

**ACCESO A CAPACIDADES IMS DESDE CLIENTES SIP-
IETF**

FABIÁN REINALDO CUÉLLAR CALDERÓN

ANEXOS

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELEMÁTICA
POPAYÁN, FEBRERO DE 2009**



TABLA DE CONTENIDO

A.	SESSION INITIATION PROTOCOL - SIP	4
A.1.	Conceptos Generales de SIP	4
A.1.1	Direcciones SIP	6
A.2.	Arquitectura SIP	6
A.2.1	Agentes de Usuario	6
A.2.2	Servidores SIP	7
A.2.2.1	Servidor Proxy	7
A.2.2.2	Servidor de Redirección	8
A.2.2.3	Servidor de Registro	8
A.2.2.4	Agente de Llamada (Call Agent)	9
A.3.	Arquitectura de Servicios SIP	9
A.4.	Métodos SIP	10
A.4.1	Cuerpo de los mensajes	10
A.4.2	Solicitudes SIP	10
A.4.2.1	REGISTER	10
A.4.2.2	INVITE	11
A.4.2.3	BYE	11
A.4.2.4	ACK	11
A.4.2.5	CANCEL	11
A.4.2.6	OPTIONS	11
A.4.3	Respuestas SIP	11
A.4.3.1	1XX	12
A.4.3.2	2XX	12
A.4.3.3	3XX	12
A.4.3.4	4XX	12
A.4.3.5	5XX	12
A.4.3.6	6XX	12
A.5.	Extensiones SIP	13
A.5.1	SUBSCRIBE	13
A.5.2	NOTIFY	13
A.5.3	PUBLISH	13
A.5.4	REFER	13
A.5.5	MESSAGE	13



A.5.6	INFO	14
A.5.7	PRACK	14
A.5.8	UPDATE.....	14
A.6.	Cabeceras SIP	14
A.6.1	Clasificación de cabeceras del protocolo SIP	15
A.6.1.1	Cabeceras generales.....	15
A.6.1.2	Cabeceras de “entidad”	15
A.6.1.3	Cabeceras de solicitud	15
A.6.1.4	Cabeceras de respuesta	15
A.6.2	Cabeceras.....	16
A.6.2.1	Via.....	16
A.6.2.2	From	16
A.6.2.3	To.....	16
A.6.2.4	Call-Id	16
A.6.2.5	Cseq	17
A.6.2.6	Contact.....	17
A.7.	Ejecución de Servicios	17
A.7.1	Procedimientos.....	18
A.7.1.1	Localización de un servidor SIP	18
A.7.1.2	Transacciones SIP	18
A.7.1.3	Localización de usuarios SIP.....	18
A.7.1.4	Registro SIP	18
A.7.1.5	Establecimiento y terminación de una sesión SIP.....	19
B.	IP MULTIMEDIA SUBSYSTEM - IMS	21
B.1.	Generalidades de IMS	21
B.2.	Arquitectura de IMS.....	21
B.2.1	Estructuración en capas de la arquitectura IMS	22
B.2.1.1	Home Subscriber Server (HSS)	23
B.2.1.2	Call Session Control Function (CSCF).....	24
B.2.1.3	Breakout Gateway Control Function (BGCF).....	24
B.2.1.4	Media Resource Function (MRF)	24
B.2.1.5	Multimedia Resource Function Controller (MRFC)	24
B.2.1.6	Media Resource Function Processor (MRFP)	24
B.2.1.7	IP Multimedia Media Gateway (IM-MGW)	25
B.2.1.8	Media Gateway Control Function (MGCF)	25
B.2.1.9	Signaling Gateway (SGW)	25
B.2.1.10	Policy Decision Function (PDF)	26
B.2.1.11	Application Server (AS).....	26
B.2.1.12	Session Border controller (SBC).....	26



B.3. Arquitectura de Servicios de IMS	26
B.3.1 Entidades de la arquitectura de servicio IMS	27
B.4. Beneficios de IMS	29
C. PASARELA DE SEÑALIZACIÓN PARA ACCESO A CAPACIDADES IMS DESDE CLIENTES SIP-IETF - I23GW	31
C.1. Consideraciones Preliminares al desarrollo del Sistema i23GW	31
C.2. Descripción General de las Clases pertenecientes al prototipo i23GW	32
C.3. Descripción de las Herramientas y Manual para la Instalación del Sistema	33
C.3.1. Descripción General de las Herramientas utilizadas	33
C.3.2. Manual de instalación de las Herramientas utilizadas	36
C.4. Manual de Usuario para la Puesta en Marcha de la Aplicación i23GW	38
C.4.1. Entorno utilizado para la Puesta en Marcha de la Aplicación i23GW	38
C.4.2. Configuración de X-lite para funcionar con i23GW	39
C.4.3. Configuración de SJPhone para funcionar con i23GW	40
C.4.4. Puesta en marcha de OpenIMS Core	40
C.4.5. Puesta en marcha de i23GW.....	41



A. SESSION INITIATION PROTOCOL - SIP

El protocolo de inicio de sesiones es un protocolo de señalización ubicado en la capa de aplicación, diseñado para crear, modificar y terminar sesiones con uno ó varios participantes. Estas sesiones incluyen llamadas de teléfono a través de Internet, distribución de contenidos multimedia y conferencias.

El Protocolo SIP ha sido inicialmente definido por la IETF en el RFC 3261 [1], y ha sido modificado y adaptado por múltiples desarrolladores de tecnologías, para hacerlo útil como protocolo base, según las necesidades dentro de distintas redes de telecomunicaciones. El 3GPP (3rd Generation Partnership Project) ha escogido al protocolo SIP como base en las tareas de señalización y control dentro de la arquitectura de IMS.

A.1. Conceptos Generales de SIP

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 Interconnection), 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) 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.

SIP está diseñado para la creación, modificación y liberación de sesiones de comunicación en tiempo real sobre redes IP con uno o más participantes. El protocolo se



encarga del establecimiento de llamadas y de la negociación de los parámetros de la sesión a establecer, pero el intercambio de flujos se realiza haciendo uso de otros protocolos, como es el caso de RTP para la transmisión de audio y video, entre otros. SIP como protocolo proporciona servicios como la localización y disponibilidad de usuarios, negociación de las capacidades de comunicación, establecimiento y gestión de sesiones, entre otros.

Se basa en una arquitectura cliente/servidor en la que todos los procesos se plasman en un intercambio de mensajes en forma de peticiones y respuestas entre una unidad cliente y otra que funciona como servidor. Una de las características principales de SIP es que incluye entornos sencillos para la programación de servicios, incluso por parte del usuario final. Este protocolo utiliza el protocolo de descripción de sesiones multimedia (SDP) para la negociación dinámica de parámetros en el establecimiento de la sesión. Estas sesiones incluyen conferencias multimedia en Internet, llamadas telefónicas por Internet (o cualquier red IP), servicio de notificación de eventos y distribución multimedia. Los miembros en una sesión pueden comunicarse vía multicast o unicast, o alguna combinación de éstas. SIP soporta descripción de sesiones que permite a los participantes ponerse de acuerdo en un conjunto de tipos de medios compatibles. SIP permite identificar al usuario por una dirección SIP única, independientemente del tipo de terminal que se utilice o del punto de acceso a la red. [1]

SIP es un protocolo sencillo que sigue un modelo transaccional similar a HTTP y codifica sus mensajes en texto, utiliza el conjunto de caracteres UCS definido por El estándar internacional ISO 10646 con codificación UTF-8 (RFC 2279 [11]), lo que permite su fácil implementación y depuración. Los direccionamientos SIP son similares a la dirección de correo electrónico: sip:user@host (protocolo sip: nombre de usuario @ en una máquina).

Las funciones principales de SIP son:

- Localización de usuario.
- Disponibilidad de usuario.
- Capacidades de usuario.
- Negociación de sesión.
- Gestión de sesión.
- No relacionadas con la sesión: movilidad, transporte de mensajes, suscripción a eventos, autenticación, entre otras.

El protocolo SIP está basado en un modelo transaccional cliente/servidor como HTTP. El direccionamiento utiliza las direcciones de tipo URL (Uniform Resource Locator) SIP parecido a una dirección e-mail. Cada participante en una red SIP es por lo tanto alcanzable, por medio de una URL SIP.

Al ser una propuesta proveniente del mundo de Internet se adapta con facilidad y flexibilidad a los constantes cambios que se operan en las tecnologías de redes y de manera similar a HTTP y SMTP ha sabido adoptar las extensiones pertinentes para mantener una funcionalidad avanzada y la compatibilidad. En resumen se trata de un protocolo joven, escalable, sencillo, ligero y muy extensible. Estas características de SIP son las requeridas por los nuevos servicios de comunicación en Internet ante el desarrollo



cada vez más rápido de nuevos esquemas y tecnologías en el mundo de las comunicaciones multimedia sobre IP.

A.1.1 Direcciones SIP

Los usuarios diseccionados con el protocolo SIP se identifican mediante URL del tipo: user@host donde:

- User: nombre de usuario ó número telefónico.
- Host: nombre de dominio o dirección numérica de red

Los SIP- URL´s son utilizados en los mensajes SIP para indicar: origen, ubicación actual y destino final, en relación con una solicitud. También para especificar direcciones de “redirección”.

A.2. Arquitectura SIP

Dentro de la arquitectura de SIP se encuentran los agentes de usuario (UA) que pueden funcionar tanto como cliente como servidor y los servidores que pueden realizar tres tipos de operaciones: Proxy (con estado o sin estado), Registro y Redirección. Lo tres últimos pueden estar empotrados en un único servidor físico.

A.2.1 Agentes de Usuario

Los Agentes de Usuario son aplicaciones que residen en las estaciones terminales SIP. Un UA Funciona como un cliente cuando hace las peticiones de inicio de sesión, y también actúa como un servidor cuando responde a las peticiones de sesión. Por tanto, la arquitectura básica es de naturaleza cliente/servidor. El Agente de Usuario es “inteligente”, en el sentido que almacena y administra el estado de la llamada. El UA establece las llamadas usando una dirección parecida a las de correo electrónico, o un número telefónico, por ejemplo: SIP:usuario@servidor.universidad.edu. Esto hace que los URL de SIP sean fáciles de asociar con la dirección de correo electrónico del usuario. Los Agentes de Usuario pueden aceptar y recibir llamadas de otros Agentes de Usuario son componentes adicionales SIP.

Sus componentes son: Agentes de Usuario Clientes (User Agent Client, UAC) y Agentes de Usuario Servidores (User Agent Server, UAS).

Los UAC originan las solicitudes SIP (asociados al extremo que origina la llamada), y los UAS responden a estas solicitudes, es decir, originan respuestas SIP (asociados al extremo que recibe la llamada).



Los UAC y UAS pueden, por si solos y sin los servidores de red, ser capaces de soportar una comunicación básica (modelo de llamada básico, directamente entre endpoints). No obstante, la potencialidad de SIP se aprovecha con el empleo de los servidores de red. En el despliegue de SIP se pueden encontrar agentes de usuario de tipo hardware (p.e. terminales telefónicos) o software. De la misma forma se pueden encontrar integrados los servidores, ya sea proxy's, de redirección o de registro, en un único sistema.

A.2.2 Servidores SIP

En la arquitectura SIP se definen cuatro tipos de servidores:

A.2.2.1 Servidor Proxy

Un tipo de servidor intermedio SIP es el Servidor Proxy SIP. Se encarga de encaminar peticiones/respuestas hacia el destino final y retienen la información por cuestiones de contabilidad o facturación. El encaminamiento se realiza salto a salto de un servidor a otro hasta alcanzar el destino final. Para estos casos, existe un parámetro incluido en las peticiones/respuestas denominado Vía que incluye los sistemas intermedios que han participado en el proceso de encaminamiento. Esto evita bucles y permite forzar que las respuestas sigan el mismo camino que las peticiones. Esto afecta únicamente a la información de control pues el transporte de medios, salvo en el caso de requerir transcodificación intermedia, se realiza directamente entre origen y destino.

