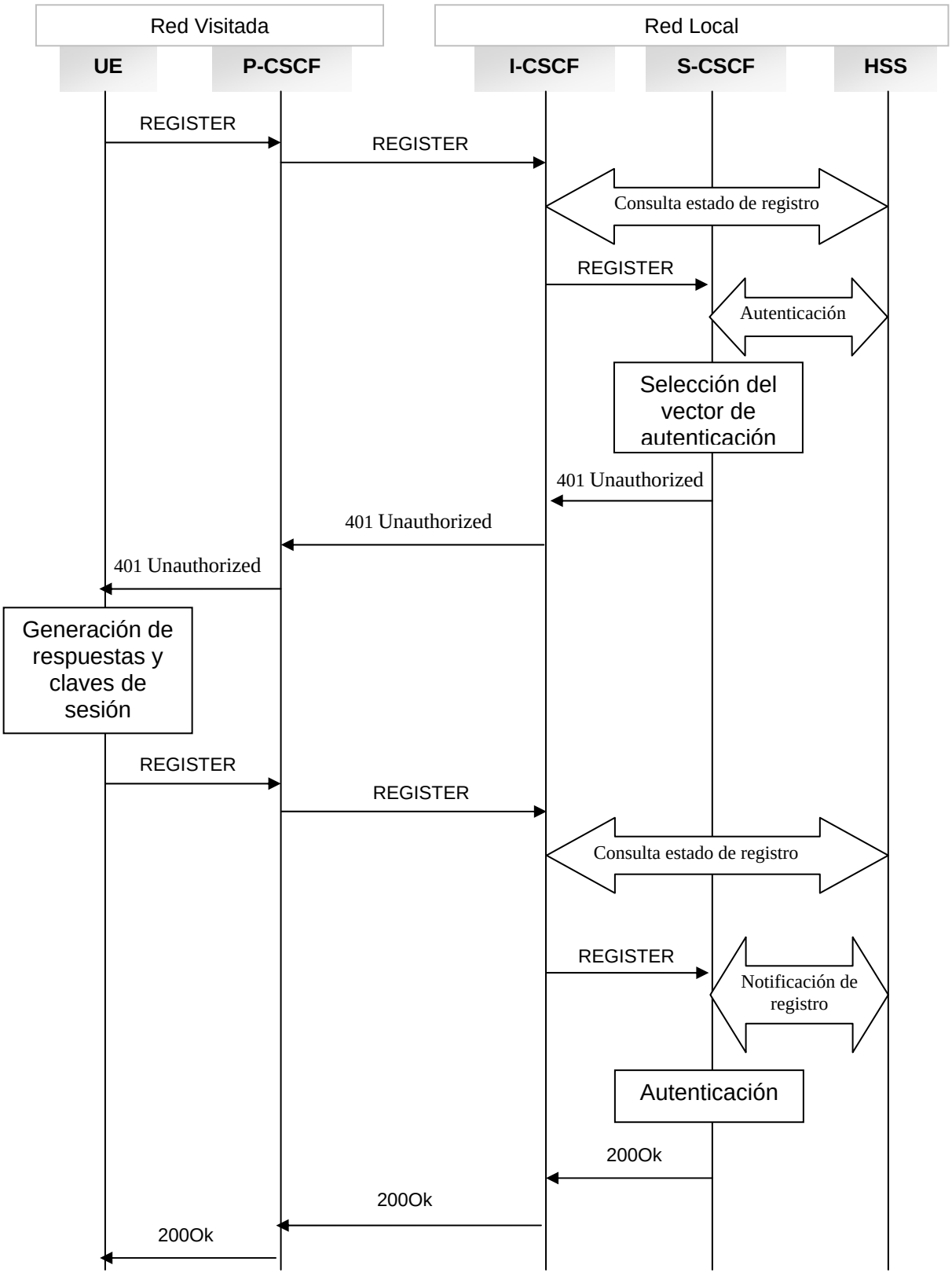


Figura 2. Registro de usuarios no registrado en la red

En IMS el proxy SIP está representado en algunas labores por la P-CSCF de la red visitada, o la P-CSCF de la red local (dependiendo de la ubicación del UE por registrar). La P-CSCF envía el REGISTER a la I-CSCF, que es la función IMS encargada de interactuar con redes IMS externas, y esta realiza una consulta en el HSS sobre la existencia y estado del usuario por registrar. Dependiendo del resultado de esta consulta, la I-CSCF decide si enviar o no el mensaje REGISTER hacia la S-CSCF, donde se desarrollará un desafío en función de los datos del usuario recibidos en el método REGISTER, y de los datos de URL del core de IMS. Dicho desafío es enviado en forma de una cabecera llamada WWW-Authenticate, dentro del método respuesta 401-Unauthorized. [29]

Con el método respuesta que llega al UE, ésta está en capacidad de generar una respuesta con los valores de sus características privadas y públicas (nombre, nombre de identidad en la red, contraseña, dominio). Dicha respuesta está cifrada utilizando el mismo método que se ha acordado al comienzo de la comunicación, y es enviada dentro de la cabecera Authorization, del segundo método REGISTER que se enviaría en secuencia hacia la P-CSCF desde el UE. [29][35]

2.2.2 Volver a registrar un usuario previamente registrado

Generalmente, la labor de volver a registrar un usuario consiste en enviar un nuevo REGISTER al SIP Registrar sin necesidad de recibir como consecuencia en el cliente un desafío contenido dentro de la respuesta 401-Unauthorized. En las tareas de registro no relacionadas con el protocolo SIP también se erradica la necesidad de efectuar algunos procesos, por ejemplo los procedimientos de DHCP por parte de la P-CSCF ya no son necesarios, además, el proceso de selección de la S-CSCF invocado por la I-CSCF se hace innecesario.

En la figura 3 se muestra un diagrama de secuencia con el flujo de información SIP necesario para establecer un registro de un usuario previamente registrado en el núcleo de una red IMS. [29][35]

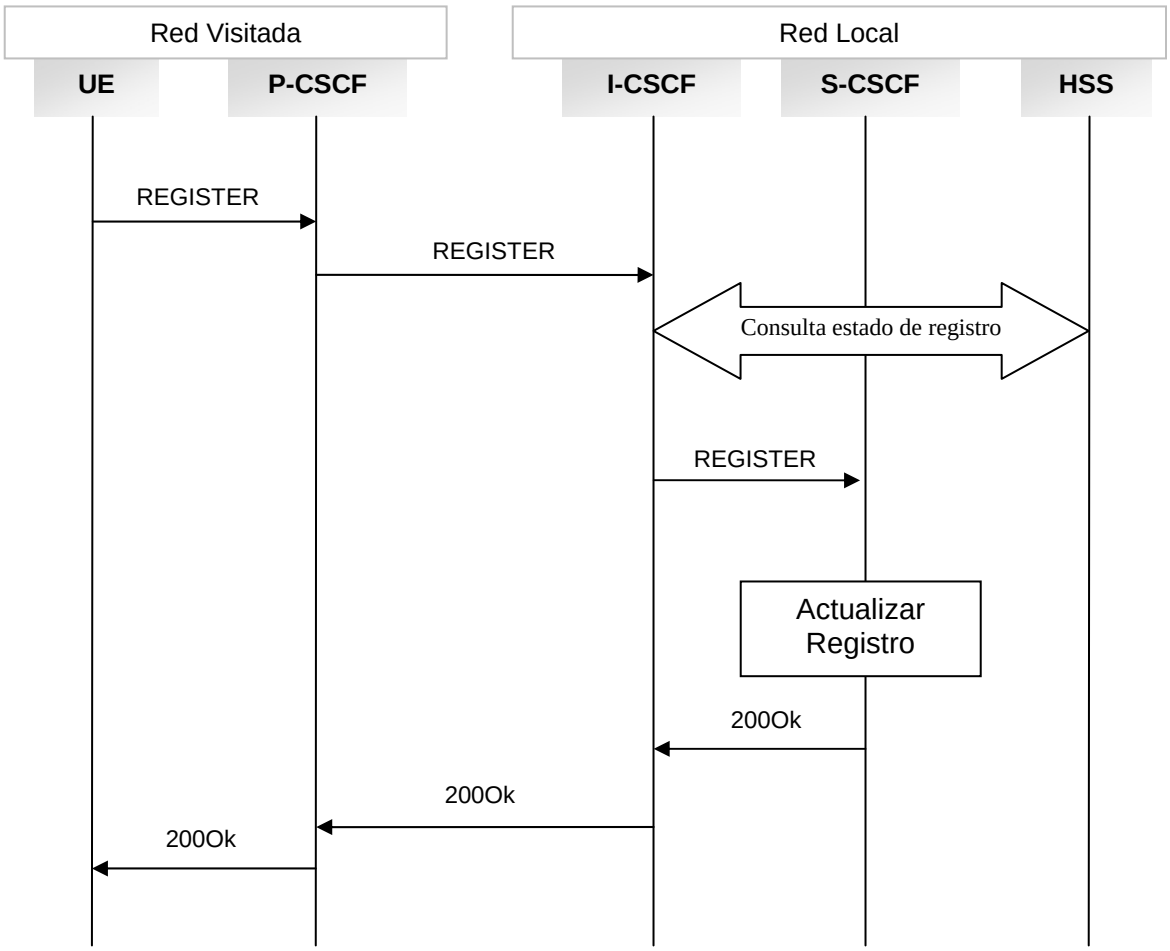


Figura 3. Volver a registrar un usuario previamente registrado en la red

En una comunicación basada en la arquitectura IMS, el REGISTER que procede del UE contiene también una cabecera **Authorization**, con información privada sobre el usuario, pero dicha información no va a ser necesaria para realizar autenticación, como en usuarios no registrados, sino que es simplemente para reconfirmar la previa validación del usuario.

2.2.3 Subscripción del UE utilizando el método SIP SUBSCRIBE

Las tareas de subscripción por parte de los Equipos de Usuario, consisten en una solicitud realizada por el UE a la S-CSCF para ser notificado por ésta cuando un evento de estado de registro ocurre. Dichos eventos podrían ser, a manera de ejemplo: eliminación del registro de usuario iniciado por alguna entidad de red, cambios de los parámetros de usuario registrados, etc. Esto permite que las distintas funciones de IMS tengan algunos privilegios sobre algunas características de los usuarios y de sus sesiones, gracias a que los eventos ocurridos dentro de la capa de control podrán ser notificados a los Equipos de Usuario, y de esta manera, actuar sobre las sesiones iniciadas por ellos. [29][35]

Se asume que el UE ha sido previamente registrado para iniciar la subscripción de un evento.

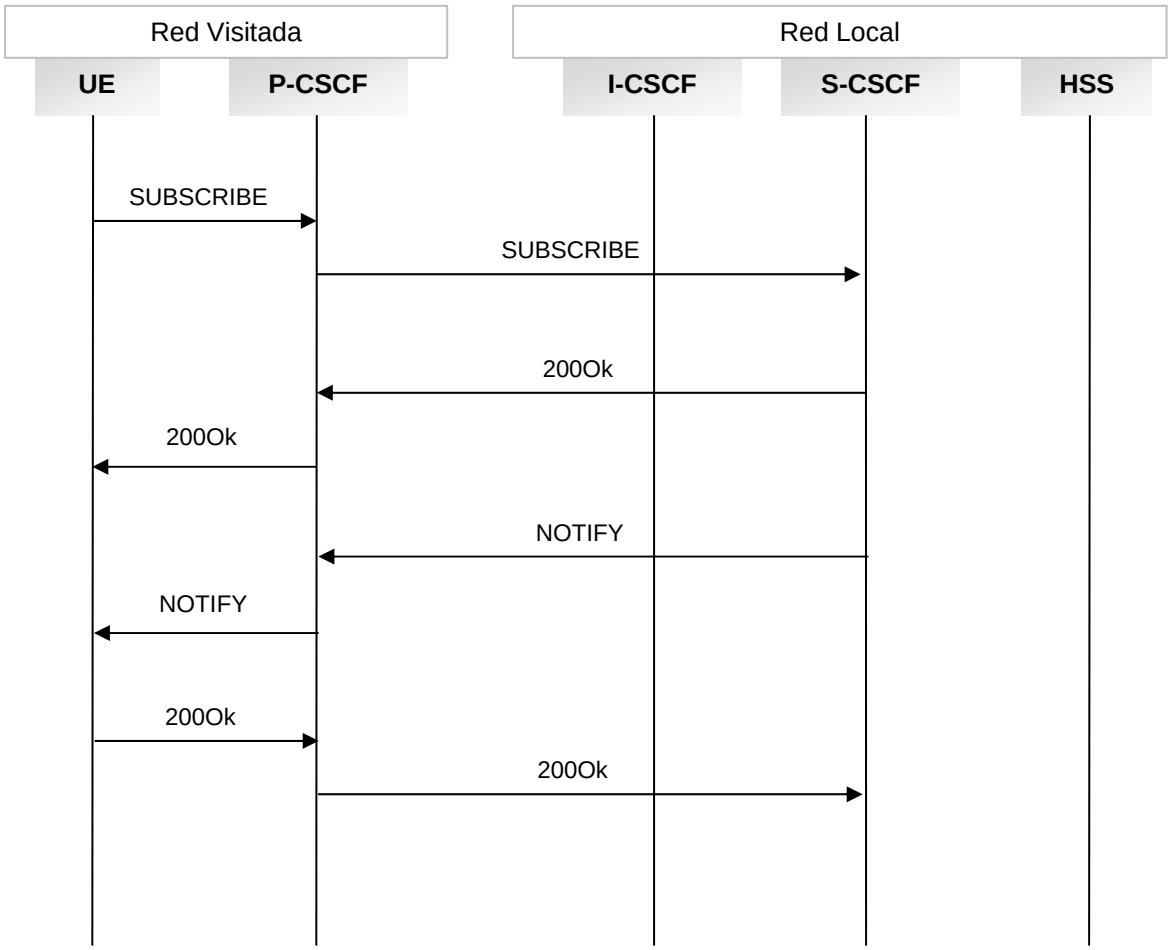


Figura 4. Subscripción del UE

La S-CSCF analiza el contenido de determinadas cabeceras del mensaje SUBSCRIBE y autoriza la subscripción para el UE almacenando un registro sobre dicho usuario en la S-CSCF. Entonces, es enviado un mensaje 200Ok, indicando que la subscripción ha sido satisfactoria. (Ver figura 4)

La S-CSCF envía el método SIP NOTIFY hacia el UE, con el objetivo de informarle a éste sobre el estado de registro del usuario monitoreado. El UE retorna un mensaje 200k, para confirmarle a la S-CSCF que ha recibido correctamente el NOTIFY.

2.2.4 Subscripción de la P-CSCF utilizando el método SIP SUBSCRIBE

En los procesos de des-registrar un usuario dentro de la arquitectura IMS se producen determinados eventos, los cuales deben ser notificados a la P-CSCF cuando ocurren. La P-CSCF solicita dicha notificación, la cual será realizada por parte de la S-CSCF como se muestra en la figura 5.

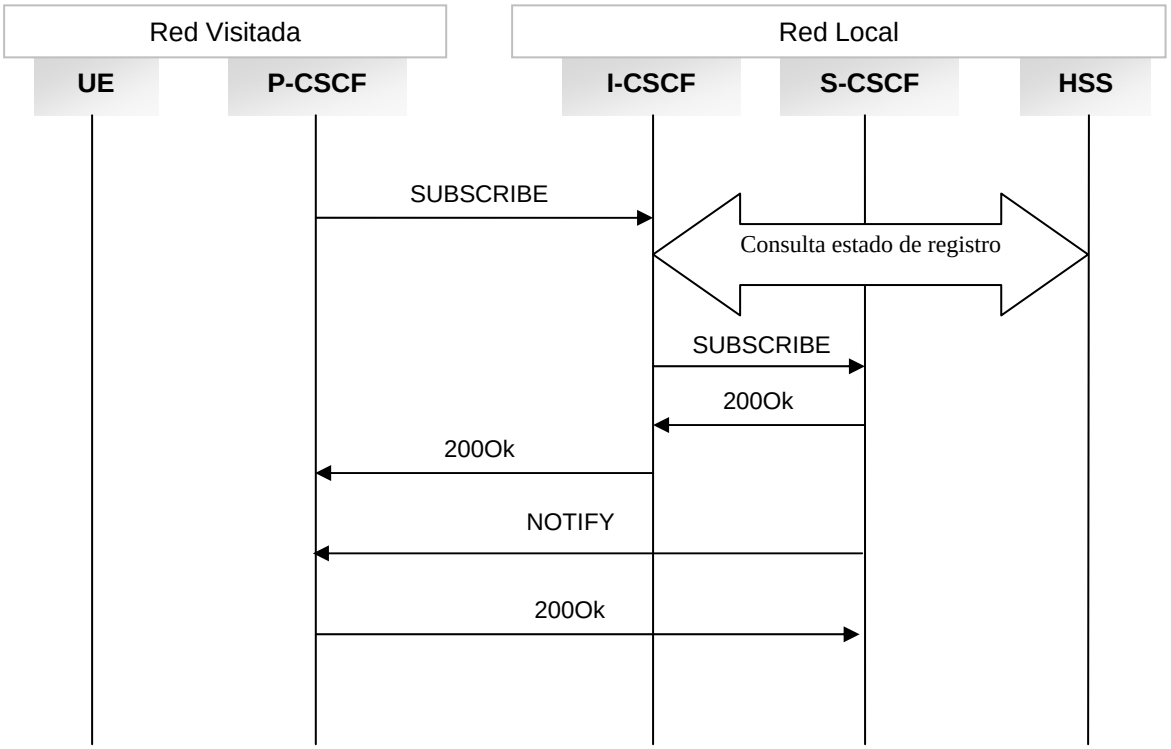


Figura 5. Subscripción de la P-CSCF

La forma en que la P-CSCF se subscribe en la red, es mediante el envío de un mensaje SUBSCRIBE hacia la S-CSCF. Si la información contenida dentro de la solicitud realizada en el SUBSCRIBE es confiable, la S-CSCF envía un mensaje de respuesta positivo, 200Ok. De esta manera, al igual que en la subscripción del UE, la subscripción de la P-CSCF también queda registrada en la S-CSCF. [29][35]

La S-CSCF envía la primera solicitud NOTIFY a la P-CSCF con el objetivo de informarle sobre el estado de registro del usuario monitoreado. En este mismo orden, la P-CSCF entrega un 200 Ok, indicando que ha sido notificado satisfactoriamente.

2.2.5 Des-registro de usuarios por parte de la S-CSCF

Una de las características más importantes de IMS tiene que ver con los privilegios que tienen las distintas funciones de control de su arquitectura sobre las sesiones, especialmente hablando de la CSCF. En este caso se hace referencia a la capacidad de terminar con el registro de un usuario desde la S-CSCF, asumiendo que tanto el UE como la P-CSCF han sido previamente subscritos, y por lo tanto, son hábiles para recibir notificaciones sobre el evento de Des-Registro iniciado en la S-CSCF.

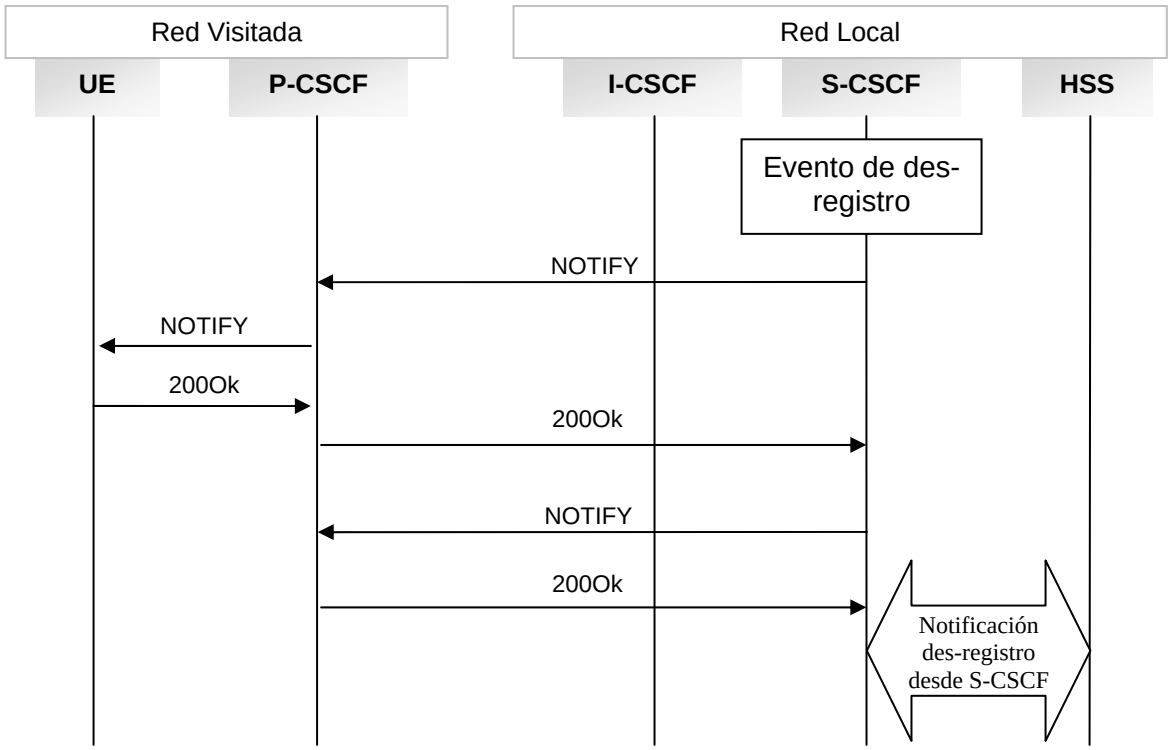


Figura 6. Notificación de Des-Registro en la S-CSCF

Como se muestra en la figura 6, la red envía una notificación hacia el UE con el objetivo de informarle que ha sido iniciada una terminación de su registro actual y que la subscripción, por consiguiente, también ha sido terminada.

De la misma manera, la S-CSCF envía una notificación a la P-CSCF, indicando también que el proceso de des-registro ha sido iniciado en la red. Tanto la P-CSCF como el UE devuelven una respuesta 200Ok hacia la S-CSCF.

2.2.6 Des-registro de usuarios por parte del HSS

Para realizar el des-registro de usuarios iniciado desde el HSS, se asume que el UE y la P-CSCF han desarrollado una previa labor de subscripción para poder ser notificados de los eventos de registro ocurridos en el HSS. De esta forma, cuando el evento de des-registro ocurre en el HSS, la S-CSCF es informada de dicho evento y empieza un mensaje de notificación enviado hacia la UE.

La notificación entregada por la S-CSCF al UE consiste en información sobre la iniciación de des-registro por parte del HSS y, por consiguiente, información sobre la terminación de la subscripción del UE des-registrado. La respuesta del UE a la notificación de des-registro, se realiza mediante el envío de un mensaje 200Ok.

De la misma manera en que se ha notificado al UE, la S-CSCF envía un mensaje de notificación a la P-CSCF, el cual responde también con un mensaje 200Ok. Al recibir el 200Ok, la S-CSCF envía una confirmación al HSS de que tanto el UE como la P-CSCF han sido satisfactoriamente notificados, para que el HSS termine las labores de des-registro.[29][35]

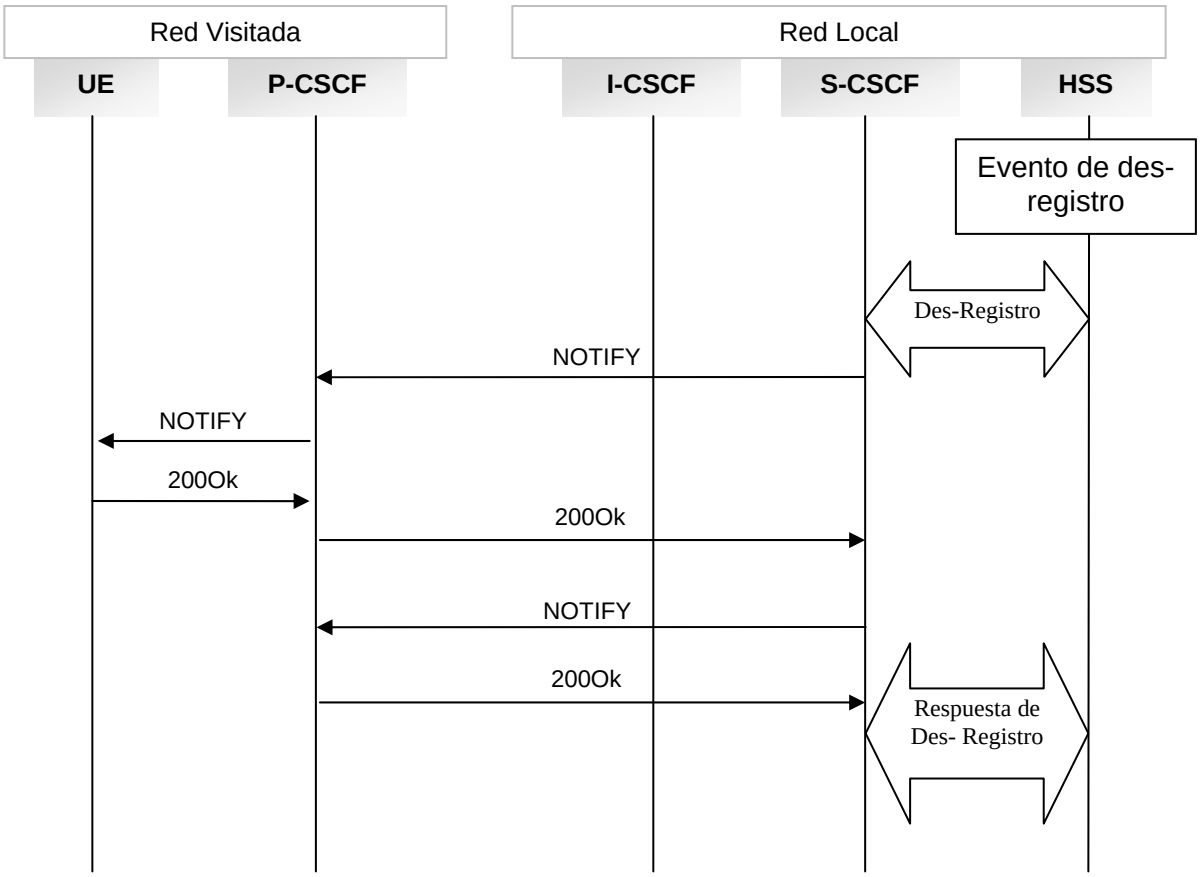


Figura 7. Notificación de Des-Registro iniciado en el HSS

2.2.7 Des-registro de usuarios iniciado por el UE y Roaming hacia una nueva red visitada

Al afirmar que la capa de control de IMS tiene ciertos privilegios sobre las sesiones iniciadas en la red, se habla de la posibilidad de implementar nuevos y mejores servicios coordinados desde el núcleo de la red IMS. Servicios independientes de la capa de acceso utilizada para ser consumidos, y con el valor agregado de ser completamente orientados a la sesión, lo que los hace ampliamente gestionables desde la capa de aplicación.

