DISEÑO DE UN MÓDULO DE CONTROL DE SESIONES DE USUARIO BASADO EN LA ARQUITECTURA DE SERVICIOS IMS PARA EL DESPLIEGUE DE APLICACIONES Y/O SERVICIOS EN REDES DE TELEFONÍA MÓVIL

GLORIA CAROLINA BENAVIDES CABRERA

MARYURY ALEXANDRA MUÑOZ BURBANO

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELEMÁTICA
POPAYÁN, OCTUBRE DE 2006

DISEÑO DE UN MÓDULO DE CONTROL DE SESIONES DE USUARIO BASADO EN LA ARQUITECTURA DE SERVICIOS IMS PARA EL DESPLIEGUE DE APLICACIONES Y/O SERVICIOS EN REDES DE TELEFONÍA MÓVIL

GLORIA CAROLINA BENAVIDES CABRERA

MARYURY ALEXANDRA MUÑOZ BURBANO

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

Director
JAVIER ALEXANDER HURTADO
Ingeniero en Electrónica y Telecomunicaciones

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELEMÁTICA
POPAYÁN, OCTUBRE DE 2006

AGRADECIMIENTOS

Nuestros agradecimientos a la Universidad del Cauca, institución que nos forjo como personas brindándonos la oportunidad a través del programa de Ingeniería de Electrónica y telecomunicaciones para realizar nuestros estudios de pregrado.

Al ingeniero Javier Alexander Hurtado por su dirección, a la Ing. Mary Cristina Carrascal por su colaboración en los momentos en que lo requerimos.

Agradecemos también a Telefónica por la información suministrada. En especial a Luis Angel Galindo experto especial de tecnologías de red de Telefónica España,. MBA de la escuela de negocios IESE. Participante activo del 3GPP, de la Unión Internacional de Telecomunicaciones (UIT) y la Asociación GSM. Galindo fue el gerente del proyecto IMS de Telefónica, donde tuvo la responsabilidad de coordinar todas las actividades relacionadas con esta arquitectura de red.

A nuestros compañeros y amigos de la universidad con los que tantos momentos compartimos.

En especial a nuestras familias, las cuales nos brindaron su apoyo incondicional. Muchas gracias.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

INTRODUCCION

Con la incorporación de los sistemas de telefonía móvil de la tercera generación (3G) se añaden a su vez novedosos servicios y aplicaciones multimedia por medio del protocolo IP que permite servicios de banda ancha. El objetivo de implementar IP es lograr conectividad con la mayor red de información y comunicación del mundo, además de abaratar costos y facilitar la integración de otras tecnologías de acceso.

Dentro de las tecnologías de tercera generación y como resultado de la cooperación entre varios organismos internacionales de estandarización, parece ganar aceptación el concepto propuesto por la arquitectura IMS (IP Multimedia Subsystem), producto del extenso trabajo que están realizando el 3GPP y TISPAN, para describir aspectos del núcleo de red (*core network*) en cuanto a las normas de movilidad. Las redes de próxima generación deberán respaldar una amplia gama de tecnologías de acceso y servicios e IMS está diseñado para satisfacer este requisito.

En el proceso de estandarización de IMS se encuentra incluida la estructuración de la señalización necesaria para el control de las sesiones de Usuario con el protocolo SIP.

Durante el desarrollo de este trabajo de grado se realizó una amplia investigación de la arquitectura IMS y de la señalización con el protocolo SIP con el propósito de llegar al diseño de la arquitectura e implementación de un Módulo de Control de Sesiones de Usuario MCSU, en el cual se procesarán los mensajes indispensables para el registro, inicio y terminación de una sesión.

1 IP MULTIMEDIA SUBSYSTEM IMS [1]

1.1 CONCEPTOS GENERALES DE IMS [2][3][4]

La arquitectura IMS facilita la convergencia de redes y servicios de nueva generación y actualmente está siendo definida por operadores que quieren continuar suministrando servicios de telefonía cuando sus redes clásicas sean sustituidas por Internet.

IMS es una arquitectura completamente nueva que proporciona varios elementos para llevar a cabo funciones tales como roaming, desvío y filtrado de llamadas, llamadas telefónicas con contenidos de voz y datos e Internet extremo a extremo.

Al no estar limitada por la telefonía clásica, la arquitectura IMS puede valerse completamente de la tecnología Internet y de su entorno, por ser de gran flexibilidad y por esta razón se puede integrar con otros servicios de Internet, como navegación por la web y aplicaciones de difusión.[6]

1.2 ARQUITECTURA IMS [5]

1.2.1 Arquitectura general [9][10][11][12]

Los estándares de IMS definen un dominio de red dedicado al control y a la integración de servicios multimedia. La arquitectura consta de una serie de funciones lógicas que emplean el protocolo de señalización llamado SIP (Session Initiation Protocol). Este protocolo sirve para establecer sesiones en una red IP.

El subsistema IMS presenta una arquitectura horizontal en capas que permite separar cada una de las funcionalidades específicas, proporcionando flexibilidad e independencia de las tecnologías de acceso. La flexibilidad se logra por la división de su arquitectura en

tres capas o niveles funcionales, como se muestra en la figura 1, cada una dedicada a brindar una funcionalidad específica**:**

- Nivel de aplicaciones y servicios
- Nivel de control
- Nivel de acceso y transporte

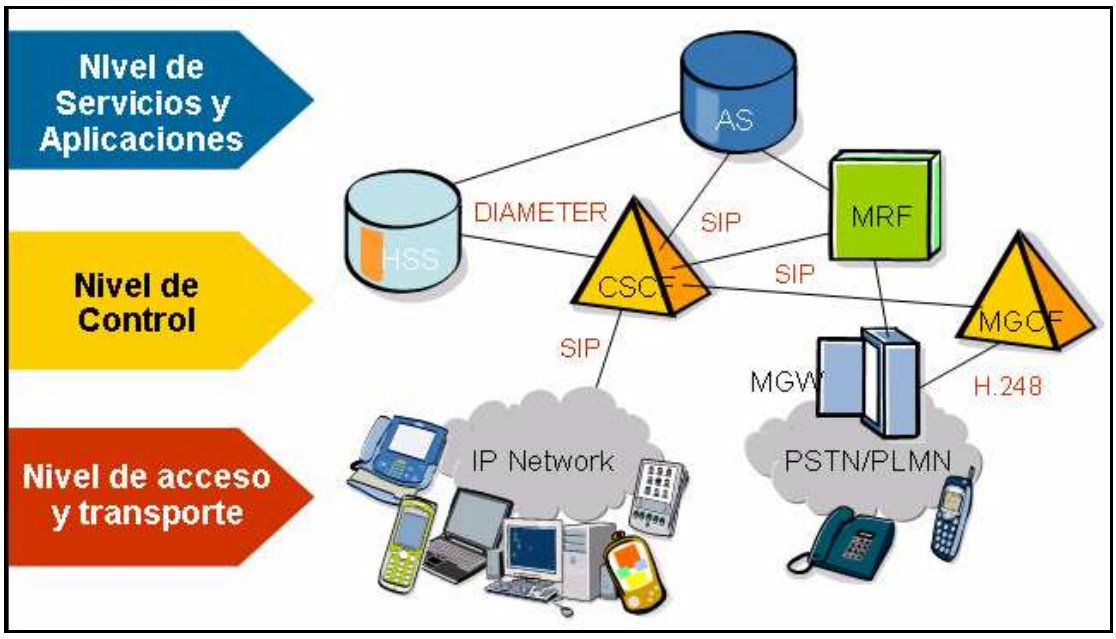


Figura 1. Arquitectura general de IMS[13]

1.2.1.1 Nivel de Aplicación y Servicios

En esta capa residen las aplicaciones a las que accede el usuario final y contiene múltiples servidores de aplicaciones, tales como servidores de aplicaciones de telefonía (TAS), función de conmutación de servicios IP Multimedia (IM-SSF), La Gateway para acceder a servicios Parlay (OSA-GW), servidores SIP etc., servidores que ejecutan múltiples servicios y aplicaciones IMS manejando señalización SIP e interactuando con otros sistemas.

El AS SIP es un servidor de aplicaciones IMS "puro", en cambio, IM-SSF y OSA GW son definidos como interfaces para los servidores de aplicaciones heredados como CAMEL (Customized Applications for Mobile network Enhanced Logic)[14].

Cada servidor es responsable de ciertas funciones en las diferentes sesiones con el propósito de mantener el estado de la llamada. Estos servidores de aplicaciones son complementados frecuentemente con servidores de contenido, que tienen bases de datos o bibliotecas relacionadas con los servicios.

Los servidores de aplicaciones también pueden incluir capacidades HTTP, permitiendo realizar el papel de un servidor de contenido. Típicamente, los AS ofrecerán un lenguaje de programación y un *framework* para crear nuevos servicios, por ejemplo Java SIP y *Servlets* HTTP.

Las estrategias a nivel de aplicación adquirirán mayor importancia con el despliegue de IMS, que con su llegada va a animar a la industria de las telecomunicaciones a cambiar de estructura vertical de acceso a las tecnologías, por una arquitectura horizontal con énfasis en aplicaciones y servicios.

Este nivel proporciona los medios para que los operadores puedan ganar una ventaja competitiva ofreciendo a los suscriptores servicios de valor agregado, atractivos e innovadores para los usuarios finales.

1.2.1.2 Nivel de control

El nivel de control es una parte fundamental de la red, en esta capa se llevan a cabo procesos de administración que involucran elementos de las otras capas, convirtiéndose en el eje central de la arquitectura IMS.

La capa del control de la red IMS consiste en los nodos para el establecimiento, administración y control de la red. Esta capa proporciona la coordinación total de medios

y recursos para proveer toda la funcionalidad que se necesita para brindar servicios de alta calidad.

Contiene los dos elementos más significativos de la red IMS: uno de ellos es el corazón de este nivel y es llamado "función de control de sesiones de llamada" (CSCF); toda la señalización SIP atraviesa este importante nodo. EL CSCF es el encargado de examinar cada mensaje SIP y determinar si la señalización debería ir a uno o más servidores de aplicaciones SIP antes de dirigirse a su destinatario final. Interactúa con el plano de transporte para garantizar calidad en la prestación de todos los servicios.

El otro elemento de gran importancia es la base de datos del servidor del suscriptor (HSS) que mantiene los perfiles de usuario incluyendo los detalles del registro, así como preferencias y similares. El CSCF interactúa con el HSS, que proporciona un repositorio central de información relacionada con el usuario.

Otros elementos importantes de este nivel son la Pasarela de Medios (Media Gateway, MGW) y la Función de Control de la Pasarela de Medios (Media Gateway Control Function, MGCF). [5][15]

1.2.1.3 Nivel de Acceso y Transporte

Este nivel compromete diferentes redes de acceso, conectándolas con el corazón de la arquitectura IMS, mediante el empleo de gateways y servidores de control y puede soportar todo tipo de acceso de alta velocidad. Algunos ejemplos de redes de paquetes son GPRS, UMTS, "CDMA2000" tecnología de acceso de banda ancha usada en las redes móviles en Estados Unidos, XDSL, redes de cable, "Wireless IP", WIFI, etc., las PSTN son un ejemplo de redes de conmutación de circuitos.

La red de acceso consiste en routers IP y switches heredados de la PSTN que proveen acceso a las redes IMS. Los dispositivos IP compatibles con IMS incorporan un agente de usuario SIP que atiende llamadas de voz o vídeo para interactuar con otros usuarios.

Los usuarios están conectados con la infraestructura IMS por medio de la capa de acceso y transporte, o directamente a través de un terminal IMS (tal como un microteléfono inalámbrico 3G), o probablemente, o por lo menos para un futuro cercano, a través de un dispositivo no IMS que se interconecte con la infraestructura de IMS a través de una gateway.

Existen varias gateway que se encuentran dentro de esta capa, que tienen como función proporcionar interconexión entre IMS y redes externas. Por ejemplo, la MGF proporciona el intercambio de los medios entre la PSTN e IMS, convirtiendo los flujos de VoIP a formatos TDM para que sean entendibles por la PSTN.

En este nivel se encuentran componentes como el MRF, también llamado el servidor de los medios MS, el cual se divide en el MRFC y el MRFP, gateways de señalización, gateways de acceso, el SBC, y otros elementos cuyo propósito principal es conectar a la red IMS con otras redes.

Todos los elementos y funcionalidades de esta capa están pensados para lograr la convergencia de redes y servicios, objetivo que permitirá a los operadores prestar servicios nuevos y de valor agregado a los usuarios, sin dejar a un lado los servicios tradicionales soportados por las redes actuales.

1.2.2 Arquitectura detallada de IMS[1][4][16]

En la figura 2 se muestra la arquitectura detallada de IMS.

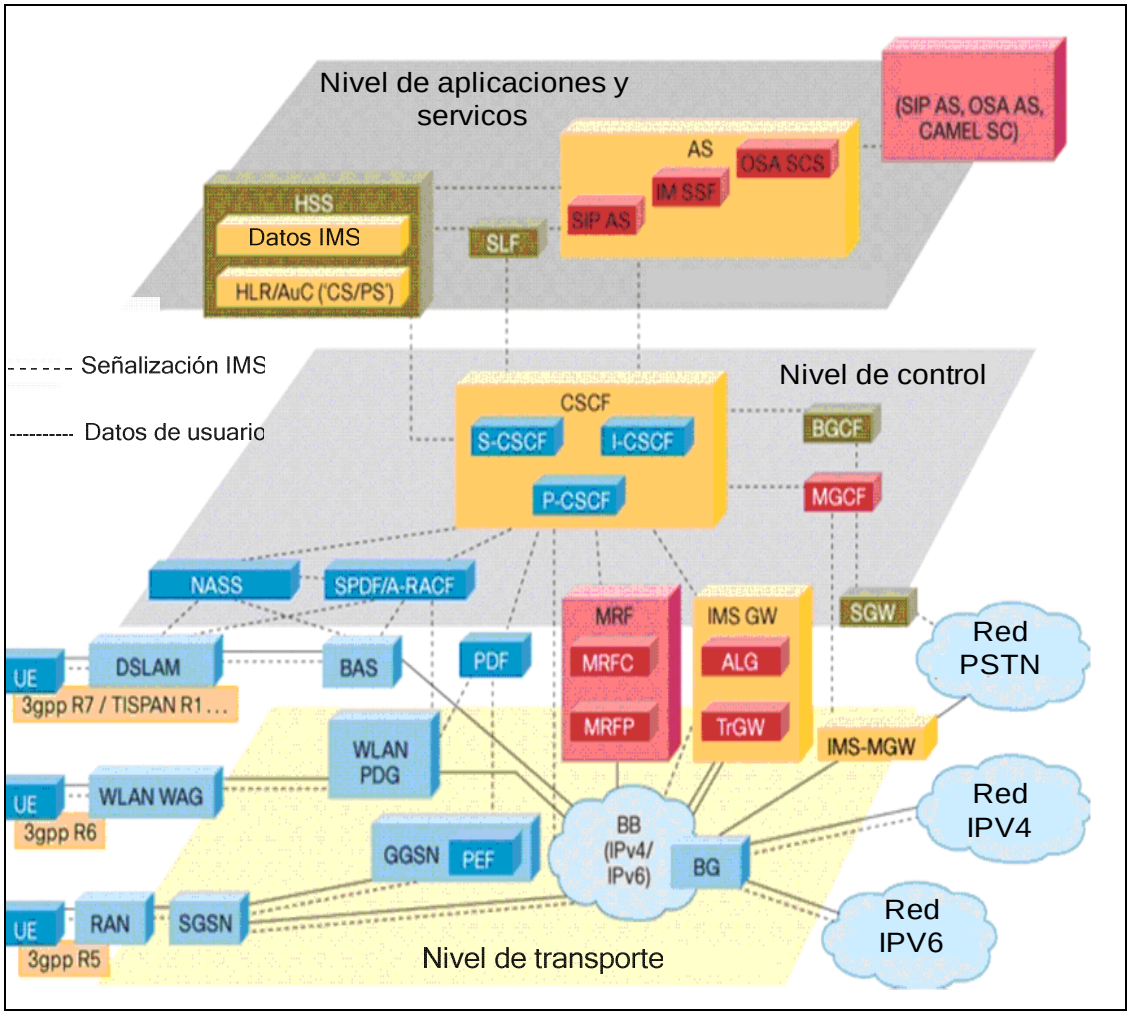


Figura 2. Arquitectura detallada de IMS[17]

En la figura anterior se puede ver la división en niveles, nivel de aplicaciones, de control y de transporte de la arquitectura IMS, además también se puede observar las entidades principales de cada uno de estos; a continuación se describirá los elementos principales de la arquitectura IMS, los demás componentes se describirán en el anexo A.