Este servidor SIP puede dirigir las llamadas entrantes hacia diversas extensiones que están activas a la vez y la primera en responder tomará la llamada. Esta capacidad significa que se puede especificar el teléfono SIP de escritorio, el teléfono móvil SIP y la aplicación de videoconferencia en casa de tipo SIP y todos esos aparatos “sonarían” cuando llegue una llamada que está tratando de localizar al usuario, de tal forma que al contestar en cualquiera de esos medios se inicia la conversación y los otros dispositivos dejan de sonar. Los Servidores Proxy SIP pueden usar varios métodos para intentar resolver la dirección destino solicitada, incluyendo búsquedas en el DNS, en bases de datos o relevando la labor hacia el siguiente Servidor Proxy Este servidor tiene una funcionalidad semejante a la de un Proxy HTTP que tiene una tarea de encaminar las peticiones que recibe de otras entidades más próximas al destinatario. Existen dos tipos de Proxy Servers: Statefull Proxy y Stateless Proxy.

- Statefull Proxy:

Mantienen el estado de las transacciones durante el procesamiento de las peticiones. Permite división de una petición en varias (forking), con la finalidad de la localización en paralelo de la llamada y obtener la mejor respuesta para enviarla al usuario que realizó la llamada.

- Stateless Proxy:



Este tipo de Proxy, no mantiene el estado de las transacciones durante el procesamiento de las peticiones, únicamente reenvían mensajes. Esta implementación provee buena escalabilidad pues los servidores no requieren mantener información referente al estado de la sesión una vez que la transacción ha sido procesada. Además, esta solución es muy robusta dado que el servidor no necesita “recordar” nada en relación con una llamada. Sin embargo, no todas las funcionalidades pueden ser implementadas en este tipo de servidor por ejemplo, las funcionalidades relativas a la contabilización y facturación de las llamadas puede requerir funcionalidades proxy stateful, de manera que se le pueda “seguir el rastro” a todos los mensajes y estados de una comunicación.

A.2.2.2 Servidor de Redirección

Un segundo tipo de servidor intermedio SIP es el Servidor de Redirección. El papel de este servidor es responder a la resolución de nombres y la ubicación del usuario. Este Servidor responde a las peticiones de los Agentes de Usuario proporcionando la información acerca de la dirección del servidor requerido.

Realiza una función equivalente al servidor proxy, pero a diferencia de este no progresa la llamada, sino que procesa y contesta a un INVITE, que son solicitudes SIP, con un mensaje de redirección, indicándole en el mismo la dirección o direcciones de la parte llamada. Es un servidor que genera respuestas de redirección a las peticiones que recibe.

Este servidor reencamina las peticiones hacia el próximo servidor. La división de estos servidores es conceptual, cualquiera de ellos puede ser físicamente una única máquina, división que se puede dar por motivos de escalabilidad y rendimiento.

A.2.2.3 Servidor de Registro

Es un servidor que acepta peticiones de registro de los usuarios; registrando las direcciones SIP (SIP – URL) y sus direcciones IP asociadas, es decir, garantizan el “mapping” entre direcciones SIP y direcciones IP y se utiliza para que los terminales registren la localización en la que se encuentran y la información de estas peticiones se guarda para poder suministrar un servicio de localización y traducción de direcciones en el dominio que controla, este servidor facilita la movilidad de usuarios, al actualizar dinámicamente la misma, permitiendo “seguir el rastro” de los usuarios, pues por diferentes razones las direcciones IP de éstos puede cambiar. Típicamente están localizados con servidores proxy o servidores de redirección.

También se les denomina servidores de localización (Location Server), pues son utilizados por los servidores proxy y de redirección para obtener información respecto a la localización o localizaciones posibles de la parte llamada.



La información registrada en los servidores de registro, como por ejemplo, el registro del mapping de direcciones SIP correspondiente a un usuario, no es permanente, requiere ser “refrescado” periódicamente, de lo contrario, vencido un “time out” (por defecto, una hora), el registro correspondiente será borrado. Este valor por defecto del “time out” puede ser modificado según valor que se especifique en la cabecera “Expires” de un mensaje de solicitud REGISTER. En consecuencia, para mantener la información de registro, el terminal (o el usuario) necesita refrescarlo periódicamente. Igualmente, un registro vigente puede ser cancelado y/o renovado por el usuario.

A.2.2.4 Agente de Llamada (Call Agent)

Es un servidor que realiza las funciones de los tres servidores anteriores, además de poder ejecutar las siguientes tareas:

- Localizar a un usuario mediante la redirección de la llamada a una o varias localizaciones.
- Implementar servicios de redirección como reenvío si está ocupado, reenvío si no contesta, etcétera.
- Implementar filtrado de llamada en función del origen o del instante de la llamada.
- Almacenar información de administración de llamadas.
- Realizar cualquier otra función de gestión.

Usualmente, un servidor de red SIP implementa una combinación de los diferentes tipos de servidores SIP ya comentados: servidor proxy + servidor de registro y/o servidor de redirección + servidor de registro. En cualquier caso deben implementar el transporte sobre TCP y UDP.

A.3. Arquitectura de Servicios SIP

La arquitectura de servicios SIP está constituida por uno o un conjunto de servidores de aplicación y servidores de medios. Los **Servidores de Aplicación** SIP ejecutan servicios tales como: Push To Talk, Presencia, Prepago, mensajería, etc. y pueden influenciar el desempeño de la sesión según el servicio que esté siendo ofrecido. El Servidor de Aplicación corresponde al SCP de la Red Inteligente.

Por otro lado, el **Servidor de Medios**, o servidor MRF (Media Resource Function o MRF) establece conferencias multimedia, toca anuncios vocales o multimedia y colecta informaciones de usuario. Se trata de la evolución de la entidad SRP (Specialized Resource Point) en el mundo multimedia.

Un **Servidor de Llamada SIP** (Proxy Server) Corresponde al punto desde el cual un servicio puede empezar a ser requerido. Dispone del perfil de servicio correspondiente al abonado, e cual le indica al servidor qué servicios han sido suscritos por el abonado y bajo qué condiciones se podrían invocar estos servicios.

A.4. Métodos SIP

El protocolo SIP está diseñado específicamente para el mundo IP e Internet y es similar a HTTP en cuanto a la sintaxis de los mensajes que se intercambian. INVITE, ACK, BYE, CANCEL, REGISTER, OPTIONS, INFO ó 1xx, 2xx, 3xx ... 6xx son los tipos de mensajes de peticiones y respuestas respectivamente que se intercambian en el protocolo. [5]

Los mensajes SIP, solicitudes (métodos) y respuestas (códigos de estado), emplean el formato de mensaje genérico establecido en la RFC 822, esto es: RFC 822)

- Una línea de inicio
- Uno o más campos de cabeceras (headers)
- Una línea vacía (indica final del campo de cabeceras)
- Cuerpo del mensaje (opcional)

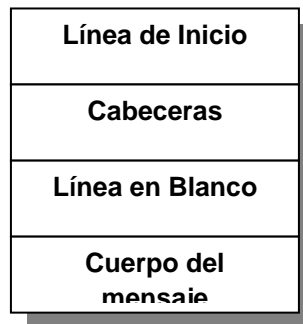


Figura 1. Estructura mensaje genérico SIP

A.4.1 Cuerpo de los mensajes

Los mensajes SIP, solicitudes o respuestas, opcionalmente pueden contener un cuerpo de mensaje. Generalmente éste es una descripción de sesión con SDP, pero puede ser también cualquier otro contenido de forma ya sea cifrado o sin cifrar. El contenido del cuerpo del mensaje sólo es de interés para los UA, no para los servidores de red, si se habla de funcionalidades SIP, ya que SIP sólo necesita conocer los contenidos de línea de solicitud, o de línea de estado, según el caso y el de las cabeceras.

A.4.2 Solicitudes SIP

A.4.2.1 REGISTER

El método es emitido en un mensaje multicast que se utiliza como un servicio de localización para ubicar al servidor SIP. Un agente de usuario utiliza este método para



registrar la correspondencia entre su Dirección IP de contacto actual y su dirección SIP a la que van a llegar las peticiones.

A.4.2.2 INVITE

Este método es usado con el fin de establecer una sesión entre Agentes de usuario. Localiza e identifica al usuario y contiene las informaciones sobre el que genera la llamada y el destinatario así como sobre el tipo de flujos que serán intercambiados

A.4.2.3 BYE

Método que permite la liberación de una sesión anteriormente establecida Y puede ser emitido por el usuario que invita a una sesión o por el que recibe la invitación.

A.4.2.4 ACK

Usado para reconocer que el mensaje Invite puede ser aceptado. Confirma que un cliente solicitante ha recibido una respuesta final desde un servidor a una solicitud INVITE, reconociendo la respuesta como adecuada. El método ACK es solo para reconocer solicitudes INVITE, y no otros mensajes de solicitud.

A.4.2.5 CANCEL

Este método es utilizado para que un abandono cancele el inicio de una sesión en curso pero no tiene ningún efecto sobre una sesión ya aceptada. De hecho, solo el método "BYE" puede terminar una sesión establecida. Además puede terminar la búsqueda de un usuario.

A.4.2.6 OPTIONS

Método utilizado para interrogar las capacidades y el estado de un Agente de usuario o de un servidor. La respuesta contiene sus capacidades (ejemplo: tipo de medio soportado, idioma soportado) o el hecho de que el UA sea indisponible, capacidades que pueden ser configuradas entre agentes o mediante un servidor SIP.

A.4.3 Respuestas SIP

Los clientes SIP envían Las solicitudes SIP (*Requests Messages*) a un servidor, el cual se encarga de procesar los mensajes y enviar una respuesta (*Response Messages*) por medio de unos Status-Code, que son respuestas identificadas por un código digital.

De hecho, la mayor parte de los códigos de respuesta SIP han sido tomados del protocolo HTTP. Por ejemplo, cuando el destinatario no esta ubicado, una respuesta 404 Not Found



es devuelta. Un requerimiento SIP esta constituido por cabeceras, al igual que un mando SMTP.

Hay seis tipos diferentes de Status-Code definidos:

A.4.3.1 1XX

Información, el requerimiento ha sido recibido y esta en proceso (100 Probando, 180 timbrando, 181 llamadas siendo reenviada):

A.4.3.2 2XX

Solicitud exitosa, el requerimiento ha sido recibido, entendido y aceptado (200 OK, 202 Aceptado)

A.4.3.3 3XX

Re-enrutamiento, la llamada requiere otros procesamientos antes de poder determinar si puede ser realizada. (300 selección múltiple, 301 Movido Permanentemente, 302 Movido temporalmente).

A.4.3.4 4XX

Error del cliente, la solicitud contiene un error en la sintaxis o no puede ser interpretado por el servidor. El requerimiento tiene que ser modificado antes de ser reenviado (400 petición incorrecta, 404 no encontrado, 482 lazo detectado, 486 ocupado aquí).

A.4.3.5 5XX

Error de servidor, el servidor fracasa en el procesamiento de una solicitud aparentemente válida (500 Error interno del servidor, 501 No implementado).

A.4.3.6 6XX

Falla global, la solicitud no puede ser procesado por ningún servidor (600 en cualquier lugar ocupado, 603 rechazo) Los mensajes respuestas 2xx, 3xx, 4xx, 5xx y 6xx son “respuestas finales”, y terminan la transacción SIP. En cambio, los mensajes de respuestas 1xx son “respuestas provisionales”, y no terminan la transacción SIP.[2]



A.5. Extensiones SIP

A pesar de que existe una lista de métodos SIP destinados a su uso dentro de las labores básicas de señalización para este protocolo, existen también algunas extensiones realizadas sobre la especificación inicial, que son útiles para asuntos específicos del cliente y los servicios que estos consumen. Algunos ejemplos para dichas extensiones son:

A.5.1 SUBSCRIBE

Método que permite la suscripción de los usuarios en la red. Esto, con el fin de que los usuarios suscritos puedan recibir notificaciones sobre su estado de registro en la red, o sobre cualquier evento que allí se produzca.

A.5.2 NOTIFY

Método utilizado para enviar notificaciones de los eventos de registro producidos en la red.

A.5.3 PUBLISH

Método que permite publicar su estado.

A.5.4 REFER

Este método reenvía el receptor hacia un recurso identificado en el método. REFER permite emular distintos servicios o aplicaciones incluyendo la transferencia de llamada. Si se contempla T1, como la entidad que origina la transferencia, T2 como la entidad transferida y T3, el destinatario de la transferencia. La transferencia de llamada permite a T1 transformar una llamada en curso entre T1 y T2 en una nueva llamada entre T2 y T3, elegida por T1. Si la transferencia de llamada se lleva a cabo, T2 y T3 podrán comunicarse mientras que T1 no podrá seguir dialogando con T2 o T3. [6]

A.5.5 MESSAGE

Método que ha sido propuesto como extensión al protocolo SIP con el fin de permitir la transferencia de mensajes instantáneos. La mensajería instantánea IM (Instant Messaging) que consiste en el intercambio de mensajes entre usuarios en pseudo tiempo real. Este nuevo método hereda de todas las funciones ofrecidas por el protocolo SIP



tales que el enrutamiento y la seguridad. La extensión MESSAGE puede transportar varios tipos de contenidos basándose en la codificación MIME. [7]

A.5.6 INFO

Este método permite transferir informaciones de señalización durante la llamada. Entre los ejemplos de información se encuentran los dígitos DTMF, las informaciones relativas a la tasación de una llamada, las imágenes etc.