Uno de estos servicios consiste en el Roaming vertical (Cambio de tecnología de acceso) con características de seamless (transparente), que consiste en el paso de una tecnología de acceso a otra durante una comunicación activa, sin ser percibido el cambio por el usuario final. En este tipo de roaming, los usuarios finales que soportan distintos tipos de red de acceso, reportan al núcleo de la red cuando han encontrado una nueva red de acceso y se

disponen a abandonar la red de acceso actual, sin la intensión de finalizar la sesión activa. La capa de control de la red recibe la solicitud de roaming y efectúa las labores necesarias sobre la sesión para terminarla e iniciar una nueva, basada en las características de la nueva red de acceso; todo, sin perder la comunicación activa. [28][34]

En la figura 8 se muestra cómo se efectúa el des-registro de usuarios iniciado por un evento de solicitud de roaming desde el UE, y cómo el CSCF de la arquitectura IMS emprende las labores para iniciar un nuevo registro para esa UE, manteniendo el registro inicial del usuario durante el tiempo necesario. [29][35]

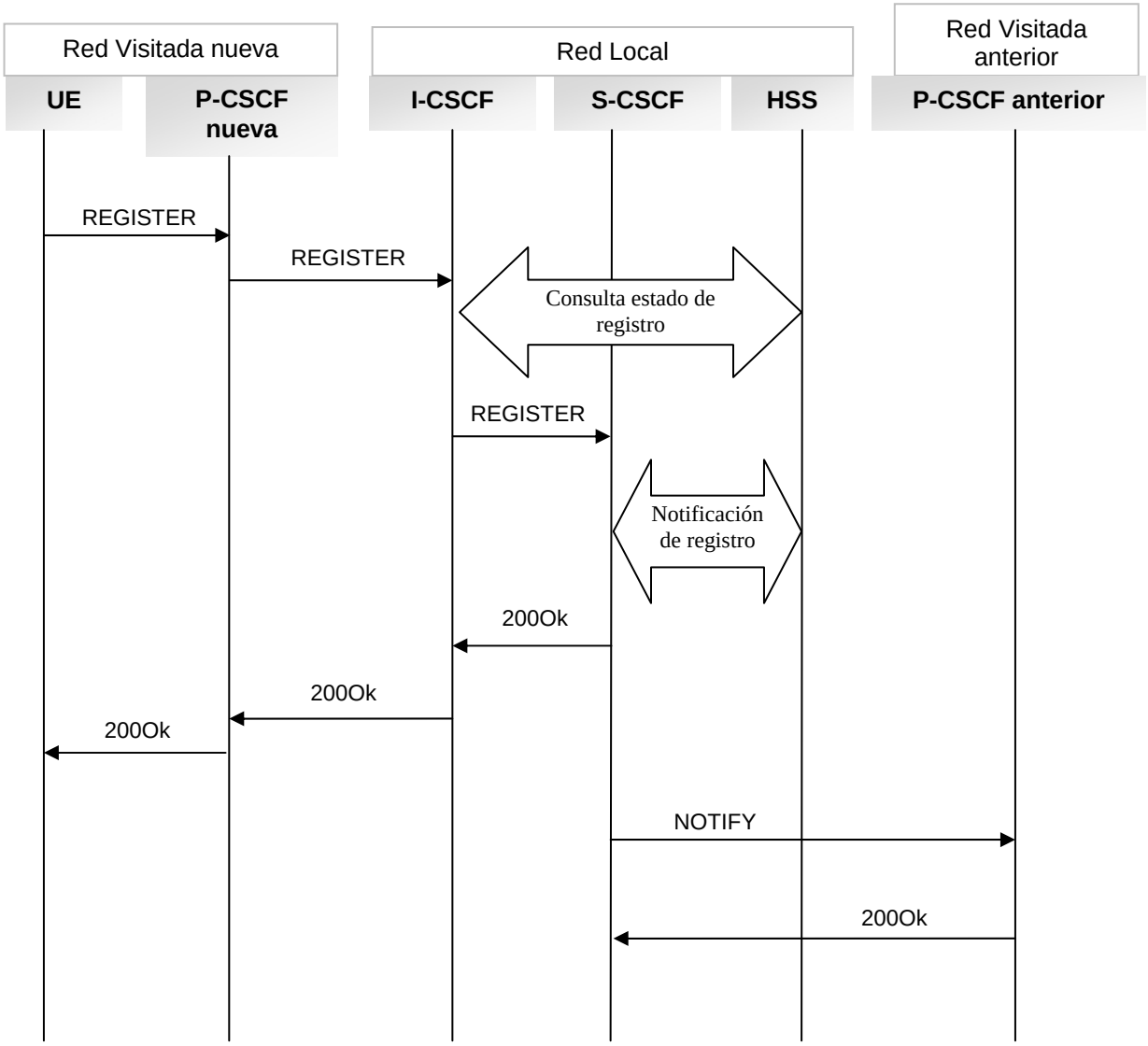


Figura 8. Des-registro de Usuario iniciado por el UE

El proceso de des-registro empieza cuando el UE pierde comunicación con la P-CSCF de la red visitada a la que pertenecía inicialmente (en la figura 8, P-CSCF anterior), y a su vez, encuentra una nueva red a la cual se puede conectar. En este caso, El UE envía una solicitud de registro (método REGISTER) a la P-CSCF que acaba de encontrar (en la figura 8, P-CSCF nueva), para que éste emprenda la tarea de registro habitual en una red IMS, es decir, enviando el método SIP REGISTER hacia la red local. [29][35]

Teniendo en cuenta que el registro inicial del UE no se ha perdido aun, no se requieren los datos de autenticación por parte del usuario para validar y terminar el registro. Entonces, se procede a enviar un mensaje de aceptación del nuevo registro hacia el UE desde la S-CSCF de la red local, enviando un 200Ok.

El UE ha sido informada de que su nuevo registro en la red local se ha llevado a cabo, y que la red local tiene información sobre su actual conexión con la P-CSCF nueva de la nueva red visitada. Entonces la S-CSCF de la red local procede a eliminar el registro inicial del UE, y a notificar dicho des-registro a la P-CSCF anterior, como se muestra en la figura 8. [29][35]

2.2.8 Re-autenticación de usuario iniciada por la red y notificada al UE

La re-autenticación de los usuarios iniciada desde la red, es uno de los privilegios sobre las condiciones de señalización que hacen parte de los valores agregados en IMS. Consiste en el inicio de un evento de re-autenticación en la S-CSCF de la red local, asignado y posteriormente notificado a un UE. Este UE debe estar previamente registrado y subscrito en la red, para poder recibir notificaciones de eventos de autenticación y registro.

Posterior a esto, el UE debe iniciar un re-registro con la S-CSCF, con los datos asignados para éste, en el proceso de re-autenticación. En caso de ocurrir un fallo en el re-registro del usuario, se debe iniciar un des-registro en la S-CSCF para el usuario en cuestión. [29][35]

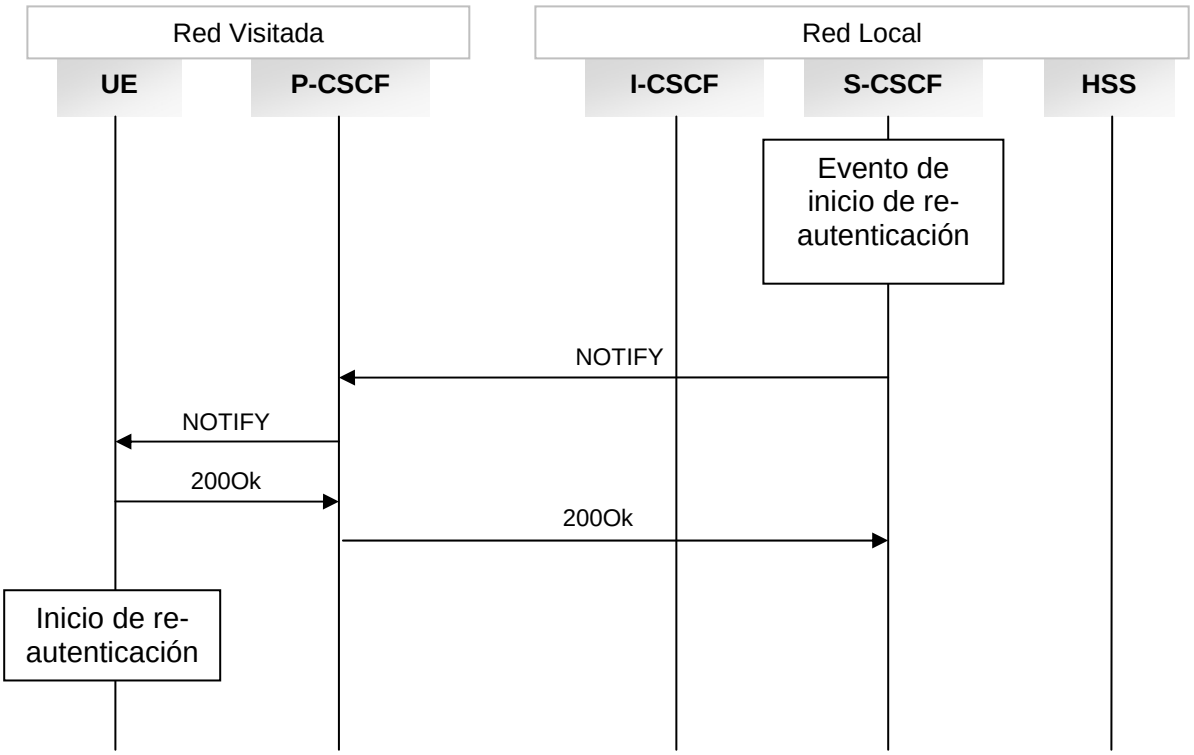


Figura 9. Re-Autenticación de Usuario iniciada por la Red

Como se muestra en la figura 9, al ser notificada del inicio de la re-autenticación desde la red, el UE debe iniciar dicha re-autenticación, respondiendo nuevamente con una solicitud de registro enviada hacia la red local. [29][35]

2.2.9 Inicio de sesión entre redes IMS distintas

Teniendo dos o más usuarios previamente registrados en la red de IMS, se puede proceder a establecer una sesión entre ellos, empezando por el envío de una invitación SIP por parte de cualquiera de los Equipos de Usuario involucrados en la comunicación.

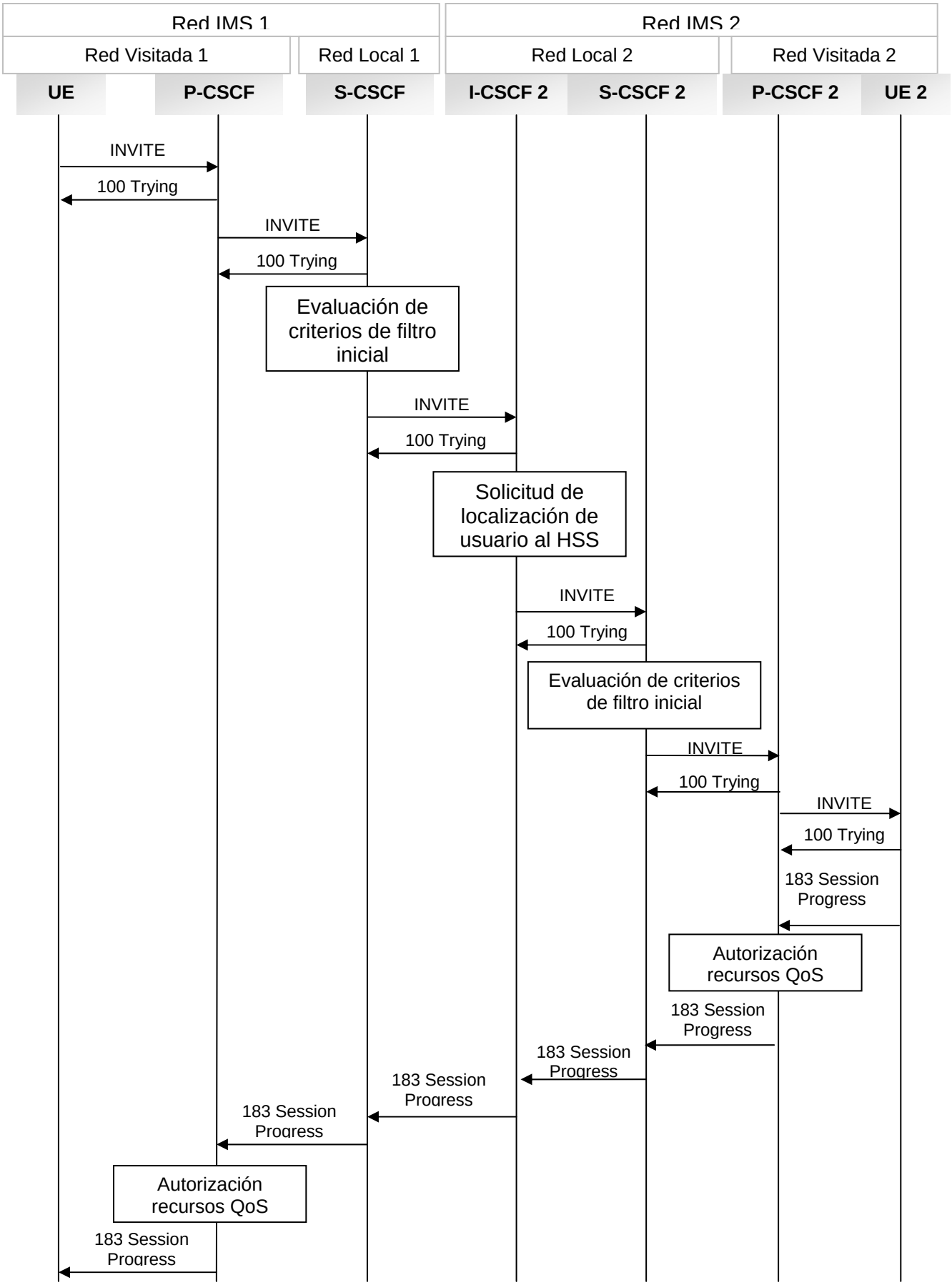
El establecimiento de una sesión SIP consiste en un conjunto de tareas necesarias para que los usuarios registrados en una red puedan tener una comunicación acorde a las capacidades de la red y a las capacidades y permisos que caracterizan tanto al usuario que inicia la sesión, como a aquellos que reciben la invitación de establecimiento de dicha sesión.

En IMS se produce el flujo descrito en la figura 10 para el establecimiento de una sesión. Dicho flujo contiene mensajes para las notificaciones de eventos sobre la sesión, y mensajes útiles en la negociación de las características y capacidades de los usuarios y de la red.

De la misma manera como se describió anteriormente para el registro de usuarios, los métodos utilizados para el establecimiento de una sesión SIP, son vistos de forma independiente a la red de acceso utilizada, asumiendo que el agente de usuario que inicia la comunicación, empieza el establecimiento a partir de un mensaje SIP, y no a partir de otros protocolos de señalización asociados con la red de acceso.

Aunque se debe tener en cuenta que una de las principales características de SIP es que por su extensibilidad y por su trabajo en paralelo con el protocolo SDP puede ser portador de información relacionada con las tecnologías que intervienen en la comunicación (UMTS, GPRS, CDMA, etc.) independientemente de la capa a que pertenecen, de tal forma que el operador de servicios pueda actuar sobre dicha información. Esta característica de SIP, tiene mayores efectos con la creación de cabeceras adicionales dentro de la definición realizada por el 3GPP para IMS, donde se han agregado cabeceras con el único objetivo de manejar la información de las redes que participan en la prestación de servicios multimedia.[12][21]

En el caso descrito en la figura 10, existen dos operadores de red distintos basados en la arquitectura de IMS, los cuales se comunican entre ellos por medio de las funciones derivadas de la CSCF, S-CSCF e I-CSCF de la red IMS 2 (ver anexo B). Como se muestra en la figura, las funciones encargadas de enviar la solicitud INVITE, producida inicialmente por el UE, son la P-CSCF y la S-CSCF de la red IMS 1. La puerta de entrada para el tráfico de señalización proveniente de redes IMS ajenas es la I-CSCF, en este caso, el de la red IMS 2. El protocolo SDP empieza a actuar en este primer INVITE enviado por el UE, al describir en su contenido las características de la sesión, los códec para audio y video, y los requerimientos de ancho de banda para dichos códec. El UE2 devuelve un mensaje SIP 183 hacia el UE de la red IMS 1, indicándole que la sesión está en progreso.


Red IMS 1
Red IMS 2
Red Visitada 1
Red Local 1
Red Local 2
Red Visitada 2
UE
P-CSCF
S-CSCF
I-CSCF 2
S-CSCF 2
P-CSCF 2
UE 2
INVITE
100 Trying
INVITE
100 Trying
Evaluación de criterios de filtro inicial
INVITE
100 Trying
Solicitud de localización de usuario al HSS
INVITE
100 Trying
Evaluación de criterios de filtro inicial
INVITE
100 Trying
INVITE
100 Trying
183 Session Progress
Autorización recursos QoS
183 Session Progress
183 Session Progress
183 Session Progress
183 Session Progress
Autorización recursos QoS
183 Session Progress

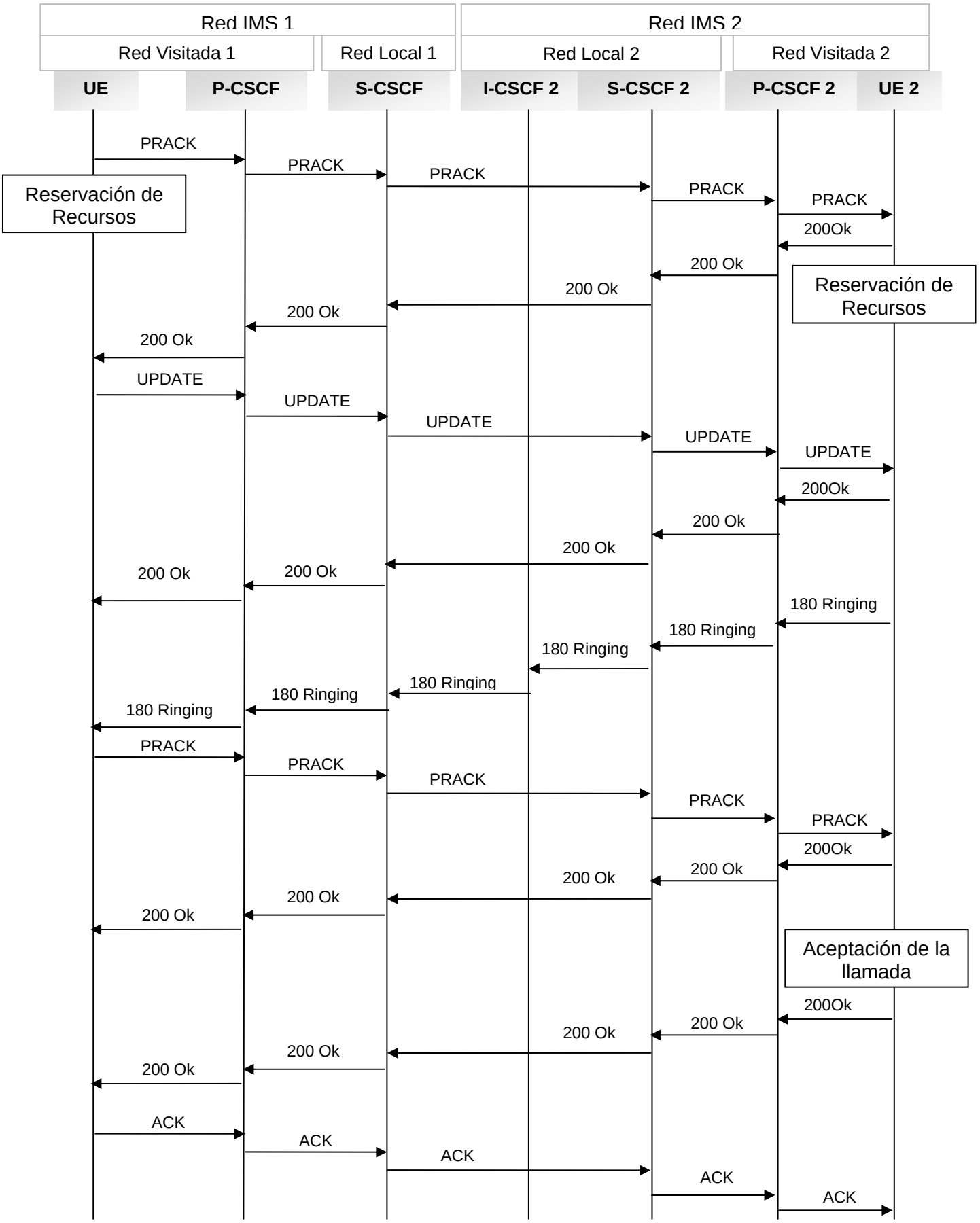


Figura 10. Establecimiento de una Sesión

Posterior al método INVITE enviado por el UE que desea establecer la sesión, y de la respuesta que indica una sesión en progreso, se procede a negociar el tipo de flujo multimedia para la comunicación entre las UE participantes. Esta tarea de negociación se realiza mediante el uso de un método SIP PRACK, donde el UE de la red IMS 1 determina el flujo multimedia que debería ser utilizado para la sesión por establecer, y qué códec se debe usar para cada uno de estos flujos multimedia. Esto se realiza mediante la inclusión de una nueva descripción SDP dentro del método PRACK enviado hacia el UE2. El UE2 responde a dicho PRACK con un mensaje de respuesta 200 Ok, que indica al UE1, que ha iniciado la reservación de recursos multimedia para esta sesión. [29][35]

Cuando la reservación de recursos se ha completado, el UE de la red IMS1 envía una solicitud UPDATE hacia el UE2, a través de la misma ruta seguida por el método INVITE transmitido inicialmente. De esta manera, el UE2 retorna una respuesta 200 Ok correspondiente a dicho UPDATE.

Antes de proceder con el establecimiento de la sesión, el UE2 espera que ocurran dos eventos. Primero, que la reservación de recursos que ha sido iniciada previamente se haya completado satisfactoriamente. Segundo, la reservación iniciada por el terminal originario se haya completado satisfactoriamente, lo cual es indicado por el mensaje UPDATE recibido por el UE2. Posterior a esto, el UE2 puede aceptar la sesión, o empezar por dar un aviso al subscriptor destino de un intento de inicio de sesión entrante. Este tipo de aviso se realiza mediante el envío por parte del UE2 de un mensaje 180 Ringing hacia el UE de la red IMS1.