1.2.2.1 Call Session Control Function. [5][15][18]

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, guardados en el perfil de usuario que se almacena en el HSS, identificando e iniciando servicios residentes en los servidores de aplicaciones.

1.2.2.1.1 Proxy CSCF (P-CSCF)

El P-CSCF es el punto de entrada al subsistema IMS que recibe directamente la señalización IMS desde el terminal de usuario, esté en su red origen o visitada. El P-CSCF re-dirige los mensajes de SIP “REGISTER” y los mensajes de establecimiento de sesión a la red origen e implementa las funciones de protección de señalización y de control de recursos del subsistema de transporte.

En sesiones de itinerancia (Roaming), el P-CSCF es el nodo en la red visitada que se encarga del enrutamiento de la señalización de registro y de una sesión desde los terminales que se encuentran en situación de itinerancia hasta la red IMS nativa. Además, ejecuta las funciones comunes a los demás CSCF: el procesamiento y enrutamiento de la señalización, la compresión de los mensajes para reducir la latencia, la consulta del perfil de usuario en el HSS y crea la información de tarificación.

El P-CSCF tiene otras funciones. Una de ellas es ser el punto donde se ejerce la política de calidad de servicio dentro de la red IMS visitada. Otra responsabilidad es proporcionar el control local para los servicios de emergencia. También realiza asistencia telefónica de los planes locales de numeración bajo dirección del Serving-CSCF.

1.2.2.1.2 Interrogating CSCF (I-CSCF)

Es un nodo intermedio que da soporte a la operación IMS. El I-CSCF ayuda a otros nodos a determinar el siguiente salto de los mensajes SIP y a establecer un camino para la señalización. Durante el registro, el P-CSCF se ayuda del I-CSCF para determinar el S-CSCF que ha de servir a cada usuario.

Una de sus funciones principales es asignarle un Serving-CSCF a un usuario durante el proceso de registro, preguntándole al HSS por la localización de uno adecuado basándose en parámetros como capacidad y carga. Otra función importante es la redirección de las peticiones SIP durante una sesión al S-CSCF del usuario que envía dicha petición.

En situaciones de itinerancia y en sesiones entre redes, el I-CSCF es el punto de entrada conocido por la red IMS externa e indica el siguiente salto a realizar para la señalización. Opcionalmente, el I-CSCF efectúa funciones de encubrimiento de la topología de la red IMS ante redes externas, de forma que los elementos ajenos a IMS no puedan ver cómo se gestiona la señalización internamente (por ejemplo, el número, el nombre y la capacidad de los CSCF).

Un sistema podría ser configurado de modo que el P-CSCF pudiera entrar en contacto con el S-CSCF directamente. Como se ve, el I-CSCF realiza un balance de carga entre S-CSCFs con la ayuda del HSS. El I-CSCF, además, puede ocultar la configuración y topología específica de la red origen de otros operadores de red proporcionando un solo punto de entrada en la red; esta función es opcional en el I-CSCF y se denomina THIG (Topology Hiding Inter-network Gateway).

El I-CSCF puede también realizar algunas formas de tarificación. Si el I-CSCF es la entrada en la red origen, debe soportar funciones de *firewall.*

1.2.2.1.3 Serving CSCF (S-CSCF)

Es el elemento en servicio de la red con el cual se registran los abonados para poder ser encontrados durante la itinerancia. Este servidor almacena temporalmente los datos relacionados con el perfil de usuario, que son cargados desde el HSS cuando se hace el registro.

El S-CSCF realiza la gestión de las sesiones en la red IMS. Puede haber varios S-CSCFs en la red con varias funcionalidades. Se pueden añadir según las necesidades basándose en las capacidades de los nodos o en los requisitos de capacidad de la red. El S-CSCF en la red origen es el responsable de todo el control de la sesión, pero podría remitir la petición específica a un P-CSCF en la red visitada basándose en los requisitos de la petición.

El S-CSCF se puede elegir basándose en los servicios solicitados o en las capacidades del móvil. A cada usuario registrado en IMS se le asigna un S-CSCF el cual se encarga del enrutamiento de la señalización SIP de las sesiones iniciadas o destinadas al usuario. También realiza el registro y autenticación del abonado IMS y la provisión de los servicios. Así mismo aplica las políticas del operador de red previniendo el uso desautorizado de servicios y generando los registros de tarificación.

1.2.2.2 Home Subscriber Server (HSS)

El HSS es la base de datos principal para cualquier usuario dado, contiene la información relacionada con abonados necesaria para la gestión de llamadas o sesiones de las entidades de capa de control.

Esta base de datos contiene toda la información de los abonados móviles, inclusive datos dinámicos, tales como la localización del abonado y el estado de servicios suplementarios, y 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. [19]

Por ejemplo, el HSS interactúa 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 los abonados y almacena la identificación del nodo S-CSCF con el que el abonado se ha registrado. [8][20]

Además, el HSS proporciona las siguientes funciones:

- Funciones de localización de suscriptor

Esta función sigue "el rastro" de cada usuario y del dominio donde está ubicado en determinado momento. Cuando el usuario necesita de funciones de itinerancia, el servicio de localización devuelve la identidad del servidor S-CSCF donde se encuentra actualmente el suscriptor y proporciona mapas de direcciones de usuario para la PLMN (Packet and Public Land Mobile Network) e información almacenada como por ejemplo, el tipo de teléfono que cada cliente está utilizando y su localización cuando desea acceder a un servicio.

- Autenticación

Esta función es usada para autenticar y autorizar a usuarios, porque el HSS almacena las claves secretas para los suscriptores móviles.

- Funciones de análisis

Se usan funciones de análisis para examinar números de abonados móviles, tales como IMSI.

Como se dijo anteriormente, existen otros elementos dentro de la arquitectura IMS, que son tratados en el Anexo A.

2 SESSION INITIATION PROTOCOL[22]

El Protocolo de Inicio de Sesión SIP es un protocolo de señalización de nivel de aplicación definido por la IETF, utilizado para controlar sesiones en una red IP. SIP es similar a protocolos ampliamente utilizados en Internet como SMTP y HTTP y forma parte de las especificaciones del IETF para comunicaciones multimedia, conjuntamente con otros protocolos como RSVP, RTP, SDP, etc., pero en su funcionalidad no depende de ninguno de estos. [23]

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.[24]

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.[24] [25]

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[1] 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). Soporta direcciones IP y nombres con dominios (*DNS*); esto simplifica la manipulación y depuración de los mensajes.[23]

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 mas rápido de nuevos esquemas y tecnologías en el mundo de las comunicaciones multimedia sobre IP. [24]

Las funciones principales de SIP son: [26]

- Resolución de direcciones.

[1] ***Universal Character Set UCS*** *contiene todos los caracteres de todos los demás estándares de conjuntos de caracteres. Pueden construir tablas de conversión de tal forma que no se pierda ninguna información cuando una cadena se convierta desde cualquier otra codificación a* ***UCS*** *y viceversa.*

- Funciones relacionadas con la sesión: establecimiento, negociación de medios, modificación, terminación, cancelación, señalización en llamada, control de llamada, configuración de QoS.

- No relacionadas con la sesión: movilidad, transporte de mensajes, suscripción a eventos, autenticación, entre otras.

2.1 SIP e IMS [21]

El 3GPP adopta el protocolo SIP, el cual fue estandarizado inicialmente por el IETF y le hizo los ajustes necesarios para proveer soporte completo a los requerimientos de una red IMS, los cuales son básicamente la definición de varias extensiones. En conjunto estas extensiones enmarcan el protocolo SIP para la arquitectura IMS que son definidas en el estándar TS.24.229 del 3GPP.

SIP ha sido extendido con el fin de soportar numerosos servicios, tales como servicios de presencia, Push To Talk, mensajería instantánea, similar al servicio SMS en las redes móviles actuales, transferencia de llamada, conferencia, servicios complementarios de telefonía, etc., SIP ha sido elegido por el 3GPP para la arquitectura IMS como protocolo para el control de sesión y el control de servicio.

Por definición SIP no es un protocolo diseñado para una red o una aplicación específica. Para utilizar SIP, se debe definir un *Perfil de uso*. Los perfiles de uso trabajan como plantillas, y proporcionan un ambiente variado y flexible según los requisitos particulares.

El perfil de SIP que se creó para IMS es uno de los más importantes en ámbito de las telecomunicaciones, pues no solo involucra las redes móviles sino toda la industria de las telecomunicaciones en conjunto y según los expertos actualmente es el más apropiado para las redes de Nueva Generación, NGN.

2.2 CABECERAS DEL PROTOCOLO SIP PARA IMS[27] [28]

2.2.1 P Associated-URI [29]

La cabecera P-Associated-URI contiene la lista de identidades públicas que el usuario autoriza, es decir, contiene un conjunto de URI`s relacionadas con una dirección registrada (*address of record*).

La primera URI en la lista de las identidades públicas del usuario provista por el HSS al S-CSCF indica la identidad pública de usuario que el S-CSCF usará por defecto. Un servidor de registro (Registrar) contiene información que permite a una URI registrada *(address of record)* asociarse a cero o más URI´s, generalmente todas estas URI`s (address of record URI y las URI`s asocidas) se asignan a un usuario específico.

Esta extensión de SIP le permite al UAC (User Agent Client) saber, sobre un registro realizado, cuales son las URI`s asociadas, si las hay. Esta cabecera es aplicable en redes SIP, donde el proveedor asigna a un usuario un conjunto de identidades que podrá usar, en este caso el proveedor tendrá conocimiento de todas las identidades de cada usuario, tanto de las que tiene en uso, como las que tiene restringidas.

El servidor de registro inserta la cabecera P-Associated-URI en una respuesta “200 OK” de una petición “REGISTER”, cuyo valor del campo de cabecera se llena con las URI`s asociadas a la URI registrada (address of record). El servidor realiza este procedimiento para un REGISTER de un procedimiento de registro, de “re-registro” y de “de-registro”.

- Sintaxis

P-Associated-URI	= "P-Associated-URI" HCOLON (p-aso-uri-spec) *(COMMA p-aso-uri-spec)
p-aso-uri-spec	= name-addr *(SEMI ai-param)
ai-param	= generic-param

Tabla 1: Sintaxis de la cabecera P-Associated-URI

2.2.2 P-Called-Party-ID

Esta cabecera es insertada por un servidor proxy con el valor de la dirección lógica registrada de un usuario, típicamente en una petición INVITE, antes de sustituir este último con la dirección que va a utilizar para encaminar la petición al usuario. De este modo se asegura que el destino reciba la dirección lógica correspondiente a la petición.

- Sintaxis

P-Called-Party-ID	="P-Called-Party-ID" HCOLON called-pty-id-spec
called-pty-id-spec	name-addr *(SEMI cpid-param)
cpid-param	= generic-param

Tabla 2: Sintaxis de la cabecera P-Called-Party-ID

2.2.3 P-Visited-Network-ID

Esta cabecera es diseñada para realizar funciones necesarias para el roaming de los usuarios, cuando un usuario se traslada de su red home a una red visitada.

Además, es usada para transmitir el identificador de red visitada desde el servidor de registro al servidor Proxy de la “red home”, el identificador es entendido por el servidor de registro o proxy de la “red home” y por la red visitada. Generalmente, la “red home” autoriza a un usuario para entrar en una red visitada, siempre y cuando existan acuerdos de Roaming entre dichas redes.

- Sintaxis

P-Visited-Network-ID	="P-Visited-Network-ID" HCOLON vnetwork-spec *(COMMA vnetwork-spec)
vnetwork-spec	= (token / quoted-string) *(SEMI vnetwork-param)
vnetwork-param	= generic-param

Tabla 3: Sintaxis de la cabecera P-Visited-Network-ID

2.2.4 P Access-Network-Info

Esta cabecera contiene información sobre la red de acceso que el UA está utilizando, esta información es conocida por el UA y requerida por el Proxy a la hora de proveer los servicios.

El protocolo SIP fue pensado para trabajar independiente de la tecnología de acceso, por lo tanto esta información no es de uso general del protocolo SIP. Además, la información que se transporta en esta cabecera es fácilmente alterable, la protección de esta información depende de la existencia de acuerdos y relaciones de seguridad entre los servidores proxy que usarán el contenido de esta cabecera y depende también del conocimiento que el UA tenga de esas relaciones. Es por eso que este mecanismo es apropiado solo para ambientes donde existan elementos de seguridad apropiados.

Cuando un UA envía una solicitud o respuesta SIP al servidor proveedor de servicios, inserta esta cabecera en el mensaje SIP. La cabecera contiene información de la red de acceso que el UA está usando para tener conectividad IP. Generalmente, esta cabecera es ignorada por los servidores intermedios que se encuentran entre UA y el servidor proveedor del servicio. El servidor que provee el servicio puede “leer” y usar la información contenida en la cabecera y luego quita la cabecera del mensaje. Para borrar la cabecera también deben existir transacciones seguras entre el UA y el servidor que

provee los servicios, estas transacciones generalmente soportan mecanismos de seguridad como IPSec, AKA, y TLS (Transport Layer Security).