Las respuestas finales 2xx, 3xx, 4xx, 5xx y 6xx a un requerimiento INVITE son satisfechas por el requerimiento ACK mientras las respuestas provisorias de tipo 1XX no son satisfechas. Ciertas respuestas temporarias tales como el 180 Ringing son críticas y su recepción es esencial para la determinación del estado de la llamada, entre otros durante el proceso de interconexión con la RTCP. [8]

A.5.7 PRACK

Este método ha sido definido con el fin de satisfacer la recepción de respuestas temporarias de tipo 1XX. [9]

A.5.8 UPDATE

Método que permite a un terminal SIP actualizar los parámetros de una sesión multimedia. El método UPDATE puede ser enviado antes de que la sesión sea establecida. UPDATE es entonces particularmente útil cuando se trata de poner al día los parámetros de sesión antes de su establecimiento, por ejemplo en puesta en espera del destinatario. [10]

A.6. Cabeceras SIP

Las cabeceras SIP son similares a las cabeceras utilizadas en el protocolo HTTP (Hyper Text Transfer Protocol), tanto en la sintaxis como en la semántica. Especifican aspectos referentes a los participantes, trayectos, etc.

Generalmente, el orden en que aparecen las cabeceras no tiene mayor importancia, siempre que se cumpla que las cabeceras del tipo “salto a salto” (hop-by-hop) deben aparecer antes que cualquier cabecera del tipo “extremo a extremo” (end-to-end). Las primeras pueden ser modificadas o añadidas por los servidores proxy, en cambio las segundas deben ser transmitidas por éstos sin modificación alguna. Los servidores proxy no deben re-ordenar las cabeceras, pero si pueden adicionar ciertos tipos de cabeceras, como por ejemplo la cabecera “Via”, así como otras del tipo “salto a salto” (hop-by-hop). Si



bien pueden modificar ciertas cabeceras, no deben alterar los campos que son autenticados.

El número total de cabeceras SIP definidas hasta ahora es 46, que rebasa el número de 37 cabeceras de la especificación inicial de SIP RFC 2543, pudiendo ser agrupadas de la siguiente forma.

A.6.1 Clasificación de cabeceras del protocolo SIP

A.6.1.1 Cabeceras generales

Se utilizan tanto en los mensajes de solicitud como en los mensajes de respuesta. Estas cabeceras son: Call-ID, Contact, CSeq, Date, Encryption, From, Organization, Retry-After, Sub-ject, Supported, Timestamp, User Agent y Via.

A.6.1.2 Cabeceras de “entidad”

Las cabeceras de entidad (entity headers) dan información adicional referente al cuerpo del mensaje, o si éste no está presente, entonces acerca del recurso identificado por la solicitud. Son las siguientes: Allow, Content-Encoding, Content- Length, Content-Type, Content- Disposition, Expires y MIME-Version.

A.6.1.3 Cabeceras de solicitud

Las cabeceras de solicitud (request headers) posibilitan que el cliente pase información adicional al servidor referente a la solicitud, y también a cerca del propio cliente. Actúan como un modificador de solicitud. Son las siguientes: Accept, Accept- Encoding, Accept-Language, Accept-Contact, Authorization, Hide, In-Reply-To, Max-Forwards, Priority, Proxy-Authorization, Proxy-Require, Record- Route, Reject-Contact, Request- Disposition, Require, Response- Key, Route, Rack y Session-Expires.

A.6.1.4 Cabeceras de respuesta

Las cabeceras de respuesta (response headers) posibilitan al servidor pasar información adicional en relación a la respuesta, información que no se puede situar en el campo “Status-Line”. Da información del servidor y también referente al recurso identificado por “Request-URI”. Las cabeceras son las siguientes: Proxy-Authenticate, Server, Unsupported, Warning, WWW-Authenticate y Rseq.



Las cabeceras se utilizan para transportar información sobre el usuario, la red, los caminos que debe seguir el mensaje y las relaciones existentes entre las distintas entidades. A continuación se detallan las cabeceras encargadas de portar dicha información.

A.6.2 Cabeceras

Determinadas cabeceras están presentes en todos los mensajes, otras no, solo en algunos. Igualmente, una aplicación que contenga el protocolo SIP no requiere necesariamente tener que comprender todas las cabeceras, aunque si es deseable. En el mismo sentido, si un servidor SIP no entiende una cabecera, la ignora. Las cabeceras no especificadas deben ser ignoradas por los servidores. A continuación se detallarán las 6 cabeceras más importantes:

A.6.2.1 Via

Indica el transporte usado para el envío e identifica la ruta de una solicitud, con el propósito de posibilitar a los servidores SIP que intervienen, enviarlas respuestas por la misma ruta guiada por la solicitud. Es por eso que cada proxy añade un valor a la cabecera Via. Esta cabecera es una de las potencialidades más importantes del protocolo SIP.

A.6.2.2 From

Indica la dirección del origen de la petición, en la pareja relacionada solicitud-respuesta. Contiene la dirección del origen y, opcionalmente, el nombre de éste, está presente en todas las solicitudes y respuestas.

A.6.2.3 To

Indica la dirección del destinatario de la petición. Debe estar presente en todos los mensajes de solicitudes y respuestas.

A.6.2.4 Call-Id

Identificador único para cada llamada y contiene la dirección del host. Debe ser igual para todos los mensajes dentro de una transacción. Se utiliza para diferentes propósitos, por ejemplo:



- Para hacer corresponder las respuestas con las correspondientes solicitudes.
- Para detectar duplicados de solicitudes INVITE.
- Para cambiar dinámicamente parámetros de una sesión

A.6.2.5 Cseq

Se inicia con un número aleatorio e identifica de forma secuencial cada petición. Está compuesta por un número decimal y el nombre del método. En una sesión SIP Cseq se incrementa por cada nueva solicitud, excepto en solicitudes ACK y CANCEL. La respuesta a una determinada solicitud lleva el mismo Cseq que dicha solicitud, esto es, el UAS copia el valor del Cseq de la solicitud en la correspondiente respuesta, por lo que la pareja relacionada solicitud- respuesta tiene el mismo valor de cabecera CSeq.

A.6.2.6 Contact

Contiene una (o más) direcciones que pueden ser utilizadas para contactar al usuario.

A.7. Ejecución de Servicios

El método de introducción del servicio depende del tipo de servicio y de su complejidad. Así mismo, un servicio puede estar sobre el terminal SIP, el servidor de medios SIP, el servidor de aplicaciones o el servidor proxy.

Ciertos servicios requieren interacciones complejas con el usuario (mensajería unificada, IVR, etc.) Para estos servicios vocales, un acercamiento centralizado es necesario con las entidades AS SIP conteniendo la lógica de aplicación y servidores de medios SIP conteniendo el escrito vocal. Cierta tipo de servicios requieren un a base de datos centralizada. Para estos servicios de traducción de número (servicios de número abreviado, servicio prepago, servicio VPN), un AS SIP que contiene la lógica de aplicación es necesario.

Algunos servicios no se prestan bien a un tratamiento centralizado. La aparición de terminales SIP basados sobre una máquina Java, ha ofrecido la posibilidad de desarrollar servicios sobre los terminales:

El servicio de timbre diferenciado permite modificar el timbre del puesto llamado según la identidad del que llama. Este servicio básico es típicamente un servicio que conviene desplegar sobre el aparato.

El servicio de filtro de llamada es una evolución del servicio anterior, en la cual la identidad del usuario llamado sirve para determinar si la llamada debería ser aceptada, reenviada o bien, rechazada.



El servicio de guía telefónica subraya el interés de una conexión directa del terminal con una guía de empresa: permite al usuario consultar una guía LDAP desde el teléfono, de tal forma que pueda seleccionar un número entre los resultados de la consulta e iniciar una llamada hacia dicho número.

A.7.1 Procedimientos

A.7.1.1 Localización de un servidor SIP

Cuando un cliente SIP desea enviar una solicitud, debe enviarla a un servidor proxy configurado localmente, o bien, enviar dicha solicitud a la dirección IP y puerto que corresponda.

A.7.1.2 Transacciones SIP

Cuando se efectúa la localización de un servidor SIP, se inicia las transacciones, las cuales corresponden a las solicitudes enviadas por el cliente al servidor, y a su vez, las respuestas que el servidor retorna al cliente. Estas solicitudes y respuestas están relacionadas entre sí y tienen determinados parámetros idénticos como Call-ID, To, From, Cseq.

A.7.1.3 Localización de usuarios SIP

Dado que el usuario llamado puede desplazarse entre diferentes terminales, para registrar estas localizaciones se usa un Servidor de localización. Este servidor puede retornar varias localizaciones, ya sea porque el usuario esté “logueado” en diferentes hosts al mismo tiempo, o porque el servidor de localización tenga temporalmente información no actualizada.

A.7.1.4 Registro SIP

El método “REGISTER” es utilizado por un UA con el fin de indicar a la función Registrar (físicamente implantada en un Proxy Server o un Redirect Server) la correspondencia entre su dirección SIP (por ejemplo: sip:usuario1@dominio1.com) y su dirección IP (ejemplo: usuario1@192.190.132.20). La dirección IP puede ser estática u obtenida de modo dinámico por DHCP. La función Registrar actualiza entonces una base de datos de localización. Desde este momento, el User Agent puede recibir llamadas ya que se encuentra ubicado.

Cuando un mensaje INVITE debe ser entregado por el Servidor proxy del dominio dominio1.com a sip: usuario1@dominio1.com, la base de datos actualizada por la función Registrar indica al Proxy Server que el mensaje tiene que ser relevado a sip:usuario1@dominio2.com. Entonces, el servidor proxy efectúa una búsqueda por el



DNS de la dirección IP del servidor proxy del dominio2.com con el fin de relevar el mensaje SIP a encaminar al destino apropiado (sip:usuario1@dominio2.com). En una red IMS, el Proxy Server corresponde a una entidad CSCF (Call State Control Function), mientras la base de datos de localización es representada por la entidad HSS. (Home Subscriber Server).

A.7.1.5 Establecimiento y terminación de una sesión SIP

En el ejemplo siguiente, el usuario que llama tiene como URL SIP la dirección: sip:usuario1@dominio2.com, mientras la URL SIP del destinatario de la llamada es sip:usuario2@dominio2.com. Un mensaje de establecimiento de llamada SIP INVITE es emitido desde UA SIP del que llama al servidor proxy. Este último interroga la base de datos de localización para identificar la ubicación del llamado (dirección IP) y encamina la llamada a su destino.

El mensaje INVITE contiene distintas cabeceras obligatorias entre las cuales la dirección SIP de la persona que llama "From", la dirección SIP de la persona que recibe la llamada "To", una identificación de la llamada "Call-ID", un número de secuencia "Cseq", un número máximo de saltos "max-forwards". El encabezamiento "Via" está actualizado por todas las entidades que participaron al enrutamiento del requerimiento INVITE. Eso asegura que la respuesta seguirá el mismo camino que el requerimiento. Por otra parte, el requerimiento SIP INVITE contiene una sintaxis "Session Description Protocol" o SDP. Esta estructura consiste en varias líneas que describen las características del medio que el usuario llamante necesita para comunicarse con el llamado. A continuación se puede ver la información de cada una de las cabeceras para el establecimiento de una sesión.

```
INVITE sip:usuario2@dominio2.com SIP/2.0
Via : SIP/2.0/UDP station1.dominio2.com:5060
Max-Forwards : 20
To : Usuario2<sip:usuario2@dominio2.com>
From : Usuario1<sip:usuario1@dominio2.com>
Call-Id: 23456789@station1.dominio2.com
CSeq: 1 INVITE
Contact: usuario1@192.190.132.20
Content-Type: application/sdp
Content-Length:162
v = 0
c = IN IP4 192.190.132.20
m = audio 45450 RTP/AVP 0 15
```

La respuesta 180 RINGING está devuelta por el destinatario a la UA del que genera la llamada. Cuando el destinatario acepta la sesión, la respuesta 200 OK está emitida por su UA y encaminada hacia la UA del que genera la llamada, como se puede ver a continuación:

```
SIP/2.0 200 OK
Via : SIP/2.0/UDP ps1.dominio2.com:5060
```



```
Via : SIP/2.0/UDP station1.dominio2.com:5060
Max-Forwards : 20
To : Usuario2<sip:usuario2@dominio2.com>
From : Usuario1<sip:usuario1@dominio2.com>
Call-Id: 23456789@station1.dominio2.com
CSeq: 1 INVITE
Contact: usuario2@192.190.132.27
Content-Type: application/sdp
Content-Length:162
v = 0
c = IN IP4 192.190.132.27
m = audio 22220 RTP/AVP 0
```

La UA del que genera la llamada devuelve un método ACK al destinatario, relevada por la entidad Proxy Server.