Nuevamente se ejecutan los procesos de negociación de recursos correspondientes al envío del mensaje PRACK y su respectiva respuesta 200 Ok. Solo cuando esto ocurre se puede devolver un mensaje respuesta de aceptación desde el UE2 hacia el UE de la red IMS 1, informando que la sesión ha sido establecida completamente y que el flujo multimedia se iniciará a partir de ese momento para esta sesión. El UE de la red IMS1 inicia el flujo multimedia y responde al 200 Ok del INVITE con un mensaje ACK. [29][35]

2.2.10 Inicio de sesión dentro de una misma red IMS

Cuando tanto el UE que origina la invitación para el inicio de sesión, y el UE2 que corresponde al usuario destino, han sido previamente registrados en una misma red IMS, los procesos de señalización necesarios para el establecimiento de una sesión entre los dos puntos terminales siguen el mismo patrón mostrado en la figura 10, la cual describe el establecimiento de una sesión para usuarios pertenecientes a dos redes IMS distintas. Como se puede notar en la figura 11., la diferencia entre el establecimiento de sesión para dos usuarios pertenecientes a la misma red IMS, y para usuarios pertenecientes a redes IMS distintas, radica principalmente en consideraciones de arquitectura y no de flujo de señalización, ya que los mensajes utilizados para invitación, negociación de las características de la sesión, avisos de actividades en proceso y acuses de recibo son prácticamente iguales. De esta manera, el flujo de tráfico de señalización para la figura 11 es muy similar al mostrado en la figura 10. [29][35]

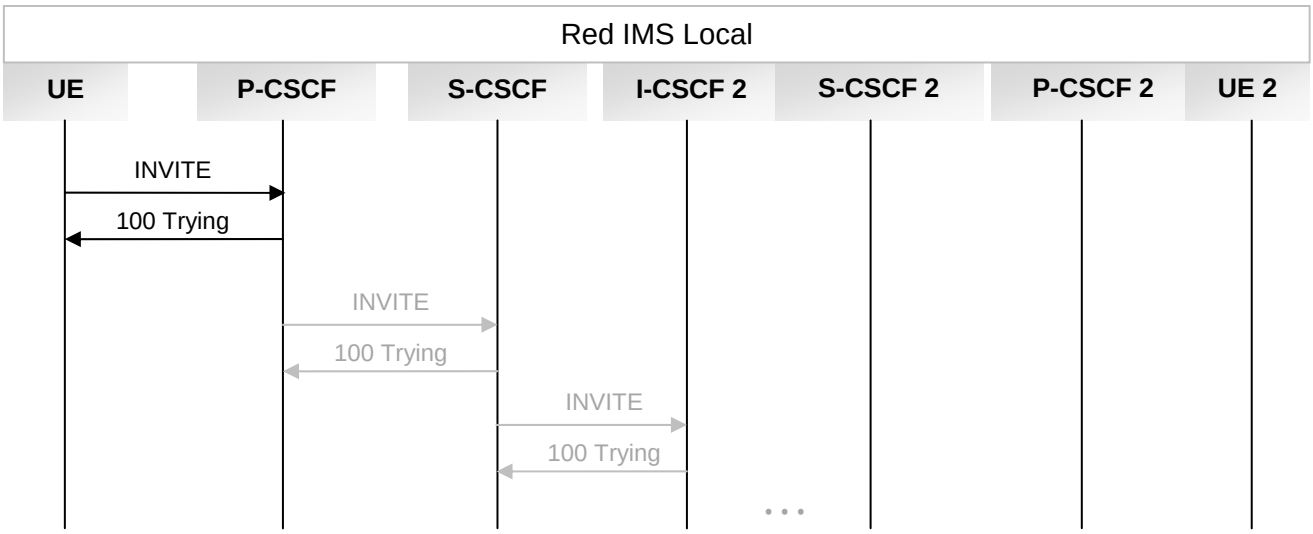


Figura 11. Inicio de una Sesión SIP dentro de una misma red IMS

2.2.11 Ocultación en los procesos de señalización SIP

Como SIP es un protocolo *basado en texto,* toda la información de señalización es enviada en texto plano, incluso algunas de las cabeceras SIP que contienen información sobre el usuario y la red que podría ser sensible a ataques e infiltraciones, como las direcciones de las entidades de la red local y los números de dichas entidades. Esta información está localizada generalmente en las cabeceras: Via, Path, Record-Route y Service-Route de los métodos SIP transmitidos. La solución para mantener a salvo dicha información es utilizando procesos de ocultación, los cuales son ejecutados por la I-CSCF, y se basan en la funcionalidad THIG (Topology Hiding Inter-Network Gateway), la cual es abordada por la I-CSCF para aquellas partes del protocolo SIP que requieren de mayores niveles de seguridad.

La I-CSCF actúa como un proxy SIP que se encuentra en la puerta de entrada al dominio administrativo de una red IMS (ver Anexo B para mayor información sobre la CSCF), y que puede estar localizado tanto en la red local, como en la red visitada, tal como se ve en algunos casos en donde se utiliza ocultación. [9]

La Funcionalidad de THIG, ejercida dentro de la I-CSCF, podría ser reemplazada, a partir de las especificaciones de encriptación y seguridad de información referidas en el Release 7 del 3GPP [36], por funcionalidades de Firewall y NAT, provistas en la función IBCF (Interconnection Border Control Function). Por lo tanto, las funciones de señalización SIP involucradas inicialmente en la ocultación de información no se deberían tener en cuenta. [9]

2.3 Diferencias entre los procesos de señalización para SIP-IETF y SIP-3GPP

SIP es utilizado dentro de IMS, asociado especialmente a un ambiente móvil y de servicios convergentes, por lo cual se hallan una serie de modificaciones para este protocolo dentro de la definición realizada por el 3GPP, teniendo en cuenta algunos parámetros de

comunicaciones de radio y de red de acceso, los cuales eran ignoradas anteriormente en las definiciones preliminares de SIP [21]. En la definición inicial de SIP, desarrollada por la IETF, se empiezan a tener en cuenta los requerimientos de las redes de comunicaciones móviles a partir del RFC-3261 [1], aunque no todos los requerimientos asociados a un ambiente móvil han sido tenidos en cuenta dentro de esta especificación. Esto, como se ya se ha mencionado en el capítulo 1, ha generado una serie de diferencias entre las definiciones IETF y 3GPP del protocolo.

A pesar de que las diferencias presentadas en el capítulo 1 son considerablemente grandes, la versión de SIP modificada por el 3GPP, más que una nueva definición, podría ser vista como un nuevo perfil del protocolo, que se suma al elevado número de implementaciones constituidas por modificaciones realizadas a la especificación inicial de SIP. En el capítulo 3 se puede ver de una manera más exacta cómo difieren entre ellas las estructuras del protocolo SIP definidas por la IETF y el 3GPP, haciendo énfasis en el contenido de las cabeceras adicionales, y del papel que éstas cumplen en la implementación de algunos servicios y capacidades exclusivas de IMS.

Aunque a lo largo del proyecto se hace una especial referencia al contenido de los métodos SIP y a las diferencias existentes entre las estructuras de las especificaciones involucradas, cabe señalar que también existen diferencias entre el flujo de señalización producido en una comunicación SIP dentro de internet (en la cual generalmente actúa el SIP-IETF) y la señalización requerida para establecer y gestionar sesiones dentro de una red IMS (utilizando señalización basada en el SIP-3GPP). Estas diferencias radican principalmente en el número de entidades participantes y procedimientos involucrados en una comunicación SIP, y además, es de gran importancia tener en cuenta que estas entidades IMS cuentan con capacidades adicionales sobre las características de las sesiones multimedia, lo cual es el motivo principal para que existan diferencias de flujo de señalización ente SIP-IETF y SIP-3GPP.

Entonces, la forma más adecuada para identificar las principales diferencias es la comparación entre las dos especificaciones desarrolladas para SIP, haciendo énfasis en los diagramas de secuencia proporcionados en estos dos documentos [1][29] para describir el flujo de señalización. Para lograr dicho paralelo, la fuente de información que ha abarcado todos los procedimientos básicos de señalización SIP destinados para comunicaciones basadas en una arquitectura IMS, es el TS 24.229 del 3GPP [21] y, por otro lado, los procesos de señalización necesarios para el establecimiento, gestión y terminación de sesiones SIP en un entorno basado en internet, están descritos en el RFC-3261 de la IETF [1].

Al realizar dicha comparación, aparentemente el flujo de señalización requerido para el establecimiento de sesiones y registro de usuarios resulta prácticamente igual entre las dos especificaciones estudiadas. Evidentemente, las mayores diferencias radican en la ruta seguida por los métodos SIP, y en las decisiones que pueden ser tomadas de lado del núcleo de la red sobre el curso de las sesiones.

Los procesos ejecutados para el registro de un usuario, y por tanto, para su posterior adquisición de una dirección IP, cambian según la red de acceso utilizada para lograr acceso a servicios IP. Esto no implica que el registro en un proxy SIP para dicho usuario tenga alguna dependencia con la red de acceso, aunque sí se hace necesaria la asignación de una red IP y la posterior localización de la P-CSCF para iniciar las labores de registro de un terminal en la red IMS.

Cabe aclarar que el registro de usuarios no es estrictamente necesario en los procesos regulares basados en el protocolo SIP-IETF, pero sí se hace obligatorio un registro previo para el establecimiento de sesiones en una red IMS.

Al igual que en una comunicación basada en SIP-IETF, en la sección 2.2.1 se ve claramente cómo en una red IMS también es utilizado el método REGISTER como base en los procesos de registro de usuarios. Aunque a diferencia de los procesos basados en SIP-IETF, en IMS el método REGISTER se ve ampliamente sobrecargado, ya que debe satisfacer los requerimientos del 3GPP definidos para IMS, en los que se busca el uso del mínimo número de mensajes SIP en el registro de usuarios, considerando las limitantes en recursos de radio utilizados.

En IMS existen algunas diferencias entre la realización del registro para usuarios cuyos terminales están dotados con un UICC (Universal Integrated Circuit Card) con aplicación ISIM (IMS Subscriber Identity Module) o terminales con aplicación USIM (Universal Subscriber Identity Module). Estos dos tipos de aplicaciones para UICC, difieren principalmente en que la ISIM ha sido desarrollada especialmente para cumplir con algunos requerimientos IMS, y contiene herramientas diseñadas especialmente para terminales móviles basados en el SIP-3GPP, y por su parte, USIM ha sido utilizada tradicionalmente tanto dentro de la conmutación de circuitos como dentro de la conmutación de paquetes, sin abordar las consideraciones concernientes a los requerimientos de IMS [9]. Por otro lado, en una comunicación basada en la definición para SIP desarrollada en el RFC-3261 [1], no son tenidos en cuenta ningunos de los requerimientos y avances desarrollados para comunicaciones móviles, asociados generalmente con las aplicaciones ISIM y USIM del UICC.

Dentro del registro de usuarios IMS existen procesos dedicados únicamente a las funciones propias de esta arquitectura. Por ejemplo, el proceso de localización de la P-CSCF ya sea dentro de la red local o en la red visitada, conlleva a que se requiera o no la verificación de *roaming* entre estas dos redes. Estos procesos de localización se asemejan con uno de los cinco aspectos básicos del SIP-IETF, el proceso de localización. Ya sea para localizar usuarios o para localizar al Proxy SIP, se utiliza este aspecto de la especificación IETF de SIP; aunque, a diferencia del SIP especificado por el 3GPP, no se tiene en cuenta ninguna clase de requerimiento para *roaming.*

De la misma manera como sucede con los procesos de registro, debe entrar en consideración la subscripción de usuarios. Ésta se realiza con el objetivo de realizar notificaciones sobre los eventos de registro y des-registro producidos en la red. Cuando se lleva a cabo un registro basado en la especificación del SIP-IETF, especialmente ubicado en un ambiente fijo con conexión a internet, dicho registro tiene un tiempo de duración acorde al tiempo de expiración inicialmente definido por el usuario en el método REGISTER hacia el servidor de registro SIP, el cual almacena la dirección del usuario registrado, para tener una ubicación dónde localizarlo, y crea un estado de registro relacionado con dicho usuario. En el momento en que exista una expiración del registro, o de que ocurra un evento de des-registro producido en el servidor de registro SIP, el agente de usuario no podrá ser notificado de dicho evento, debido a que el SIP-IETF no soporta este mecanismo. En contraste, éste es uno de los principales avances alcanzados en la definición de la arquitectura IMS: Cuando un usuario ha sido previamente registrado en la red IMS, y tanto el usuario como la P-CSCF están subscritos en la red, ésta puede enviar notificaciones sobre la ocurrencia de un evento de des-registro localizado en la capa de control, o iniciado por el mismo terminal IMS[29][9].

En IMS se han heredado de GSM algunos requerimientos para el usuario, como por ejemplo que dicho usuario sea informado si es alcanzable por la red o no, es decir, si está dentro del cubrimiento de radio o no; o si este usuario se encuentra registrado en la red. Este requerimiento se ha cumplido mediante la implementación de un paquete de registro basado en una solución inicialmente planteada por la IETF. Dicho paquete consiste en el registro, subscripción y posible notificación del estado de registro y cobertura del usuario en la red, de la misma manera como se ha implementado para la notificación de eventos de registro en la red.

En conclusión, las principales diferencias entre los procesos de señalización requeridos para el manejo de sesiones entre una comunicación basada en la especificación inicial de SIP desarrollada por la IETF, y el nuevo perfil diseñado para trabajar en IMS desarrollado por el 3GPP, radican en las nuevas capacidades y privilegios adicionados en las redes IMS sobre las características generales de las sesiones, y que no han sido abordados en la especificación inicial del protocolo. Estas nuevas capacidades y privilegios que estarían ubicados específicamente en la capa de control de la arquitectura IMS, no solamente proveen la oportunidad de prestar nuevos y mejores servicios al usuario, sino que también adicionan cambios en los procesos SIP tradicionales de señalización, agregando nuevos participantes del lado de la red, cuyo comportamiento está en ocasiones más relacionado con el de un terminal que con el de un módulo de red SIP tradicional. Es el caso de las funciones derivadas del CSCF, las cuales en ocasiones actúan como un cliente que se debe registrar y subscribir en algunos módulos de la red, y por otro lado, cumplen con su papel de lado de servidor, cumpliendo generalmente con tareas de proxy SIP.

Es importante mencionar también, a manera de conclusión, que el particular enfoque de IMS en un ambiente móvil tiene grandes efectos sobre los procesos de señalización SIP, y específicamente, sobre el limitado número de mensajes que se permiten enviar y recibir entre los Equipos de Usuario y la red, para que se pueda desarrollar cualquier tarea de registro, o modificar las características de las sesiones. Esto, debido a la escasez de recursos de radio que generalmente caracteriza a las comunicaciones móviles, lo cual conlleva a que se deban sobrecargar de cierta forma en su contenido los métodos SIP utilizados.

3. INTEGRACIÓN DE LAS CAPACIDADES Y SERVICIOS IMS CON EL TRÁFICO DE SEÑALIZACIÓN SIP-IETF

Una de las principales consideraciones abordadas a la hora de escoger a SIP como protocolo base en el desarrollo de la arquitectura de IMS, es que este protocolo cumple con los requerimientos planteados por el 3GPP para alcanzar el objetivo principal de esta tecnología: la convergencia. Esta convergencia está orientada dentro de la idea de fusionar todas las distintas tecnologías de acceso de las redes tradicionales en un solo punto, que a su vez haga el acceso a las redes IMS independiente de la tecnología utilizada. Con esto se logra, entre otras cosas, que la mayor responsabilidad en la gestión de sesiones multimedia recaiga sobre la capa de control. Es precisamente en la capa de control donde se produce la mayor cantidad de flujo de señalización basado en el protocolo SIP, y donde se genera una interacción directa con los servicios convergentes, que generalmente estarían alojados en los distintos servidores de aplicaciones de la capa superior, y es gracias a esta interacción y a las capacidades encontradas en el protocolo SIP, que se pueden desplegar servicios convergentes.

Como se plantea en el primer y segundo capítulo, el 3GPP ha definido una serie de requerimientos para el protocolo de señalización SIP, con el objetivo de hacerlo útil dentro de la arquitectura IMS. Entre otros requerimientos, los relacionados con los altos niveles de convergencia procurados en IMS, a la cual el protocolo SIP debe responder mediante la implementación y uso de una serie de cabeceras adicionales. En este capítulo, teniendo en cuenta la integración de los servicios convergentes con el tráfico de señalización, se exponen los cambios, adiciones y avances que se hacen sobre la estructura básica del protocolo SIP, realizando un especial énfasis en cada una de las cabeceras adicionales involucradas, y exponiendo la forma en que éstas interactuarían con los servicios convergentes y las múltiples capacidades propuestas dentro de la arquitectura IMS.

3.1 Descripción básica de la arquitectura general de acceso a capacidades IMS desde clientes SIP-IETF

Con el fin de lograr una completa descripción de las variaciones que debe sufrir la estructura del protocolo SIP-IETF, para que clientes basados en esta especificación puedan acceder a capacidades y servicios IMS, es conveniente realizar una previa y general descripción de la pasarela de señalización desarrollada en el marco del presente proyecto.

La pasarela de señalización desarrollada, de ahora en adelante denominada i23GW (IETF to 3GPP Gateway), corresponde a una herramienta software B2B (Back to Back), la cual de manera bidireccional captura e interpreta los mensajes que hacen presencia, por un lado, desde clientes SIP-IETF y por el otro, desde el núcleo de la red IMS. Esto, con el objetivo de adaptar la estructura de los mensajes SIP y con ello lograr una comunicación correcta entre los dos elementos de red, agregando o eliminando las cabeceras adicionales de IMS según sea el caso, o modificando los valores de las cabeceras tradicionales del protocolo para adaptarlos a las necesidades tanto del cliente SIP-IETF como de la red IMS.

Como se ha mencionado en capítulos anteriores, la puerta de entrada para los agentes de usuario basados en SIP hacia todos los servicios IMS, es la función P-CSCF [9], perteneciente a la capa de control de la arquitectura. La función P-CSCF es el punto de llegada para los clientes basados en el perfil 3GPP del protocolo SIP, y por lo tanto, se consolida como el punto de interacción inicial y de toma de decisiones sobre todas las cabeceras SIP, incluyendo las cabeceras adicionales. Entonces, la ubicación más adecuada para una pasarela de señalización como i23GW, sería entre los clientes SIP-IETF y la P-CSCF, como se muestra en la figura 12.

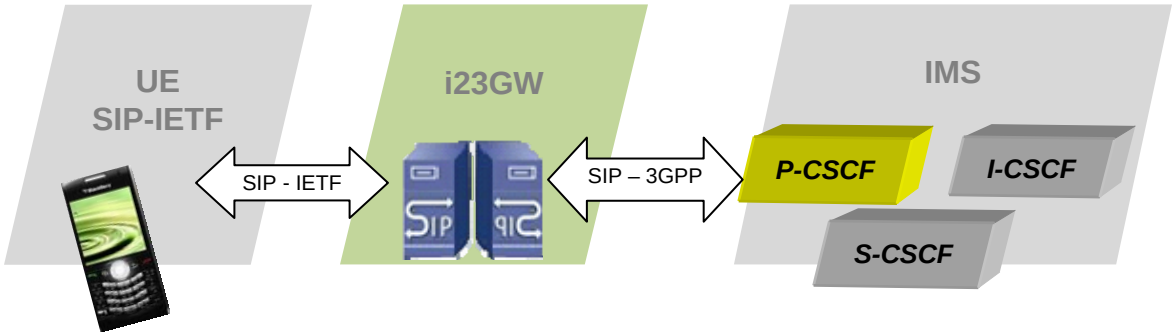


Figura 12. Arquitectura General del Sistema

i23GW está conformada por un grupo de funciones software para generar la conexión SIP inicial, realizar un análisis sobre los mensajes entrantes y modificar los elementos necesarios. Una descripción más completa de i23GW se puede encontrar en el capítulo 4 de este documento, o en el Anexo C. En el presente capítulo entran en consideración solamente los valores de entrada y de salida de i23GW, señalados en la figura 12 con las flechas bidireccionales.

3.2 Comparación entre la estructura de SIP-IETF y las cabeceras adicionales SIP-3GPP bajo la utilización de i23GW

De la misma manera como existen diferencias en el flujo de los mensajes SIP (número de mensajes, entidades involucradas, etc.) entre la especificación inicial de la IETF y el perfil para IMS del 3GPP, también existen diferencias entre estos dos en el contenido de los mensajes, principalmente en las cabeceras utilizadas para lograr los distintos procedimientos de señalización SIP requeridos por IMS. A continuación se muestran estas diferencias puntuales para los distintos procesos de señalización SIP, tales como registro, subscripción y establecimiento de las sesiones.

3.2.1 Diferencias en la estructura de los mensajes SIP-IETF y SIP-3GPP bajo la utilización de i23GW para el Registro de usuarios no registrados

El único proxy SIP conocido inicialmente por el UE es la P-CSCF, entonces, el procedimiento de registro de usuarios debe empezar por el envío de un mensaje SIP REGISTER hacia este proxy. El método REGISTER contiene generalmente información sobre el usuario, y sus

características de conexión, como por ejemplo el nombre de contacto, IP de localización y puertos utilizados para la comunicación SIP [1][29]. A continuación se muestra un esquema del contenido del mensaje REGISTER que se utilizaría generalmente para registrar un usuario SIP basado en la especificación inicial de la IETF, y que constituiría la información de entrada para el lado del UE hacia i23GW para efectos de registrar dicho usuario en la red.

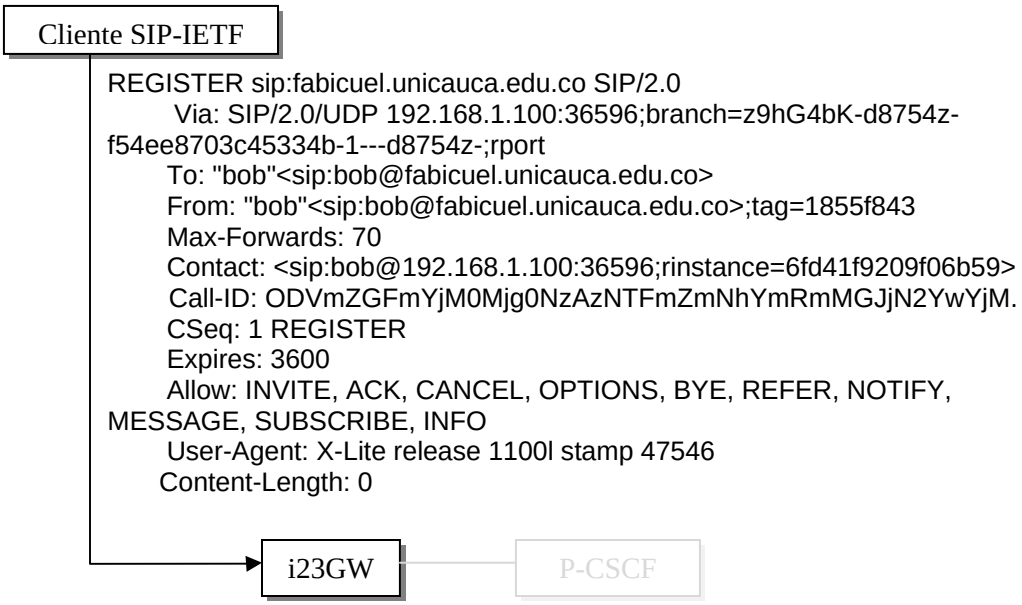


Figura 13. REGISTER entre el Cliente SIP-IETF e i23GW

La cabecera Via contiene la dirección en la cual el usuario, para este caso “Bob”, espera recibir las respuestas SIP (SIP Responses) a sus mensajes de solicitud (SIP Request). Además cuenta con un parámetro *branch* útil en la identificación de la transacción actual. Esta cabecera se irá actualizando según los proxy SIP que debe atravesar en el trayecto hacia su destino final.[1]

La cabecera To indica la identidad pública con la cual el usuario va a ser registrado y por medio de la cual las otras entidades conocerán al subscriptor. En la cabecera From se porta la identidad pública de la entidad que está solicitando el registro.[1]

Max-Fordwards sirve para limitar el número de saltos que la solicitud puede dar antes de llegar a su destino. En la cabecera Contact, indica el punto de presencia para el subscriptor, específicamente la IP del UE. La cabecera Expires denota el tiempo relativo después del cual el mensaje expiraría. Existen algunos métodos que se transfieren entre las distintas entidades de manera iterativa, variando solo algunas de sus cabeceras según sea el caso, como por ejemplo el método REGISTER. CSeq lleva un conteo de esas iteraciones, mediante el uso de un número que se incrementa cada vez que determinado método repite su paso por el Equipo de Usuario. En la cabecera Allow, se listan los métodos soportados por el Equipo de Usuario que ha realizado la solicitud de registro. User Agent contiene datos específicos sobre el software base del cliente utilizado por el Equipo de Usuario. La cabecera Content-Lenght contiene el tamaño del cuerpo del mensaje transferido.[1]

Todas estas cabeceras serían útiles en el registro de un usuario dentro de un Servidor de Registro SIP basado en la especificación IETF del protocolo. Las cabeceras adicionadas por

la 3GPP para la optimización de SIP dentro del entorno de IMS se muestran en la figura 14. En esta figura se enseña el contenido del primer método REGISTER que saldría modificado de la pasarela i23GW hacia la P-CSCF.

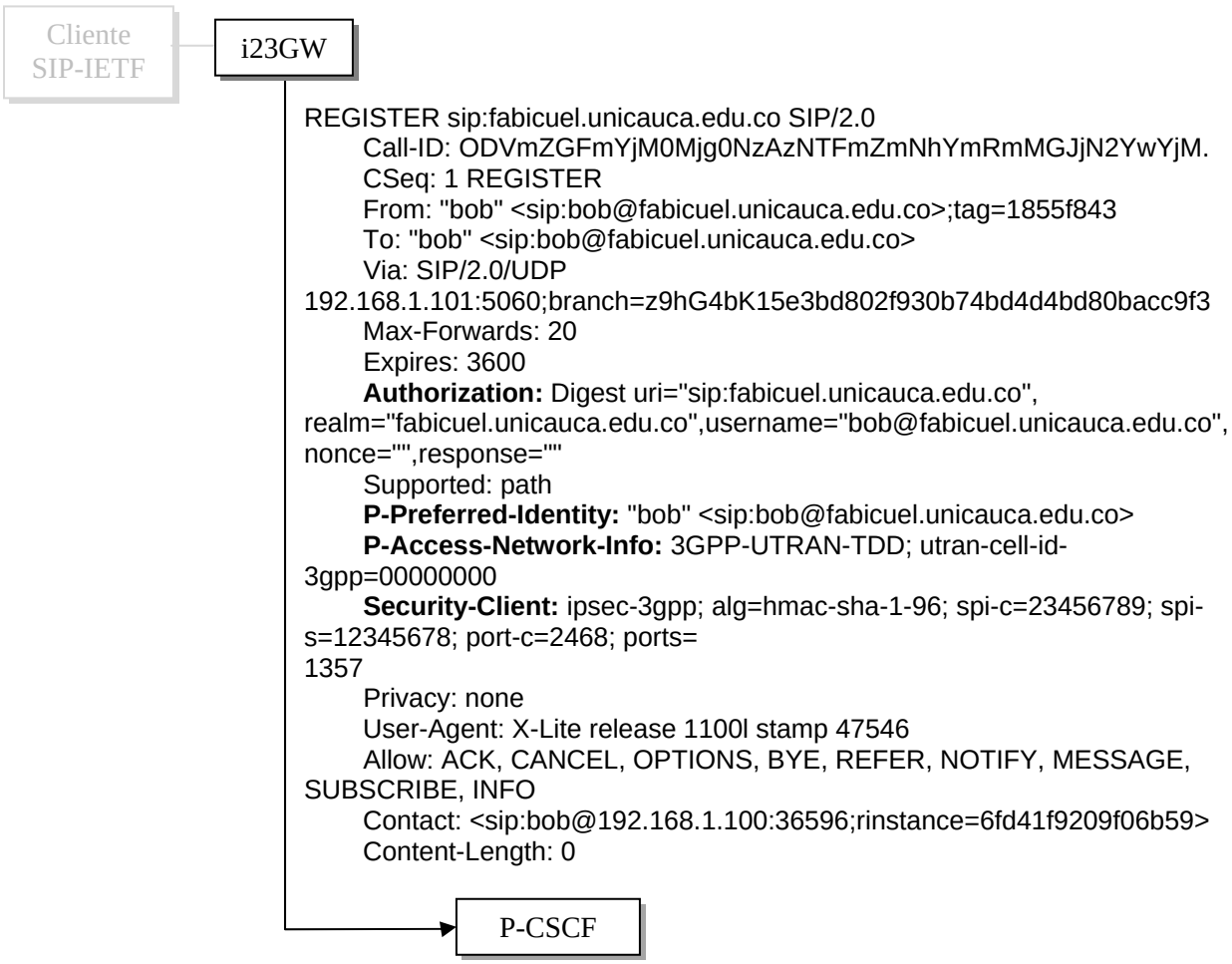


Figura 14. REGISTER modificado por i23GW y enviado hacia la P-CSCF

Uno de los principales objetivos dentro de la arquitectura IMS es lograr un nivel de seguridad mucho más elevado que en las redes tradicionales, especialmente en las tareas de AAAC. Estos niveles de seguridad, además de las capacidades adicionales de IMS para calidad de servicio, diferenciación de servicios y despliegue de servicios convergentes, como se ha mostrado en el Capítulo 1, tienen algunos requerimientos sobre el protocolo SIP, los cuales se ven reflejados en la implementación de las siguientes cabeceras:

Authorization: Esta cabecera actúa eventualmente también dentro de las comunicaciones basadas en la especificación SIP-IETF, aunque difiere en su contenido con la estructura del perfil SIP-3GPP, principalmente en el sistema de cifrado utilizado. Esto, teniendo en cuenta que para IMS han evolucionado los sistemas de cifrado tradicionales, como MD5 (Message-Digest Algorithm 5), hacia nuevas versiones del mismo, como AKA-MD5 [15], definida especialmente para IMS, y que cuenta con un esquema de claves integradas, compatibles con IPSec, que es un protocolo utilizado para mantener la integridad y seguridad en capa de red. Además, una de las diferencias más relevantes radica en que en la mayoría de los

procesos necesarios para registrar usuarios en una comunicación basada en SIP-IETF, la cabecera Authorization no es estrictamente necesaria en este primer mensaje REGISTER enviado al proxy SIP, sino como respuesta al desafío de autenticación encontrado en la respuesta 401 Unauthorized enviada por la red, pero sí es obligatoria en el primer mensaje REGISTER enviado a la P-CSCF de una red IMS.