Un servidor proxy no es la entidad que inserta la cabecera y no debe hacerlo, tampoco debe modificar la información que ésta contiene. El servidor presta los servicios según el valor que contiene la cabecera, este provee diferentes servicios dependiendo de la red de acceso; por ejemplo, para una red de radio acceso el servidor SIP localizado en la "red home" puede usar el ID de la celda para proveer servicios de localización básica.

El servidor que provee los servicios al usuario generalmente esta ubicado en la "red home" y por lo tanto es confiable, entonces se debe borrar la cabecera cuando la señalización SIP es enviada a un servidor ubicado en un dominio poco confiable.

- Sintaxis

P-Access-Network-Info	="P-Access-Network-Info" HCOLON access-net-spec
access-net-spec	= access-type *(SEMI access-info)

Tabla 4: Sintaxis de la cabecera P-Access-Network-Info

2.2.5 P-Charging-Function-Addresses[30]

Esta cabecera contiene los nombres de los host o de las direcciones IP de los nodos que reciben la información de facturación. En esta cabecera se introduce una lista de direcciones de una o más entidades de facturación a las cuales un Proxy puede enviar información relacionada con la tarificación. La solución que provee el 3GPP define dos tipos de entidades funcionales de tarificación una es la CCF (Charging Collection Function) y la otra es ECF (Event Charging Function).

- CCF: es usada para cobro off-line para facturación de usuarios post-pago.[31]
- ECF: es usada para cobro on-line para facturación de usuarios pre-pago.[31]

La cabecera P-Charging-Function-Addresses no se incluye en los mensajes SIP enviados fuera del dominio de la red, tampoco si el domino no provee una función de facturación.

- Sintaxis

P-Charging-Addr	= "P-Charging-Function-Addresses" HCOLON charge-addr-params *(SEMI charge-addr-params)
charge-addr-params	= ccf / ecf / generic-param
ccf	= "ccf" EQUAL gen-value
ecf	= "ecf" EQUAL gen-value

Tabla 5: Sintaxis de la cabecera P-Charging-Function-Addresses

2.2.6 P-Charging-Vector[30][32]

Cabecera que proporciona información para poder correlacionar los registros de tarificación generados por cada una de las entidades de red involucradas en una misma sesión.

Existen tres tipos de información de correlación que se puede trasmitir: El valor de la identidad de tarificación de IMS llamada ICID (IMS Charging Identity), la dirección del servidor proxy SIP que crea el valor del ID y el IOI (Inter operador identifiers).

- ICID: Es usado para correlacionar archivos de tarificación y debe ser un valor único global.

- IOI: Se usa para identificar la red que origina y la de dónde finaliza una transacción SIP. Existe un parámetro IOI para cada lado de la transacción, es decir uno para la red origen llamado ori-IOI y otro para la red destino llamado term-IOI.

El vector de tarificación es definido como un recolector de información de tarificación que es usado para trasportar información de facturación, como por ejemplo el valor del ICID

♦ Sintaxis

P-Charging-Vector	= "P-Charging-Vector" HCOLON icid-value *(SEMI charge-params)
charge-params	= icid-gen-addr / orig-ioi / term-ioi / generic-param
icid-value	= "icid-value" EQUAL gen-value
icid-gen-addr	= "icid-generated-at" EQUAL host
orig-ioi	= "orig-ioi" EQUAL gen-value
term-ioi	= "term-ioi" EQUAL gen-value

Tabla 6: Sintaxis de la cabecera P-Charging-Vector

Más información de estas cabeceras se podrá encontrar en el RFC 3455 del IETF.[27]

2.3 SIP Y REDES 3G [33][34]

Las redes de tercera generación están utilizando tecnología IP punto a punto para entregar contenido multimedia a dispositivos móviles. El control de llamada y la función de señalización se realizan con SIP, debido a la adopción en gran escala de este protocolo y a la simplicidad y ubicuidad de la tecnología que éste utiliza para la realización de servicios.

Las redes de tercera generación están utilizando el protocolo SIP para el control de la llamada de las siguientes formas: SIP desde el terminal hacia la red, entre los nodos de llamada de la red y toda la señalización de llamadas multimedia IP será realizada por SIP

A través de la adopción de estas tecnologías las redes 3G podrán prestar servicios de forma rápida y a bajo costo, y además muchos desarrolladores tendrán la posibilidad de proporcionar más y mejores servicios.

Los usuarios serán identificados con URLs SIP y/o números E.164[2], el sistema de numeración de telefonía. El sistema portador (GPRS o IP móvil) manejará micro-movilidad, es decir, el desplazamiento del usuario móvil de una estación base a otra. SIP se encargará de la macro-movilidad, el desplazamiento del usuario móvil desde un dominio a otro.

[2] *E.164 Recomendación de la UIT (Unión Internacional de Telecomunicaciones) que describe el plan internacional de numeración telefónica.*

3 DISEÑO DEL PROTOTIPO DEL MÓDULO DE CONTROL DE SESIONES MCSU

Este módulo se desarrolló teniendo en cuenta las especificaciones técnicas del 3GPP para IMS que se encuentran en los documentos TS.24.228 y TS.24.229, donde se encuentra detalladamente los procedimientos necesarios para el procesamiento de los diferentes tipos de mensajes SIP y el control de las sesiones, además, el desarrollo también cumple con los requerimientos técnicos del RFC 3261 del IETF, donde se puede encontrar una explicación detallada del protocolo SIP.

3.1 DISEÑO DE LA ARQUITECTURA DEL MÓDULO MCSU

3.1.1 Descripción de la arquitectura del módulo

Teniendo en cuenta la funcionalidad de cada componente y pensando siempre en la forma de permitir la escalabilidad, se ha dividido el módulo en dos componentes principales: el submódulo de control de sesiones y el de administración del módulo, como se puede ver en la figura 11, adicional a esta arquitectura, el sistema también cuenta con un prototipo de HSS para poder almacenar los datos necesarios para llevar a cabo los procedimientos del módulo de control de sesiones de usuario.

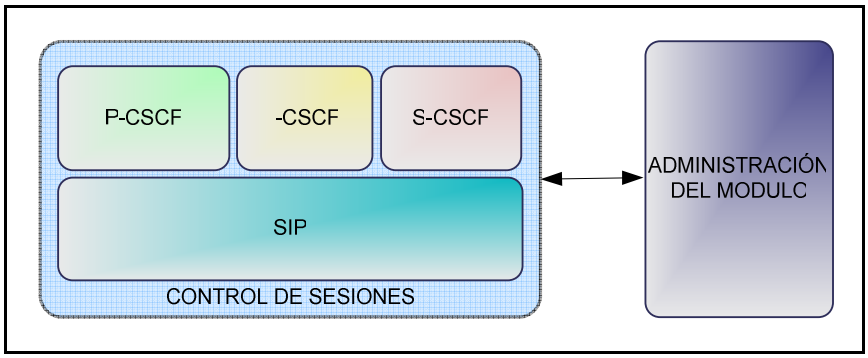


Figura 3. Arquitectura del Módulo de Control de Sesiones

En la figura anterior se puede apreciar la división del módulo y la subdivisión del componente de control de sesiones, que se compone de tres servidores, el P-CSCF, el I-CSCF y el S-CSCF, cada uno con funciones específicas. La señalización que se transmite por estos tres servidores, se soporta en el protocolo SIP.

3.1.1.1 Administración del módulo

Este componte se realizó con el propósito tener una interfaz de fácil interacción con el módulo y tiene tres funciones esenciales, iniciar, configurar y detener el módulo, es necesario destacar que el módulo de administración esta presente encada uno de los servidores, teniendo en cuenta que los servidores estarán en máquinas físicamente separadas.

Las funciones deberán ser realizadas por una persona que hace las veces de administrador del sistema, el cual es un actor importante en el manejo adecuado del módulo desarrollado y es el encargado de realizar las tres funciones mencionadas.

El ingreso al sistema es protegido por un login y una contraseña, datos que serán ingresados por el administrador en la interfaz que aparece al iniciar cada uno de los servidores.

Para que un servidor del módulo pueda ser iniciado, es necesario que el administrador, después de identificarse por medio de un login y una contraseña, lo configure ingresando datos necesarios según el tipo de servidor, los datos de configuración son diferentes para cada uno de los servidores, esta configuración es explicada detalladamente en el manual de usuario.

Después de realizada la configuración de un servidor, el administrador puede iniciar o detener el servidor, las veces que sea necesario.

3.1.1.2 Control de sesiones

El componente de control de sesiones es el elemento central del MCSU, por ser en este componente donde se realizan todas las funciones específicas para el control de las sesiones entre usuarios que, básicamente, son el manejo de tres mensajes de señalización, REGISTER, INVITE Y BYE que se procesarán de forma diferente dependiendo del modo de operación del módulo, que puede ser: P-CSCF, I-CSCF o S-CSCF.

3.1.1.2.1 Sub-Módulo P-CSCF del MCSU

Este componente está realizado bajo los criterios que especifica el 3GPP para un servidor P-CSCF que hace parte del CSCF dentro de la arquitectura IMS:

Este servidor se encarga del enrutamiento de los mensajes de señalización SIP desde el equipo del usuario hacia la red correspondiente, es decir, el P-CSCF del MCSU se encarga de recibir y enviar las peticiones y respuestas al cliente

Los mensajes pueden ser SIP REGISTER, SIP INVITE Y SIP BYE, el primero para el proceso de registro, el segundo para el inicio de sesión y el tercero para terminar una sesión establecida.

El P-CSCF del MCSU se comporta como un proxy statefull[3], así como se especifica en el RFC 3261, documento que explica detalladamente la arquitectura de los servidores SIP y señalización con dicho protocolo.

[3] *Servidor Statefull: Servidor que mantienen el estado de las transacciones durante el procesamiento de las peticiones*

3.1.1.2.2 Sub-Módulo I-CSCF del MCSU

Este componente está realizado bajo los criterios que especifica el 3GPP para un servidor I-CSCF que hace parte del CSCF dentro de la arquitectura IMS:

Este servidor recibe y procesa los mensajes que provienen del servidor P-CSCF del MCSU. Los mensajes que procesa son el SIP REGISTER y el SIP INVITE, es decir recibe el mensaje SIP REGISTER cuando un usuario desea registrarse y un SIP INVITE cuando el usuario de sea iniciar una comunicación con otro usuario.

Además, el I-CSCF del MCSU tiene la función de acceder a la base de datos, para consultar el perfil del usuario durante el proceso de registro, luego se encarga de comparar las capacidades del servidor S-CSCF del MCSU con las características contenidas dentro del perfil del usuario para realizar la asignación correspondiente.

Además del proceso de registro, un cliente puede enviar una solicitud de eliminación de registro, entendiendo este último como el proceso mediante el cual se elimina el registro del cliente de la base de datos. De esta forma se tiene que:

- Si se trata de la solicitud de un registro, la base de datos le envía el nombre del servidor S-CSCF del MCSU que se le asignará al usuario.

- En el proceso de des-registro, la base de datos no le envía ningún dato.

El proceso de asignación del S-CSCF del MCSU se hace teniendo en cuenta el resultado de la comparación anterior. Después el I-CSCF del MCSU le envía un mensaje SIP-REGISTER al S-CSCF del MCSU para que continúe con el proceso de registro del cliente.

3.1.1.2.3 Sub-Módulo S-CSCF del MCSU

Este componente esta realizado bajo los criterios que especifica el 3GPP para un servidor I-CSCF que hace parte del CSCF dentro de la arquitectura IMS:

Este servidor recibe los mensajes que le llegan desde el servidor I-CSCF o desde la base de datos. El servidor S-CSCF está encargado de las funciones de registro de usuario y validación de su perfil.

Durante el procedimiento de registro, el servidor recibe un mensaje SIP REGISTER proveniente del I-CSCF con la información necesaria para descargar de la base de datos el perfil del usuario. Dicho perfil es almacenado por el servidor hasta que la duración del registro del usuario expire.

3.1.1.2.4 HSS del MCSU

Adicional a la arquitectura del módulo se tiene un prototipo de HSS desarrollado también según las especificaciones técnicas del 3GPP TS 29.288, documento que especifica cada componente de la arquitectura IMS.

Es en este módulo donde se guarda el perfil de usuario, los datos del administrador del módulo, las capacidades del S-CSCF y el registro de los usuarios.

3.1.2 Procedimientos del Módulo de Control de Sesiones de Usuario MCSU

3.1.2.1 Procedimiento de registro en el MCSU

Para tener acceso a los servicios de la red, el usuario debe registrarse en el sistema. Mediante este proceso se registran las identidades públicas[4] que el usuario desea emplear en sus sesiones multimedia y se asigna el S-CSCF del MCSU que le dará soporte a los servicios solicitados por el usuario.

El usuario inicia el proceso enviando un mensaje SIP REGISTER hacia el servidor P-CSCF del MCSU, que detecta que se trata de un mensaje de registro inicial. En ese mensaje se encuentran la identidad privada del usuario, y las identidades públicas que desea registrar para que lo contacten.

En esta fase, el P-CSCF del MCSU envía el mensaje hacia un I-CSCF del MCSU, que se encarga de seleccionar un S-CSCF del MCSU hacia el que reenvía la petición de registro.

Cuando dicho S-CSCF recibe el mensaje, comprueba que se trata de un usuario no registrado y se contacta con el prototipo de HSS del MCSU para obtener los datos necesarios para identificarlo.

Posteriormente, el S-CSCF informa al HSS del MCSU que el abonado se ha registrado satisfactoriamente y descarga desde allí la suscripción IMS del usuario. El proceso finaliza con el asentimiento SIP 200 OK enviado hacia el cliente.

En la figura 12 se puede ver la secuencia de mensajes de señalización que se intercambian entre los diferentes componentes de módulo de control de sesiones y el cliente que se realizó con el propósito de validar la solución.

[4] Las identidades públicas son aquellas que se dan a conocer a otros abonados y se emplean para establecer sesiones. La identidad privada identifica unívocamente la suscripción IMS de un abonado, y se utiliza exclusivamente confines de seguridad y administrativos. Esta identidad no se da a conocer a otros usuarios.