El servidor proxy, participa al encaminamiento de la señalización entre UAs mientras que las UAs establecen directamente canales RTP para el transporte de la voz o del video en forma de paquetes sin implicación del servidor proxy en este transporte. Cuando el Usuario1 cuelga, su UA envía un requerimiento BYE para terminar la sesión. Este requerimiento esta entregado al servidor proxy quien lo encamina a la UA del Usuario2. Este último, devuelve la respuesta 200 OK. El Usuario1 cuelga y envía un requerimiento BYE:

```
BYE sip:usuario2@dominio2.com SIP/2.0
Via : SIP/2.0/UDP station1.dominio2.com:5060
Max-Forwards : 20
To : Usuario2<sip:usuario2@dominio2.com>
From : Usuario1<sip:usuario1@dominio2.com>
Call-Id: 23456789@station1.dominio2.com
Ahora el Usuario2 recibe el BYE:
CSeq: 2 BYE
SIP/2.0 200 OK
Via : SIP/2.0/UDP ps1.dominio2.com:5060
Via : SIP/2.0/UDP station1.dominio2.com:5060
Max-Forwards : 20
To : Usuario2<sip:usuario2@dominio2.com>
From : Usuario1<sip:usuario1@dominio2.com>
Call-Id: 23456789@station1.dominio2.com
CSeq: 2 BYE
```

En el anterior ejemplo se puede ver claramente como se hace el establecimiento y la liberación de una sesión, en el RFC3261 se puede encontrar todos los procedimientos de una sesión. Por otra parte, los campos de cabeceras SIP pueden no contener SIP-URL's, por ejemplo, en el caso que una llamada desde un teléfono convencional pase por Internet con el empleo del protocolo SIP, entonces la cabecera "from" puede contener un URL telefónico.



B. IP MULTIMEDIA SUBSYSTEM - IMS

C.1. Generalidades de IMS

Siguiendo una tendencia mundial hacia las redes y tecnologías de tipo All-IP, o Todo sobre IP (Internet Protocol), nace IMS, como una arquitectura definida por el 3GPP (3rd Generation Partnership Project) con el objetivo principal de prestar a los operadores de red tradicionales, una plataforma sobre la cual se pudieran desplegar más y mejores servicios, de manera independiente a la red de acceso utilizada por dichos operadores.

IMS está basado en nuevos conceptos, nuevas tecnologías, nuevos actores así como un nuevo ecosistema. Sobre una red totalmente IP, IMS soporta las sesiones aplicativos de tiempo real (voz, video, conferencia, etc.) y las de no tiempo real (“Push To Talk” o “PTT”, Presencia, Mensajería Instantánea, etc.). Además, integra adicionalmente el concepto de convergencia de servicios soportados por redes de naturaleza distinta: fijo, móvil o Internet.

Uno de los principales objetivos en la definición de IMS, es la combinación de los servicios tradicionales de los operadores de red. Esta combinación incluye la posibilidad de acceder a la información desde cualquier punto de la red y desde cualquier dispositivo, además de poder definir comunidades de interés utilizando a la par mensajería unificada, el servicio de presencia, y aplicaciones de agenda y de correo electrónico.

A pesar de todo esto, IMS no define las aplicaciones o servicios que pueden ser ofrecidos en la red, sino que proporciona una plataforma que abarca características de capa de aplicación, control/señalización, además de transporte, para que los operadores la puedan emplear con el fin de construir sus propias aplicaciones y servicios.

C.2. Arquitectura de IMS

La introducción del “IP Multimedia Subsystem” o IMS en las redes fijas y móviles representa un cambio fundamental en las redes de telecomunicaciones de tipo voz. Las nuevas capacidades de las redes y de los terminales, el “matrimonio” entre el Internet y la voz, el contenido y la movilidad hacen aparecer nuevos modelos de redes y más que todo ofrecen un potencial fantástico para el desarrollo de nuevos servicios. Con esta meta, el IMS es concebido para ofrecer a los usuarios la posibilidad de establecer sesiones multimedia usando todo tipo de acceso de alta velocidad y una conmutación de paquetes IP.

El IMS provee una red IP multi-servicio, multi-acceso, securizada y confiable:

- Multi-servicios: todo tipo de servicios ofrecidos por una red soportando diferentes niveles de calidad de servicio podrán ser ofrecidos al usuario.



- Multi-acceso: toda red de acceso “banda ancha”, fija y móvil, podrá interfazarse al IMS.

El IMS no es una única red sino diferentes redes que ínter-operan gracias a distintos acuerdos de roaming IMS fijo-fijo, fijo-móvil, móvil-móvil.

El IMS es un “enabler” o **catalizador** que hace posible a los proveedores de servicios ofrecer:

- Servicios de comunicaciones no tiempo real, pseudo-tiempo real y tiempo real según una configuración cliente-servidor o entre entidades **pares**,
- La movilidad de servicios / movilidad del usuario (nomadismo),
- Varias sesiones y servicios simultáneamente sobre la misma conexión de red.

A.2.1 Estructuración en capas de la arquitectura IMS

La arquitectura IMS puede ser estructurada en capas. Cuatro capas importantes son identificadas:

- La capa de TRANSPORTE representa una red IP. Esta red IP podrá integrar mecanismos de calidad de servicios con MPLS, Diffserv, RSVP, etc... La capa de transporte esta compuesta de enrutadores o routers (edge routers para el acceso y core routers para el tránsito), conectados por una red de transmisión. Distintas pilas de transmisión pueden ser contempladas para la red IP: IP/ATM/SDH, IP/Ethernet, IP/SDH, etc.
- La capa CONTROL consiste en controladores de sesión responsables del encaminamiento de la señalización entre usuarios y de la invocación de los servicios. Estos nodos se llaman “Call State Control Function” o CSCF. El IMS introduce entonces un ámbito de control de sesiones sobre el campo de paquetes.
- La capa APLICACIÓN introduce las aplicaciones (servicios de valor agregado) propuestas a los usuarios. El operador puede posicionarse gracias a su capa CONTROL como integrador de servicios ofrecidos por el mismo o bien por terceros. La capa aplicación consiste en servidores de aplicación “Application Server” o “AS” y “Multimedia Resource Function” o “MRF” que los proveedores llaman Servidores de Media IP (“IP Media Sever” o “IP MS”). La arquitectura global IMS esta descrita a continuación (Figura1).

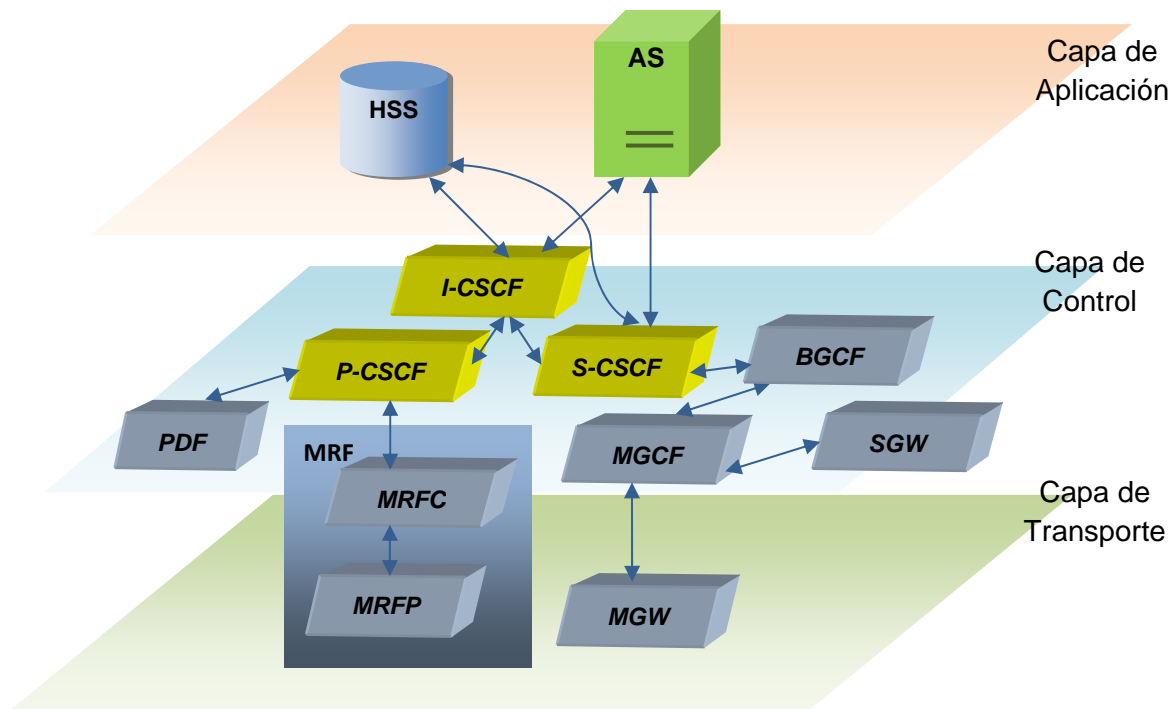


Figura 2. Arquitectura General de IMS

B.2.1.1 Home Subscriber Server (HSS)

El HSS es el repositorio principal de la información de usuario. Contiene datos relacionados con abonados útiles en la gestión de trámites de señalización, autenticación y establecimiento de sesiones entre las entidades de capa de control.

HSS contiene toda la información de los abonados móviles, incluyendo datos dinámicos, tales como la localización del abonado y el estado de servicios suplementarios. Además, datos permanentes, tales como números asociados a abonados e información de categoría. También se incluyen los datos de autenticación y cifrado para cada abonado móvil.

Por ejemplo, el HSS interactúa con los servidores de control de llamada para completar los procedimientos de encaminamiento o itinerancia, al gestionar dependencias de colocación de nombres y direcciones.

El HSS hereda las funciones del HLR, almacena y gestiona el perfil del servicio IMS de cada abonado, almacena las claves de seguridad y realiza las funciones de autenticación, validación y administración (AAA), además registra el estado de registro de los abonados y almacena la identificación del nodo S-CSCF con el que el abonado se ha registrado.



B.2.1.2 Call Session Control Function (CSCF)

Su función es procesar los mensajes de señalización para controlar la sesión multimedia de los usuarios. El núcleo de la red de conmutación de paquetes existente se utiliza para soportar el camino que siguen los datos de sesiones multimedia. El CSCF realiza diversas funciones, la primera es la función de control de la sesión multimedia. Ésta es una evolución de la función de control de llamada del MSC. Después se tiene la función de traducción de la dirección (que es la evolución de la función de traducción de dígitos). El CSCF debe realizar el manejo del perfil del suscriptor. El CSCF puede desempeñar tres roles: el de Proxy-CSCF (P-CSCF), el de Interrogating- CSCF (I-CSCF) y el de Serving-CSCF (S-CSCF). El P-CSCF es el primer punto de contacto de un móvil en la red IMS. La función del I-CSCF es determinar el S-CSCF basado en carga o capacidad de la red. El S-CSCF es responsable de gestionar la sesión del móvil y de los servicios de usuario, almacenados en el perfil de usuario almacenado en el HSS, identificando e iniciando servicios residentes en los servidores de aplicaciones.

B.2.1.3 Breakout Gateway Control Function (BGCF)

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

B.2.1.4 Media Resource Function (MRF)

Esta entidad permite multiconferencias mezclando las sesiones multimedia de varios participantes. Está dividido en el MRFC (Media Resource Function Controller) y el MRFP (Media Resource Function Processor), similares en función al MGCF y al MGW.