P-Preferred-Identity: Uno de los principales avances en la búsqueda de satisfacer los requerimientos de IMS propuestos por el 3GPP sobre el protocolo SIP, ha sido el desarrollo de las P-Headers (Private Headers) [14][37]. Estas son cabeceras adicionadas exclusivamente para funcionar sobre la arquitectura IMS, y cubren varios de los propósitos más relevantes de IMS, tales como obtener información sobre las redes de acceso local y visitada (información de la celda, en el caso de las comunicaciones móviles), y la determinación de las diferentes identidades que se pueden encontrar en un mismo cliente o dispositivo.

En el caso específico de la cabecera P-Preferred-Identity [37], es utilizada desde el agente de usuario hacia un proxy confiable, con el fin de portar en ella el valor de la identidad del usuario iniciador del mensaje. Si esta cabecera es recibida desde un cliente que no es confiable, el proxy envía una pista con las sugerencias de las identidades que el usuario podría utilizar. Como un avance especial en IMS, existe el hecho de utilizar múltiples identidades para un mismo usuario, en este caso, la P-Preferred-Identity debería contener en su campo “Value” una lista con esas identidades utilizadas.

P-Access-Network-Info: Teniendo en cuenta el requerimiento de IMS que trata sobre la eliminación de la dependencia tecnológica hacia la red de acceso, fue creada la cabecera adicional P-Access-Network-Info. El usuario envía en esta cabecera el tipo de acceso utilizado y alguna información específica sobre la red de acceso en servicio[29]. Esta cabecera es utilizada principalmente en las comunicaciones basadas en SIP en las cuales se despliegan servicios de conectividad de capas 2 y 3. En IMS se ha propuesto que el núcleo de red, en especial las funciones de capa de control que actúan como SIP-Proxy en determinado momento, utilicen esta información para optimizar los servicios ofrecidos al usuario. Por ejemplo, disminuyendo el número de mensajes requeridos para determinada labor SIP y sobrecargando los mensajes restantes enviados a dicho usuario con la información necesaria. Esto, para el caso en que la interfaz descrita en la P-Access-Network-Info sea de radio frecuencia.[14]

La aplicabilidad está radicada en los servicios provistos por el operador, como por ejemplo localización de la celda donde se conecta un usuario que realiza una llamada de emergencia, o la diferenciación de los servicios según la descripción de la red de acceso encontrada en la cabecera. Incluso, teniendo en cuenta que los servicios de IMS están basado en el principio de “Todo sobre IP o IP para Todo”, es de suponerse que estos servicios deberían ser independientes de la red de acceso, y por lo tanto la información contenida en esta cabecera no tenga una utilidad relevante. Pero el alcance de la P-Access-Network-Info, puede ir mucho más allá de los servicios SIP proveídos especialmente en una red IMS, y podría suponer el desarrollo de muchos más servicios que se basen en esta información. [14]

La modificación del contenido de esta cabecera está destinado solamente a los agentes de usuario, ya que el proxy proveedor de servicios no debe modificar este contenido, y aun menos los proxy intermedios entre el agente de usuario y el proxy proveedor, los cuales ni siquiera deben manipular esta información.[14]

Security-Client: En IMS se hace obligatorio el uso del protocolo IPSec para el establecimiento de Asociaciones de Seguridad (Security Associations - SA) entre el UE y la P-CSCF. Para los procesos de registro SIP, se han definido tres nuevas cabeceras que son de gran importancia para el establecimiento de las Asociaciones de Seguridad, estas son: Security-Client, Security-Server y Security-Verify.[9][17]

El terminal adhiere al contenido del método REGISTER la cabecera Security-Client, la cual contiene los mecanismos de seguridad (en la figura 14, “ipsec-3gpp”), los algoritmos (en la figura 14, hmac-sha-1-96), y el esquema de seguridad que el cliente soporta, además de los parámetros necesitados para el establecimiento de las Asociaciones de Seguridad.[29]

A continuación del envío de este primer mensaje REGISTER con la información básica del usuario y de las características principales que debe tener el registro del mismo, se recibe en i23GW la respuesta SIP 401 Unauthorized, la cual se constituye como un desafío definido por la red y que es enviado al terminal, con el objetivo de completar de forma segura las tareas de AAAC necesarias para el establecimiento del registro.

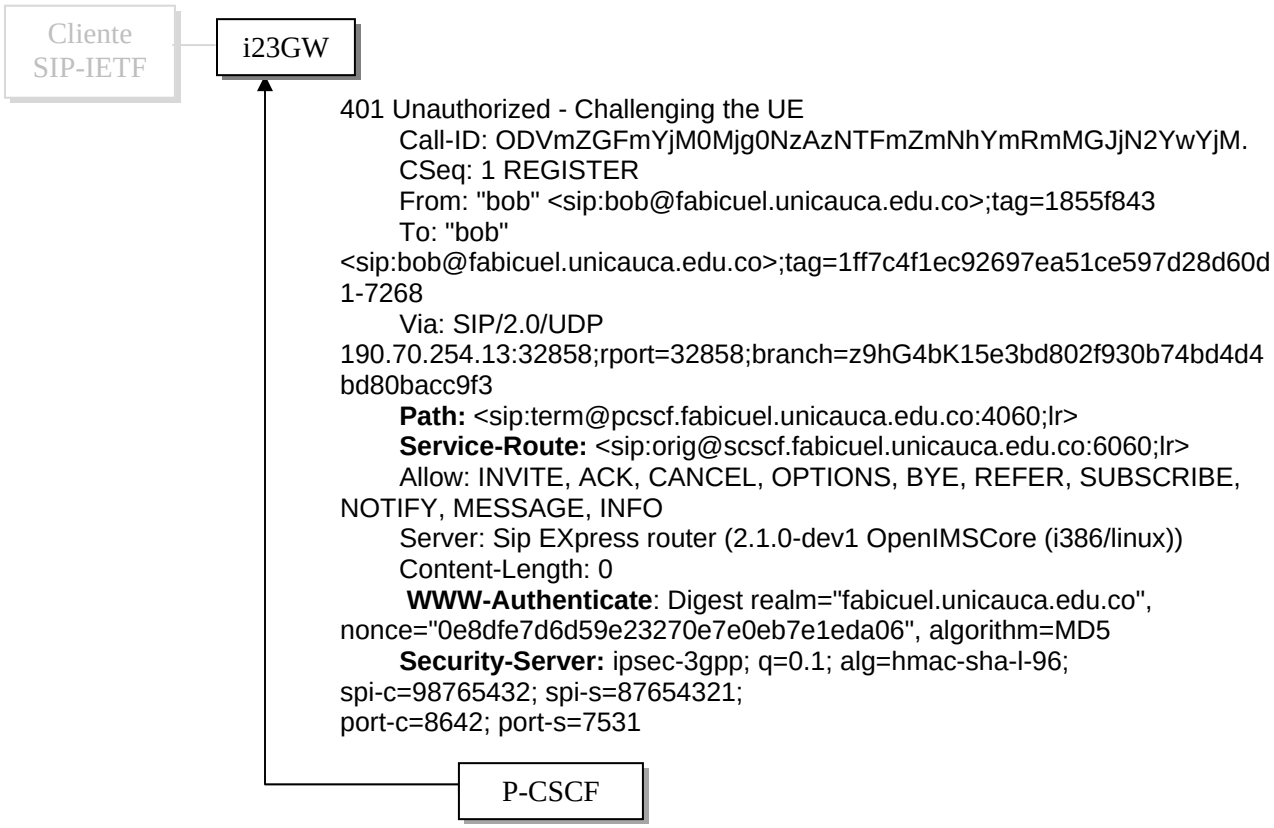


Figura 15. 401 Unauthorized devuelto por la P-CSCF hacia la i23GW

Path: Esta cabecera contiene la URI de la P-CSCF, es adicionada generalmente por la P-CSCF dentro de los mensajes enviados a la S-CSCF o al UE, con el fin de informarles dónde le pueden enviar las siguientes solicitudes SIP.[29]

Service-Route: Esta es una cabecera adicionada en la S-CSCF, con el objetivo de informar su URI a las entidades hacia las cuales envía los mensajes. Además de una cadena de caracteres que sirve para diferenciar entre las solicitudes móviles de inicio y de terminación.

WWW-Authenticate: Generalmente, SIP utiliza un mecanismo simple de autenticación heredado de HTTP basado en Digest [38]. Este es un mecanismo de intercambio de desafíos y respuestas, en el cual el SIP-Registrar responde a una solicitud de autorización del UE con un desafío, reflejado principalmente en una serie de datos a los cuales el usuario debe responder, generando una respuesta acertada y basada en dicha información. La base principal de este desafío es un código denominado *nonce,* el cuál está desarrollado en el lenguaje de cifrado asignado al usuario que se está registrando. En el SIP-IETF este lenguaje de cifrado generalmente es MD5, y aunque IMS soporta este cifrado, esta arquitectura generalmente usa AKA-MD5 para mayor seguridad.

Security-Server: Es una cabecera adicionada por la P-CSCF dentro de la respuesta 401 Unauthorized. Contiene el mecanismo de seguridad (en la figura 15, “ipsec-3gpp”) y los algoritmos (en la figura 15, hmac-sha-1-96) que la P-CSCF, además de los parámetros necesitados para el establecimiento de las Asociaciones de Seguridad.[29]

El servidor espera que después del envío de la cabecera Security-Server, el terminal agregue al siguiente método REGISTER una cabecera denominada Security-Verify, la cual contendría una copia del contenido de la cabecera Security-Server agregada anteriormente por la P-CSCF, para que la red se asegure de que no hay intrusos en puntos intermedios entre la red y el usuario real.[9]

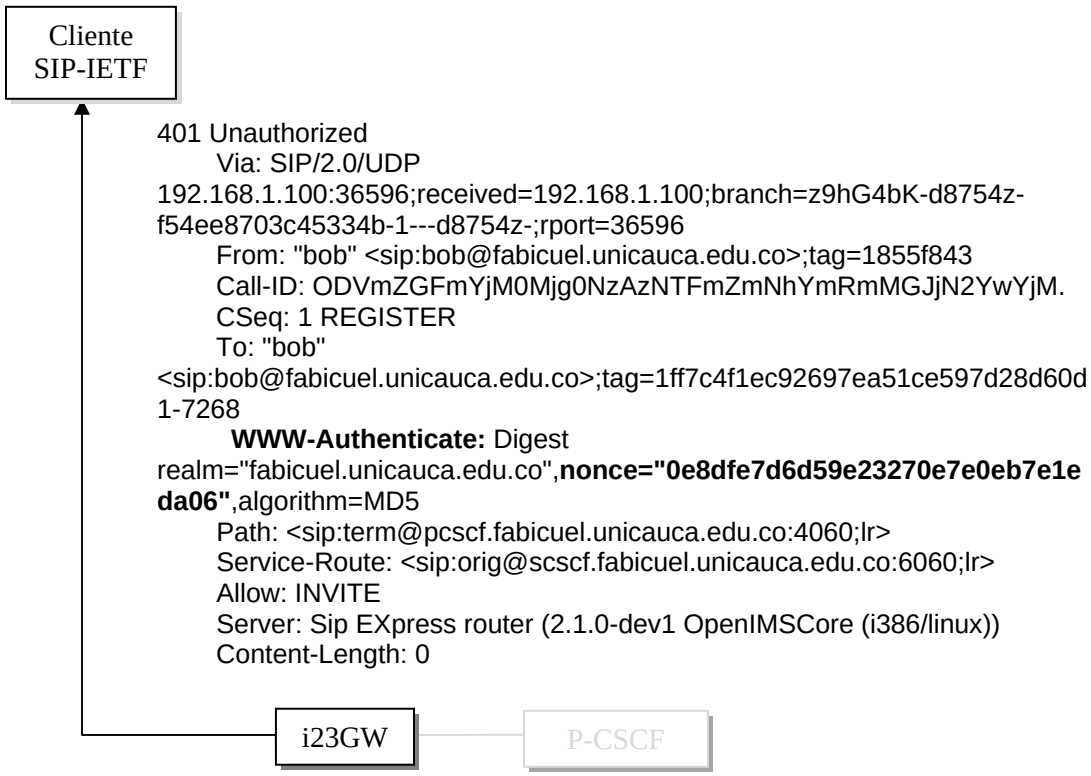


Figura 16. 401 Unauthorized modificado por i23GW y enviado hacia el UE

La P-CSCF solamente soporta el mecanismo ipsec-3gpp, aunque el objetivo de IMS con la declaración de las cabeceras Security-Client, Security-Server y Security-Verify, es precisamente que no existan traumatismos a la hora de agregar en las redes nuevos y mejorados mecanismos de seguridad, ya que con estas cabeceras simplemente habría necesidad de cambiar el valor en el nombre del mecanismo de seguridad aceptado tanto por la P-CSCF, como en el UE.[9]

i23GW recibe esta respuesta de 401 Unauthorized, y la envía hacia el UE prácticamente sin modificar ninguna de sus cabeceras más relevantes, teniendo en cuenta que con estas cabeceras el UE debe generar una segunda solicitud REGISTER, que corresponde a una respuesta al desafío recibido en el mensaje 401.

Es necesario que las cabeceras adicionales se agreguen al mensaje enviado hacia el UE, ya que es posible que algunos clientes soporten dichas cabeceras. Además, éstas pueden ser utilizadas para desarrollar servicios adicionales del lado de la pasarela con la información allí contenida. Por ejemplo, i23GW podría tener una relación directa con la S-CSCF de la red, gracias a que conoce la URI.

La respuesta que el UE hace al desafío realizado por el servidor, se realiza mediante el envío de un segundo método REGISTER, el cual contiene una contraseña cifrada en el mecanismo especificado dentro de la cabecera WWW-Authenticate del mensaje 401 Unauthorized.

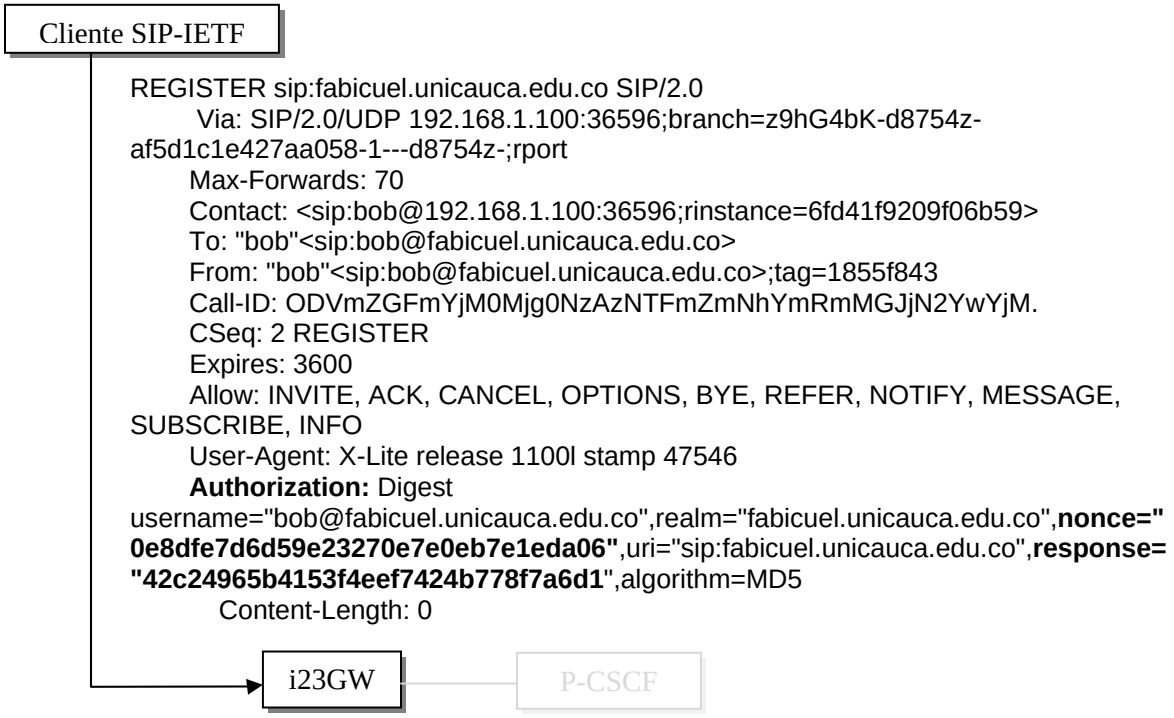


Figura 17. Segundo REGISTER, en respuesta al desafío de la Red

Como se muestra en la figura 17, el UE crea y agrega a la cabecera Authorization, un valor *response,* en base del valor del *nonce* recibido dentro del mensaje 401 Unauthorized. i23GW recibe este mensaje REGISTER y lo procesa, agregándole las cabeceras adicionales. En

este caso se agrega la cabecera Security-Verify, con un contenido elaborado a partir del valor de la cabecera Security-Server recibida en el 401 Unauthorized. Además, se agregan las mismas cabeceras que se han agregado en el primer REGISTER enviado, incrementando el valor del número secuencial de la cabecera CSeq. Este segundo REGISTER por enviar, tendría la forma descrita en la figura 18.

Las respuestas que se podrían recibir de la red a este segundo REGISTER, están relacionas con el hecho de que el usuario por registrar se encuentre o no en el repositorio del HSS. Esto no implica necesariamente que el usuario haya realizado un registro previo, sino que desde la red se haya adicionado manualmente en el repositorio un conjunto de datos relacionados con las identidades públicas y privadas del usuario.

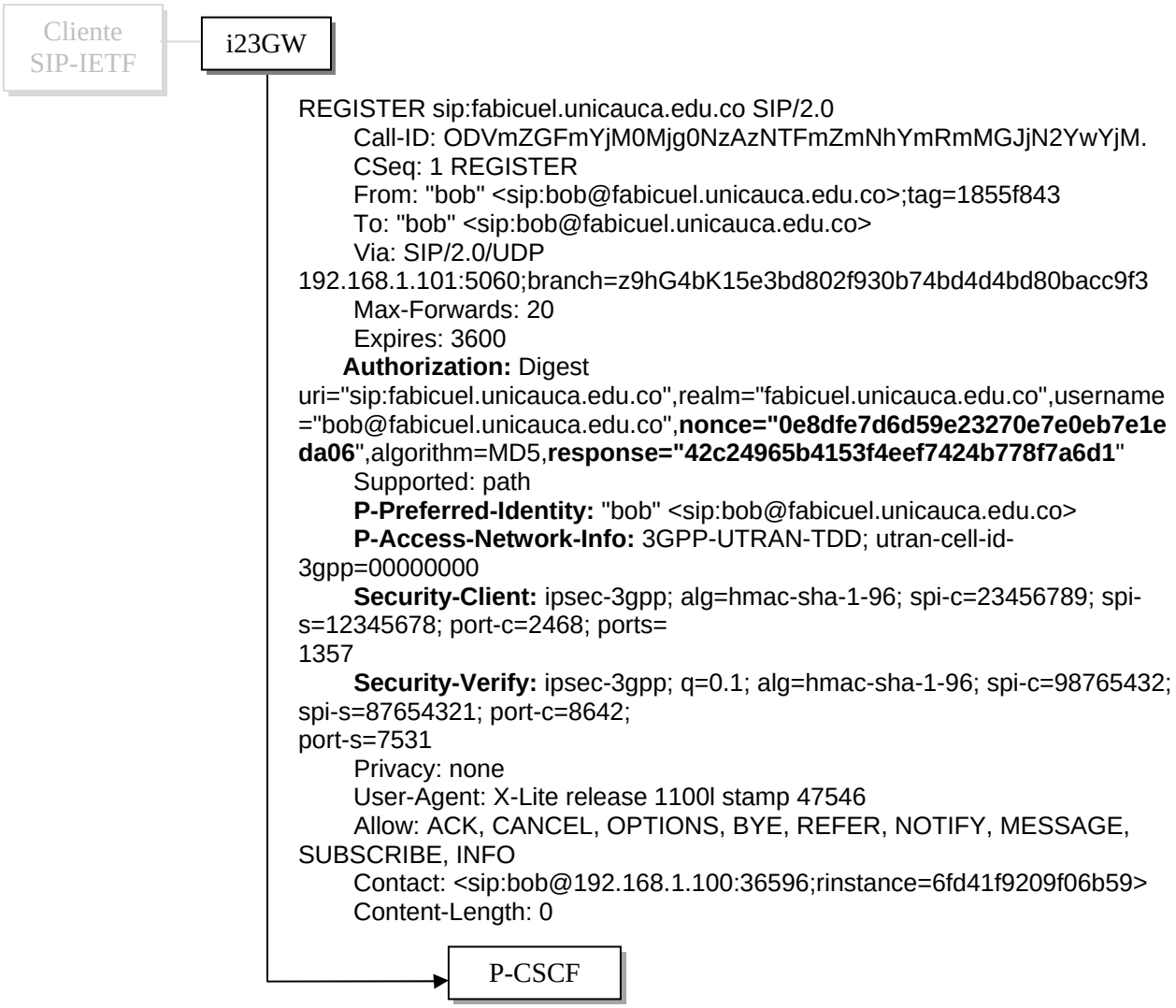


Figura 18. Segundo REGISTER, modificado por i23GW y enviado hacia la P-CSCF

Si la respuesta del UE al desafío generado por la red es acertada, y todos los datos de la cabecera Authorization corresponden con los esperados, el mensaje de respuesta SIP por enviar hacia el UE es un 200 Ok. Este mensaje se origina en la S-CSCF y es enviado

posteriormente a la I-CSCF indicando que el registro se ha realizado satisfactoriamente, y ésta lo reenvía hacia la P-CSCF. El 200 Ok entregado por la P-CSCF hacia i23GW se muestra en la figura 19.