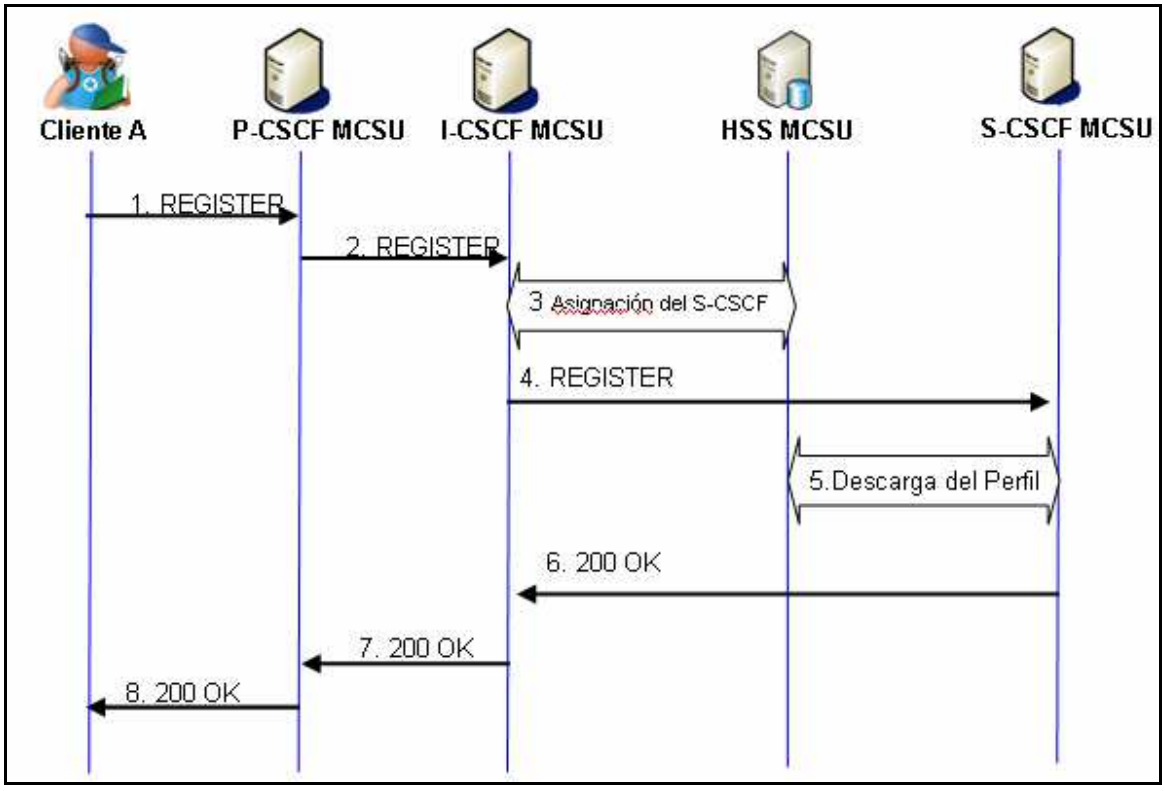


Figura 4. Procedimiento de registro en el MCSU

3.1.2.2 Procedimiento de inicio de sesión en el MCSU

Una vez que el usuario se ha registrado en la base de datos, puede iniciar sesiones con otros usuarios previamente registrados. El objetivo de este intercambio de señalización es el establecimiento de una sesión, mediante la cual se contactará con el nodo destino.

Para poder realizar lo anterior, el usuario origen deberá enviar un mensaje SIP INVITE, el cual pasará al P-CSCF y luego al S-CSCF que se le asignó durante el registro.

A continuación el terminal destino enviará de vuelta al nodo origen un mensaje SIP de progreso de sesión (*180: Ringing*).

Es entonces cuando el terminal destino avisa a su usuario de que lo están llamando, a la vez que envía la señalización SIP para indicar al terminal origen que el usuario destino está siendo alertado.

Por último, cuando el usuario destino acepta recibir la sesión, su terminal envía otro mensaje 200 OK, con el que se confirma el establecimiento definitivo de la sesión desde el usuario remoto.

En la figura 8 se muestra el tratamiento de un mensaje SIP INVITE, procedimiento necesario para el inicio de una sesión.

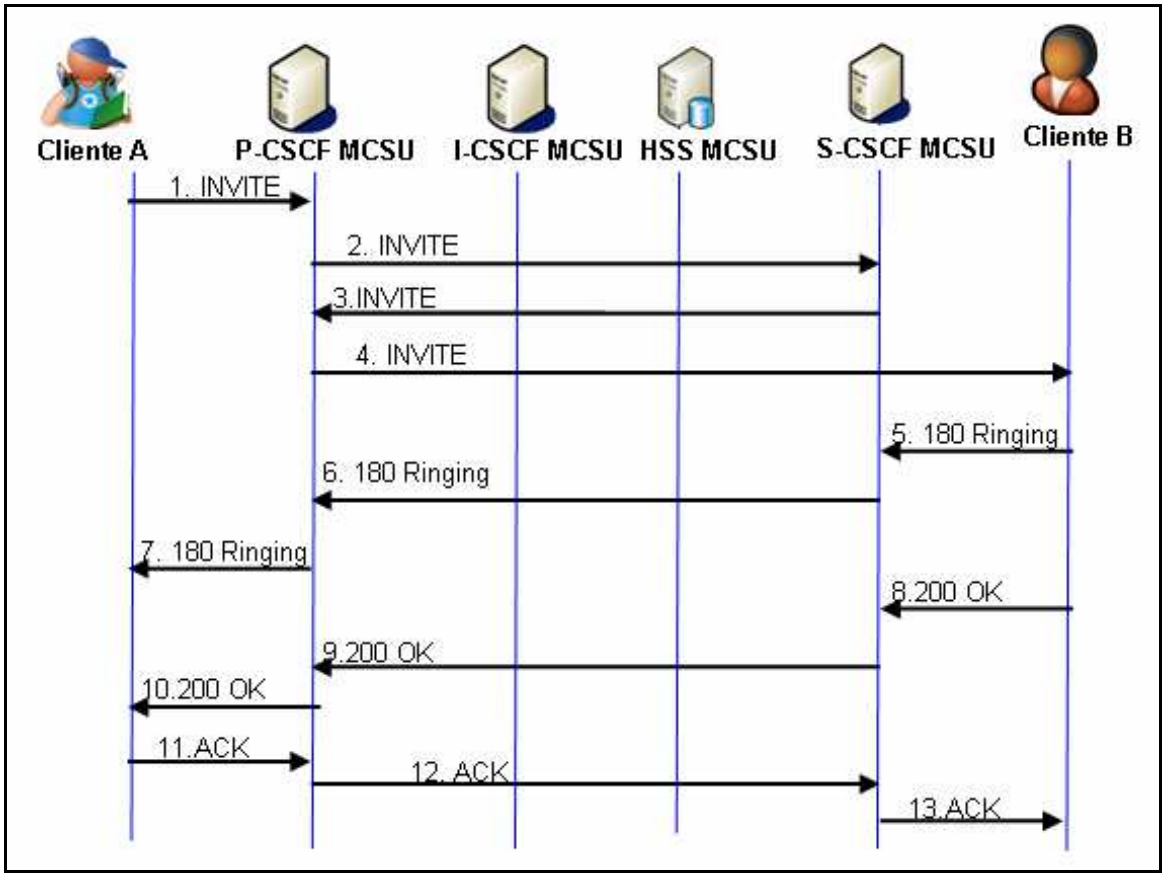


Figura 5. Procedimiento de inicio de sesión en el MCSU

3.1.2.3 Procedimientos de terminación de sesión en el MCSU

Este procedimiento hace referencia a la finalización de la sesión establecida entre dos equipos de usuario. Inicia en el momento en que un usuario cuelga, lo que genera un mensaje BYE del equipo de usuario a través del sistema.

Los clientes, son independientes a la hora de finalizar la comunicación. El que decida terminarla enviará una petición de tipo BYE al otro de forma directa.

El equipo del segundo usuario participante de la sesión responde con un mensaje de reconocimiento (200 OK) que es enviado a través de los servidores al equipo que terminó la sesión.

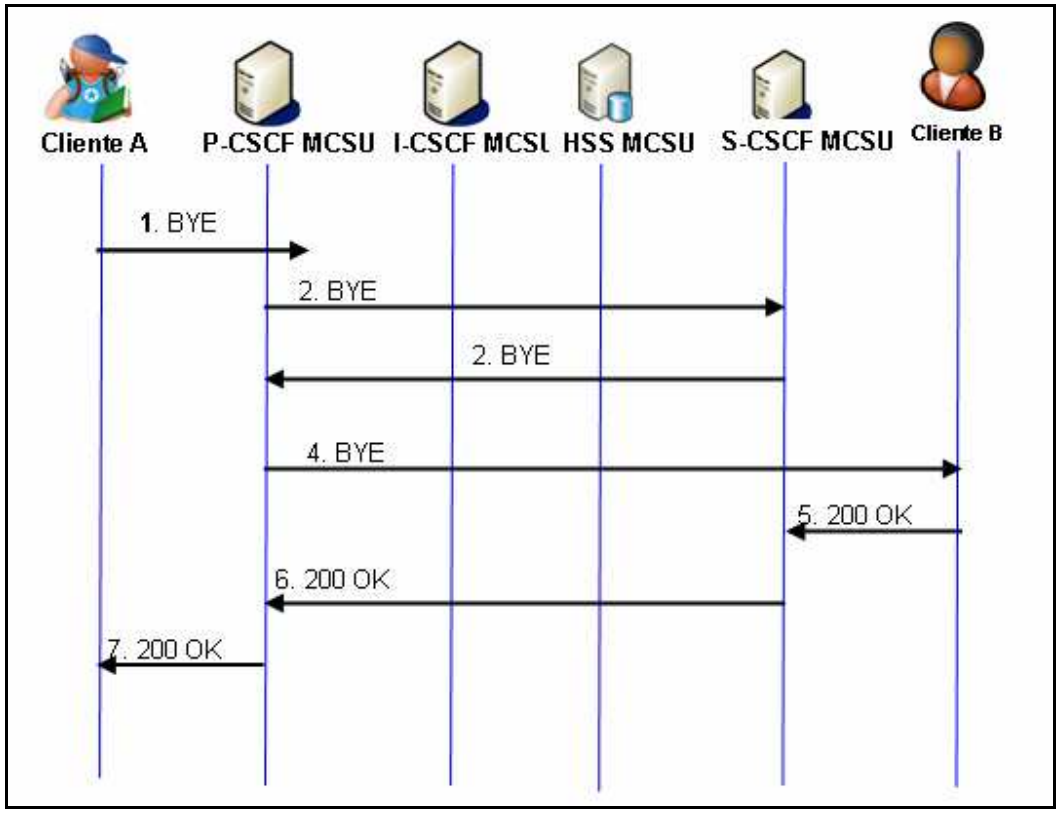


Figura 6. Procedimiento de terminación de sesión

3.2 DISEÑO DEL PROTOTIPO DEL MÓDULO DE CONTROL DE SESIONES DE USUARIO Y DEL PROTOTIPO DE CLIENTE SIP

Para el desarrollo del prototipo del módulo de control de sesiones de usuario y el prototipo de Cliente SIP, se tomó como guía metodológica el Modelo de Construcción de Soluciones (MCS), cuyo autor es el Ingeniero Carlos Serrano, miembro del Grupo de Ingeniería Telemática (GIT) de la Facultad de Ingeniería Electrónica y Telecomunicaciones. Éste Modelo define 4 fases de referencia: estudio de prefactibilidad, formulación del proyecto, ejecución del proyecto y validación de la solución. Es así como el presente capítulo se divide en estas fases de referencia, mencionando los aspectos de mayor importancia en cada una de ellas, y referenciado al respectivo Anexo para profundizar en cada fase.

3.2.1 Fase 2: Estudio de Factibilidad[5] del MCSU

3.2.1.1 Descripción del Sistema MCSU

El Módulo de Control de Sesiones de Usuario es un sistema que se encargan de manejar la señalización correspondiente al registro de usuarios, establecimiento y terminación de sesiones dentro una misma red.

Este sistema tiene tres servidores, cada uno con un comportamiento especial, los servidores son prototipos de los servidores P-CSCF, el I-CSCF y el S-CSCF que en conjunto forman el CSCF definido dentro de la arquitectura IMS.

1.1 [5] *Para mayor información se puede remitir al Anexo A, sección 2: "Modelo de Establecimiento de Responsabilidades"*

Los mensajes de señalización que procesa este módulo son los mensajes SIP REGISTER, SIP INVITE Y SIP BYE, tal como se dijo en el diseño de la arquitectura del módulo MCSU.

Adicional a los servidores, el sistema cuenta con una base de datos donde se van a almacenar los datos necesarios para el funcionamiento del módulo.

3.2.1.2 Identificación de Actores para el MCSU

Administrador: es la persona que interactúa con el módulo de control de sesiones para configurarlo, iniciar y detener su funcionamiento.

Cliente SIP: se comporta como un actor frente al módulo de control de sesiones debido a que iniciará los procedimientos de procesamiento de los mensajes SIP por parte de la aplicación.

3.2.1.3 Diagrama de casos de uso del sistema MCSU

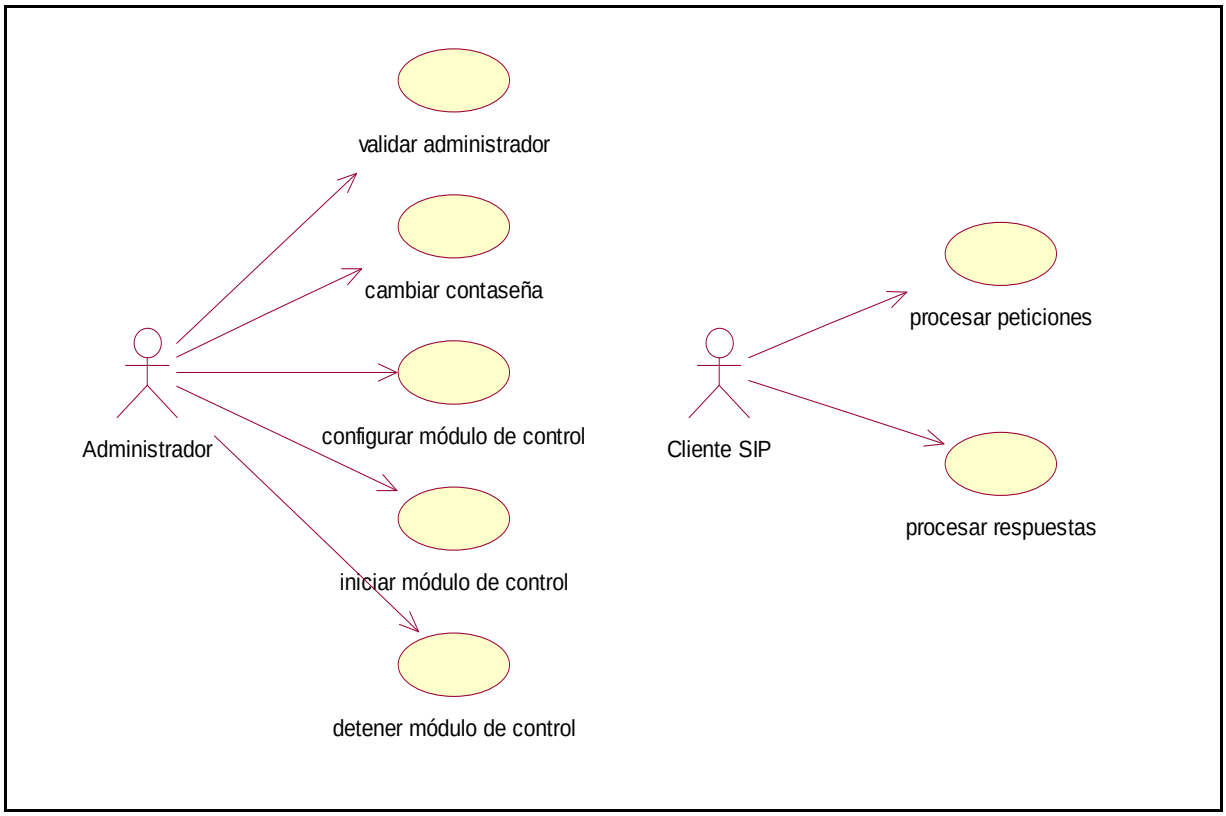


Figura 7. Diagrama de casos de uso del sistema MCSU

3.2.1.4 Diagrama de paquetes de análisis esenciales del MCSU

La funcionalidad del Módulo de Control de Sesiones de Usuario, se dividió en tres paquetes: v*iew*, *control* y *model*.