B.2.1.5 Multimedia Resource Function Controller (MRFC)

Encargado de controlar los recursos multimedia establecidos por el MRFP e interactúa con él a través del protocolo MEGACO, basándose en información suministrada por el SCSCF y el servidor de aplicaciones.

B.2.1.6 Media Resource Function Processor (MRFP)

Funciona bajo el control del MRFC y provee funciones como las de duplicar paquetes y modificar el medio, realizando acciones como convertir texto a audio.



B.2.1.7 IP Multimedia Media Gateway (IM-MGW)

Es una pasarela multimedia encargada de relacionar la red IMS con las redes de circuitos a través de la interfaz Iu. La MGW soporta conversión multimedia, control de portadoras y procesamiento de carga útil. En las redes de circuitos se encarga de la trans-codificación de flujos IMS sobre IP a datos de usuario. Además, realiza el procesamiento de la información multimedia entre los usuarios finales y su función principal es convertir medios de un formato a otro. Es probable que el MGW sea una plataforma basada en hardware que realiza procesamiento en tiempo real. Teniendo en cuenta este aspecto, la velocidad de procesamiento de información es algo crítico y lo más probable es que añada un poco de retraso a la transmisión de la información.

B.2.1.8 Media Gateway Control Function (MGCF)

Hace parte de la arquitectura de interoperación de IMS con las redes de circuitos. El MGCF controla uno o más MGWs, permitiendo más escalabilidad en la red. Las principales funciones realizadas por la MGCF son: controlar el estado de llamada relacionado con el control de conexiones para canales multimedia en un MGW, comunicándose con el CSCF y seleccionar el CSCF dependiendo del número de encaminamiento de la llamada entrante desde las redes heredadas, realizando conversión de protocolos.

En concreto, el MGCF puede realizar funciones como traducir la señalización IMS SIP/SDP a SS7, y viceversa, convierte mensajes SIP en mensajes MEGACO o ISUP. Cuando el MGCF recibe un mensaje SIP del CSCF se encarga de determinar qué conexión realizar con el IM-MGW y también puede crear el mensaje apropiado de ISUP y enviarlo, vía IP, al SGW (Signaling Gateway).

B.2.1.9 Signaling Gateway (SGW)

Característica esencial del Subsistema Multimedia IP. La SGW es la encargada de crear un puente entre la red SS7 y la red IP bajo el control del MGCF. Una Signaling Gateway establece el protocolo, el tiempo y requerimiento de las redes SS7, también como las equivalentes funcionalidades de la red IP.

La mayoría de la comunicación entre los componentes de IMS está basada en IP. Solamente hay dos interfaces que no están basadas en IP. Ambas se utilizan para interactuar con una red tradicional (la PSTN o una red móvil anterior). Estas dos interfaces son el camino del portador y el de señalización hacia la red antigua. Su función es convertir SS7 a IP. Los protocolos de la capa de aplicación no se verán afectados. Un ejemplo de un protocolo de capa de aplicación es el ISDN User Part (ISUP) que se utiliza para establecer llamadas con la PSTN.



B.2.1.10 Policy Decision Function (PDF)

El PDF se encarga de negociar con la red de transporte los recursos necesarios para proveer la clase de servicio requerida para cada sesión.

B.2.1.11 Application Server (AS)

Es un servidor especializado que se encarga de proveer la lógica y las funciones relacionadas con cada servicio. Estos servidores se pueden situar en la red local o en una red visitante, y en el último caso, estos servidores no se interconectan con el HSS.

Los servidores de aplicación son componentes del nivel de aplicaciones y servicios de IMS. El 3GPP define interfaces IMS entre el S-CSCF y el plano de servicios. De esta manera la señalización puede desviarse hacia el plano de aplicaciones y servicio en base a una serie de criterios almacenados en el perfil de abonado que el HSS alberga y que el S-CSCF descarga durante el registro de cada abonado. Por tanto, el S-CSCF puede transferir la señalización de un registro o sesión hacia un servidor de aplicaciones SIP.

B.2.1.12 Session Border controller (SBC)

Este es un elemento muy importante dentro de la arquitectura IMS. Existen dos tipos diferentes de SBC, el ISBC y el ASBC, que integran la señalización y el control de medios. Algunos de los beneficios de esta integración son:

- Seguridad

El SBC previene ataques contra los elementos de IMS por el descubrimiento dinámico y el bloqueo de ataques malignos. Los SBC avanzados pueden tener elementos Hardware que ayudan a la protección contra ataques sin pérdida del servicio.

- Flexibilidad

El SBC incorpora funciones múltiples del IMS dando por resultado pocos elementos de la red, pocos protocolos de red, y una administración más robusta de funcionamiento y de fallos.

C.3. Arquitectura de Servicios de IMS

La arquitectura de servicio IMS básico es constituida de entidades servidores de aplicación, de servidores de media IP y de S-CSCF equivalentes a servidores de llamadas (Ver figura 2). El **servidor de aplicación** SIP “Application Server” o AS, ejecuta los servicios (Push To Talk, Presencia, Prepago, Mensaje Instantáneo, etc..) y puede

influenciar el desempeño de la sesión sobre pedido del servicio. El servidor de aplicación corresponde a la entidad “Service Control Function” o “SCF” de la Red Inteligente. El **servidor de media IP** pone en obra la entidad funcional “Multimedia Resource Function” o “MRF”. El establece conferencias multimedia, difunde avisos vocales o multimedia y recolecta informaciones de usuario. Se trata de la evolución de la entidad “Specialized Resource Function” o “SRF” de la red inteligente en el mundo multimedia.

El servidor de llamadas SIP llamado “Serving – Call State Control Function” o “S-CSCF” tiene el papel de punto desde el cual un servicio puede ser invocado. Dispone del perfil de servicio del usuario que le indica los servicios suscritos por el usuario y bajo cuales condiciones invocar dichos servicios. Corresponde a la entidad SSF de la arquitectura de Red Inteligente.

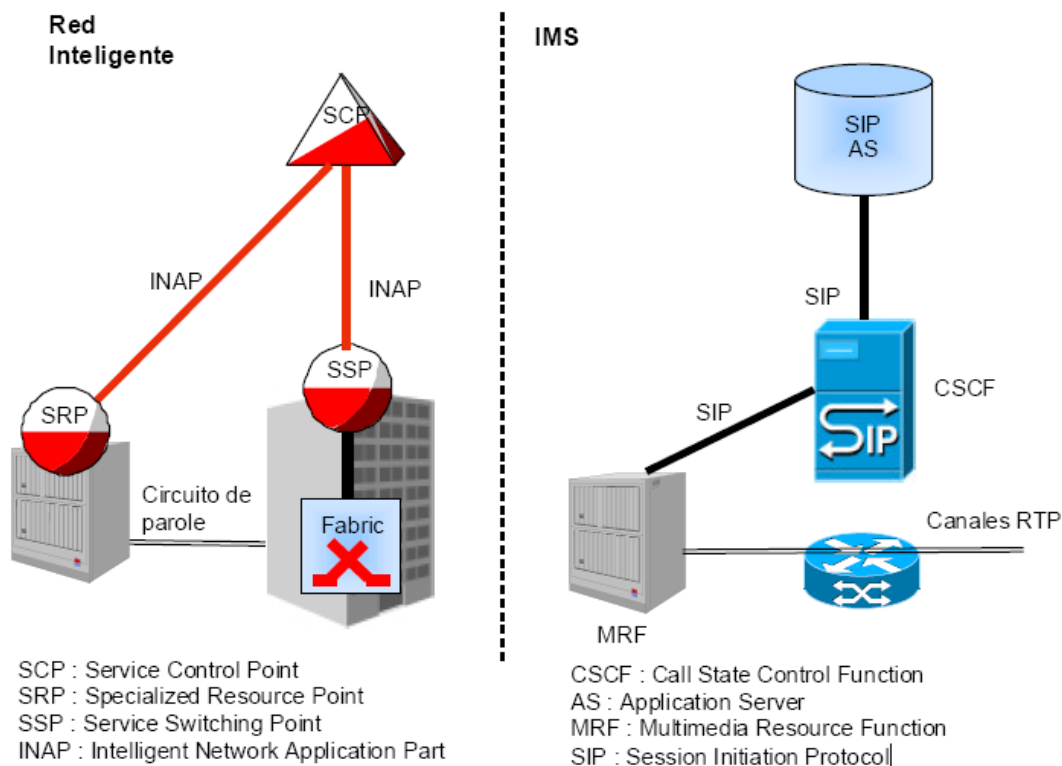


Figura 3. Red Inteligente Vs. Arquitectura de servicios de IMS

B.3.1 Entidades de la arquitectura de servicio IMS

La arquitectura de servicio IMS consiste en un conjunto de servidores de aplicación interactuando con la red IMS (S-CSCF) a través del interfaz “IP Multimedia Service Control” o ISC soportada por el protocolo SIP (Figura 3).



Los servidores de aplicación son:

- Los servidores de aplicación SIP (SIP AS) quienes ejecutan servicios (Push To Talk, Presencia, Prepago, Mensajería Instantánea, Videoconferencia, Mensajería Unificada, etc.) y que pueden influenciar en el desempeño de la sesión a pedido del servicio.
- El punto de conmutación al servicio IM, “IP Multimedia Service Switching Function” o “IM-SSF” quien es un tipo particular de servidor de aplicación SIP quien termina la señalización SIP sobre interfaz ISC por una parte y que tiene un papel de SSP RI/CAMEL por otra parte (dispone de los modelos de llamada O-IM-BCSM y T-IMBCSM, de puntos de detección RI/CAMEL y del protocolo INAP/CAP) para interactuar con los SCP RI/CSE CAMEL.
- La pasarela OSA, “OSA Service Capability Server” o “OSA SCS” que es un tipo específico de servidor de aplicación SIP que termina la señalización SIP sobre interfaz ISC y que interactúa con servidores de aplicación OSA usando el API OSA.
- Un tipo especializado de servidor de aplicación SIP llamado gestor de interacción de servicios “Service Capability Interaction Manager” o “SCIM” que permite el manejo de las interacciones entre servidores de aplicación SIP

Además de los servidores de aplicación, existe un servidor de media llamado Multimedia Resource Function, o MRF. Establece conferencias multimedia, difunde anuncios vocales o multimedia y recauda informaciones de usuario. Se trata de la evolución de la entidad “Specialized Resource Function” o “SRF” hacia el mundo multimedia. Las funciones de la entidad MRF son dos:

- La función “MRF Processor” o “MRFP que procesa el media a través del transporte RTP/UDP/IP.
- La función “MRF Controller” o MRFC que procesa la señalización.

El interfaz MR entre las entidades S-CSCF y MRFC es soportada por el protocolo SIP.

Todos los servidores de aplicación (IM-SSF y OSA SCS incluido) se comportan como servidores de aplicación SIP. Por otra parte, estos servidores de aplicación pueden interactuar con la entidad MRFC a través del S-CSCF para controlar las actividades multimedia puestas en obra por la entidad MRFP.