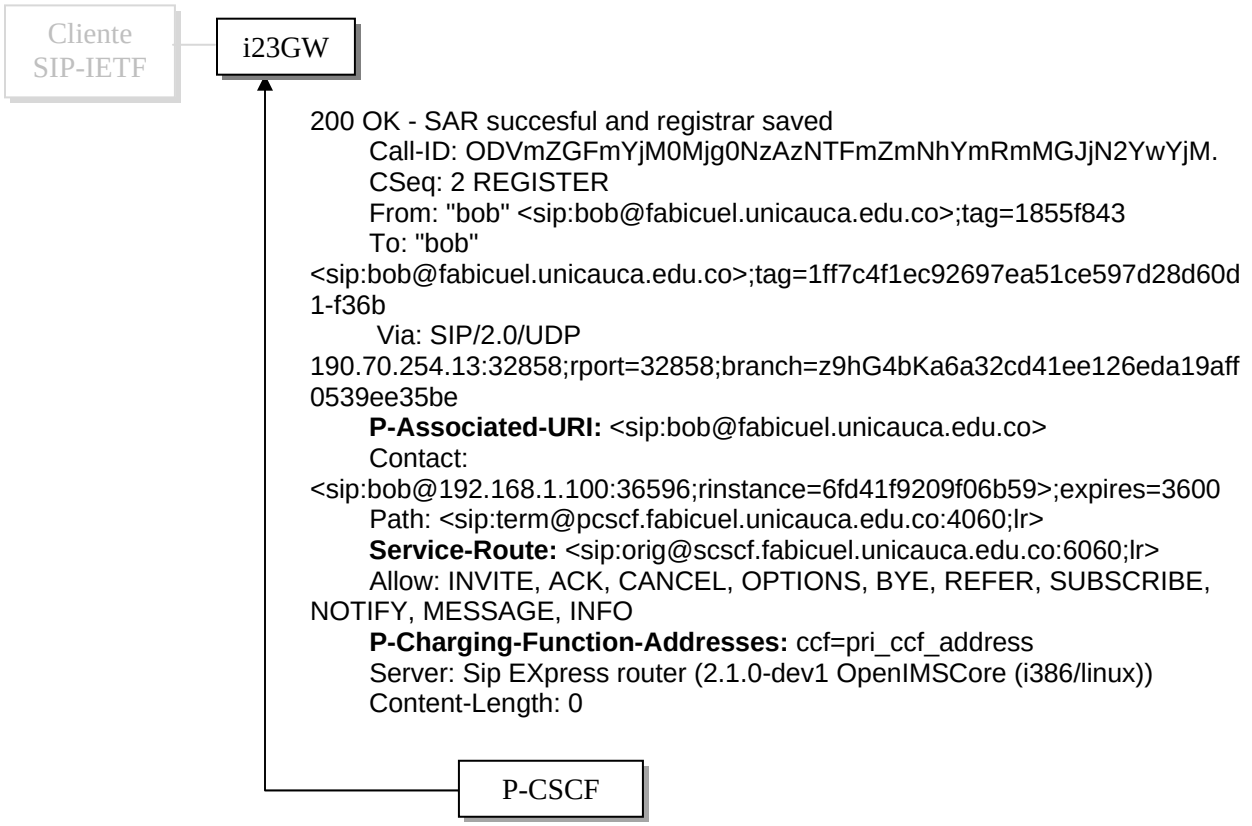


Figura 19. 200 Ok en aceptación a la Autenticación del usuario en la red y Registro exitoso

Existen nuevas cabeceras adicionales involucradas dentro de este mensaje. Estas cabeceras han sido definidas también dentro de las P-Headers [14] para IMS.

P-Charging-Function-Addresses: Teniendo en cuenta que la arquitectura IMS está dividida en distintas entidades de red dedicadas a la prestación de acceso y de servicios, surge la necesidad de informar a cada proxy SIP involucrado en una transacción, sobre los eventos y registros de tarificación producidos durante dicha transacción. El 3GPP ha definido dos tipos de entidades de tarificación para suplir esta necesidad. Por un lado la Función Colectora de Tarificación (Charging Collection Function, CCF), que es utilizada en tareas de tarificación off-line, tales como cuentas post-pago. Para comunicaciones sobre las que se realizan tarificación on-line, como por ejemplo las cuentas prepago, se utiliza la Función de Eventos de Tarificación (Event Charging Function, ECF).[14]

Un proxy SIP que recibe un mensaje el cual incluye la cabecera P-Charging-Function-Addresses, podría usar tanto el nombre o la IP del host que aparece en esta cabecera, como el destino de los eventos (ECF) y la información (CCF) de tarificación. Es entonces necesario que esta cabecera sea capturada por i23GW, más que por el UE final basado en SIP-IETF, ya que la pasarela podría dar algún uso a la información allí contenida, o simplemente reenviar esta información hacia alguna entidad encargada de servicios de tarificación. Los UE deberían incluir esta cabecera, cuando éstas están localizadas dentro de un dominio

administrativo de una red privada, la cual tendría que conocer y poder acceder a las direcciones de las entidades de tarificación.

P-Associated-URI: Esta es una cabecera incluida dentro de las consideraciones de seguridad d el RFC 3455 [14]. Contiene una lista de las URIs asignadas por la red local al usuario (No se debe confundir con la lista de URIs registrada implícitamente) [9]. A pesar de estar incluida esta cabecera dentro de los parámetros de seguridad de IMS, La información devuelta en el P-Asociado-URI no se considera como especialmente sensible. Por el contrario, se trata simplemente de información de carácter informativo, proporcionando la apertura al UE con respecto a la asociación automática realizada por el Registrar. Si de extremo a extremo, la protección no se utiliza en la capa SIP, es posible que los proxy entre el registro y el UA puedan modificar el contenido del valor de la cabecera. Esta intromisión no debería tener un impacto significativo en las tareas de señalización.

Las cabeceras adicionales que se encuentran en estos mensajes son de especial interés en el entorno de la pasarela, pero en su mayoría no serían entendidas por los UE basados en la especificación de la IETF para SIP. Por lo tanto, en algunos casos, no resulta necesario enviar estas cabeceras desde i23GW hacia el UE. Por ejemplo, como se muestra en la figura 20, en el mensaje 200 Ok se han eliminado estas cabeceras adicionales, para enviarlo hacia el UE.

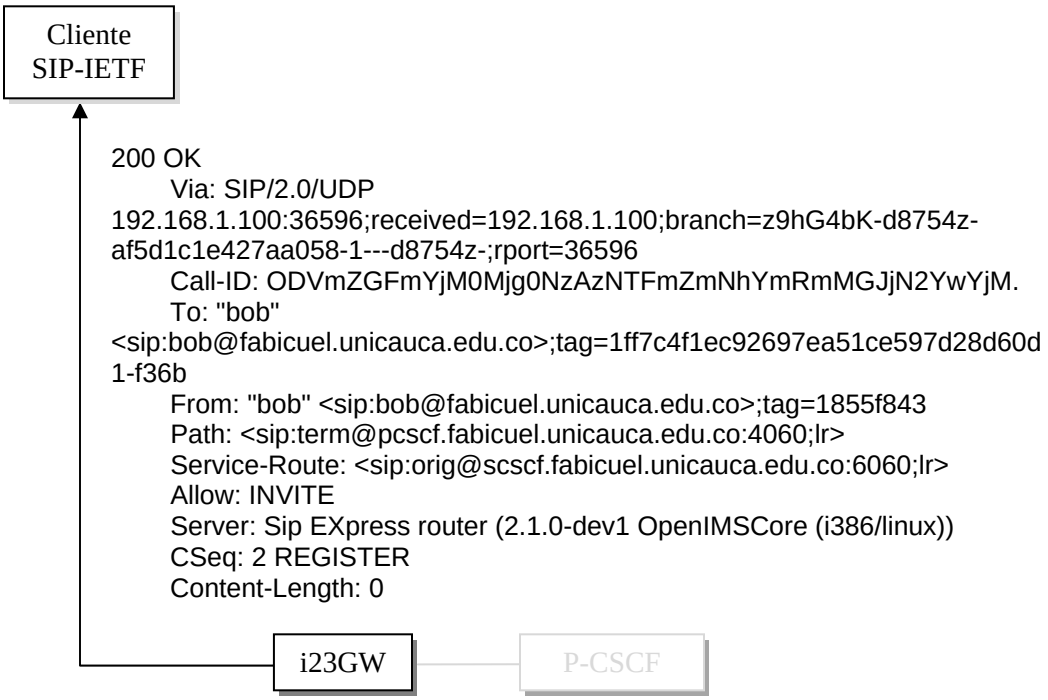


Figura 20. 200 Ok de aceptación al registro modificado por i23GW y enviado hacia el UE

Todos los métodos SIP anteriormente descritos corresponden al flujo de señalización necesario para registrar un usuario basado en el SIP-IETF dentro de una red IMS. Los mensajes necesarios para efectuar todas las tareas de señalización descritas en la sección 2.2 de este documento (des-registro, subscripción, notificaciones y establecimiento de la sesión) están descritos de manera específica en el TS 24.228 [29], en cuanto al tráfico SIP-

3GPP, y se puede complementar con la especificación del flujo de señalización SIP-IETF encontrada en el RFC 3261 [1].

3.2.2 Cabeceras adicionales en el flujo de señalización interno de IMS

Aparte del tráfico generado entre la P-CSCF y el UE, como se muestra en el capítulo 2, es necesario el envío de mensajes SIP entre otras entidades de IMS, tales como la P-CSCF, S-CSCF, I-CSCF, el HSS, y el servidor de aplicaciones SIP, con el fin de establecer y modificar las sesiones en la red. Para lograr esta tarea, las distintas entidades de IMS, al igual que la P-CSCF y el UE, agregan a los mensajes enviados cabeceras adicionales, con el fin de transmitir información acerca de los Equipos de Usuario, los identificadores de red, los parámetros de tarificación y del tráfico multimedia por utilizar.

Estas cabeceras adicionales no pertenecen al centro de estudio de i23GW, aunque por su utilidad dentro de las capacidades adicionales de IMS se hace necesario mencionarlas a continuación.

P-Charging-Vector: IMS es una arquitectura distribuida conformada por múltiples entidades de red diseñadas para proveer acceso y servicios a los usuarios. Los operadores de red tienen la necesidad de cobrar estos servicios y el acceso a la red, lo cual supone la coordinación entre las entidades, como por ejemplo los proxy SIP, y entre los registros de tarificación generados por todas las entidades involucradas en una misma sesión.

Las labores de facturación se hacen mucho menos complejas mediante la utilización de un identificador único de tarificación, el cual está incluido en la información de los registros de tarificación, y a su vez, dentro de un vector de tarificación.

Un vector de tarificación (Charging Vector), es una colección de todos los datos de tarificación producidos en el establecimiento de un diálogo, o en transacciones independientes y externas a un diálogo (denominadas de tipo *Standalone*), tales como el registro y la subscripción de usuarios. La información de tarificación es insertada dentro del vector por múltiples entidades de red, incluyendo los proxy SIP. De esta misma manera, las entidades de red son las encargadas de obtener esta información, interpretándola y conmutándola hacia los módulos pertenecientes a la capa de aplicación, encargados de prestar los servicios de tarificación.

Existen tres tipos de información que se debe transferir incluida dentro del vector de tarificación: el valor para la Identidad de tarificación IMS (IMS Charging Identity - ICID), La dirección del proxy SIP que crea el valor ICID, y los Identificadores de Interoperación (Inter operator). ICID es un valor que identifica un diálogo o una transacción standalone, y debe ser globalmente único, lo cual se logra mediante la integración de un valor único local, y el nombre de host o dirección IP del proxy SIP encargado de generar este identificador. El IOI identifica tanto a la red origen, como a la red destino involucradas en un diálogo o en una transacción standalone, con el fin de identificar cada uno de los lados de la red involucrados.

La cabecera P-Charging-Vector es aplicable dentro de un dominio administrativo de seguridad simple, o entre diferentes dominios administrativos donde hay una relación completamente confiable. De no ser así, los proxy SIP no deben incluir esta cabecera a los mensajes de respuesta ni de solicitud. La cabecera no es aplicable si el dominio

administrativo maneja tarificación que no requiere correlación de registros de múltiples entidades de red, como por ejemplo distintos proxy.

Los detalles más específicos sobre el modo de utilización para la cabecera P-Charging-Vector, se encuentran descritos en la definición de las cabeceras privadas para el 3GPP realizada en [14].

P-Asserted-Identity: Esta cabecera es usada por entidades SIP confiables, generalmente intermediarias, con el objetivo de transportar el identificador del usuario que ha enviado un mensaje SIP, siempre y cuando este usuario haya sido previamente autenticado en la red. [37]

Por ejemplo, cuando el UE envía un mensaje INVITE con el objetivo de establecer una sesión, la P-CSCF que recibe dicho INVITE agrega la cabecera P-Asserted-Identity y remueve la cabecera P-Preferred-Identity que ha sido incluida por el Equipo de Usuario de IMS o por la i23GW. El valor de la cabecera P-Asserted-Identity que se inserta al INVITE, generalmente corresponde a la URI SIP o URI telefónica del usuario. Si esta cabecera contiene dos valores distintos, uno de ellos debe ser una URI SIP, y el otro, una URI telefónica que identifique al usuario. [29][37]

El INVITE con la cabecera P-Asserted-Identity es enviado hacia la S-CSCF perteneciente a la red donde se origina la llamada, y ésta adiciona a la cabecera una URL telefónica (TEL URL) con el objetivo de que esta URL sea reconocida por la red de destino, en caso que el INVITE sea reenviado a una MGCF. [29]

Teniendo en cuenta que el INVITE debería viajar hacia una red destino donde se encuentra el Equipo de Usuario llamado, se debe repetir el mismo procedimiento que se ha efectuado en la P-CSCF y la S-CSCF de la red origen, pero en este caso, en la P-CSCF y S-CSCF de la red destino. [29][37]

Los detalles específicos sobre el modo de utilización de esta cabecera, se encuentran definidos en el RFC 3325. [37]

P-Called-Party-ID: Un servidor proxy inserta la cabecera P-Called-Party-ID generalmente dentro de un mensaje INVITE. La cabecera contiene el valor de la URI del solicitante, que ha sido recibido por el proxy en la solicitud SIP. Los servidores de agentes de usuario identifican a cuál de las múltiples identidades de usuario destino ha sido enviado el mensaje INVITE (dado el caso de que el usuario tenga registradas más de una identidad, por ejemplo, una para el domicilio y otras para el trabajo).[14]

El servidor de agentes de usuario puede utilizar la información de esta cabecera para distinguir los recursos audiovisuales para los tonos de alerta que se enviarán al usuario, dependiendo de la URI utilizada para recibir la invitación a establecer una sesión.

Para el 3GPP, ha sido de especial importancia en IMS que los usuarios puedan tener múltiples identificadores, con lo cual se puedan proveer mejores y más diferenciados servicios, como por ejemplo, el de aparecer indisponible ante otros usuarios con su identidad de trabajo, y por otro lado, aparecer como disponible con su URI personal, y poder establecer sesiones con usuarios familiares.

Se podría suponer que la información de la URI destino en un mensaje INVITE podría estar contenida dentro de la cabecera To, que es enviada generalmente dentro de cualquier mensaje SIP basado en la especificación realizada por la IETF para el protocolo. El problema surge cuando, por ejemplo, un mensaje INVITE es creado por un UE que ha introducido dentro del valor de la cabecera To, una identidad de usuario distinta a aquella con que el usuario destino se ha registrado en la red. Este problema no podría ser solucionado por los proxy, ya que éstos no tienen la capacidad de modificar dicha cabecera.[14]

Otra posible alternativa para la no utilización de la extensión P-Called-Party-ID, sería la generación de múltiples valores identificadores en la cabecera Contact, a la hora de registrar el usuario que va a ser llamado. El problema con esta posible solución, es que no todos los usuarios tienen un total control sobre las identidades de usuario que tienen asignadas.
[14]
Por lo tanto, se hacía necesaria esta nueva cabecera, que contuviera la información de las múltiples URI llamadas y diferenciadas, y a su vez, pudiera hacer parte de las labores de señalización de los Proxy SIP intermedios, pertenecientes a la arquitectura de IMS

Los detalles específicos sobre la utilización de la cabecera P-Called-Party-ID se encuentran definidos en la especificación del 3GPP para las cabeceras privadas, realizada en el RFC 3455 [14]

P-Media-Authorization: Esta cabecera es insertada dentro de un mensaje INVITE, por parte de la P-CSCF de la red destino, y es enviado hacia el Equipo de Usuario llamada. La cabecera P-Media-Authorization contiene uno o varios de símbolos identificadores de autorización de medios. Estos símbolos están dispuestos para ser incluidos en las reservaciones subsecuentes de recursos para los flujos de medios asociados con la sesión. Esto significa que se pasan estos símbolos hacia un mecanismo independiente de reservación de recursos, el cual no se especifica en la definición de esta cabecera. [20]

Los símbolos de autorización de medios son usados en la negociación de parámetros de QoS para el flujo multimedia. Los detalles específicos sobre el uso de esta cabecera y su contenido, está descrito en la especificación para cabeceras privadas encontrada en el RFC 3313 [20].

4. PROTOTIPO DE PASARELA DE ACCESO A CAPACIDADES IMS DESDE CLIENTES SIP-IETF – "i23GW"

4.1 Introducción

En el capítulo 1 se describen las diferencias más relevantes entre las especificaciones estudiadas del protocolo SIP, IETF y 3GPP con el objetivo de establecer una base teórica sobre los requerimientos para el uso del protocolo SIP en IMS y las soluciones que ha planteado el 3GPP. Basándose en estas diferencias y en la definición de las extensiones de SIP, en el capítulo 3 se presenta una propuesta sobre las modificaciones estructurales al protocolo, que deberían ser adoptadas en el diseño y desarrollo de una pasarela de señalización, de tal forma que clientes SIP-IETF puedan acceder a capacidades de IMS.

Teniendo en cuenta los avances obtenidos en los capítulos anteriores, se presenta el diseño y la construcción de la pasarela i23GW, en la cual se consideran las diferencias existentes entre las dos especificaciones del protocolo SIP y, en especial, el flujo de entrada y salida de la pasarela de señalización, descrito en el capítulo 3.

i23GW es una pasarela de señalización ubicada en la capa de aplicación, destinada a trabajar sobre la estructura del protocolo SIP, y que satisface la necesidad de adaptar los mensajes SIP provenientes de clientes basados en la especificación de la IETF, agregando y modificando las cabeceras del 3GPP necesarias para buscar la compatibilidad con la versión SIP del 3GPP. De esta forma, i23GW logra que dichos clientes accedan a las capacidades propias dentro de una red IMS, relacionando cada una de las cabeceras adicionales con los servicios de IMS que se piensa brindar. Además, i23GW permite agregar nuevas funciones de adaptación (en caso de surgir nuevas extensiones del 3GPP para el protocolo SIP) y complementarse con servicios y aplicaciones que no tengan una relación directa con el servidor de aplicaciones de la arquitectura IMS, como aplicaciones independientes de terceros, tales como aplicaciones de tarificación, localización o diferenciación de servicios, que son orientadas a un solo grupo de clientes, y que por razones comerciales y técnicas no podrían ser desplegadas en el servidor de aplicaciones de la red IMS.

A continuación se describe la forma en la cual i23GW adapta los mensajes SIP de entrada, procedentes tanto del Cliente SIP-IETF, como desde una red IMS, y cómo entrega los mensajes adaptados, necesarios para lograr el acceso a las capacidades IMS y para que los clientes puedan ser plenamente identificados y aceptados en la red.

4.2 Análisis de Requerimientos para el Diseño y Desarrollo de i23GW

Los requerimientos generales del sistema están relacionados estrechamente con los requerimientos que propone el 3GPP para SIP, descritos en la sección 1.4; debido a que en ellos se refleja claramente el interés del 3GPP por asignar tareas a SIP relacionadas con las capacidades más importantes de IMS, tales como Calidad de Servicio, seguridad, diferenciación de servicios y mejora en las tareas de AAAC (Authentication, Authorization, Accounting and Charging).

A pesar de que los requerimientos del 3GPP sobre SIP para IMS están planteados según las capacidades y servicios de IMS, al hablar de SIP es más conveniente establecer dichos requerimientos con base en las funciones generales para las cuales el protocolo está diseñado. De esta forma, para el presente capítulo se han definido una serie de requisitos para i23GW, basados en los requerimientos del 3GPP para SIP, y a su vez, orientados a las labores que SIP está destinado a cumplir para inicio, gestión y terminación de sesiones multimedia (Registro, Subscripción, Invitación y Terminación de Sesiones, etc.).

4.2.1 Requisitos para el Registro de usuarios

La pasarela i23GW debe cumplir con los siguientes requisitos para el registro de usuarios SIP-IETF dentro de una red IMS:

- Se deben adaptar los mensajes de solicitud REGISTER provenientes del cliente SIP-IETF, y enviar los mensajes adaptados hacia el núcleo de la red IMS, de tal forma que la red pueda identificar cualquier solicitud de este tipo, y por consiguiente, los datos necesarios del usuario para responder a esta solicitud con un desafío de autenticación, o con una respuesta de aceptación, dado el caso de que el usuario haya cumplido previamente con dicho desafío de autenticación.

- La pasarela podría permitir identificar el tipo de tecnología de acceso que está utilizando el cliente SIP-IETF. Esto tiene cierta dependencia con el tipo de cliente SIP-IETF que realiza la solicitud, ya que no todos los clientes existentes en el mercado cuentan con mecanismos para portar esta información.

- La pasarela debe estar en condiciones de capturar los mensajes respuesta de IMS, los cuales portan información de autenticación, y debe a su vez permitir que cualquier tipo de cifrado utilizado en las labores de autenticación sea aceptado.

4.2.2 Requisitos para Subscripción y Notificación de usuarios

Algunas de las redes basadas en la arquitectura de IMS prestan la posibilidad de subscribir a un usuario de manera automática al momento de registrar dicho usuario. Esto podría ahorrar en la pasarela el desarrollo de un módulo para permitir la subscripción de usuarios. Pero no todos los desarrollos actuales basados en IMS cuentan con esa herramienta de subscripción automática, es por eso que uno de los requerimientos para el diseño y desarrollo de i23GW debe ser el permitir que un cliente SIP-IETF pueda ser subscrito en la red, y de esta forma, recibir notificaciones de des-registro por parte del S-CSCF de la red.

Teniendo en cuenta este requerimiento de subscripción, surgen los siguientes requisitos para la pasarela:

- Se deben adaptar los mensajes de solicitud SUBSCRIBE provenientes del cliente SIP-IETF, y enviar los mensajes adaptados hacia el núcleo de la red IMS, de tal forma que la red pueda identificar cualquier solicitud de este tipo, y por consiguiente, los datos

necesarios del usuario para responder a esta solicitud con un mensaje de respuesta SIP.

- La pasarela podría permitir identificar el tipo de tecnología de acceso que está utilizando el cliente SIP-IETF. Esto tiene cierta dependencia con el tipo de cliente SIP-IETF que realiza la solicitud, ya que no todos los clientes existentes en el mercado cuentan con mecanismos para portar esta información.

4.2.3 Requisitos para Establecimiento y Terminación de las sesiones

El establecimiento de sesiones tiene ciertos requerimientos particulares con relación al registro, subscripción y otras labores de señalización SIP. Esto, debido a que en ella actúa más de un Equipo de Usuario en la misma transacción, y por lo tanto las consideraciones para herramientas B2B (Back to Back), como el caso de i23GW, varían de una manera razonable con relación a las transacciones de registro y subscripción, donde los mensajes del lado del cliente que deben ser identificados por la pasarela provienen solamente de una Equipo de Usuario.

De esta manera, la pasarela debe cumplir con los siguientes requisitos para el establecimiento de sesiones en las cuales actúa por lo menos un cliente SIP-IETF:

- La pasarela debe poder recibir mensajes SIP de solicitud INVITE o cualquier tipo de respuesta SIP, provenientes del cliente SIP-IETF o de la red IMS. De la misma manera en que recibe los mensajes de solicitud y respuesta, debe poder diferenciar entre cuál cliente SIP-IETF (en caso de que más de uno participe en la sesión) es el origen, y cuál de ellos es la entidad de destino.

- Teniendo en cuenta que para IMS se manejan múltiples identidades para un mismo usuario, la pasarela debe contar con un mecanismo de captación y reenvío de estas identidades, sin causar traumatismos en el flujo de señalización y en las labores de reconocimiento de usuarios SIP origen y destino.

- La pasarela podría permitir la identificación de la tecnología de acceso que está utilizando el cliente SIP-IETF. Esto tiene cierta dependencia con el tipo de cliente SIP-IETF que realiza la solicitud INVITE, ya que no todos los clientes existentes en el mercado cuentan con mecanismos para portar esta información.

4.2.4 Requisitos Generales del Sistema

- El sistema debe contar con una arquitectura modular, extensible y portable, de tal forma que pueda ser fácilmente adaptada a cualquier implementación de red basada en IMS.

- La aplicación correspondiente a i23GW debe ser útil para reconocer los mensajes SIP más relevantes encontrados en la definición de la IETF, consignada en el RFC 3261 [1]. Esto significa que debe estar en capacidad de leer los mensajes SIP, procesar una respuesta o una solicitud de acuerdo con la tarea de señalización que se esté

realizando, e iniciar una nueva tarea, ya sea de señalización (enviando un mensaje SIP modificado hacia el núcleo de IMS), o activar cualquier aplicación adicional a la funcionalidad básica de la pasarela (por ejemplo, una aplicación para tarificación).

- i23GW debe poder reconocer los mensajes provenientes de clientes IMS y diferenciarlos plenamente de los producidos por clientes SIP-IETF. Los mensajes de un cliente SIP IMS no deben llegar directamente desde el cliente a la pasarela, sino que ya han sido procesados y redirigidos por los proxy SIP de la red IMS.

- La estructura de los mensajes producidos por los Clientes SIP-IETF debe ajustarse estrechamente a la definición del protocolo realizada en el RFC-3261 [1], debido a que i23GW basa la lectura, modificación y envío de dichos mensajes en esta definición.

- La CSCF debe reconocer a i23GW como un cliente IMS basado en SIP-3GPP. De esta forma, los mensajes enviados a todos los clientes SIP-IETF desde el núcleo de red, son dirigidos inicialmente hacia i23GW y no de manera directa al UE.