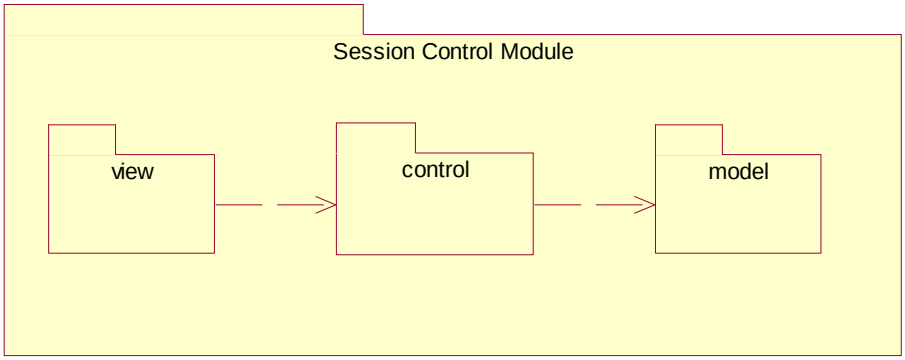


Figura 8. Diagrama de paquetes del MCSU

- View

Este paquete contiene las clases necesarias para que el administrador pueda interactuar directamente con el sistema, de forma rápida y con mucha facilidad.

- Control

Dentro de éste paquete se encuentran las clases que hacen posible el manejo lógico del módulo, mediante la ejecución de procesos que permiten dar respuesta a las solicitudes hechas por el administrador a través del paquete interface y por el cliente SIP a través del prototipo de cliente.

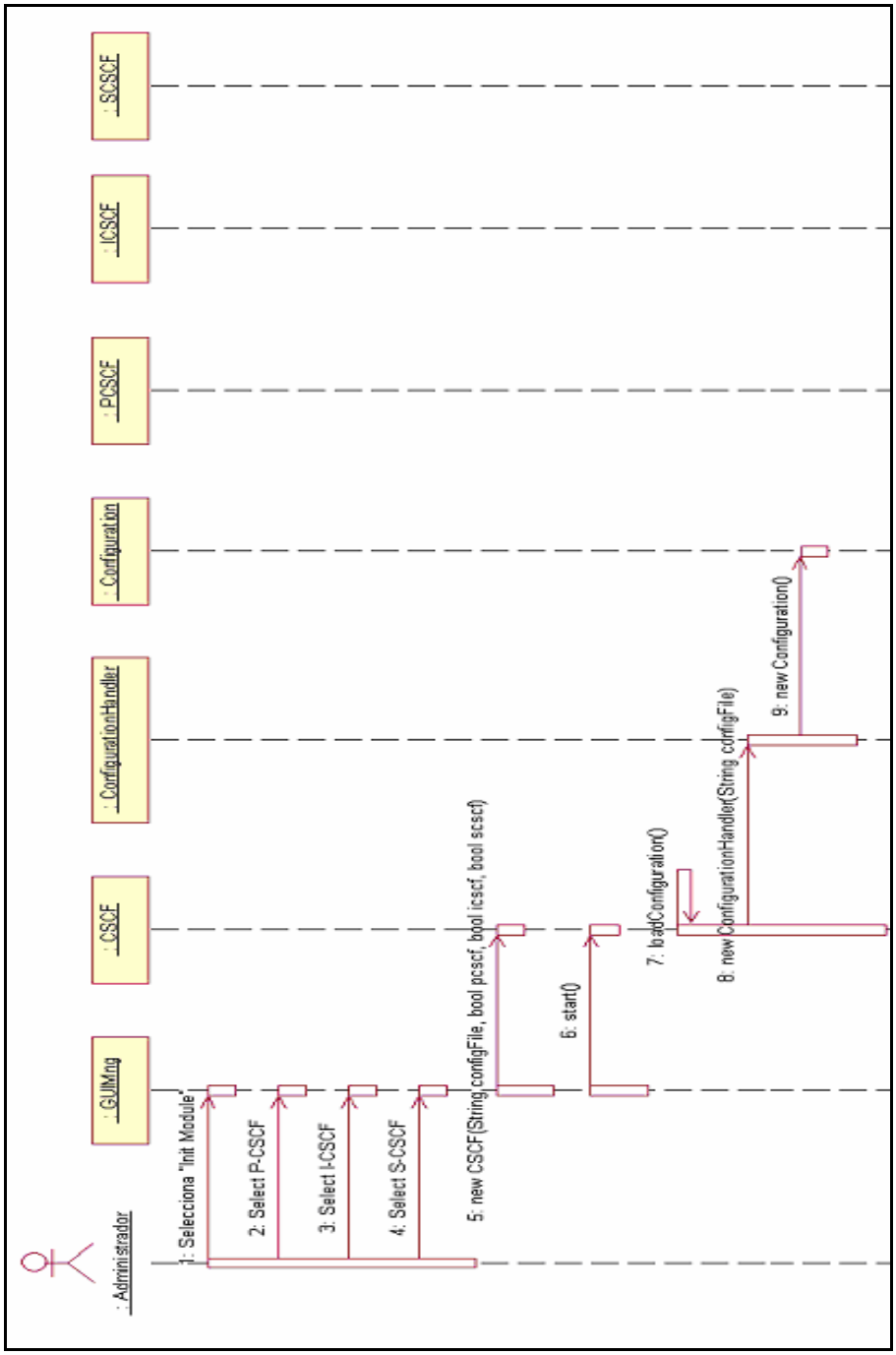
- Model

El paquete Model contiene las clases de entidad que dan soporte al sistema en su funcionalidad lógica.

3.2.1.5 Diagramas de Secuencia para los Casos de Uso Esenciales del MCSU

3.2.1.5.1 Casos de uso iniciados por el Administrador

- Iniciar módulo de control



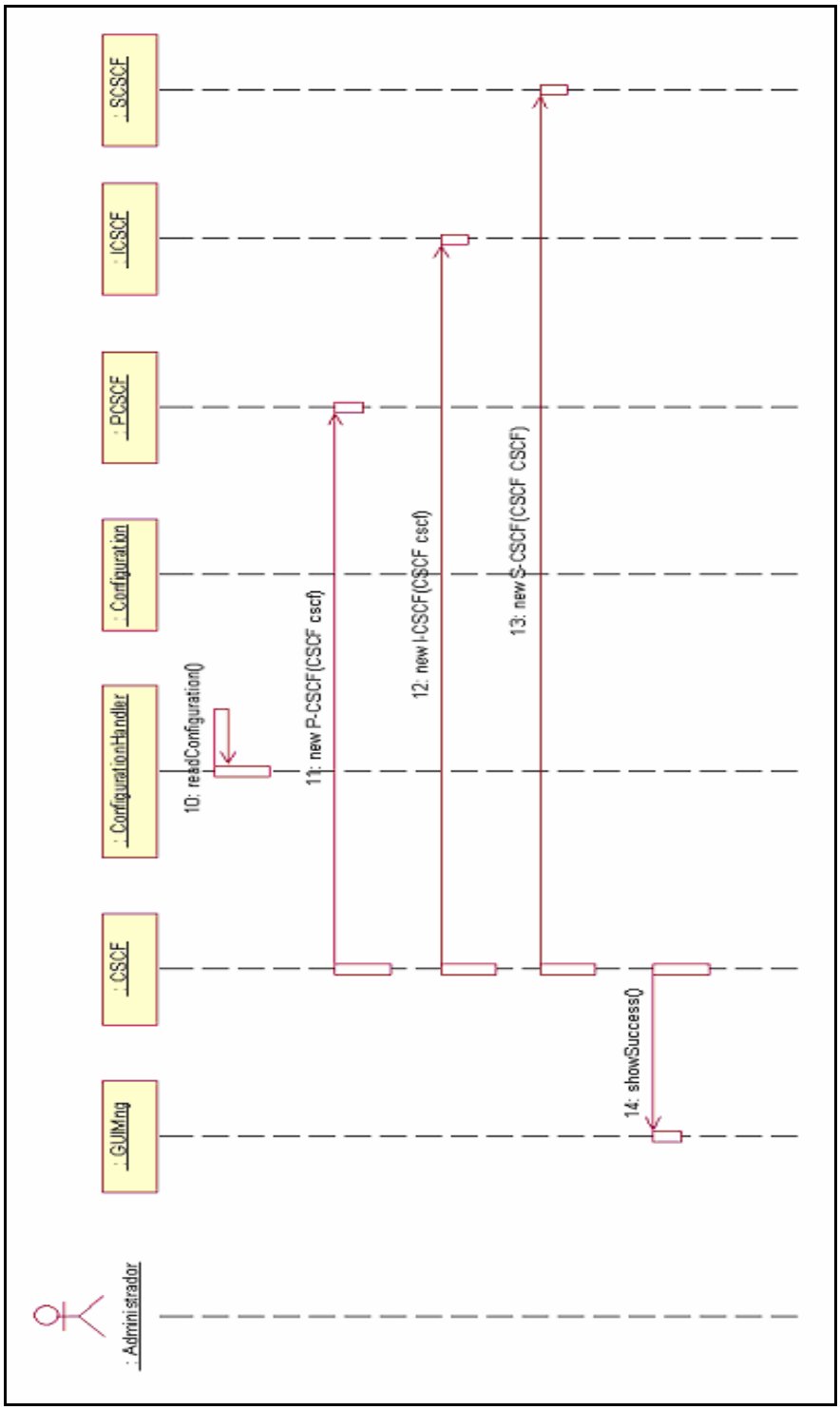


Figura 9. Diagrama de secuencia caso de uso Iniciar Módulo

♦ Configurar módulo de control

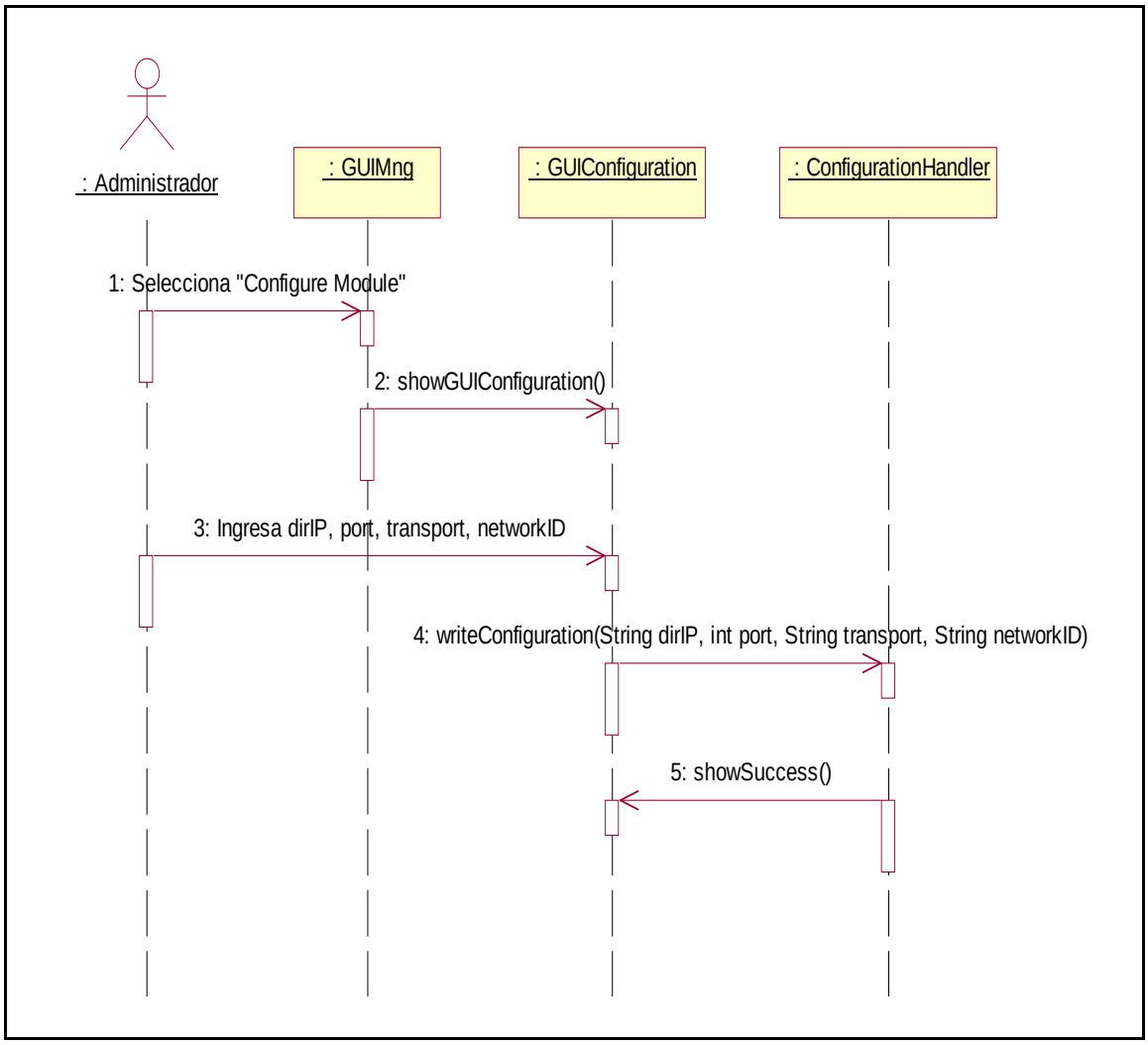
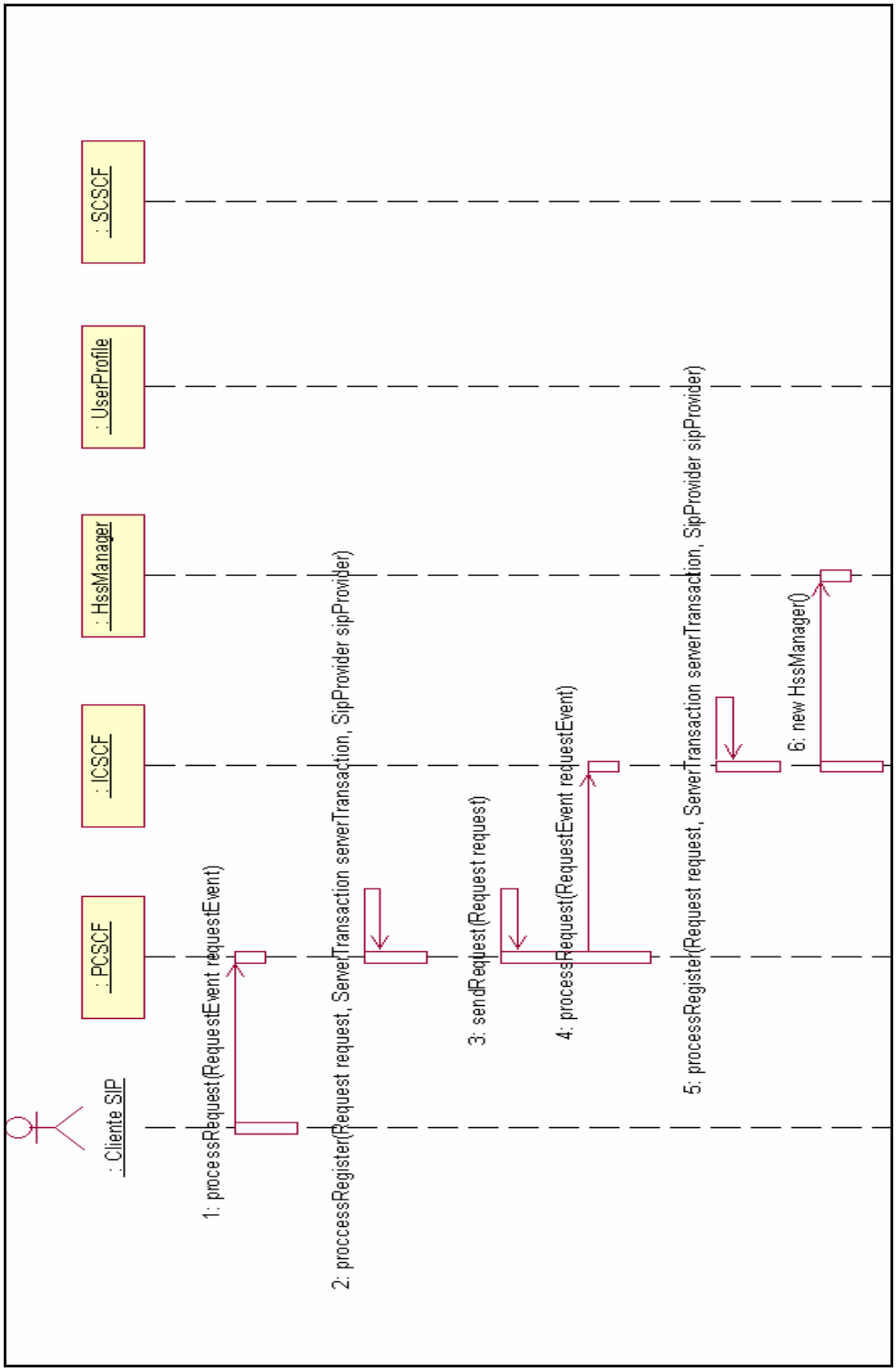