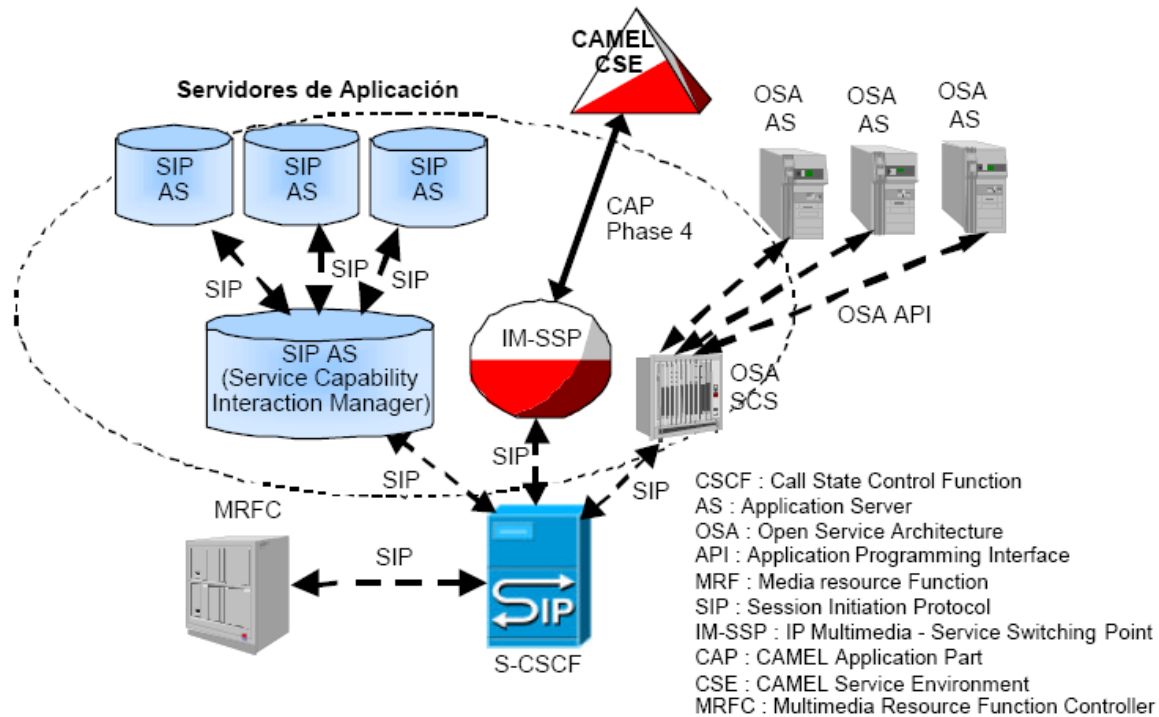


Figura 4. Arquitectura de Servicios de IMS

C.4. Beneficios de IMS

La arquitectura IMS no está confinada al soporte de telefonía Internet. También es la base de una amplia gama de nuevos servicios que enriquecen las interacciones y experiencias de un usuario. Como se basa en Internet y controla las sesiones SIP, IMS puede integrar APIs de alto nivel necesarias para desarrollar e invocar aplicaciones, enriqueciendo por ello las comunicaciones multimedia SIP.

- Facilita la introducción rápida de servicios a través de las interfaces estandarizadas entre IMS y las plataformas de servicios. Esto promueve la innovación y el desarrollo de nuevas aplicaciones por parte de terceros.
- Es independiente de la red de acceso. La comunicación puede ser a través de una red móvil como a través de una red fija. Esta ventaja abre la puerta para una integración de redes móviles con redes fijas.
- Los recursos de la red pueden ser compartidos por todos los servicios. Por ejemplo, los MRFPs y los MGWs pueden ser utilizados por diferentes aplicaciones ya que son controlados centralmente por sus respectivas funciones dentro de IMS. Esta ventaja puede llegar a reducir el costo de inversión en plataformas.
- IMS permite la coordinación y sincronización efectiva de varios medios en una sesión o en varias sesiones a través del controlador central (CSCF). Esto le puede proporcionar una experiencia más enriquecida al usuario al permitir que el



subscriber inicie varias sesiones o una sesión entre diferentes contactos con diferentes medios, por ejemplo, una sesión con audio, otra con video, otra con texto, etc.

- Hace posible la interacción e integración de servicios. Por ejemplo, un usuario puede tener el servicio walkie-talkie móvil y el de mensajería instantánea y lanzarlos desde una misma aplicación en su terminal y combinarlos como quiera en una sesión.



C. PASARELA DE SEÑALIZACIÓN PARA ACCESO A CAPACIDADES IMS DESDE CLIENTES SIP-IETF - i23GW

C.1. Consideraciones Preliminares al desarrollo del Sistema i23GW

Para el diseño y desarrollo de i23GW se tuvieron en cuenta los siguientes valores de entrada:

- Lista de métodos definidos por la IETF para el protocolo SIP en el RFC 3261 [1]. Además, las consideraciones para el flujo de estos métodos SIP en el Registro, Suscripción y Establecimiento de Sesión básico.
- Lista de métodos SIP definidos conjuntamente por el 3GPP y la IETF para IMS. De igual manera, la secuencia con que estos métodos son empleados en el Registro, Suscripción y Establecimiento de Sesión con una red IMS. Esta información ha sido referida al TS 24.228 [2].
- Lista de las capacidades de IMS que se piensan acceder por clientes SIP-IETF mediante i23GW, y su relación con las cabeceras adicionadas por el 3GPP a SIP para IMS.
- Diferencias técnicas entre la definición SIP-IETF y el perfil SIP-3GPP.

Las tareas que debe realizar i23GW para lograr una completa adaptación entre los mensajes SIP-IETF y SIP-3GPP, se mencionan a continuación:

- Conectarse tanto con la red IMS, como con los clientes SIP-IETF que hagan la solicitud de conexión.
- Guardar los mensajes SIP entrantes en un Objeto Java, el cual pueda ser utilizado posteriormente para la modificación de dichos mensajes.
- i23GW debe identificar qué tipo de mensaje ha sido guardado en dicho objeto Java, ya sean mensajes provenientes de la red IMS o de los clientes SIP-IETF.
- i23GW debe identificar qué tipo de método representa al mensaje entrante, ya sean métodos de Respuesta o de Solicitud.
- i23GW implementa funciones Java para la modificación de los mensajes entrantes. Esto se realiza para los mensajes SIP provenientes de la red IMS, y para los mensajes producidos en los clientes SIP-IETF.

Los valores de salida de la pasarela i23GW están representados en términos de los mensajes SIP modificados, tanto los que son enviados hacia la red IMS, como aquellos que son dirigidos hacia los clientes SIP-IETF. Además, esta modificación y posterior envío de mensajes, debe verse reflejado en el acceso a las capacidades de registro, suscripción y establecimiento de sesiones de IMS.

C.2. Descripción General de las Clases pertenecientes al prototipo i23GW

La figura 1 ilustra los paquetes pertenecientes a la aplicación i23GW, las clases contenidas dentro de estos paquetes, y la relación existente entre dichas clases.

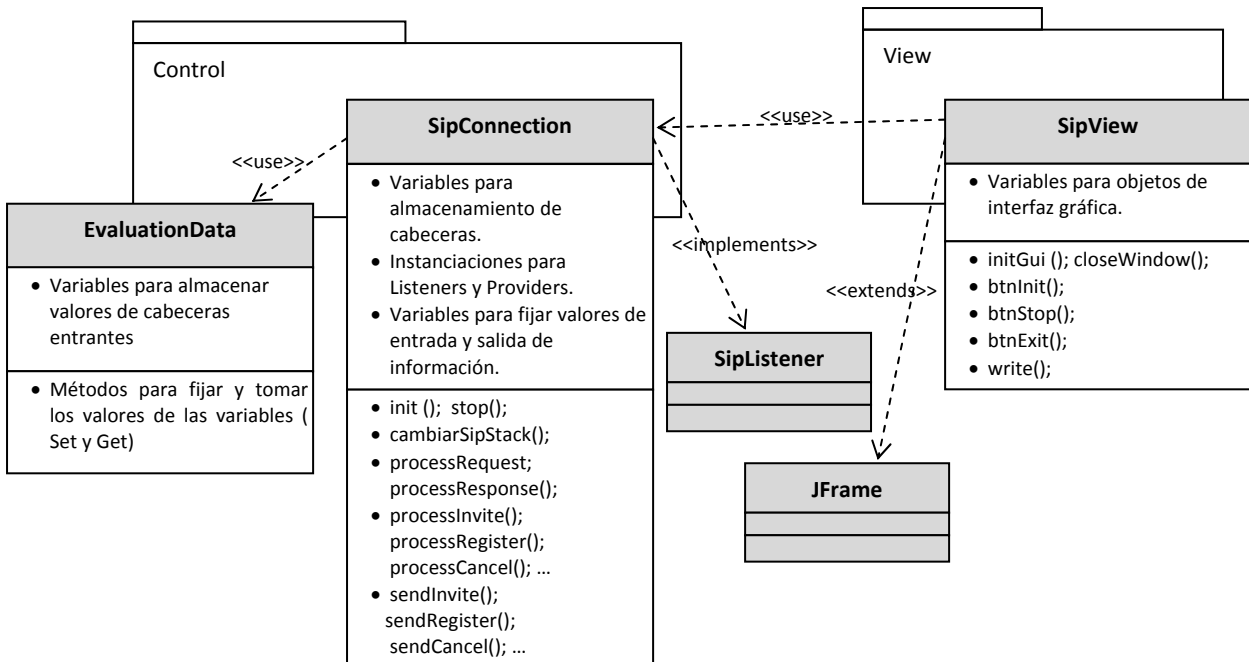


Figura 5. Diagrama de Clases del prototipo i23GW

- **SipView**

Paquete: View

Descripción: Clase encargada de implementar la interfaz gráfica de la aplicación. Implementa métodos para la carga de los botones y demás elementos gráficos en la aplicación, además de gestionar los eventos producidos en la interfaz. Extiende de la Clase JFrame perteneciente a la librería javax.swing.

- **EvaluationData**

Paquete: Control

Descripción: Clase usada por SipConnection. Es instanciada cada vez que entra un mensaje SIP a la pasarela, y se realiza con el objetivo de almacenar los valores de algunas cabeceras SIP, para posteriormente modificar su contenido, y evaluar si los mensajes entrantes se repiten.

- **SipConnection**

Paquete: Control

Descripción: Implementa de la clase SipListener, de la librería javax.sip. Esta clase está encargada de las funciones más importantes de i23GW, como la conectividad SIP, el procesamiento de los mensajes entrantes, el envío de los mensajes SIP modificados. Contiene métodos processRequest() y processResponse(), los cuales capturan los eventos entrantes, tanto para solicitudes, como para respuestas SIP. Posee también algunos métodos denominados *send* (sendRegister(), sendInvite(), send401(), etc), los cuales se encargan de modificar los mensajes SIP, dependiendo del tipo de salida que se desea generar, y además, se encargan de enviar los mensajes modificados.

C.3. Descripción de las Herramientas y Manual para la Instalación del Sistema

En este apartado se mencionan cuáles fueron las herramientas utilizadas en la creación y puesta en marcha del prototipo i23GW. Una de las principales consideraciones abordadas en la escogencia de dichas herramientas, ha sido la asequibilidad de las mismas. Generalmente en un entorno académico, resultan de gran utilidad las herramientas de libre distribución, y más aquellas que son abiertas a modificaciones.

C.3.1. Descripción General de las Herramientas utilizadas

La figura 2 ilustra las herramientas con que han sido creadas o puestas en marcha cada una de las componentes generales del sistema.

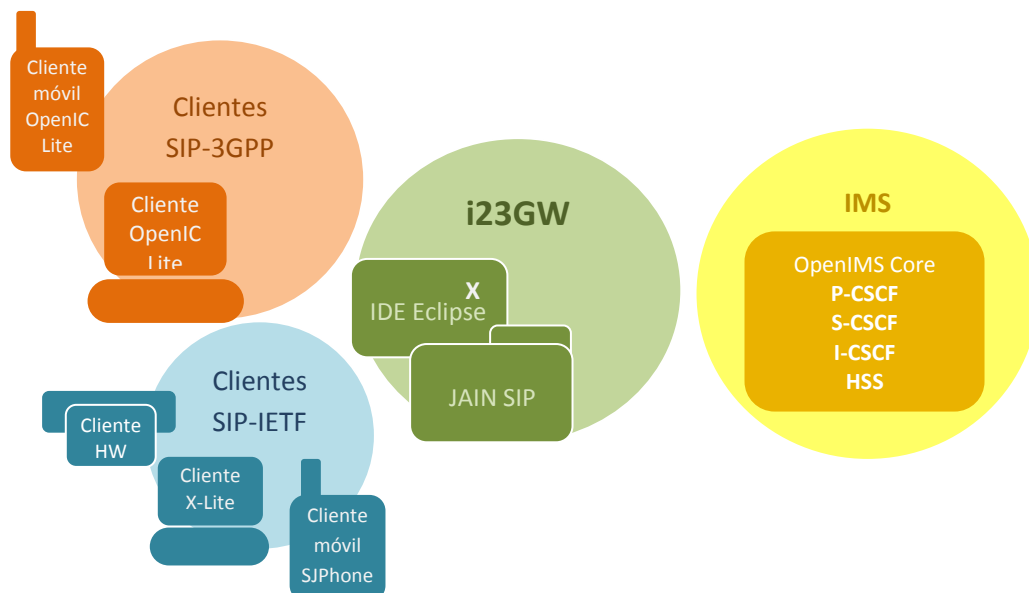


Figura 6. Herramientas utilizadas para cada entidad del sistema



C.3.2.1 Herramientas para Clientes SIP-IETF

La definición inicial del protocolo SIP, realizada por la IETF, ha sido utilizada de manera muy amplia por gran parte de los desarrolladores de tecnologías de telecomunicaciones, en especial, aquellos que se han involucrado en el mercado de la Voz sobre IP (VoIP). Esto, gracias a que el protocolo es sumamente extensible, y puede ser adaptado a las necesidades de implementación y comunicación que los desarrolladores puedan tener. Estas necesidades generalmente se ven reflejadas en el tipo de servicio que la red proporciona, y en la responsabilidad que tiene el protocolo SIP sobre dicho servicio.