4.3 Formulación de la Arquitectura General del Sistema

En consecuencia con el análisis de requerimientos, en la figura 21 se propone la arquitectura general del sistema:

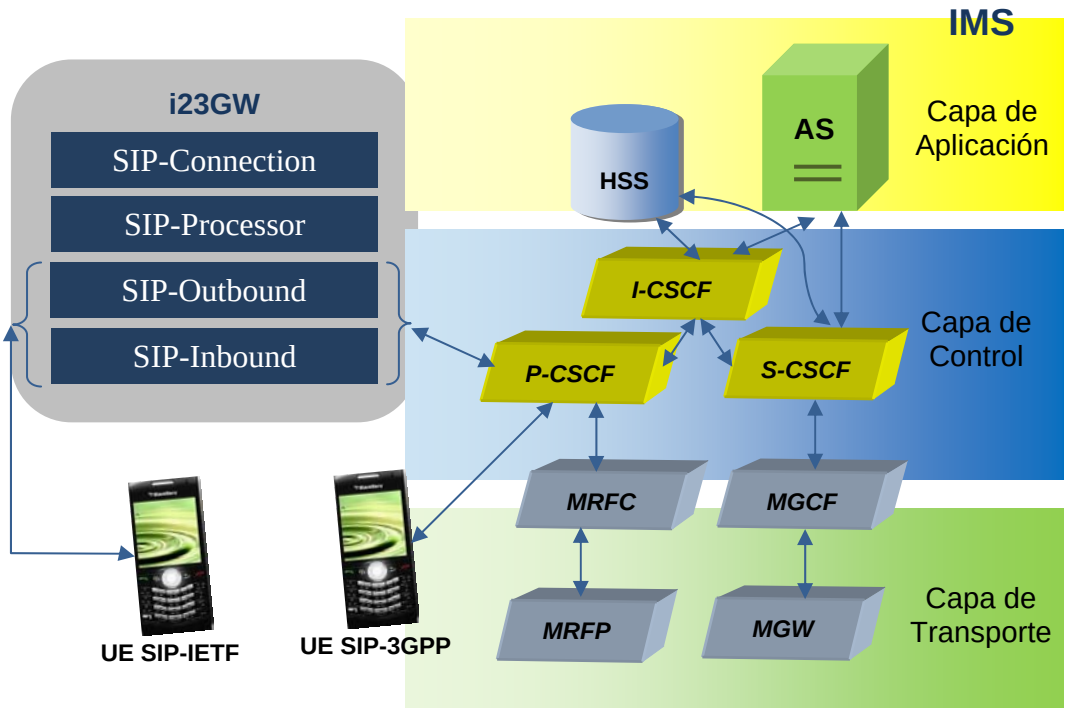


Figura 21. Formulación de la Arquitectura General del Sistema

4.3.1 UE SIP-IETF

Corresponde a todos los clientes que cumplen con la especificación básica del protocolo SIP, definida en el RFC 3261[1]. Dentro de la arquitectura general del sistema, cumple el papel de Equipo de Usuario iniciador de las tareas de señalización típicas de SIP, tales como registro, subscripción, inicio y terminación de sesiones.

Estos UE deben ser configurados de tal forma que todos sus mensajes sean enviados hacia i23GW, y de allí, modificados y reenviados hacia la P-CSCF de la red. Esta configuración se realiza ajustando el dominio de i23GW como proxy destino, e incluyendo dicho dominio dentro del (los) nombre(s) de usuario SIP asignado(s) al UE. Una descripción más completa de esta entidad de red, y de los mensajes producidos por ella se encuentra en el anexo A, y en el RFC 3261 [1].

4.3.2 UE SIP-3GPP

Los Equipos de Usuario que cumplen con los mecanismos de señalización definidos por el 3GPP, no requieren el reconocimiento y conexión directa con i23GW. Sin embargo, uno de los principales aportes de la pasarela de señalización es permitir que estas entidades puedan ser interconectadas con clientes SIP-IETF, estableciendo una sesión entre ellos.

En la actualidad existen distintos clientes en proceso de desarrollo, dentro de los cuales uno de los más populares para el entorno académico, por ser de libre distribución, es el cliente OpenIC Lite [39], desarrollado por el grupo alemán Fraunhofer Fokus Group. Este cliente hace parte de un conjunto de herramientas software basadas en la arquitectura de IMS desarrolladas por el mismo grupo.

4.3.3 i23GW

Corresponde a una pasarela de señalización entre SIP-IETF y SIP-3GPP. El funcionamiento de i23GW está basado en el desarrollo de un sistema Software que actúa como herramienta B2B de señalización, recibiendo mensajes SIP provenientes de la red IMS y del cliente SIP-IETF, modificándolos, y entregándolos a su destino. Todo esto, sin interrumpir las labores de señalización esperadas por todas las entidades involucradas, y sin causar traumatismos en cuestiones de tiempo de procesamiento, ancho de banda, seguridad y calidad de servicio esperados por dichas entidades.

i23GW está compuesto por tres módulos principales, destinados a escuchar, procesar y reenviar los mensajes SIP. Estos módulos se describen a continuación:

4.3.3.1 SIP-Inbound

Este módulo es el encargado de recibir los mensajes SIP que provienen de la red IMS y desde los distintos clientes SIP-IETF. La recepción de los mensajes consiste en la

generación de un evento software en la pasarela que alerte la entrada de un nuevo mensaje, y la consignación de los datos (cabeceras y su contenido) entrantes en un registro, de tal forma que el SIP-Processor pueda utilizar y modificar dicha información de manera posterior a su llegada.

4.3.3.2 SIP-Processor

Éste es el módulo principal de la pasarela i23GW. Utiliza la información de las cabeceras de los mensajes SIP entrantes para tomar decisiones sobre la modificación de los mismos. El objetivo principal de este módulo es agregar las cabeceras adicionales a los mensajes SIP provenientes de clientes IETF. Además, debe adaptar los mensajes provenientes de la red IMS de tal forma que sean aceptables por cualquier cliente SIP-IETF.

Los mensajes SIP generalmente portan la información referente a su procedencia y hacia dónde se dirigen. Esto último es enviado hacia el SIP-Outbound, de tal forma que este tenga conocimiento de hacia dónde enviar los mensajes adaptados.

4.3.3.3 SIP-Connection

Módulo encargado de fijar todos los parámetros de conexión SIP entre i23GW, los clientes y la red IMS. Además de fijar los parámetros, debe crear la conexión y establecer un vínculo entre las distintas entidades de red, utilizando ya sea el protocolo UDP o TCP.

4.3.3.4 SIP-Outbound

Los mensajes modificados deben ser enviados por el SIP-Outbound, ya sea hacia el cliente SIP-IETF, como hacia la red IMS para completar las labores de señalización. Esto se realiza utilizando la conexión SIP previamente existente y la información de destino que ha sido definida en el SIP-Processor.

4.3.4 Red IMS

Es de suponerse que los mensajes provenientes y salientes de la red IMS no sufran ningún traumatismo. El comportamiento de la red IMS debe ser exactamente el mismo con relación a la pasarela de señalización, como lo es con los clientes SIP-3GPP. Dicho comportamiento se describe completamente en el Anexo B y en las secciones 1.2 y 2.2 de este documento.

4.4 Diseño e Implementación del Sistema

Para la ejecución del proyecto se ha elegido como metodología de desarrollo al Modelo para la Construcción de Soluciones (MCS), el cual es una síntesis de los resultados obtenidos en estudios realizados sobre procesos sistemáticos de mejoramiento de la calidad de los procesos de desarrollo, que se llevan a cabo en el departamento de Telemática de la FIET. [40]

El Modelo para la Construcción de soluciones propone el seguimiento iterativo de cuatro fases de desarrollo: Estudio de Prefactibilidad, Formulación del Proyecto, Ejecución del Proyecto y Validación de la Solución. Estas fases son útiles en el análisis del alcance y dominio del problema, y en el desarrollo y validación de las diferentes versiones entregadas del proyecto.

En el presente capítulo se detalla lo relacionado con la etapa de ejecución del proyecto. Partiendo del análisis de los componentes esenciales del sistema ya definidos, se puede iniciar la fase de diseño e implementación de cada componente de acuerdo al soporte teórico con el que se cuenta.

La selección de las herramientas que permitieron el desarrollo de cada componente tuvo en cuenta principalmente:

- la disponibilidad de acceso a la herramienta, y que ésta contara con una buena documentación de instalación y uso.
- La herramienta debería contar con ejemplos de aplicaciones previamente realizadas.
- También debería permitir un desarrollo rápido debido a experiencias previas en su utilización.

En lo que respecta a esta última consideración, se decidió utilizar como lenguaje general de programación el lenguaje Java, en especial, la implementación de Java para SIP, Jain-SIP [41]. En el Anexo C se encuentra una detallada descripción de las herramientas utilizadas para la creación y puesta en marcha de cada módulo del sistema.

En las siguientes secciones se realiza el diseño y se especifican las herramientas que se seleccionaron para el desarrollo de cada componente del sistema, de acuerdo a los requerimientos que se plantearon en la Fase de Análisis y a la Formulación de la Arquitectura General del Sistema. Esto constituye la etapa de ejecución del proyecto.

4.4.1 Diagrama de Casos de Uso del Sistema

En la definición de casos de uso del sistema se identifican dos actores principales, el Cliente SIP-IETF y el administrador. En la figura 22 se ilustra el diagrama de casos de uso del sistema iniciados por estos dos actores.

Este diagrama representa las capacidades del sistema que pueden ser accedidas o iniciadas desde distintos actores. Esto resulta de gran importancia para evidenciar los avances obtenidos gracias a la aparición de i23GW, sobre todo, aquellos casos de uso que ahora podrán ser iniciados desde el Cliente IETF, como por ejemplo el registro o des-registro de un UE dentro de una red IMS a modo de usuario válido de la misma.

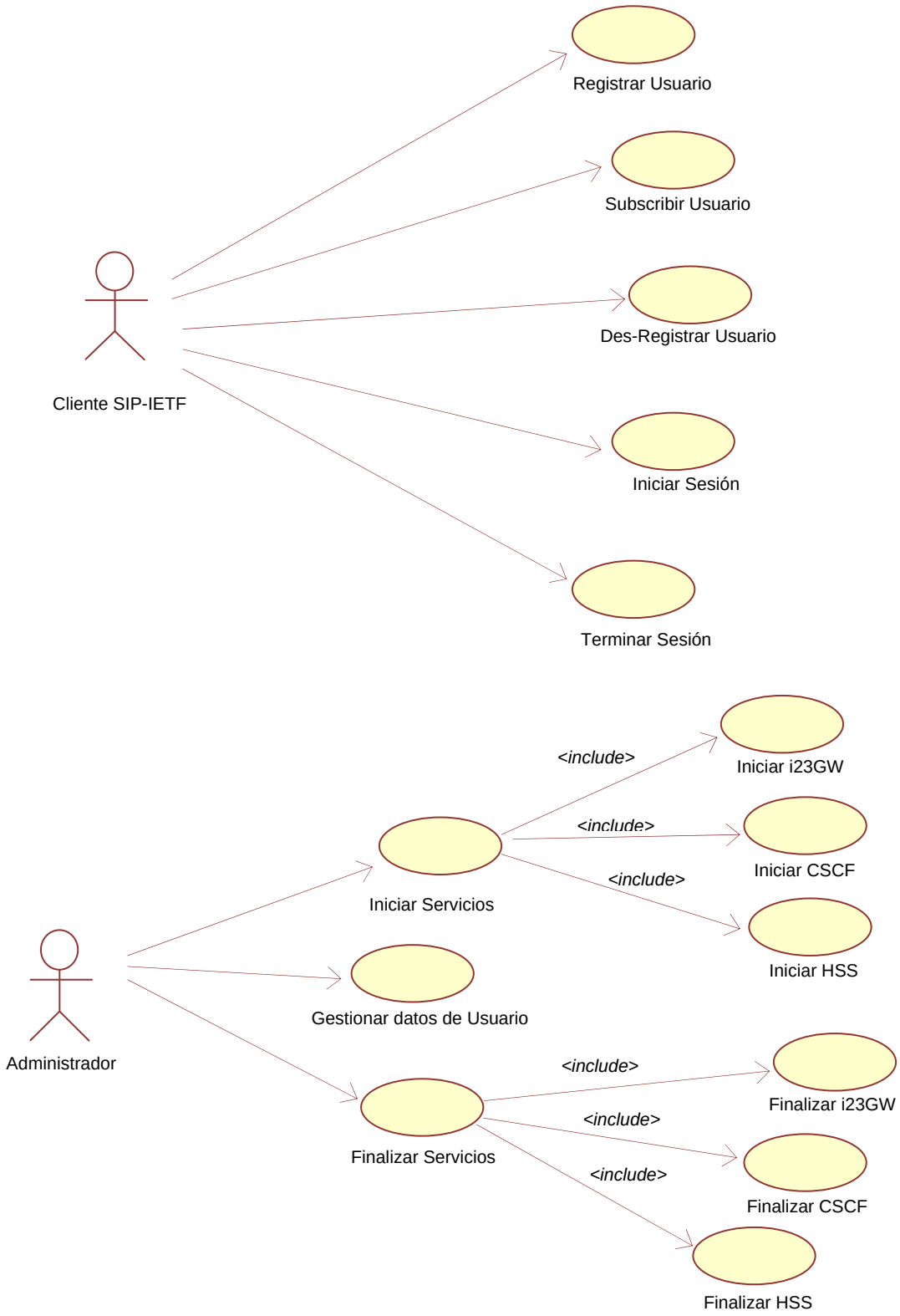


Figura 22. Diagrama de Casos de Uso del Sistema

4.4.1.1 Descripción Casos de Uso Iniciados por el Cliente SIP-IETF

Nombre	Registrar Usuario
Iniciador	Cliente SIP-IETF
Propósito	Registrar las identidades de usuario dentro de la red IMS
Resumen	I23GW recibe el primer mensaje REGISTER proveniente del cliente SIP-IETF, lo modifica agregando las cabeceras adicionales, y la cabecera Authorization con un valor inicial en blanco. Después recibe y modifica el mensaje 401Unauthorized enviado por la red y lo modifica para después enviarlo nuevamente hacia el usuario. Posterior a ello, i23GW captura y modifica el segundo mensaje REGISTER proveniente del UE, y lo reenvía hacia la red IMS. Además, debe también recibir y modificar la respuesta de aceptación de la red: mensaje 200 Ok.

Tabla 6. Caso de Uso Registrar Usuario

Nombre	Subscribir Usuario
Iniciador	Cliente SIP-IETF
Propósito	Subscribir al usuario en la S-CSCF, para que éste pueda recibir posteriores notificaciones de eventos concernientes a su estado de registro en la red.
Resumen	Para lograr la subscripción de un usuario i23GW debe capturar y modificar los mensajes SUBSCRIBE, agregándole las cabeceras adicionales y reenviándolo hacia la red. I23GW también toma todos los posibles mensajes de respuesta enviados por la para la subscrición de usuarios, los modifica, y reenvía hacia el cliente.

Tabla 7. Caso de Uso Subscribir Usuario

Nombre	Des-Registrar Usuario
Iniciador	Cliente SIP-IETF
Propósito	Eliminar el registro del usuario en la red.
Resumen	La pasarela de señalización recibe un mensaje REGISTER, y entiende que es un mensaje de des-registro si éste contiene en su cabecera Expires un valor igual a 0. De esta forma, i23GW adapta y reenvía el mensaje REGISTER hacia la P-CSCF, en espera de que la red genere un nuevo desafío, tal cual se realizó previamente para el registro del mismo usuario.

Tabla 8. Caso de Uso Des-Registrar Usuario

Nombre	Iniciar Sesión
Iniciador	Cliente SIP-IETF
Propósito	Invitar a un usuario SIP-IETF o SIP-3GPP a establecer una comunicación multimedia.
Resumen	i23GW recibe los mensajes de invitación: INVITE, les agrega las cabeceras adicionales y lo direcciona hacia la red IMS o hacia el cliente SIP-IETF. De la misma manera hace con los demás mensajes de respuesta o solicitud involucrados en el establecimiento de la sesión, como por ejemplo, con los mensajes 180 Ringing, CANCEL, BYE, etc.

Tabla 9. Caso de Uso Iniciar Sesión

Nombre	Terminar Sesión
Iniciador	Cliente SIP-IETF
Propósito	Terminar una sesión multimedia establecida.
Resumen	Cualquiera de los Equipos de Usuario involucradas en la sesión puede terminarla. Para el proyecto actual se considerará solamente la terminación de sesiones realizada por parte del Cliente SIP-IETF, ya que las consideraciones del cliente SIP-3GPP están por fuera del alcance de los objetivos planteados. La terminación de una sesión establecida, es iniciada por un cliente SIP-IETF por medio de un mensaje BYE. El cual es enviado a la pasarela i23GW, para que ésta procese dicho mensaje y lo envíe hacia la red IMS. Posteriormente, este mensaje será dirigido al cliente IETF o 3GPP con el que se haya establecido la sesión por terminar.

Tabla 10. Caso de Uso Terminar Sesión

4.4.1.2 Descripción Casos de Uso Iniciados por el Administrador

Nombre	Iniciar Servicios
Iniciador	Administrador
Propósito	Activar todos los servicios necesarios para que el usuario pueda iniciar cualquiera de sus casos de uso.
Resumen	Los servicios por iniciar son: • Herramienta Software para las distintas clases de CSCF: I-CSCF, S-CSCF y P-CSCF. • Herramienta Software para el repositorio HSS. • Activación del servicio SIP B2B correspondiente a la i23GW.

Tabla 11. Caso de Uso Iniciar Servicios

Nombre	Gestionar Datos de Usuario
Iniciador	Administrador
Propósito	Agregar, Eliminar y modificar la información correspondiente a los usuarios dentro del registro.
Resumen	Al iniciar el servicio de registro del HSS, se inicia también una consola de administración de usuarios, donde se pueden eliminar, modificar y agregar nuevos datos sobre los usuarios registrados en el sistema.

Tabla 12. Caso de Uso Gestionar Datos de Usuario

Nombre	Finalizar Servicios
Iniciador	Administrador
Propósito	Desactivar todos los servicios necesarios para que el usuario pueda iniciar cualquiera de sus casos de uso.
Resumen	Los servicios que el Administrador puede finalizar son: • Herramienta Software para las distintas clases de CSCF: I-CSCF, S-CSCF y P-CSCF. • Herramienta Software para el repositorio HSS. • Servicio SIP B2B correspondiente a la i23GW.

Tabla 13. Caso de Uso Finalizar Servicios

Una descripción más detallada de las funciones internas de cada uno de estos casos de uso se encuentra en el Anexo C, representadas por un diagrama de las clases que componen el sistema, además de las herramientas utilizadas para su creación y puesta en marcha.

4.4.2 Diseño de los Componentes Principales del Sistema i23GW

A continuación se describe el diseño interno y, de manera general, las herramientas involucradas dentro del módulo i23GW, lo cual hace parte de la formulación General de la Arquitectura del Sistema (ver Figura 21). Este módulo se constituye como el centro principal de estudio del actual proyecto, ya que representa el cumplimiento del objetivo principal del mismo: “Diseñar una Pasarela para que terminales IP basados en el protocolo de señalización SIP especificado por la IETF, puedan acceder a servicios proporcionados por una red IMS”.

Para lograr dicho acceso, se ha optado por el diseño y desarrollo de un sistema Software constituido por cuatro elementos principales: SIP-Connection, SIP-Inbound, SIP-Outbound y SIP-Processor. Estos cuatro elementos actúan en conjunto para lograr que los mensajes SIP provenientes de un cliente SIP-IETF o de una Red IMS, puedan ser entendidos, adaptados y reenviados hacia su destino.

La totalidad de los módulos internos de i23GW han sido desarrollados mediante la utilización de herramientas de programación de libre distribución, y utilizando el lenguaje Java, específicamente la implementación en este lenguaje para SIP, JAIN SIP [41]. JAIN SIP es una Interface de Programación de Aplicación (Application Programming Interface - API) de Java que hace parte de la iniciativa Java API para las Redes Integradas (Java API for Integrated Networks - JAIN) la cual se constituye como un grupo de trabajo dentro del JCP

(Java Community Process) para el manejo de estándares de telecomunicaciones. JAIN SIP contiene la mayor parte de las cabeceras y extensiones de SIP definidas en las distintas especificaciones del protocolo (RFC 3261, TS.24228, etc.), representadas por un conjunto de clases Java. De esta manera, la API puede ser utilizada especialmente para aplicaciones del lado del cliente, o dado el caso, aplicaciones B2B entre cliente y servidor. Existen otras tecnologías, tales como SIP Servlet API [42], destinadas preferiblemente al desarrollo de aplicaciones en el lado del servidor, y que no resultarían adecuadas para el desarrollo de i23GW, ya que esta pasarela se podría considerar como una aplicación B2B ubicada arquitecturalmente entre los clientes SIP-IETF y la red IMS. Además, el API de SIP Servlet brinda un nivel de abstracción mayor sobre el protocolo SIP que limitaría la manipulación necesaria de los mensajes SIP.

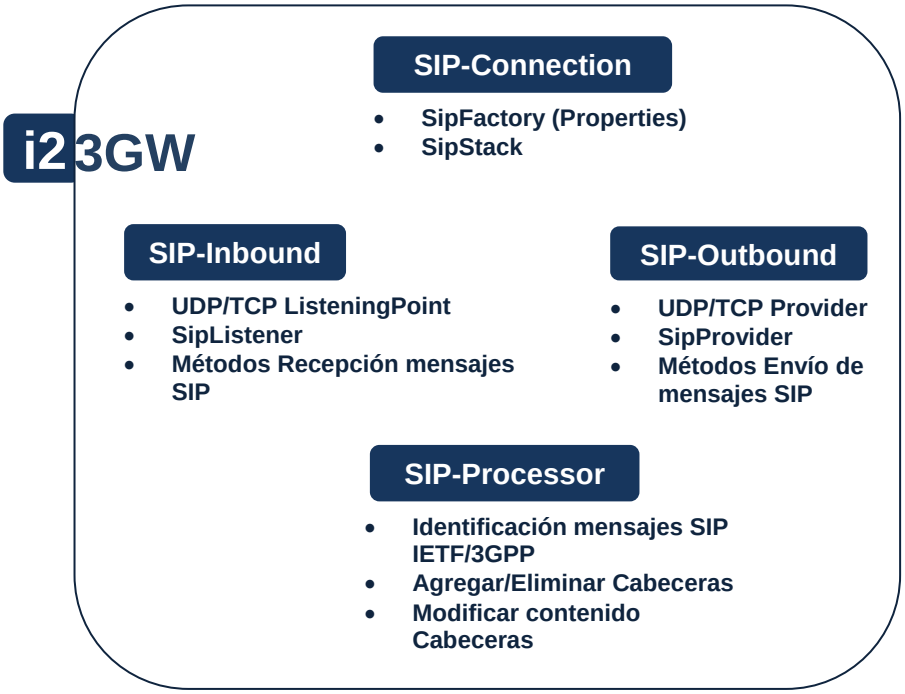


Figura 23. Módulos Internos de i23GW

A continuación se describen los módulos internos de la pasarela de señalización i23GW, las herramientas utilizadas para su desarrollo, y las funciones principales que realizan (Ver figura 23).

Para la descripción interna de los módulos, es necesario entender ciertos conceptos relacionados con la API JAIN SIP, tales como SipStack, SipFactory, ListeningPoint, SipProvider, entre otros. La descripción de estos elementos se encuentra de manera detallada en [41].

4.4.2.1 Módulo Interno SIP-Connection

SIP-Connection es el módulo encargado de generar una conexión SIP inicialmente con la red IMS, de manera específica, con la P-CSCF que actúa como proxy de entrada a la red. Además, SIP-Connection tiene que crear un vínculo con los clientes SIP-IETF que desean establecer un diálogo, lo cual se debe hacer de manera múltiple y asíncrona.

Para lograr estos objetivos, SIP-Connection ejecuta las siguientes labores:

- Realizar una implementación de la clase SipFactory, perteneciente a JAIN SIP, para la gestión de componentes relacionados con SIP.

- SipFactory posee métodos para la creación de un SipStack. Antes de crearlo, se deben fijar diferentes propiedades, iniciando por aquellas que darían un perfil a la i23GW para que pueda conocer la dirección de la P-CSCF. Además, se deben fijar las propiedades del servidor local, por ejemplo su nombre y dirección IP.

- El SipStack contiene métodos para la creación de ListeningPoint y SipProvider, los cuales son la base para el trabajo en los módulos SIP-Inbound y SIP-Outbound respectivamente.

4.4.2.2 Módulo Interno SIP-Inbound

Este módulo es el encargado de capturar y almacenar los mensajes provenientes tanto de los clientes SIP-IETF, como de la red IMS. Para que se pueda realizar la captura y almacenamiento de dichos mensajes se deben cumplir de las siguientes tareas:

- Mediante el uso de los métodos de la clase SipStack, crear uno o varios Listening Point, para los cuales se debe especificar el Puerto de escucha y el protocolo por utilizar (ya sea TCP o UDP). Cabe aclarar que se pueden crear Listening Point que difieran entre sí en los valores de puerto y protocolo utilizados. Esto es necesario para escuchar los mensajes que hacen referencia al puerto destino de la P-CSCF (generalmente definido en el puerto 4060), y a su vez, poder escuchar los mensajes que tienen como puerto destino el 6060, utilizado generalmente por la S-CSCF.

- Posterior a ello, se crean los SipListener, utilizando el SipProvider al cual van a estar asociados. Los SipListener también deben ser creados según el protocolo (TCP o UDP) por utilizar.

- Los mensajes SIP entrantes generan en la pasarela un evento, ya sea de tipo RequestEvent o ResponseEvent, lo cual llama automáticamente a los métodos principales del módulo Sip-Processor, que son: processRequest(RequestEvent) y processResponse(ResponseRequest), respectivamente.

- Los mensajes SIP son almacenados en un buffer, de tal forma que puedan se utilizados posteriormente para su análisis y modificación.

4.4.2.3 Módulo Interno SIP-Outbound

Este módulo contiene las herramientas necesarias para enviar los mensajes SIP modificados hacia su destino. Se encarga de recibir los mensajes provenientes del SIP-Processor, identificar el destino de dichos mensajes, y enviarlos. Esto lo realiza de la siguiente manera:

- La instanciación de la clase SipStack contiene métodos para la creación de los SipProvider necesarios, ya sea para el protocolo TCP o UDP. A estos métodos de creación se les pasa el objeto ListeningPoint previamente instanciado.

- Posterior a la creación de los SipProvider, cada vez que se desea enviar un mensaje SIP fuera de i23GW, se debe llamar al método getNewTransaction(); al cual se le pasa el Request o Response SIP que el módulo SIP-Processor ha creado.

4.4.2.4 Módulo Interno SIP-Processor

SipProcessor contiene la lógica de programación necesaria para identificar y modificar los mensajes SIP entrantes a la pasarela, con el objetivo principal de lograr una correcta interacción entre las entidades involucradas en una comunicación SIP.