Figura 10. Diagrama de secuencia caso de uso Configurar módulo

3.2.1.5.2 Casos de Uso iniciados por el Cliente SIP

- Procesar REGISTER



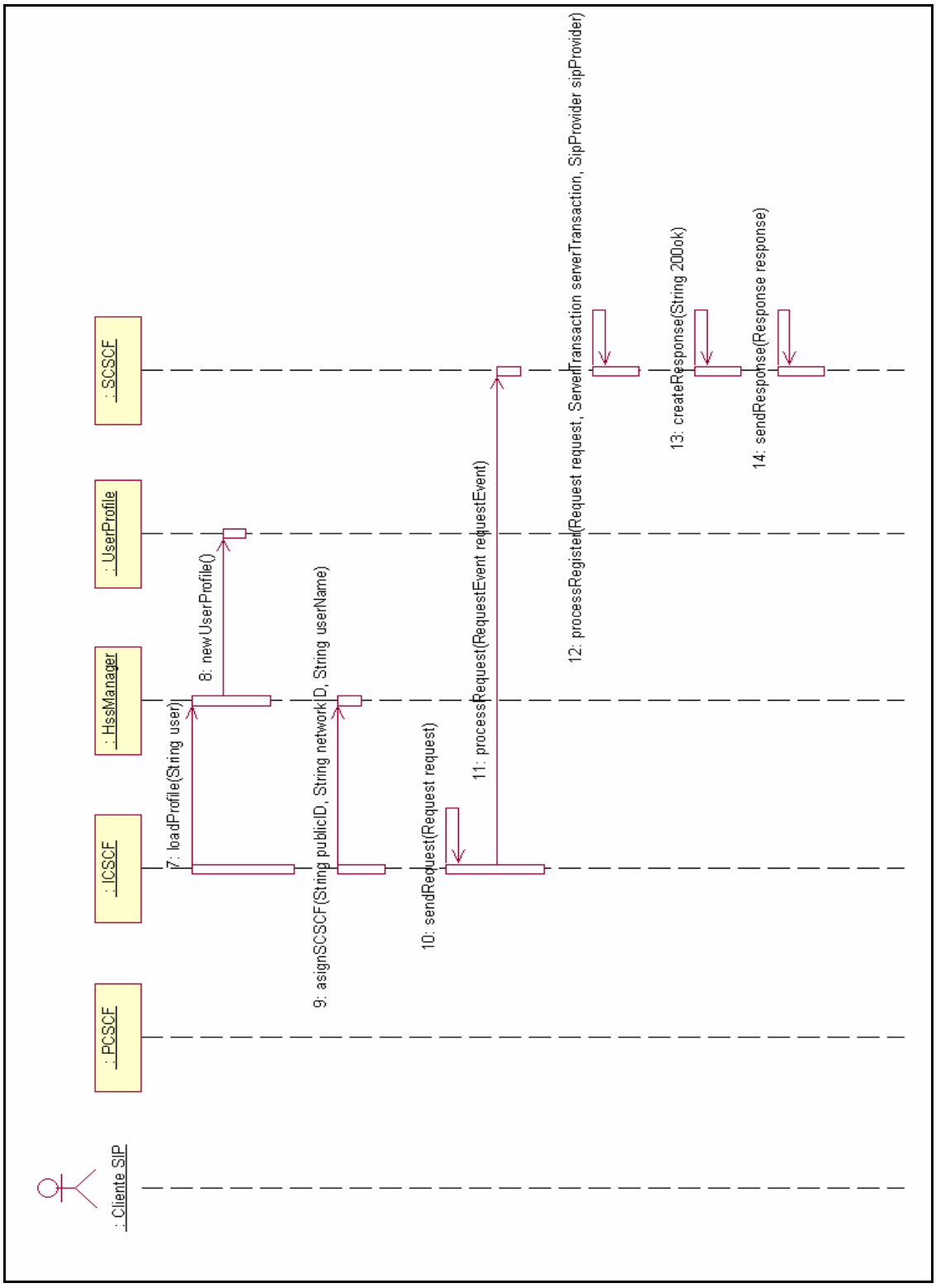
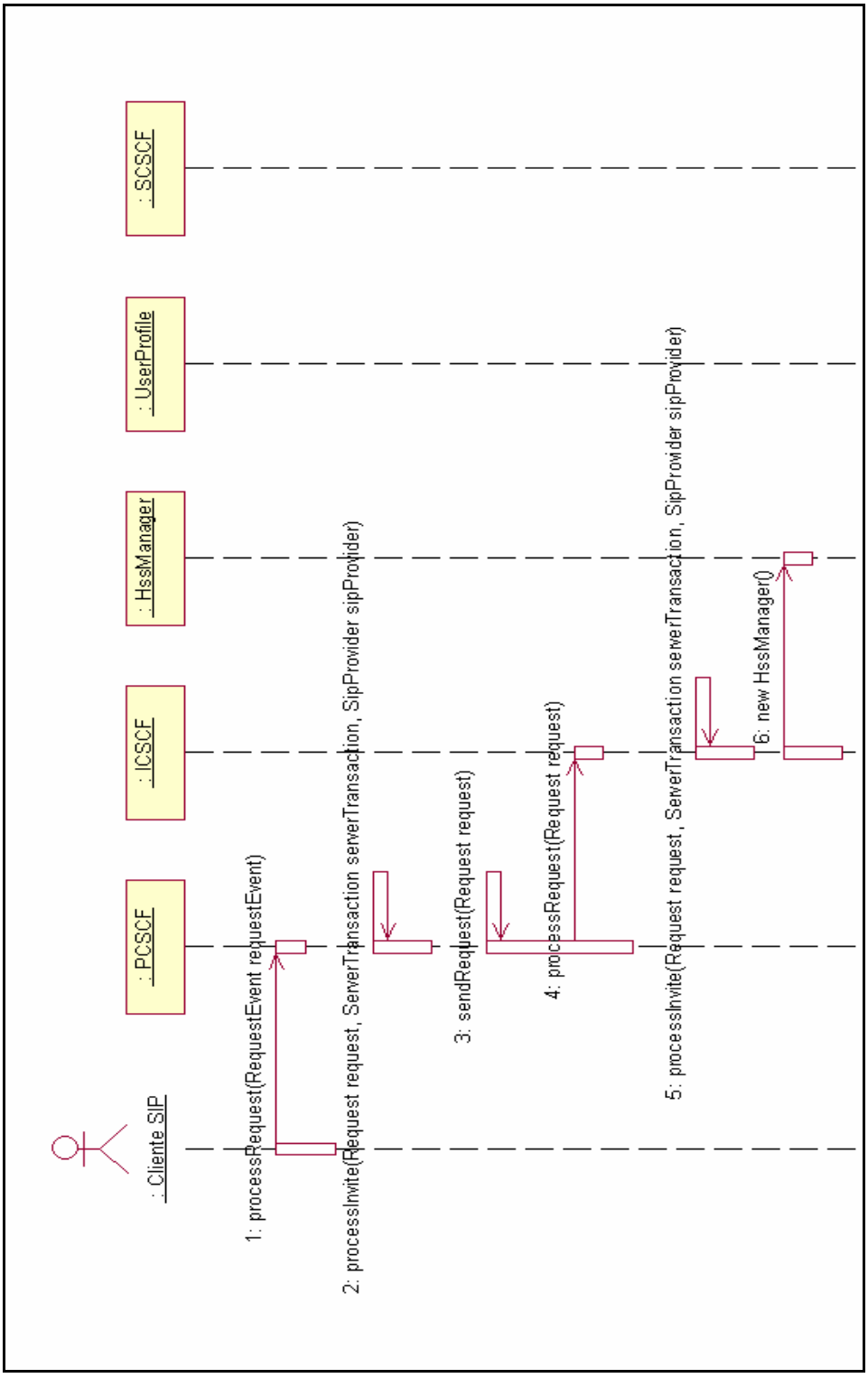


Figura 11. Diagrama de secuencia caso de uso procesar REGISTER

♦ Procesar INVITE



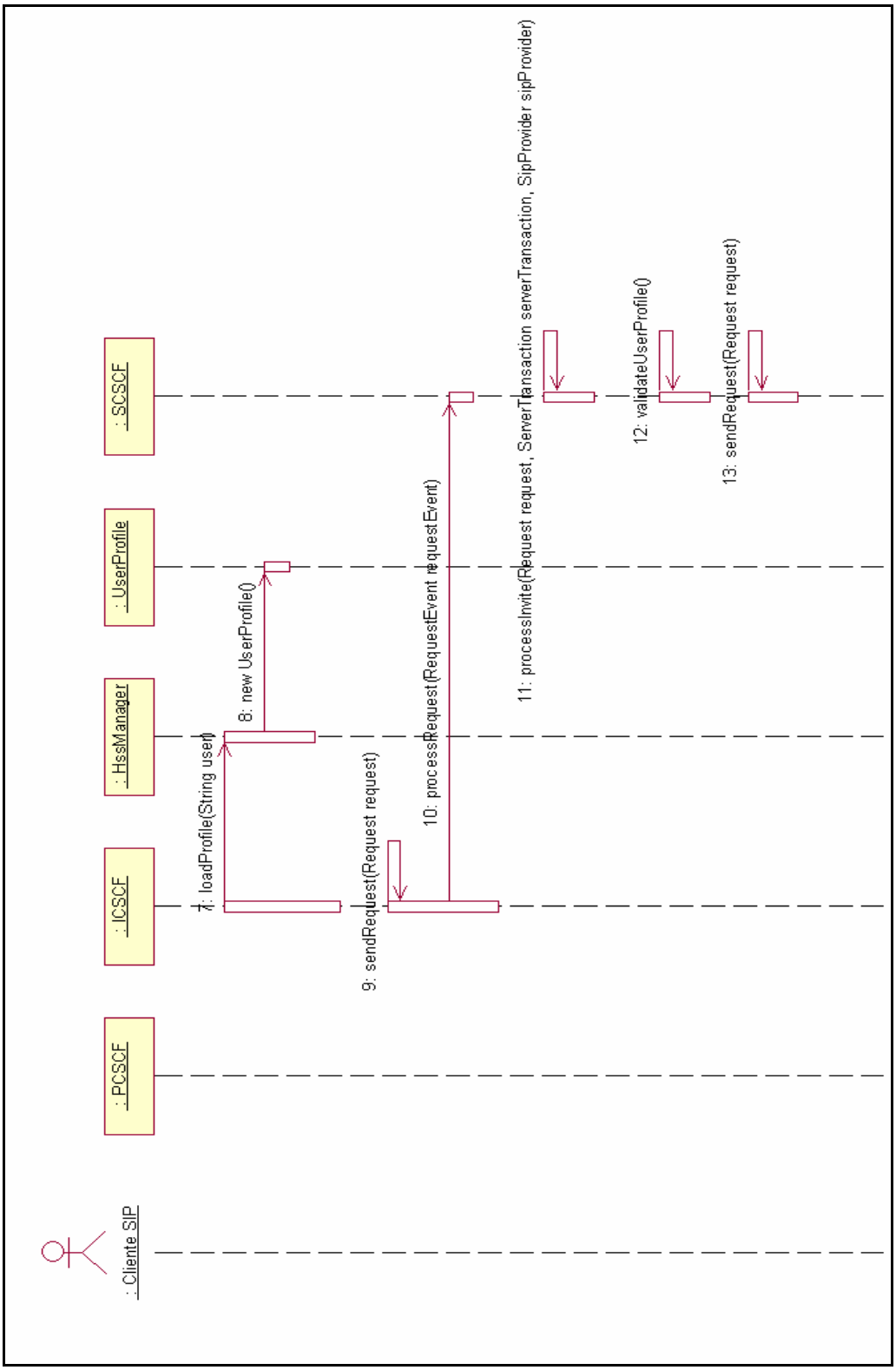


Figura 12. Diagrama de secuencia caso de uso Procesar INIVITE

3.2.1.6 Diagrama de Despliegue del MCSU

La arquitectura física del modulo de control de sesiones de usuario se muestra en la Figura 15. Cada servidor se ejecuta en un nodo diferente, y en cada uno de ellos se encuentra el modulo de administración que permite configurar las propiedades necesarias para cada tipo de servidor. Los servidores intercambian información de señalización mediante el protocolo SIP y acceden a la base de datos a través de la interfaz JDBC.