A pesar de la extensibilidad de SIP, y de los múltiples perfiles para este protocolo que han surgido en la actualidad, la más universal de las definiciones sigue siendo la realizada por la IETF en el RFC 3261[1]. Para representar este tipo de clientes dentro del sistema propuesto en la arquitectura general, y verificar que efectivamente pueden acceder a las capacidades de IMS, se han escogido dos clientes de libre distribución, tanto para funcionar en un ambiente fijo de Internet, como para funcionar dentro de un dispositivo móvil con conectividad inalámbrica. Estos dos clientes son, respectivamente, X-lite [3] y SJPhone [4]. X-lite es un teléfono SIP Software (Softphone) construido por la firma CounterPath con el objetivo de poner en el mercado una versión libre del también popular producto bajo cargo, EyeBean, conservando las características de calidad de servicio (QoS) en la voz y el video de este producto. Con X-lite se pueden realizar distintas tareas multimedia, tales como conferencia de voz y video, gestión de presencia y mensajería instantánea.

SJPhone es una iniciativa de SJLabs Inc., la cual se constituye en la mejor alternativa para realizar pruebas sobre distintos sistemas operativos, ya que contiene perfiles para Windows XP/2000, Windows Mobile, Windows CE, Linux y MAC. SJphone es un teléfono VoIP Software que permite establecer comunicaciones SIP con cualquier Softphone que corra sobre un computador o dispositivo móvil. Es completamente interoperable con cualquier red fija o móvil, y soporta la interacción con la mayoría de los proveedores de VoIP y con los Proveedores de Servicios de Telefonía en Internet (Internet Telephony Service Provider - ITSP).

C.3.2.2 Herramientas para clientes SIP-3GPP

A pesar de que IMS se constituye como una tecnología relativamente nueva, existe una gran lista de productos de libre distribución y comerciales que se han introducido en el mercado para funcionar con redes basadas en esta arquitectura. Algunos de ellos son:

- HelloSoft [5]: Ampliamente testado para interactuar con la mayoría de las redes basadas en IMS
- Agile Mobile Sip Client [6]: útil en múltiples sistemas operativos. Licencia comercial.
- Mercurio IMS Client [7]: Softphone compatible con SIP/3GPP/IMS y RCS.
- OpenIC Lite, PC y móvil [8]: Desarrollado por Fokus Group, con el objetivo de interactuar con el core de IMS implementado por este mismo grupo.



De todos los clientes considerados para las pruebas de registro, subscripción y establecimiento de sesiones SIP, fue escogido OpenIC lite, para producir el tráfico SIP-3GPP necesario. Esta elección se realizó, gracias a que OpenIC lite es un software de libre distribución que ha sido orientado especialmente a trabajar con el Open IMS Core, el cual corresponde a la herramienta de red utilizada para representar la red IMS requerida en las pruebas del prototipo.

C.3.2.3 Herramientas para la Creación de i23GW

El Entorno Integrado de Desarrollo (Integrated Development Environment - IDE) escogido para el desarrollo de i23GW, ha sido Eclipse. Ésta es una herramienta de libre distribución y código abierto que permite la creación de múltiples aplicaciones basadas en Java, además de distintas plataformas y lenguajes de programación. Eclipse posee la capacidad de integrarse con múltiples funcionalidades añadidas, mejor denominadas Plugins, las cuales interactúan con las tareas básicas del IDE. Esto hace del IDE una herramienta extensible y muy útil en el desarrollo de aplicaciones que requieran conectividad, ya que interactúa de manera precisa con el Kit de Desarrollo Java (Java Development Kit - JDK), y por lo tanto, con las Interfaces de Programación de Aplicación (Application Programming Interface - API), entre ellas, la más utilizada para la creación de i23GW: JAIN SIP (Java API for Integrated Networks SIP).

JAIN SIP contiene la mayor parte de las cabeceras y extensiones de SIP definidas en las distintas especificaciones del protocolo (RFC 3261 [1], TS.24228 [2], 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 [9], destinadas preferiblemente al desarrollo de herramientas 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.

C.3.2.4 Herramientas para la representación de una red IMS

Una de las herramientas más importantes para probar los resultados de i23GW, es aquella correspondiente a la red basada en la arquitectura IMS. Esta importancia radica en que la herramienta utilizada debe soportar las capacidades de IMS que se pretenden alcanzar desde clientes SIP-IETF mediante i23GW, debido a que ese es centro de estudio del presente proyecto. Por lo tanto, se evaluaron varios sistemas desarrollados por organizaciones comerciales e investigativas con el fin de encontrar uno de ellos que se ajustara en mayor medida a los requerimientos del 3GPP dentro de una red IMS. Algunos de estos sistemas evaluados son:

- Service Development Studio (SDS) de Ericsson [10]. Esta es una herramienta de desarrollo de aplicaciones convergentes IMS para cliente y servidor. Contiene también un sistema completo de simulación de red IMS, con emuladores de servicios de comunicación. Esta herramienta está integrada con el lenguaje Java, y el IDE Eclipse, y permite agregar APIs tales como la diseñada para IMS, descrita



en el JSR 281. A pesar de que es una herramienta de libre distribución, no es tenida en cuenta para las pruebas de i23GW, debido a que corresponde más a una herramienta de desarrollo de servicios que a una plataforma sobre la cual dichos servicios IMS puedan ser desplegados.

- OpenIMS Core [11]. Esta es una implementación desarrollada por Fokus Group, para la Función del Control de Sesión de Llamada (Call Session Control Function - CSCF) y para Servidor de Subscriptor Local (Home Subscriber Server - HSS). Es una herramienta de libre distribución, que permite hacer un control de subversiones, de tal forma que los avances desarrollados para ella por el Fokus Group pueden ser automáticamente agregados a la versión inicialmente instalada. OpenIMS Core corresponde a una solución práctica y adecuada para la representación de la red IMS dentro de la arquitectura general del sistema en que actuaría i23GW, gracias a que es una herramienta de libre distribución que se relaciona especialmente con la definición que el 3GPP ha realizado para el tráfico SIP en IMS.

C.3.2. Manual de instalación de las Herramientas utilizadas

C.3.2.1 Instalación de X-lite:

- Descargar el archivo instalador del sitio: <http://www.counterpath.com/x-lite.html&active=4>. La actual versión más estable es la 3.
- Hacer doble clic en el archivo instalador.
- Aceptar los términos de licencia de usuario de CounterPath, escoger el directorio en el cual quedarán instalados los archivos, y fijar algunos valores sobre la ejecución del programa.

C.3.2.2 Instalación de SJPhone en un dispositivo móvil con Windows Mobile 5:

- Descargar el archivo instalador del sitio: <http://www.sjilabs.com/sjp.html> (también existen manuales de usuario y documentos de referencia en este sitio).
- Algunas de las versiones estables para PC de bolsillo son útiles en Windows Mobile 5. Se puede descargar directamente el archivo con extensión .CAB.
- Copiar el archivo .CAB a la memoria del dispositivo móvil y ejecutarlo allí, o ejecutarlo directamente desde el PC, mediante el uso de ActiveSync.
- Escoger la ruta de instalación y finalizar.

C.3.2.3 Instalación de Eclipse:

- Descargar el paquete completo del sitio: <http://www.eclipse.org/downloads/>.
- Descomprimir en el directorio donde se desea instalar.
- Correr los archivos ejecutables.



C.3.2.4 Instalación de JAIN SIP:

- Descargar las librerías del sitio oficial del proyecto JAIN: <https://jain-sip.dev.java.net/>
- Se deben descargar:
 - JainSipApi1.2.jar: Interfaces SIP, y clases principales.
 - JainSipRi1.2.jar: Implementación de referencia SIP.
 - log4j-1.2.8.jar (Disponible dentro del archivo jain-sip-1.2.jar bajo el directorio jain-sip/lib): Servicio de validación de usuario.
 - concurrent.jar (Disponible dentro del archivo jain-sip-1.2.jar bajo el directorio jain-sip/lib): Utilidades para concurrencia.
- Estas librerías se deben copiar en la carpeta lib del proyecto de i23GW, y se deben importar en el contenido de las clases que las necesitan.

C.3.2.5 Instalación del OpenIMS Core:

- Existe un manual para la instalación de OpenIMS Core en el sitio: http://www.openimscore.org/installation_guide
- El sistema está diseñado para funcionar sobre Linux, y se debe instalar previamente Subversion en el equipo.
- Crear la ruta: /opt/OpenIMScore
- Crear dentro de esta ruta un directorio: ser_ims.
- Crear también un directorio llamado FHoSS
- Dentro de ser_ims, hacer el chequeo de archivos con control de subversiones para la CSCF:
svn checkout http://svn.berlios.de/svnroot/repos/openimscore/ser_ims/trunk ser_ims
- De igual manera, dentro de la carpeta FHoSS, descargar los archivos necesarios con control de subversiones:
svn checkout <http://svn.berlios.de/svnroot/repos/openimscore/FHoSS/trunk> FHoSS
- Instalar los archivos necesarios dentro de ser_ims:
make install-libs all
- Instalar en el equipo una versión igual o más reciente del JDK 1.5.
- Hacer una compilación y despliegue con el paquete *ant* dentro del directorio FHoSS:
cd FHoSS
ant compile
ant deploy
- Para configurar el entorno de trabajo (DNS, IP, contraseñas de bases de datos) se debe utilizar el archivo de configuración: ser_ims/cfg/configurator.sh:
pwd
/opt/OpenIMScore
ser_ims/cfg/configurator.sh ser_ims/cfg/scscf.cfg ser_ims/cfg/icscf.xml \
FHoSS/deploy/hss_db.sql FHoSS/deploy/hss.properties
- Se debe crear un DNS local, de tal forma que se pueda utilizar un nuevo nombre de dominio para el servidor de IMS.
- Con el FHoSS se instalan bases de datos en MySQL, las cuales pueden ser verificadas después de correr los siguientes scripts sql:
mysql -u root -p -h localhost < ser_ims/cfg/icscf.sql

```
mysql -u root -p -h localhost < FHoSS/scripts/hss_db.sql  
mysql -u root -p -h localhost < FHoSS/scripts/userdata.sql
```

- Revisar los valores de DNS e IP para los archivos de configuración tanto de la CSCF, como del FHoSS. Estos archivos se encuentran dentro de la carpeta `ser_ims/cfg/` y `FHoSS/deploy/`, respectivamente.
- Con el cumplimiento de todos estos pasos, la CSCF y la FHoSS quedan disponibles para funcionar en el dominio e IP especificados. Ahora se pueden gestionar los parámetros de registro de la red IMS y de los usuarios en la interfaz Web para gestión: `http://host:8080/hss.web.console/`

C.4. Manual de Usuario para la Puesta en Marcha de la Aplicación i23GW

C.4.1. Entorno utilizado para la Puesta en Marcha de la Aplicación i23GW

En la figura 3 se muestra el entorno utilizado para poner en marcha la aplicación de i23GW. Este entorno ilustra todas las entidades de prueba utilizadas, teniendo en cuenta la IP asignada a cada entidad, y el dominio al cual pertenece cada una de ellas.