La base de este módulo está en los métodos ProcessRequest y ProcessResponse, los cuales están destinados inicialmente a la identificación del tipo de mensaje que ha entrado a la pasarela, ya sea proveniente de la red IMS o de los distintos clientes SIP-IETF. Posteriormente, debe modificar los mensajes, utilizando los distintos métodos Send implementados para i23GW (SendRegister, Send401, Send200, SendInviteIetf, SendInviteIms, etc). Estas labores de identificación y modificación de los mensajes SIP se realizan de la siguiente manera:

- Se debe identificar a qué *método SIP* corresponde el mensaje entrante (REGISTER, INVITE, 200Ok, 401 Unauthorized, etc) y empezar un procesamiento diferenciado para dicho método SIP.

- El procesamiento diferenciado corresponde a un método asignado a la modificación, eliminación y adición de las cabeceras necesarias para adaptar el mensaje SIP. Estos métodos se han denominado según el *método SIP* al que corresponden, por ejemplo, SendInvite, SendRegister, Send200, etc.

- La labor principal de los métodos *Send* es agregar las extensiones adicionales a la estructura del protocolo SIP-IETF provenientes del cliente. Esto lo realiza mediante el reconocimiento de las cabeceras básicas del mensaje entrante, rescatando la información útil en ellas para rellenar el valor de las cabeceras adicionales. Por ejemplo,la cabecera privada P-Preferred-Identity, enviada en un mensaje REGISTER hacia la P-CSCF, podría contener como valor principal el mismo valor de la cabecera básica From.

5. VALIDACIÓN Y PRUEBAS DEL PROTOTIPO DESARROLLADO

5.1 Pruebas de Validación del Sistema

El Objetivo Principal del proyecto hace referencia a las capacidades ofrecidas por una red IMS, y de especial manera, al acceso que tendrían los clientes basados en la especificación IETF del protocolo SIP a dichas cabeceras. Es entonces este objetivo el punto de partida para la definición de las pruebas de validación que se realizan sobre el sistema. Esto, teniendo en cuenta que en términos prácticos, una validación positiva del sistema dependería estrictamente de determinar qué capacidades ofrecidas por IMS pueden ser accedidas desde un cliente SIP-IETF y de la misma manera, se debería determinar si algunos los clientes SIP más representativos, pertenecientes al amplio número de aquellos basados en la especificación realizada en el RFC 3261, podrían acceder a dichas capacidades.

La determinación de cuáles capacidades IMS han podido ser accedidas por un cliente SIP-IETF al utilizar i23GW, está relacionada con las lista de cabeceras adicionales del 3GPP que la pasarela permite manipular y agregar a los mensajes SIP provenientes de un cliente SIP-IETF. También tiene relación con las cabeceras adicionales provenientes de la red que i23GW logra interpretar, y a su vez utilizar para la activación de servicios o aplicaciones adicionales.

En la sección 3.2.1 se ha presentado una amplia descripción de los mensajes SIP que son adaptados por i23GW y entregados a su destino (Red IMS o cliente SIP-IETF). Además, se muestra una descripción de las cabeceras adicionales involucradas en una comunicación SIP entre el UE y la P-CSCF. La adición por parte de i23GW de estas cabeceras exclusivas para IMS, corresponde al cumplimiento del objetivo principal. Lo anterior, teniendo en cuenta que cada una de estas cabeceras, como se describió en el capítulo 3, representa la intervención del protocolo SIP en el aprovechamiento de las capacidades de IMS, tales como compresión de mensajes, seguridad, mejoras en AAAC, utilización de múltiples identidades públicas para un mismo usuario, etc.

5.1.1 Plan de Pruebas de Validación

La validación del sistema vista desde el lado de los clientes SIP-IETF que pueden o no acceder a las capacidades de IMS, se lleva a cabo mediante la realización de pruebas de interacción SIP entre los clientes y la red IMS. Estas pruebas se realizaron para un determinado número de dichos clientes, y mediante la utilización del sistema i23GW como pasarela de señalización SIP, y se llevaron a cabo mediante la realización de las siguientes labores de señalización SIP:

- Registro y des-registro de usuarios SIP-IETF en la red
- La subscripción de un Cliente SIP-IETF en la S-CSCF

- El establecimiento de una sesión entre un Cliente SIP-IETF y un Cliente IMS basado en la especificación SIP-3GPP.

El cumplimiento satisfactorio de estas tres labores brinda una respuesta positiva en el resultado de las pruebas de validación, y su descripción se muestra a continuación.

5.1.2 Validación para el Registro y Des-Registro de Clientes SIP-IETF en la red.

Inicialmente se ponen en marcha todos los elementos necesarios para la realización de las pruebas de validación. Ellos son: módulos software para P-CSCF, S-CSCF e I-CSCF, además del HSS (Simulado con una Base de datos utilizando MySQL); todos ellos pertenecientes al Core de IMS diseñado por Fokus Group [43]. También se debe poner en marcha la aplicación java para i23GW (Los detalles de la activación de todos estos elementos está descrito en el manual de usuario en el Anexo C).

Posterior a la inicialización de estos elementos, se procede a la activación del cliente SIP-IETF, de tal manera que automáticamente éste haga su primer intento de registro con la red, mediante el uso de i23GW. La prueba es satisfactoria si en el área de despliegue de mensajes del cliente aparece un mensaje señalando que éste ha sido registrado, como se muestra en la figura 24. En esta figura aparece un cliente X-lite [44] en su tercera versión, el cual está basado en el protocolo SIP-IETF. También se realizaron pruebas para la cuarta versión del mismo, y para un cliente móvil que funciona bajo la plataforma de Windows Mobile, denominado SJPhone. Estas pruebas adicionales se muestran también en la figura 24, donde se ilustra cómo en la pantalla del dispositivo móvil aparece un mensajes de registro satisfactorio.

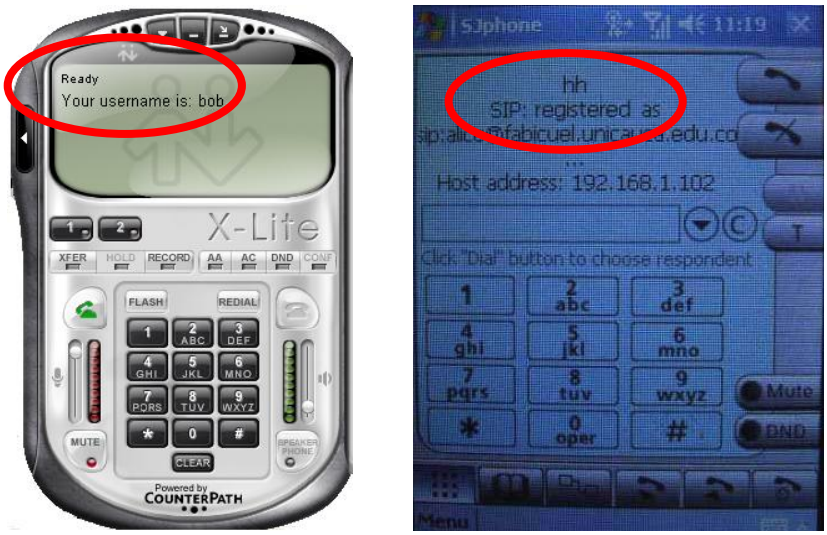


Figura 24. Validación del registro para los Clientes SIP-IETF

A su vez, en las consolas del CSCF y HSS aparece el usuario registrado, como se muestra en las figuras 25 y 26.

```
 5(9413) INF:P-CSCF:----------  Registrar Contents begin --------
 5(9413) INF:P-CSCF:[  88] C: <0://190.70.249.88:33882> Exp:[3578] R:[ 1] <sip:190.70.
249.88:33882>
 5(9413) INF:P-CSCF:          SR: <sip:orig@scscf.fabicuel.unicauca.edu.co:6060;lr>
 5(9413) INF:P-CSCF:           P: D[X] <sip:bob@fabicuel.unicauca.edu.co>
 5(9413) INF:P-CSCF:----------  Registrar Contents end ----------
 5(9413) INF:P-CSCF:----------  Subscription list begin ---------
 5(9413) INF:P-CSCF:[ 137]      P: <sip:bob@fabicuel.unicauca.edu.co> D:[ 3630] E:[ 36
08] Att:[-1]
 5(9413) INF:P-CSCF:----------  Subscription list end -----------
```

Figura 25. Validación del Registro de usuarios en la P-CSCF

```
The UserData XML document which is sent to the S-CSCF:
<?xml version="1.0" encoding="UTF-8"?><IMSSubscription><PrivateID>bob@fabicuel.unicauc
a.edu.co</PrivateID><ServiceProfile><PublicIdentity><Identity>sip:bob@fabicuel.unicauc
a.edu.co</Identity><Extension><IdentityType>0</IdentityType></Extension></PublicIdenti
ty><InitialFilterCriteria><Priority>0</Priority><TriggerPoint><ConditionTypeCNF>1</Con
ditionTypeCNF><SPT><ConditionNegated>0</ConditionNegated><Group>0</Group><Method>PUBLI
SH</Method><Extension></Extension></SPT><SPT><ConditionNegated>0</ConditionNegated><Gr
oup>0</Group><Method>SUBSCRIBE</Method><Extension></Extension></SPT><SPT><ConditionNeg
ated>0</ConditionNegated><Group>1</Group><SIPHeader><Header>Event</Header><Content>.*p
resence.*</Content></SIPHeader><Extension></Extension></SPT></TriggerPoint><Applicatio
nServer><ServerName>sip:10.200.2.157:5065</ServerName><DefaultHandling>0</DefaultHandl
ing></ApplicationServer></InitialFilterCriteria></ServiceProfile></IMSSubscription>
2009-01-20 17:56:52,375 INFO  de.fhg.fokus.hss.cx.op.SAR - processRequest
User with Public Identity: sip:bob@fabicuel.unicauca.edu.co and all its coresponding i
mplicit-set identities are Registered!
```

Figura 26. Validación del Registro de usuarios en el HSS

El des-registro del usuario se realiza mediante el cierre del cliente, momento en el cuál éste envía un mensaje de des-registro hacia i23GW, la cual se encarga de recurrir a la red para terminar con el registro de dicho usuario. De la misma manera como sucedió con el registro, las consolas de la CSCF y el HSS demuestran que el usuario ha sido satisfactoriamente des-registrado (ver figura 27). En la consola de la P-CSCF simplemente dejan de aparecer los usuarios des-registrados en el Registrar Content.

```
2009-01-20 18:20:17,035 DEBUG de.fhg.fokus.hss.main.Task - execute Processing UAR!
2009-01-20 18:20:17,056 DEBUG de.fhg.fokus.hss.main.Task - execute Processing SAR!
2009-01-20 18:20:17,090 INFO  de.fhg.fokus.hss.cx.op.SAR - processRequest User with Pu
blic Identity: sip:bob@fabicuel.unicauca.edu.co and all its coresponding implicit-set
identities are De-Registered!
```

Figura 27. Validación del Des-Registro de usuarios en el HSS

5.1.3 Validación para la Subscripción de un Cliente SIP-IETF en la S-CSCF

El sistema del OpenIMS Core realiza la subscripción de manera automática en el momento en que el usuario ha sido satisfactoriamente registrado en la red. Esto sucede gracias a que una de las intenciones principales de IMS es sobrecargar (Overload) los mensajes SIP transmitidos en la red y a su vez evitar la necesidad de enviar muchos mensajes (Overhead) para realizar el mismo número de labores. Lo anterior, teniendo en cuenta que IMS está diseñado para un ambiente especialmente móvil, donde la interfaz de radio implicaría el uso de poco flujo de señalización para cumplir labores cada vez más complejas.

Sin embargo, para el desarrollo de i23GW se ha tenido en cuenta que los clientes SIP-IETF en su mayoría no han sido diseñados para este tipo de subscripciones automáticas. Esto quiere decir que los clientes SIP-IETF, envían un mensaje de solicitud de subscripción hacia i23GW de manera indiferente a que ya hayan sido subscritos automáticamente en la red, y además, quedan esperando una respuesta a dicho mensaje de subscripción. Además, uno de los objetivos de i23GW es ser lo suficientemente portable para poder ser utilizado con otros sistemas distintos al OpenIMS Core, los cuales no necesariamente tengan implementado un método de subscripción automática. Es por ello que en i23GW se han tenido en cuenta las consideraciones para la adaptación de los mensajes SIP de subscripción. La subscripción de los usuarios arroja el resultado mostrado en la figura 28 dentro de la consola de la S-CSCF.

```
5(9434) INF:S-CSCF:[ 137] P: <sip:bob@fabicuel.unicauca.edu.co> R[ 1] Early-IMS: <>
5(9434) INF:S-CSCF:         CCF1: <pri_ccf_address> CCF2: <>
5(9434) INF:S-CSCF:         C: <sip:190.70.249.88:33882> Exp:[3582]
5(9434) INF:S-CSCF:           Path:<sip:term@pcscf.fabicuel.unicauca.edu.co:4060;lr>
5(9434) INF:S-CSCF:           UA: <X-Lite release 11001 stamp 47546>
5(9434) INF:S-CSCF:         S: Event[0] Exp:[3621] <sip:pcscf.fabicuel.unicauca.edu.c
o:4060>
```

Figura 28. Validación de la Subscripción de usuarios en la S-CSCF

En lo que respecta a los Clientes SIP-IETF que han sido subscritos en la red, i23GW les envía un mensaje de aceptación a la subscripción, lo cual se muestra en la figura 29

```
192.168.1.100      192.168.1.101      SIP      Request: SUBSCRIBE sip:bob@fabicuel.unicauca.edu.co
192.168.1.101      192.168.1.100      SIP      Status: 200 OK

⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 200 OK
  ⊟ Message Header
    ⊞ Via: SIP/2.0/UDP 192.168.1.100:2390;received=192.168.1.100;branch=z9hG4bK-d8754z-d77e8667af64170d-1-
    ⊞ To: "bob" <sip:bob@fabicuel.unicauca.edu.co>;tag=dcfc34a8
    ⊞ From: "bob" <sip:bob@fabicuel.unicauca.edu.co>;tag=22139546
      Call-ID: MDdjZDMzNzJmY2Q5NDU1MzU2YjgONzg2NzAxYWM4MDc.
    ⊞ CSeq: 1 SUBSCRIBE
      Expires: 300
      Content-Length: 0
```

Figura 29. Validación de la aceptación de Subscripción de usuarios hacia el cliente SIP-IETF

5.1.4 Validación para el Establecimiento de sesión entre un Cliente SIP-IETF y un Cliente SIP-3GPP

Tras un previo registro de los clientes SIP-IETF y SIP-3GPP en la red, se puede iniciar una conversación multimedia entre estas dos entidades. La validación del acceso para los Clientes SIP-IETF a capacidades IMS en dicha conversación multimedia, radica en la realización de pruebas sobre el establecimiento de una sesión SIP, iniciada por cualquiera de las dos entidades. El establecimiento de la sesión inicia con la petición realizada por cualquiera de las partes. Esta petición es procesada inicialmente por la red y luego pasada a i23GW, en el caso de clientes SIP-3GPP, o directamente por i23GW y luego enviada a la red, para los clientes SIP-IETF. Posterior a ello, la invitación llega a su destino, y si hay aceptación por parte de la entidad llamada, se establece la sesión.

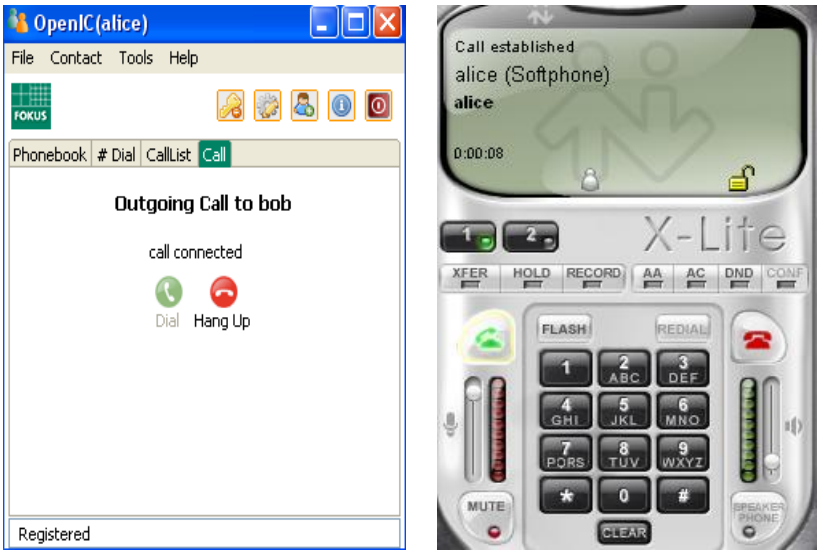


Figura 30. Validación del Establecimiento de sesión vista desde los Clientes SIP-3GPP y SIP-IETF

Una sesión satisfactoriamente establecida se logra confirmar en los distintos clientes involucrados, y en el tráfico de RTP que se produce de manera directa entre dichos clientes. La confirmación del establecimiento de la sesión se puede ver en la figura 30. Los clientes utilizados han sido: X-Lite v3 para representar al Cliente SIP-IETF, y OpenIC Lite [38], desarrollado por el Fokus Group, en calidad de cliente SIP-3GPP.

El tráfico RTP que se produce entre ambas partes se describe en la figura 31.

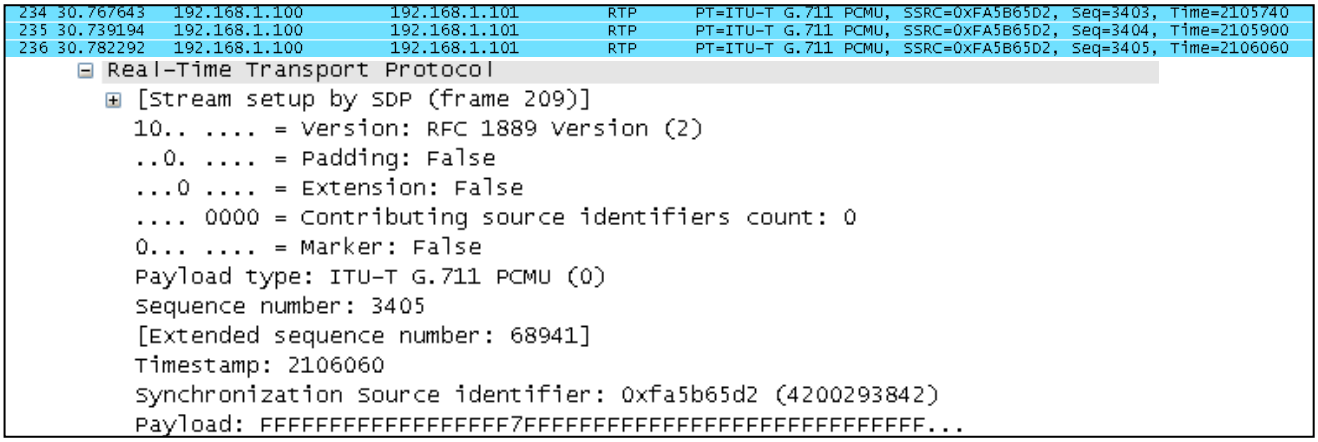


Figura 31. Validación de establecimiento de la sesión, basada en el tráfico RTP

De esta manera, el Sistema queda validado tanto por la determinación de que los clientes SIP-IETF sí pueden tener acceso a las capacidades IMS, como por la definición de las capacidades IMS en cuestión y su relación con las distintas cabeceras adicionales. Todo lo anterior, gracias a que se ha utilizado la pasarela i23GW para la adaptación de los diferentes mensajes SIP involucrados en las labores de señalización anteriormente mencionadas.

5.2 Pruebas de Desempeño

Las Pruebas de Desempeño del sistema han sido efectuadas en el computador donde está instalada la pasarela i23GW. Estas pruebas dan una razón del uso de memoria RAM (Random Access Memory) y CPU (Central Process Unit) en este equipo, ya sea para el uso básico de la pasarela en el registro de usuarios, como para el uso de la misma en el establecimiento de una sesión.

5.2.1 Prueba de desempeño con i23GW en funcionamiento

Inicialmente se midió el desempeño del equipo donde i23GW está funcionando, sin ninguna labor de señalización realizándose hasta el momento. El resultado arrojado se ve en la figura 32. Se percibe cómo el consumo de memoria es mínimo con relación al momento en que la pasarela estaba cerrada, es decir, 608 MB consumidos durante el funcionamiento de i23GW Vs 604 MB antes de iniciar la pasarela. Esto da un consumo de memoria RAM de solo 4 MB para i23GW.

El consumo de CPU no sufre muchas variaciones en su porcentaje al iniciar i23GW, se puede ver en la figura 32 que los picos de consumo en el historial de la CPU no son demasiado elevados.

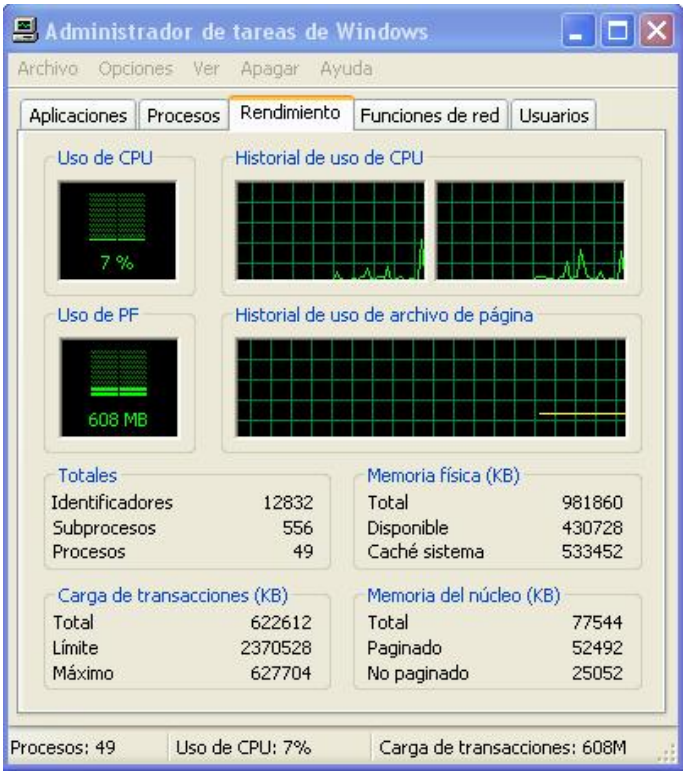


Figura 32. Prueba de desempeño con i23GW en funcionamiento

5.2.2 Prueba de desempeño para el registro de usuarios

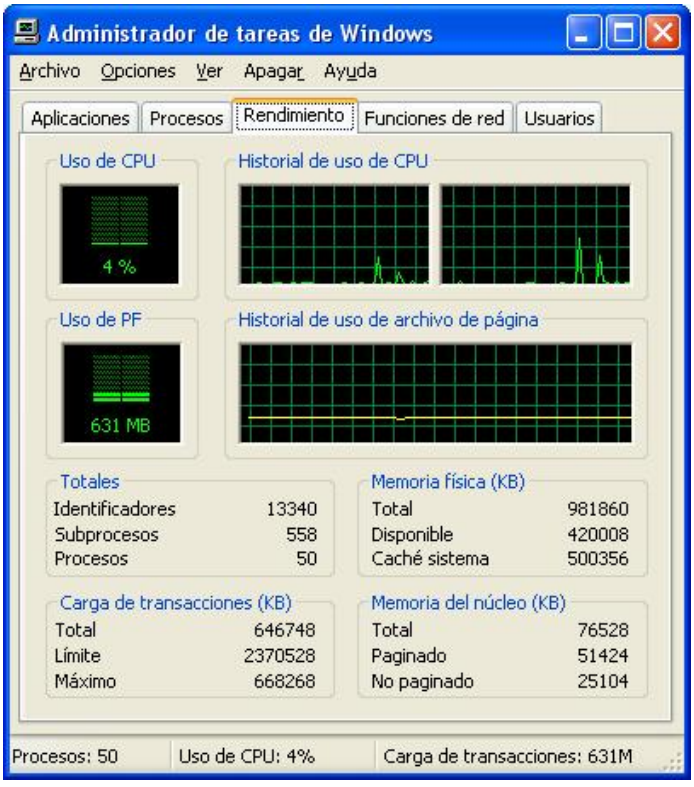


Figura 33. Prueba de desempeño durante el registro de usuarios

Durante el registro de un usuario que utiliza un cliente SIP-IETF X-Lite, se puede notar un incremento considerable en la memoria RAM consumida por la máquina donde reside i23GW (ver figura 33). Es un incremento de alrededor de 20MB, lo cual indica que el número de mensajes SIP (REGISTER, 200OK, 401Unauthorized, etc) utilizados en el registro del usuario tienen un contenido de tamaño relativamente alto. Además, los picos en el historial de consumo de CPU tienen una mayor prolongación que aquello ocurridos cuando la pasarela estaba en funcionamiento básico.