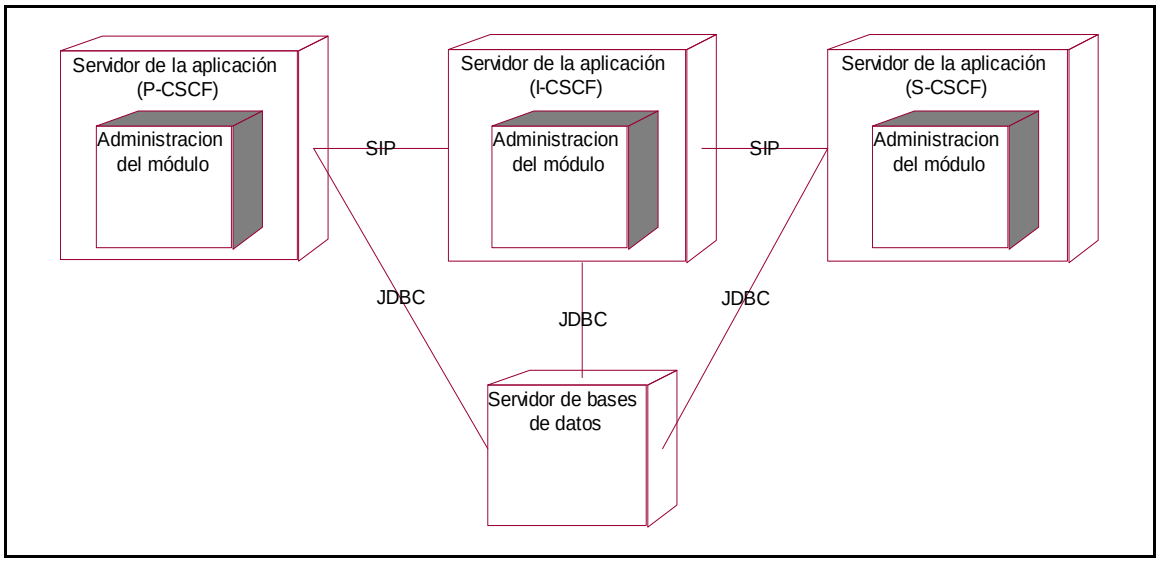


Figura 13. Diagrama de despliegue general

3.2.2 Fase 2: Estudio de Factibilidad Cliente SIP

3.2.2.1 Descripción del Sistema Cliente SIP

El cliente SIP es un sistema que se encarga de enviar y recibir mensajes SIP, principalmente peticiones de tipo REGISTER, INVITE, BYE y MESSAGE, y respuestas 200OK, TRYING y RINGING, realizando el procesamiento adecuado para cada tipo de mensaje. El intercambio de estos mensajes se realiza con el MCSU. Este sistema es

manipulado por un usuario que es quien decide en que momento generar y enviar las peticiones SIP mencionadas anteriormente.

Cuando el usuario decide enviar un mensaje de tipo REGISTER, debe proporcionar los datos correspondientes al nombre de usuario, dominio al que pertenece, dirección IP, puerto y protocolo de transporte del servidor Proxy a través del cual se comunica con la red (MCSU funcionando como P-CSCF), nombre del servidor de registro hacia el cual va dirigida la petición, y el tiempo de duración de dicho registro.

Para el envío de una petición de tipo INVITE, el usuario debe proporcionar el nombre de usuario y dominio de la persona a quien desea enviarle la invitación, el Cliente SIP construye el mensaje correspondiente, le adiciona la ruta previamente guardada en el procedimiento de registro, y lo envía al punto indicado en la ruta; espera por una respuesta 200OK que le indica la aceptación de la petición por parte del usuario de destino y al recibirla genera y envía una petición ACK basada en dicha respuesta.

Si el Cliente SIP recibe una petición de tipo INVITE, le informa al usuario que se desea establecer una sesión, dándole la oportunidad de aceptarla o rechazarla, y genera y envía una respuesta provisional de tipo RINGING. En caso de que el usuario acepte la invitación, el Cliente SIP construye y envía una respuesta 200OK basada en dicha petición y espera por la llegada de un ACK que le confirma la recepción de la respuesta por parte del usuario que origina la invitación. Si el usuario decide rechazar la invitación, el Cliente SIP no realiza ninguna tarea.

Para el envío de una petición de tipo BYE, el usuario no necesita proporcionar información adicional al Cliente SIP, éste cuenta ya con los datos necesarios para construir el mensaje correspondiente y enviarlo a su destino. Después de hacerlo, espera por una respuesta 200OK que le confirma que el dialogo ha finalizado. Si el Cliente SIP recibe una petición de tipo BYE, construye y envía una respuesta 200OK basada en dicha petición y le informa al usuario que el dialogo ha terminado.

Para el envío de una petición de tipo MESSAGE, se proporciona la información correspondiente al nombre del usuario y el dominio del usuario hacia quien va dirigido el

mensaje e introduce el mensaje que desea enviar. El Cliente SIP construye y envía el mensaje correspondiente teniendo en cuenta la ruta guardada con el procedimiento de registro. El Cliente SIP espera por la llegada de una respuesta 200OK para confirmar que el mensaje ha sido recibido por el Cliente SIP de destino, esto no garantiza que el usuario de destino haya visto el mensaje. Si el Cliente SIP recibe una petición de tipo MESSAGE, el Cliente SIP extrae la información correspondiente al usuario que la originó y el mensaje texto para mostrárselo al usuario.

3.2.2.2 Identificación de actores para el Cliente SIP

Usuario: es la persona que interactúa directamente con el Cliente SIP para realizar los procedimientos de registro, inicio y finalización de sesión, y envío de mensajes cortos.

MCSU: interactúa con el Cliente SIP a través del intercambio de peticiones y respuestas.

3.2.2.3 Diagrama de casos de uso del Cliente SIP

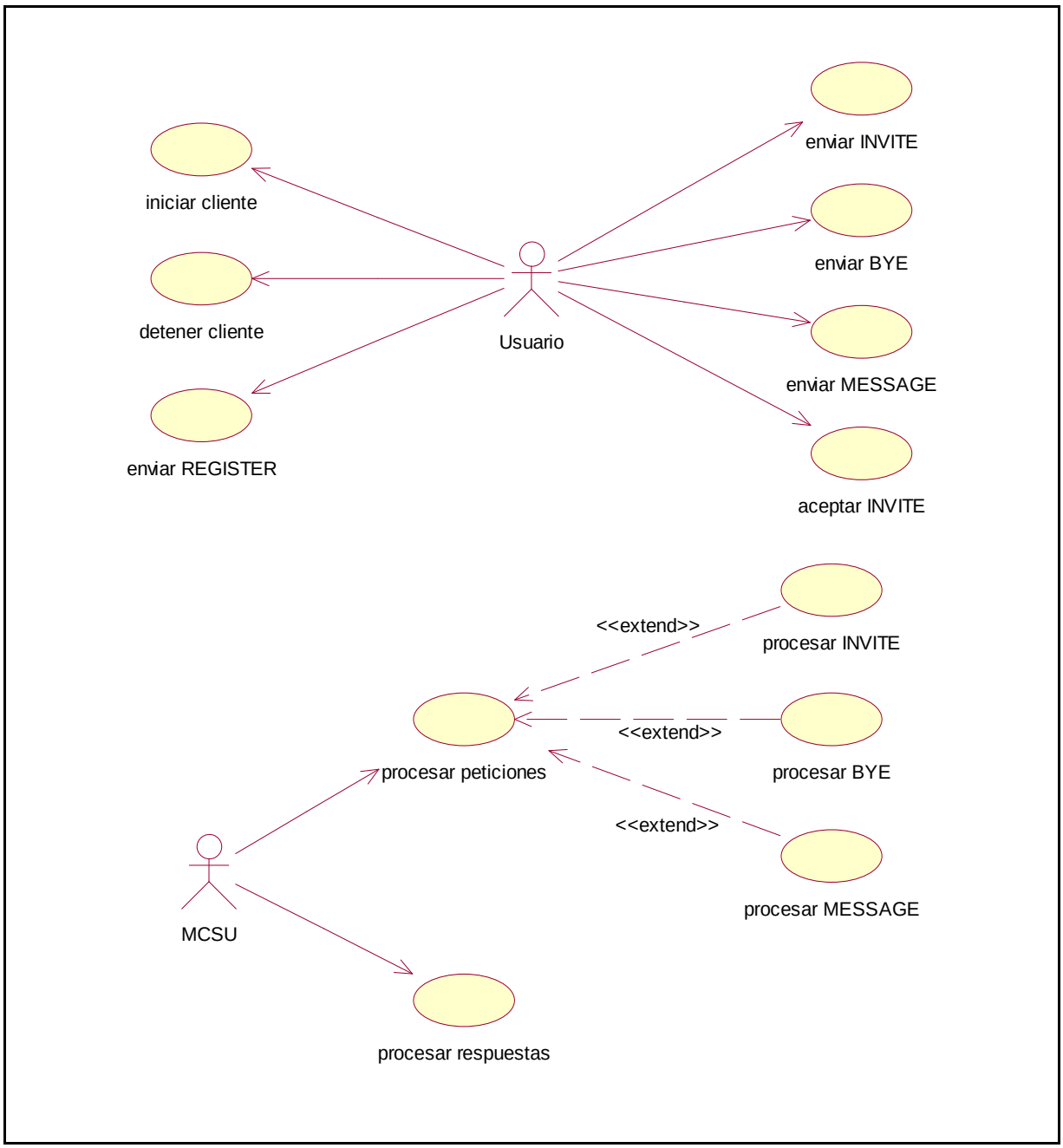


Figura 14. Diagrama General de Casos de Uso del Cliente SIP

3.2.2.4 Diagrama de Paquetes de Análisis Esenciales del Cliente SIP

La funcionalidad del Cliente SIP se dividió en 2 paquetes: *view* y *control*, como se puede observar en la figura 15.

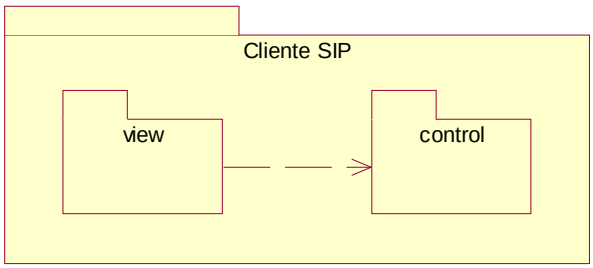


Figura 15. Diagrama de paquetes del Cliente SIP

- view: Este paquete contiene las clases que le permiten al usuario interactuar directamente con el Cliente SIP.

- control: Este paquete contiene las clases que contienen la lógica de operación del Cliente SIP, que se encarga de la ejecución de procesos que permiten dar respuesta a las solicitudes hechas por el usuario a través del paquete interface y por el MCSU.