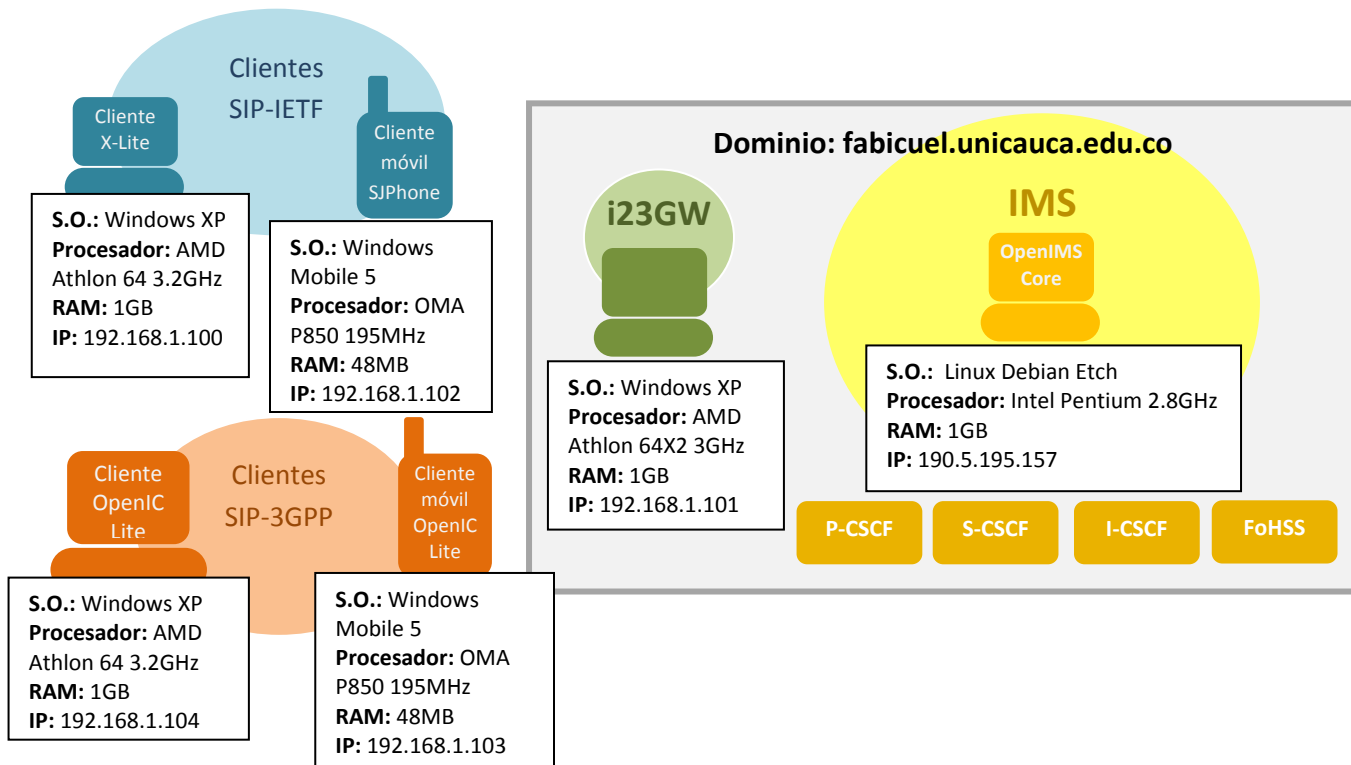


Figura 7. Entorno de Pruebas

C.4.2. Configuración de X-lite para funcionar con i23GW

Habiendo instalado el cliente X-lite correctamente, se puede proceder a configurarlo de tal manera que éste pueda reconocer la i23GW. Primero se debe hacer clic derecho sobre la pantalla de despliegue del cliente, y SIP Account Settings. Se desplegará una ventana tal como la mostrada en la figura 3.

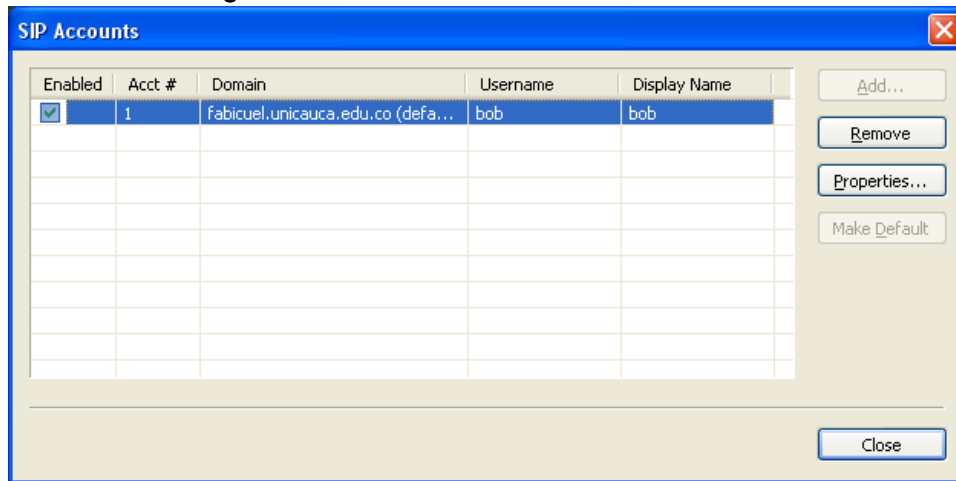
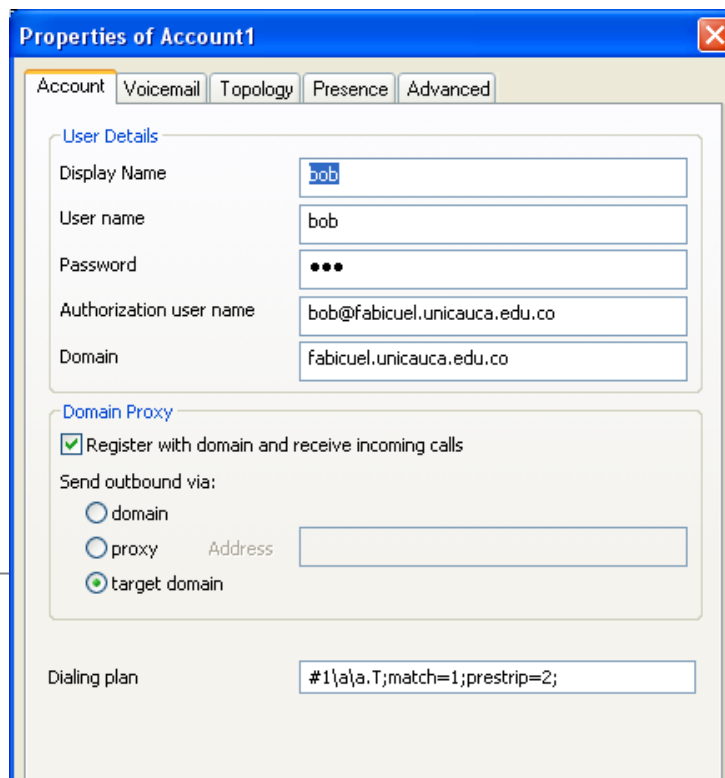


Figura 8. Configuración de cuenta X-lite 1

Si existe una cuenta de usuario anteriormente creada, ésta se puede modificar haciendo clic en el botón Properties... Si se desea agregar una nueva cuenta, se puede hacer clic en Add... En cualquiera de estos casos, los valores que debería tener una cuenta con la que se va a conectar a i23GW se muestran en la figura 4. Para este caso, el dominio de i23GW es fabicuel.unicauca.edu.co, igual que el dominio con que se ha configurado la red IMS. Para el ejemplo de la figura 4, se ha configurado el cliente X-Lite con un nombre de usuario "bob", de la misma manera que la contraseña.





C.4.3. Configuración

Figura 9. Configuración de Cuenta X-lite 2

Al tener instalado correctamente en el dispositivo móvil el cliente SJPhone, se puede proceder a configurarlo para que éste funcione de manera adecuada con i23GW. La configuración empieza por desplegar el “menú”, y escoger “Options”. Allí se pueden fijar los valores generales para el usuario, tales como e-mail, nombre, etc. También se puede escoger la opción “Profiles”, donde se puede modificar un perfil existente, o crear uno nuevo. Un perfil útil para conectar el cliente con la i23GW sería el siguiente:

- En “General”: fijar cualquier nombre de perfil, en tipo de perfil escribir SIPProxy, y los otros valores pueden ser arbitrarios.
- En la pestaña “SIP Proxy”: en el campo Proxy Domain escribir fabricuel.unicauca.edu.co con puerto 5060. En User Domain poner fabricuel.unicauca.edu.co. Señalar la opción de registrar con proxy y la de proxy como estricta salida.

De esta manera el cliente intentará registrarse con i23GW al ser ejecutado o reiniciado.

C.4.4. Puesta en marcha de OpenIMS Core

Teniendo los módulos de CSCF y FHoSS correctamente instalados, se puede proceder a iniciar uno por uno ejecutando los siguientes comandos en la consola Linux.

Para arrancar la P-CSCF:

```
cd /opt/OpenIMSCore/  
sh pcscf.sh
```

Para iniciar la S-CSCF:

```
cd /opt/OpenIMSCore/  
sh scscf.sh
```

Para iniciar la I-CSCF:

```
cd /opt/OpenIMSCore/  
sh icscf.sh
```

Para iniciar el FHoSS:

```
cd /opt/OpenIMSCore/FHoSS/deploy/  
sh startup.sh
```

C.4.5. Puesta en marcha de i23GW

- Abrir el IDE Eclipse
- Abrir el proyecto de i23GW
- En el paquete view se encuentra la clase SipView, sobre la cual se debe hacer clic derecho, y luego, Run As ... Java Application
- Se despliega la ventana de consola para i23GW, como se muestra en la figura 5.

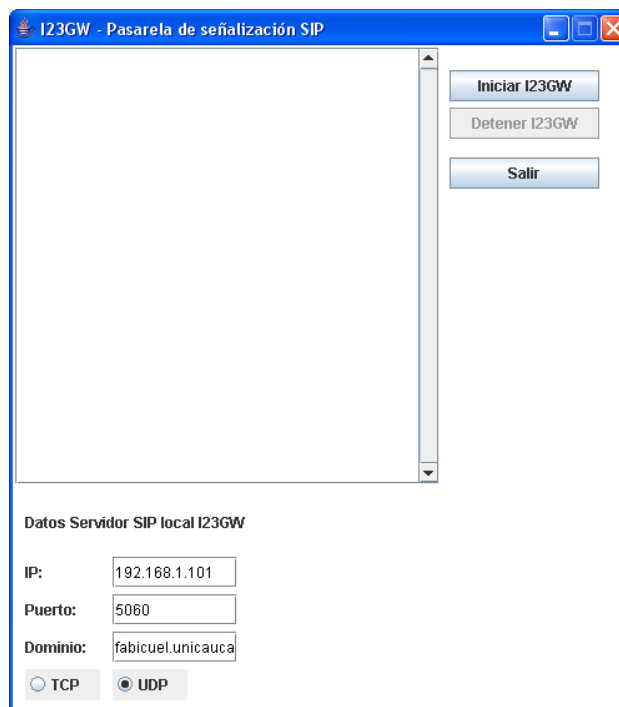


Figura 10. Configuración inicial de i23GW

- Los valores con que debe ser configurada la i23GW son los siguientes. IP: ip del equipo donde está instalada i23GW. Puerto: en el cual va a recibir las solicitudes y respuestas SIP, también está habilitado el puerto 6060, para pasar mensajes hacia la S-CSCF del core. El dominio debe ser el mismo con que se ha configurado el OpenIMS Core, para no causar traumatismos en el contenido de los mensajes SIP enviados. Esta igualdad entre los dominios utilizados para i23GW y OpenIMS Core se realiza mediante la ubicación de la pasarela dentro del mismo servidor de dominio de la red IMS, o creando un espejo de este dominio, mediante la configuración de un servidor de dominio local, que direcciona el dominio deseado hacia la IP 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] (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)
- [3] (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).
- [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] (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).
- [6] (RFC) R. Sparks (2003); “*The Session Initiation Protocol (SIP) Refer Method*”; IETF RFC 3515; Disponible en: <http://www.ietf.org/rfc/rfc3515.txt> (Visitada en julio de 2008).
- [7] (RFC) B. Campbell, J.Rosenberg, H. Schulzrinne (2002); “*Session Initiation Protocol (SIP) Extensions for Instant Messaging*”; IETF RFC 3428; Disponible en: <http://www.ietf.org/rfc/rfc3428.txt> (Visitada en septiembre de 2008).
- [8] (RFC) S. Donovan (2000); “*The SIP Info Method*”; IETF RFC 2976; Disponible en: <http://www.ietf.org/rfc/rfc2976.txt> (Visitada en septiembre de 2008).
- [9] (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).
- [10] (RFC) J.Rosenberg (2002); “*The SIP UPDATE Method*”; IETF RFC 3311; Disponible en: <http://www.ietf.org/rfc/rfc3311.txt> (Visitada en julio de 2008).
- [11] (RFC) F. Yergeau (1998); “*UTF-8 A transformation format of ISO 10646*”; IETF RFC 2279; Disponible en: <http://www.ietf.org/rfc/rfc2279.txt> (Visitada en agosto de 2008).