5.2.3 Prueba de Desempeño para el establecimiento de una sesión entre un Cliente SIP-IETF y otro SIP-3GPP

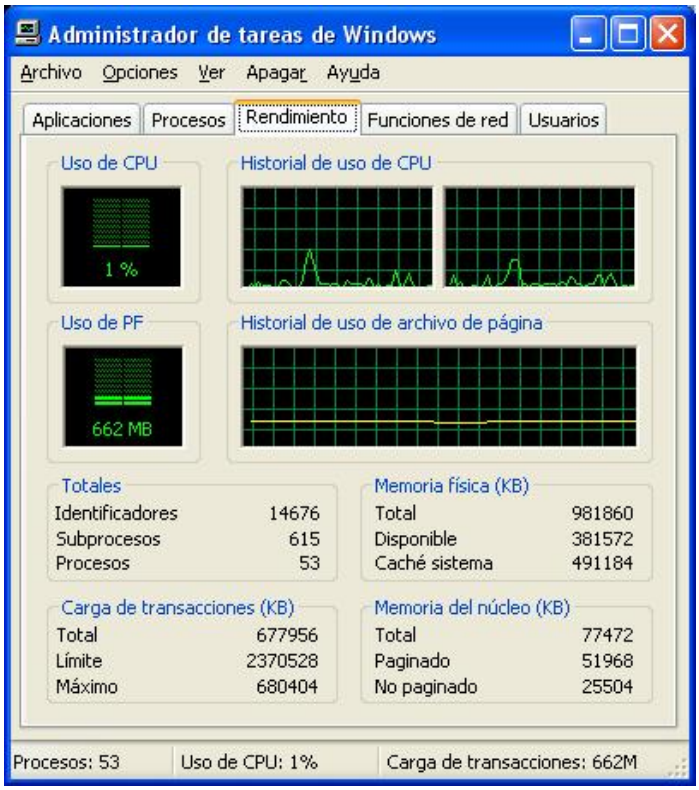


Figura 34. Prueba de desemeño durante el establecimiento de una sesión

Para la realización de esta prueba, se estableció una sesión SIP entre un cliente OpenIC Lite ubicado en el mismo equipo de la pasarela, y un cliente X-Lite remoto. De esta forma, se debe restar al consumo de memoria RAM considerado, aquel realizado por el cliente OpenIC Lite, que está alrededor de los 3 MB. Aun así, es evidente en la figura 34, que el incremento en consumo de memoria RAM es bastante alto para el establecimiento de una sesión, con relación al funcionamiento básico de la pasarela, y también con relación al funcionamiento de la máquina durante el registro de usuarios. Esto se debe a que el flujo de mensajes es mayor para el establecimiento, y a que el contenido de los mensajes también se incrementa por causa del uso de protocolo SDP dentro de su contenido. También es notable que ahora aparecen más frecuentes los picos prolongados en el consumo de CPU, debido a que existe un mayor número de mensajes SIP produciendo eventos de entrada y salida en el equipo donde reside i23GW.

5.3 Pruebas de Uso y Funcionalidad de i23GW

La usabilidad del sistema está relacionada con la experiencia que hayan obtenido tanto los usuario finales que utilizan un Cliente SIP-IETF, como los usuarios finales SIP-3GPP que por medio de i23GW han establecido una sesión con un cliente SIP-IETF. De esta manera, las pruebas de usabilidad corresponden a una encuesta realizada a tres distintos usuarios, los cuales han probado el sistema mediante el uso de un Cliente SIP-IETF (X-Lite), y de manera alternada, un cliente SIP-3GPP (OpenIC Lite).

En la tabla 14 se muestran los resultados de las pruebas de funcionalidad de i23GW:

Usuarios	¿Puede conectarse con la red mediante i23GW de manera rápida y sin problemas?	¿La configuración del cliente SIP para su funcionamiento con i23GW es intuitiva y fácil?	¿Tuvo algún problema con el registro o el establecimiento de sesiones SIP?
Usuario 1	Sí	Sí	El usuario se queda esperando a ser subscrito en la red.
Usuario 2	Sí	Sí	No
Usuario 3	Sí	No, hay problema para registrar el usuario cuando en el Nombre Autorizado del cliente no se especifica el dominio de i23GW	En ocasiones el tráfico RTP en una conversación es unilateral, debido a conflictos con el DNS del usuario remoto.

Tabla 14. Pruebas de Uso y Funcionalidad

Las pruebas de Uso y funcionalidad del sistema arrojaron resultados positivos, teniendo en cuenta que se logró el objetivo principal en el desarrollo de la pasarela i23GW, permitiendo el acceso transparente desde clientes SIP-IETF a capacidades de IMS. La transparencia en este acceso a las capacidades de IMS se valoró considerando los posibles traumatismos que podrían surgir en el tiempo de espera necesario para el establecimiento de las sesiones, y en la forma fácil e intuitiva de configurar a los clientes SIP-IETF, de tal forma que éstos pudieran reconocer a i23GW. Todas estas valoraciones dieron resultados positivos, teniendo pequeñas variaciones negativas en la experiencia de los usuarios. Estas variaciones se vieron reflejadas principalmente en conflictos propios del comportamiento regular de un cliente SIP-IEFT, y algunos otros, del entorno de DNS utilizado. Estas variantes negativas no tienen una relación directa con el centro de estudio del proyecto, pero han sido consideradas y corregidas de manera previa a una versión final del prototipo.

5.4 Pruebas de Ancho de Banda requerido

El ancho de banda consumido por el sistema i23GW, está relacionado con el tráfico de mensajes SIP entrantes y salientes de la pasarela. Por lo tanto, las pruebas para determinar el ancho de banda requerido por i23GW se hacen en relación a la tasa de bytes consumida por los mensajes SIP en una unidad de tiempo, según el tráfico de señalización que entra y sale de i23GW.

En la figura 35 se muestra una relación entre los bytes transmitidos y el tiempo transcurrido, pertenecientes al tráfico de mensajes SIP, y al flujo RTP entre las partes involucradas en el registro y posterior establecimiento de una sesión.

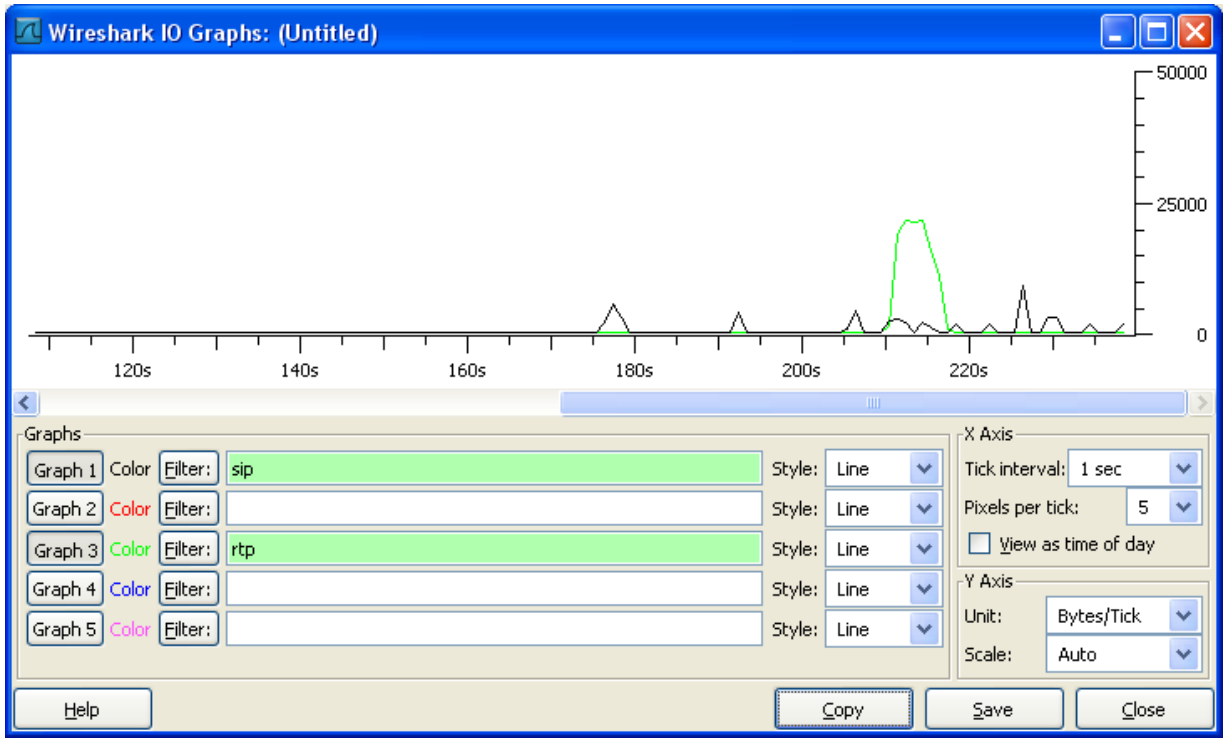


Figura 35. Prueba de Ancho de Banda Requerido

Como se muestra en la figura 35 el tráfico RTP solamente aparece después de iniciada la sesión. Este tráfico RTP es de aproximadamente 25Kbps, lo cual está dentro de un margen normal de requerimiento de ancho de banda, con relación a las tradicionales comunicaciones multimedia que utilizan este protocolo. El tráfico RTP no interfiere en el comportamiento de i23GW, debido a que este protocolo es utilizado únicamente entre las dos terminales comunicadas, y no requiere de una entidad intermedia.

En cuanto a lo que se refiere al protocolo SIP, todo el tráfico proveniente de los clientes SIP-IETF o desde la red IMS debe pasar por i23GW, lo que supondría que en el equipo donde está instalada la pasarela recaería la mayor responsabilidad en cuanto a consideraciones de Ancho de Banda. A pesar de esta alta responsabilidad, es claro en la figura 35, que el mayor flujo de bytes correspondientes a los mensajes SIP se ubica alrededor del punto 225 en el eje X (después de 225 segundos de prueba), donde el tráfico alcanza aproximadamente los 10Kbps, lo cual no representa un enorme ancho de banda requerido para el servidor donde

se aloja la aplicación de i23GW. De esta manera, y si se considera un número mayor de clientes simultáneos (Aproximadamente 1000 usuarios) registrándose y estableciendo sesiones en la red, se deduce de estos resultados que el ancho de banda requerido no sobrepasa los 10Mbps, lo cual es relativamente bajo, teniendo en cuenta que una adaptación del prototipo a un entorno comercial, contaría con equipos y conexiones mucho mejores que las utilizadas en las pruebas.

De esta manera se concluye el trabajo de validación y pruebas para el prototipo, y por consiguiente el proyecto presentado en este documento. Logrando una satisfactoria relación entre los beneficios proporcionados por una red IMS, y los clientes basados en la especificación de la IETF para SIP.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Las diferencias entre la especificación de la IETF para SIP, y el perfil de este protocolo definido por el 3GPP para IMS, son de gran importancia dentro de las intensiones del 3GPP por lograr convergencia entre IMS y las tecnologías tradicionales. Estas diferencias han sido identificadas y listadas en el presente proyecto, abarcando todas aquellas relacionadas con la estructura del protocolo y con el flujo de mensajes SIP. Este listado de diferencias se constituye como la base para el diseño y desarrollo de i23GW.

- La arquitectura modular de IMS permite que entidades externas a una red de este tipo, puedan acceder a servicios y aplicaciones convergentes. Esto, siempre y cuando exista de por medio una herramienta de adaptación para los protocolos de señalización involucrados. Con la realización de i23GW se puede concluir que existe una fácil integración de las herramientas de adaptación con la arquitectura IMS, gracias a su esquema modular.

- Es posible el desarrollo de una pasarela de señalización que adapte los mensajes provenientes de un cliente SIP-IETF, permitiendo que dicho cliente pueda acceder a servicios de Registro, Subscripción y Establecimiento de Sesiones, proporcionados por una red IMS.

- Las tareas para realizar una completa migración hacia IMS resultan demasiado complejas dentro de un entorno latinoamericano [45]. La alternativa de adaptación de las tecnologías tradicionales hacia IMS, mediante el desarrollo de herramientas Software, puede representar la más viable solución para el acceso a servicios convergentes en dicho entorno, al menos, durante una etapa inicial.

- La mayoría de las soluciones actuales relacionadas y comparables con i23GW, han sido desarrolladas de manera propietaria. Por lo tanto, son orientadas únicamente al manejo de la señalización SIP dentro un entorno propio del ente desarrollador, ya sea para el acceso a un servidor de aplicaciones en particular, o para permitir que tan solo un selecto grupo de clientes SIP puedan acceder a una red IMS. En contraste a ello, i23GW se puede considerar como una alternativa universal, capaz de permitir que prácticamente cualquier cliente basado en SIP-IETF pueda acceder a las capacidades de cualquier red sujeta a la arquitectura de IMS. Esto, gracias a que implementa una lista de las cabeceras adicionales del 3GPP, las cuales corresponden una a una con las capacidades de IMS.

- Una de las características principales del protocolo SIP es su extensibilidad. Pero esta característica puede ser vista como un problema a la hora de lograr un estándar en la estructura del protocolo. Gracias a la realización del presente proyecto, se concluye que la implementación de Pasarelas de Señalización es una solución muy

adecuada para lograr la adaptación de las múltiples definiciones y perfiles que han venido surgiendo para SIP, y lograr así, la estandarización final del protocolo.

RECOMENDACIONES

- El producto del presente proyecto permite pensar en el desarrollo de aplicaciones SIP que se integren con i23GW. Una de estas aplicaciones podría ser un sistema completo de tarificación, el cual aproveche los beneficios obtenidos con el manejo de las identidades múltiples de usuario, que son característica elemental de IMS, y que ahora pueden ser aplicadas a clientes SIP-IETF.

- Los clientes SIP basados en la definición de la IETF no cuentan con ninguna herramienta para enviar información sobre el tipo de red de acceso que están utilizando. Hace falta la implementación de un sistema de registro, que se integre con i23GW y que permita reconocer, según el contenido de las cabeceras de los mensajes SIP-IETF y los datos de usuario registrados, cuál es el tipo de red de acceso utilizado por dicho cliente. Esto permitiría pensar en el desarrollo de aplicaciones útiles en la diferenciación de servicios y aprovechamiento del ancho de banda para los clientes SIP-IETF.

- Aunque IMS contiene algunas funciones destinadas a las redes fijas, es claro que la principal iniciativa de esta arquitectura ha sido la prestación de servicios convergentes en redes móviles. Por lo tanto, el aprovechamiento de las características y de la información manejada por estas redes en IMS sería de gran utilidad para la prestación de servicios de roaming y localización de usuarios. La definición IETF de SIP ha sido diseñada principalmente para su funcionamiento en la Internet, no precisamente con funciones orientadas a las redes móviles. Entonces, la creación de i23GW es un precedente para el desarrollo de una completa adaptación hacia un entorno móvil para este tipo de clientes.

- Es claro que dos de los principales objetivos en la definición de IMS ha sido la Calidad de Servicio, y la seguridad en la red. Se podría proponer como trabajo futuro el desarrollo de un completo esquema de Calidad de Servicio y seguridad para los puntos de red existentes entre i23GW y los equipos de usuario.

- I23GW no constituye una herramienta introducida dentro de un entorno comercial, simplemente brindan una base para pensar en el desarrollo de futuras y mejores herramientas de adaptación que se integren de manera completa con el mundo real de las telecomunicaciones. Para ello, es preciso la consideración de muchos más parámetros de adaptación y comunicación, más relacionados con la red de acceso que con la estructura misma del protocolo. La implementación de estos parámetros podría ser propuesta como un trabajo futuro al desarrollo de i23GW.

BIBLIOGRAFÍA

[1] (RFC) J. Rosenberg et al.(2002); *"SIP: Session Initiation Protocol"*, IETF RFC 3261. Disponible en: http://www.ietf.org/rfc/rfc3261.txt (Visitada en diciembre de 2006)

[2] (RFC) R. Fielding, J. Gettys, J.Mogul, H. Frystyk, L. Masinter, P. Leach (1999); "*Hipertext Transfer Protocol*", IETF RFC 2616; Disponible en: http://www.ietf.org/rfc/rfc2616.txt (Visitada en junio de 2008).

[3] (RFC) J. Postel (1982); "*Simple Mail Transfer Protoco*", IETF RFC 821; Disponible en: http://www.ietf.org/rfc/rfc0821.txt (Visitada en junio de 2008).

[4] (RFC) A. Vemuri, J.Peterson (2002); "*Session Initiation Protocol for Telephones SIP-T Context and Architectures*", IETF RFC 3372; Disponible en: http://www.ietf.org/rfc/rfc3372.txt (Visitada en julio de 2008).

[5] (Documento Técnico) RADVISION (2006); *"IMS SIP and Signaling, The RADVISION perspective";* Disponible en: http://www.sipcenter.com/sip.nsf/html/Whitepapers (requiere registro) (Visitada en julio de 2007)

[6] (Documento Técnico) RADVISION; *"sip:overview radvision";* Disponible en: http://www.radvision.com/NR/rdonlyres/51855E82-BD7C-4D9D-AA8A-E822E3F4A81F/0/RADVISIONSIPProtocolOverview.pdf (Visitada en abril de 2007)

[7] (Artículo) 3G Americas (2006); *"IMS Application Enabler and UMTS/HSPA Growth Catalyst"* Disponible en: http://www.3gamericas.org/PDFs/white_papers/wp_IMS_UMTS-HSPA_Growth_Catalyst.pdf (Visitada en julio de 2007)

[8] (Documento Técnico) ETSI Mobile Competence Centre; *"Overview of 3gpp release 5*" ; Disponible en: http://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_20/Docs/PDF/RP-030375.pdf (Visitada en julio de 2007)

[9] G. Camarillo y M. García; "*The 3G IP Multimedia Subsystem (IMS)*". (Consultado en abril de 2008).

[10] (Documento Técnico) M. García (2002); "*3rd-Generation Partnership Project (3GPP) Release 5 Requirements on the Session Initiation Protocol (SIP)*"; Disponible en: http://tools.ietf.org/html/draft-ietf-sipping-3gpp-r5-requirements-00 (visitado en julio de 2008).

[11] (Página Web) Internationa Telecomunication Union; "*ENUM*"; Disponible en: http://www.itu.int/osg/spu/enum/ (Visitada en julio de 2008)

[12] (Artículo) F. Galán Márquez, M. Gómez, Ágora Systems, S. A.; T. Robles, T. de Miguel, Universidad de Madrid; L. Ángel, Telefónica Móviles de España, S. A. (2005); *"Interworking of IP multimedia Core Networks between 3GPP and WLAN";* Disponible en: http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/7742/31203/01452855.pdf (Acceso Restringido) (Visitada en abril de 2008)

[13] (RFC) R.Price, C. Bormann (2003); "*Signaling Compression (SigComp)*"; IETF RFC 3320; Disponible en: http://www.ietf.org/rfc/rfc3320.txt (Visitada en Julio de 2008).

[14] (RFC) M. García, E.Henrikson (2003); "*Private Headers (P-Headers) to de Session Initiation Protoco (SIP) for the 3rd Generation Partnership Project*"; IETF-3GPP RFC 3455; Disponible en: http://www.ietf.org/rfc/rfc3455.txt (Visitada en junio de 2008).

[15] (RFC) J. Arkko, V. Torvinen, G.Camarillo (2003); "*Security Mechanism Agreement for the Session Initiation Protocol (SIP)* "; IETF RFC 3329; Disponible en: http://www.ietf.org/rfc/rfc3329.txt (visitada en julio de 2008).

[16] (RFC) A.Niemi, J.Arkko, V.Torvinen (2002); "Hipertext Transfer Protocol (HTTP) Digest Authentication using Authentication and Key Agreement (AKA)"; IETF RFC 3310; Disponible en: http://www.ietf.org/rfc/rfc3310.txt (visitada en julio de 2008).

[17] (RFC) R. Atkinson, S. Kent (1998); "*Security Architecture for the Internet Protocol IP*"; IETF RFC 2401; Disponible en: http://www.ietf.org/rfc/rfc2401.txt (Visitada en julio de 2008).

[18] (RFC) J. Rosenberg (2004); "A Session Initiation Protocol (SIP) Event Package for Registrations"; IETF RFC 3680; Disponible en: http://www.ietf.org/rfc/rfc3680.txt (Visitada en julio de 2008).

[19] (RFC) M.Handley, V. Jacobson (1998); "*SDP: Session Description Protocol*"; IETF RFC 2327; Disponible en: http://www.ietf.org/rfc/rfc2327.txt (Visitada en julio de 2008).

[20] (RFC) W. Marshall (2003); "*Private Session Initiation Protocol (SIP) Extensions for Media Authorization*"; IETF RFC 3313; Disponible en: http://www.ietf.org/rfc/rfc3313.txt (Visitada en julio de 2008).

[21] (Documento Técnico) 3GPP (2005); "*3rd Generation Partnership Project; Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 5)"*; 3GPP TS 24.229; Disponible en: http://www.arib.or.jp/IMT-2000/V440Mar05/5_Appendix/Rel5/24/24229-5b1.pdf (visitada en mayo de 2008).

[22] (RFC) J. Rosenberg, H. Schulzrinne (2002); "*Reliability of Provisional Responses in the Session Initiation Protocol (SIP*)"; IETF RFC 3262; Disponible en: http://www.ietf.org/rfc/rfc3262.txt (Visitada en julio de 2008).

[23] (RFC) J. Peterson (2002); "A Privacy Mechanism for the Session Initiation Protocol (SIP)"; IETF RFC 3323; Disponible en: http://www.ietf.org/rfc/rfc3323.txt (Visitada en septiembre de 2008).

[24] (RFC) G. Camarillo, W. Marshall, J. Rosenberg (2002); "Integration of Resource Management and Session Initiation Protocol"; IETF RFC 3312; Disponible en: http://www.ietf.org/rfc/rfc3312.txt (Visitada en julio de 2008).

[25] (RFC) A.B. Roach (2002); "Session Initiation Protocol (SIP) Specific Event Notification"; IETF RFC 3265; Disponible en: http://www.ietf.org/rfc/rfc3265.txt (Visitada en julio de 2008).

[26] (RFC) D. Willis, B Honeisen (2002) "*Session Initiation Protocol (SIP) Extension Header Field for Registering Not-Adjacent Contacts*"; IETF RFC 3327; Disponible en: http://www.ietf.org/rfc/rfc3327.txt (Visitada en septiembre de 2008).

[27] (RFC) E. Guttman, C. Perkins (1999); "*Service Location Protocol*"; IETF RFC 2608; Disponible en: http://tools.ietf.org/html/rfc2608 (Visitada en septiembre de 2008).

[28] (RFC) B. Campbell, J.Rosenberg, H. Schulzrinne (2002); "*Sessioin Initiation Protocol (SIP) Extensions for Instant Messaging*"; IETF RFC 3428; Disponible en: http://www.ietf.org/rfc/rfc3428.txt (Visitada en septiembre de 2008).

[29] (Documento Técnico) 3GPP (2002); "*3rd Generation Partnership Project; Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3 (Release 5)*"; 3GPP TS 24.228 Disponible en: http://www.arib.or.jp/IMT-2000/V310Sep02/S3g/Rel5/24/24228-510.pdf (Visitada en octubre de 2008).

[30] (Documento Técnico) S. Znaty, J Dauphin, R. Geldwerth; "*IP Multimedia Subsystem: Principios y Arquitectura*"; Disponible en: http://www.efort.com/media_pdf/IMS_ESP.pdf (Visitada en agosto de 2008).

[31] (RFC) P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Akkon (2003); "*Diameter Base Protocol*"; IETF RFC 3588; Disponible en: http://tools.ietf.org/html/rfc3588 (Visitada en agosto de 2008).

[32] (RFC) C. Rigney, S. Willens, A. Rubens, W. Simpson (2000); "*Remote Authentication Dial in User Services (RADIUS*)"; IETF RFC 2865; Disponible en: http://www.ietf.org/rfc/rfc2865.txt (Visitada en agosto de 2008).

[33] (RFC) C. Grove, M. Pantaleo, T. Anderson, T. Taylor (2003); "*Gateway Control Protocol*"; IETF RFC 3525; Disponible en: http://tools.ietf.org/html/rfc3525 (Visitada en julio de 2008).

[34] (RFC) D. Durham, J. Boyle, R. Cohen, S. Herzog (2000); "*The COPS (Common Open Policy Service Protocol)*"; IETF RFC 2748; Disponible en: http://tools.ietf.org/html/rfc2748 (Visitada en julio de 2008).

[35] (Página Web) Tech-Invite; "*Tech-Invite: a Portal Devoted to SIP and Surrounding Technologies*"; Disponible en: www.tech-invite.com (Visitada en Junio de 2008).

[36] (Pagina Web) 3GPP; "*3GPP Release 7*"; Disponible en: http://www.3gpp.org/article/release-7 (Visitada en Septiembre de 2008).

[37] (RFC) C. Jennings, J. Peterson, M. Watson (2002); *"Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks"*; IETF RFC 3325; Disponible en: http://www.ietf.org/rfc/rfc3325.txt (Visitada en Agosto de 2008).

[38] (RFC) J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart (1999); "*HTTP Authentication: Basic and Digest Acces Authentication*"; IETF RFC 2617; Disponible en: http://tools.ietf.org/html/rfc2617 (Visitada en septiembre de 2008).

[39] (Página Web) Fokus Group; "*Open IC – The Fokus Open IMS Client*"; Disponible en: http://www.fokus.fraunhofer.de/en/fokus_testbeds/open_ims_playground/components/openic/index.html (Visitada en julio de 2008).

[40] (Artículo) C. Serrano, Universidad del Cauca (2005); "*Modelo de Construcción de Soluciones*"; Disponible en: http://atenea.unicauca.edu.co/~msolarte/enfasis2.htm (Visitada en julio de 2008).

[41] (Página Web) Community Development of Java Technologies Communication; "*JSR-000032 JAIN SIP Specification*"; Disponible en: http://jcp.org/aboutJava/communityprocess/final/jsr032/ (Visitada en julio de 2008).

[42] (Página Web) Community Development of Java Technologies Communication; "*JSR-000116 SIP Servlet API*"; Disponible en: http://jcp.org/aboutJava/communityprocess/final/jsr116/ (Visitada en julio de 2008).

[43] (Página Web) Fokus Group; "*Open Source IMS Core Page*"; Disponible en: http://www.openimscore.org/ (Visitada en Julio de 2008).

[44] (Página Web) CounterPath; "*Products – X-lite*"; Disponible en: http://www.counterpath.net/X-Lite-Download.html (Visitada en Julio de 2008).

[45] (Artículo) AHCIET, Telefónica I+D (2005); "*Las Telecomunicaciones y la Movilidad en la Sociedad de la Información*"; Disponible en: http://www.telefonica.es/sociedaddelainformacion/pdf/publicaciones/movilidad/telecoymovilidad.pdf (Visitada en octubre de 2008).