3.2.2.5 Diagramas de Secuencia para los Casos de Uso Esenciales del Cliente SIP

3.2.2.5.1 Casos de Uso iniciados por el Usuario

- Iniciar cliente

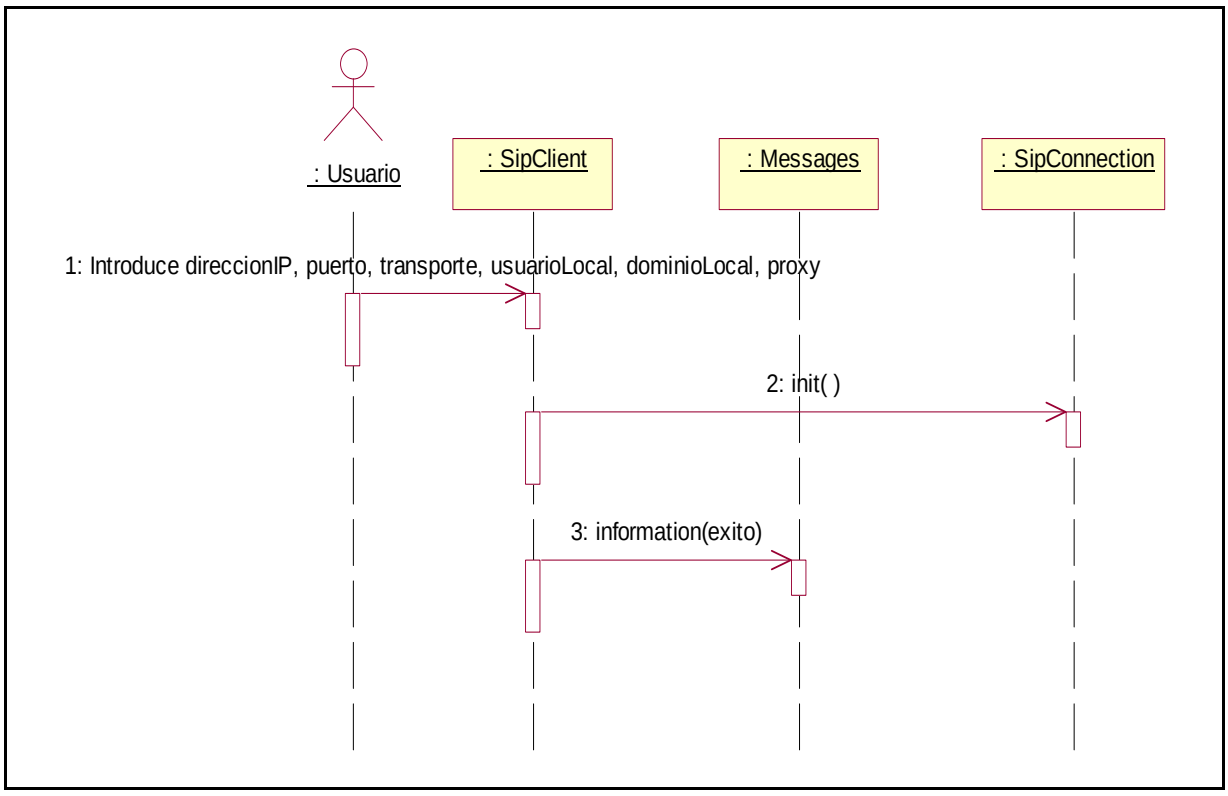


Figura 16. Diagrama de secuencia caso de uso iniciar cliente

- Enviar REGISTER

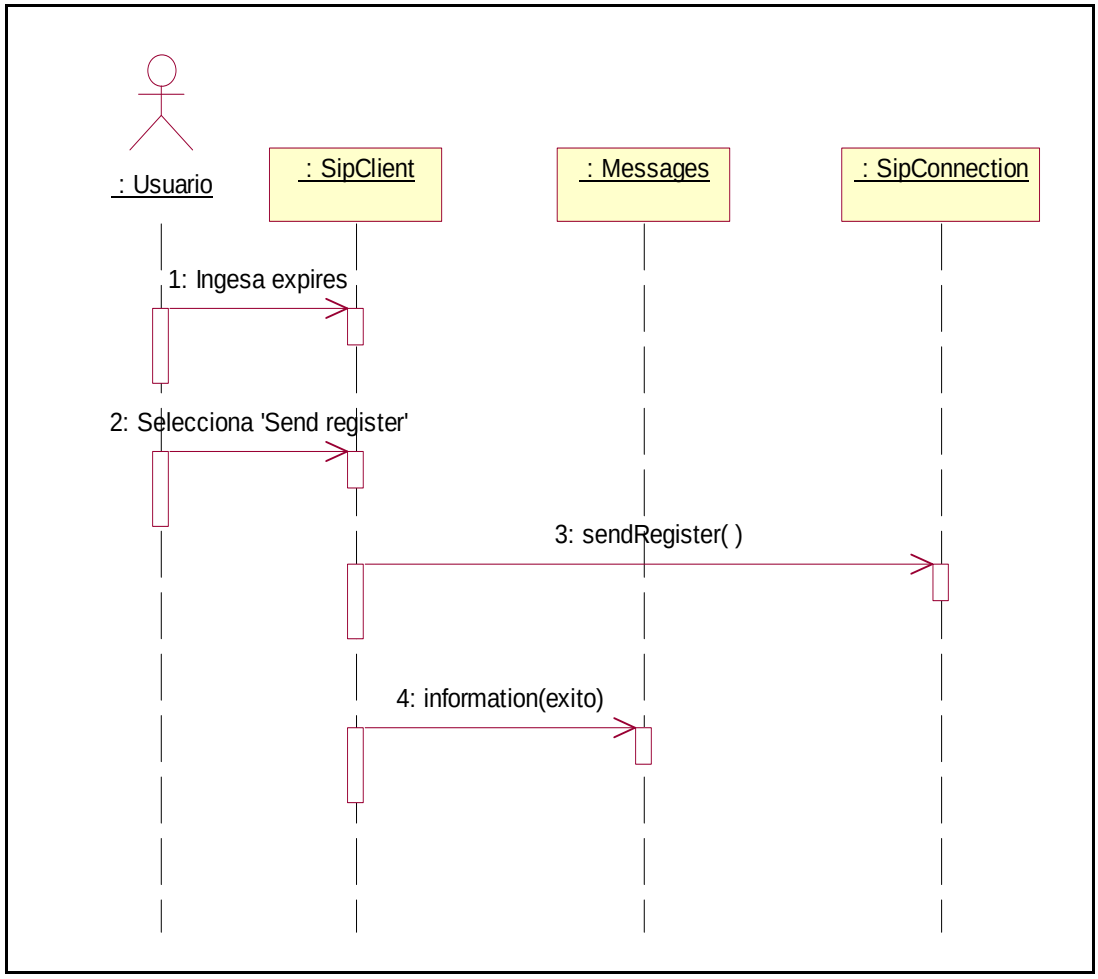


Figura 17. Diagrama de secuencia caso de uso enviar REGISTER

- Enviar MESSAGE

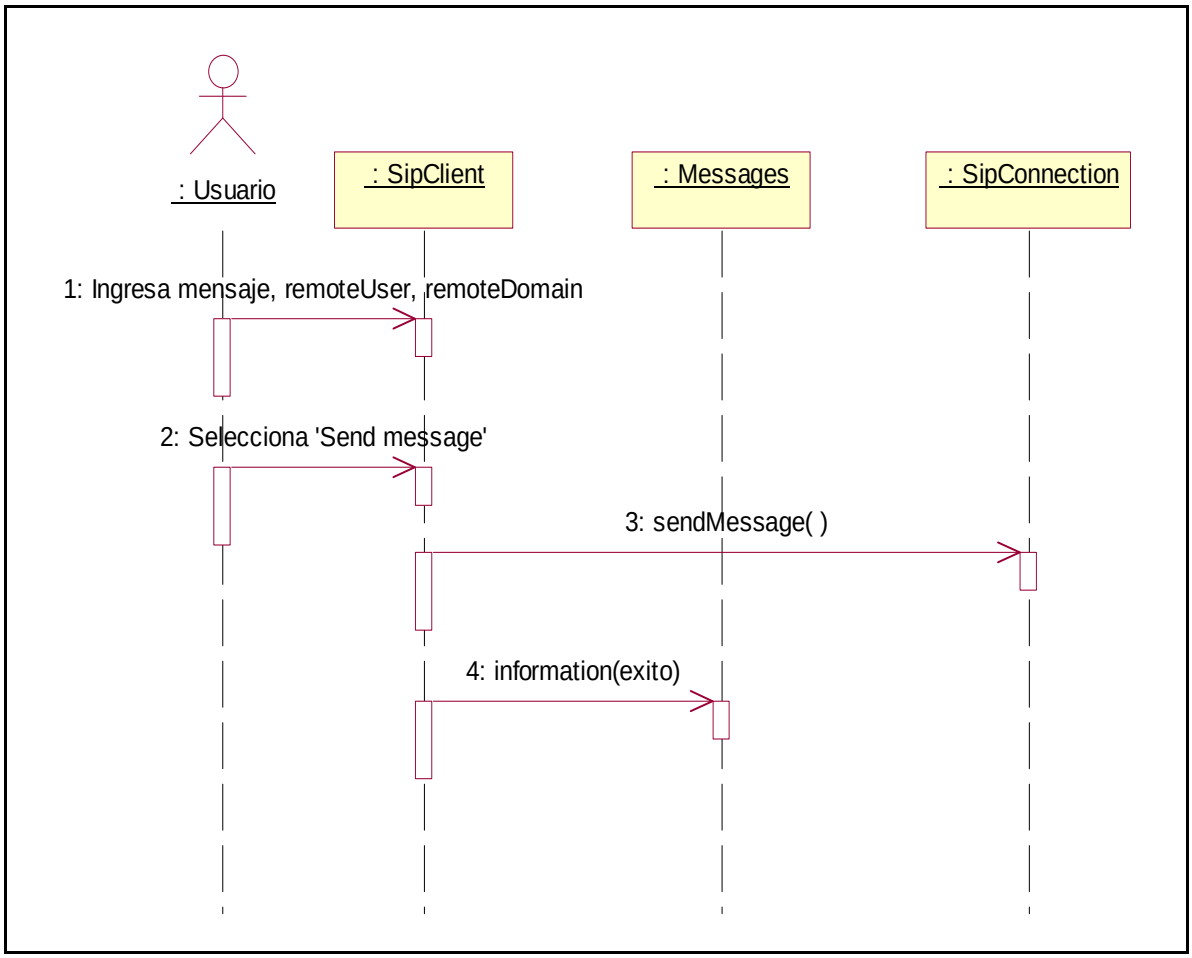


Figura 18. Diagrama de secuencia caso de uso enviar MESSAGE

3.2.2.5.2 Casos de uso iniciados por el MCSU

- Procesar MESSAGE

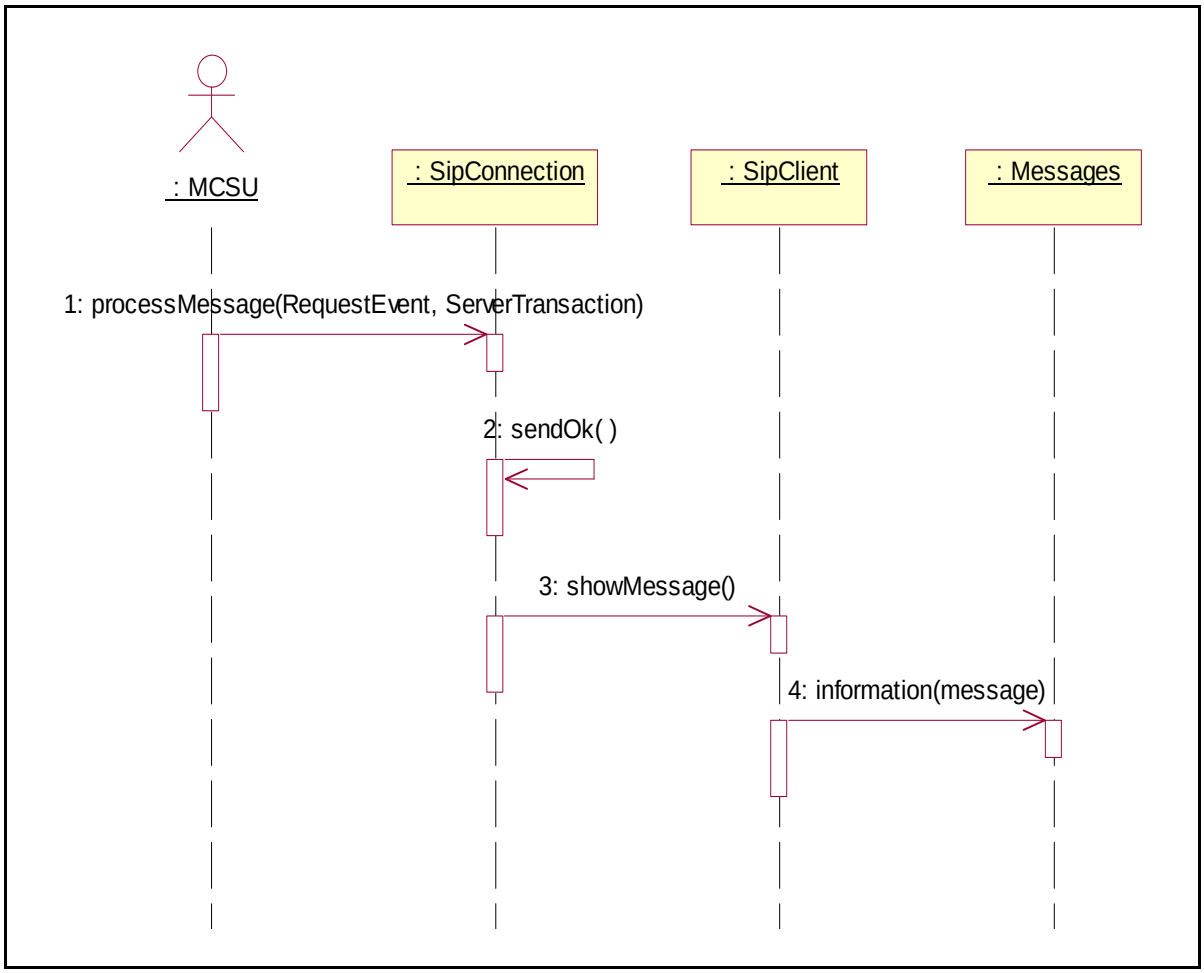


Figura 19. Diagrama de secuencia caso de uso procesar MESSAGE

3.2.3 Fase 3: Ejecución del proyecto

En la fase de ejecución del proyecto se mencionan los detalles de implementación del prototipo del módulo de control de sesiones y del cliente SIP, principalmente se hace referencia a las tecnologías que se utilizaron para dichas implementaciones.

Para el proceso de selección de las tecnologías utilizadas para la implementación de los prototipos se tuvo en cuenta los siguientes requisitos generales:

- Ser preferiblemente software libre.
- Tener el mínimo costo posible.
- Contar con una buena documentación de instalación y uso.
- Facilitar ejemplos de aplicaciones previamente realizadas.

La función del módulo de control de sesiones es principalmente el procesamiento de mensajes SIP de acuerdo a lo especificado por la arquitectura IMS. Para la construcción del prototipo se requiere de una tecnología que permita el desarrollo fácil y rápido de aplicaciones basadas en el protocolo SIP, principalmente en las funcionalidades de los servidores SIP. Así mismo para el prototipo del cliente, que se encarga de construir los mensajes SIP iniciales e intercambiarlos con el MCSU.

3.2.3.1 Java

Se eligió Java como lenguaje de programación, especialmente por ser un lenguaje de desarrollo de propósito general válido para realizar todo tipo de aplicaciones, entre sus principales características se encuentran:

- Ser intrínsecamente orientado a objetos.
- Funcionar perfectamente en red.
- Tener una gran funcionalidad gracias a sus librerías (clases).
- Gestionar el manejo de la memoria.

- Generar aplicaciones con pocos errores posibles, principalmente porque la gestión de memoria y punteros la realiza el propio lenguaje.

3.2.3.2 JAIN-SIP

Se eligió trabajar con JAIN SIP por las siguientes razones: Proporciona una implementación de referencia con una funcionalidad completa de la implementación SIP. Estandariza la interfaz para el modelo de transacciones genéricas definidos por el protocolo SIP y proporciona acceso para la funcionalidad de diálogo desde la interfaz de transacciones.

Define varias clases factory para la creación de mensajes Request, Response y encabezados SIP. Define un interfaz para cada encabezado que soporta, los cuáles pueden ser adicionados a mensajes Request, Response.

El diseño es extensible, definiendo una interfaz genérica de encabezados que se puede usar para aplicaciones que utilicen encabezados que no son soportados directamente por JAIN SIP.

3.2.3.3 NIST-SIP

NIST SIP es la implementación de referencia oficial para el API JAIN SIP 1.2.

La elección de NIST SIP JainSipRI1.2 se soporta en las siguientes razones:

- La especificación JAIN–SIP 1.2 no define soporte específico para las extensiones de IMS, esta característica fue adicionada dentro de la implementación realizada por NIST-SIP, lo que la convierte en la herramienta mas adecuada para el desarrollo de los prototipos.

- Es gratis y de pertenencia al dominio público, además de las garantías de continuidad y estabilidad que ofrece NIST.

3.2.3.3.1 Aporte a la implementación de referencia NIST-SIP

En el transcurso del desarrollo los prototipos, se observaron algunas fallas en el momento de utilizar las extensiones para IMS, exactamente en el proceso de extracción de las cabeceras IMS que hacían parte de los mensajes SIP. En el siguiente ejemplo se muestra una sección de código que utiliza la interfaz PreferredIdentityHeader, para la cabecera P-Preferred-Identity:

PreferredIdentityHeader preferredIdentity = (PreferredIdentityHeader) request.getHeader (PreferredIdentityHeader.NAME);

La anterior línea lanzaba la siguiente excepción:

java.lang.ClassCastException: gov.nist.javax.sip.header.ExtensionHeaderImpl

El mismo problema presentaban las siguientes interfaces definidas para manejar las cabeceras:

- AccessNetworkInfoHeader, para la cabecera P-Access-Network-Info
- AssertedIdentityHeader, para la cabecera P-Asserted-Identity
- PreferredIdentityHeader, para la cabecera P-Preferred-Identity
- VisitedNetworkIDHeader, para la cabecera P-Visited-Network-ID

La descripción de estas cabeceras se encuentra en el capitulo 2 de este documento.
Estos errores fueron reportados a la lista de problemas de NIST-SIP, contribuyendo de esta forma a la depuración del API, en la parte del manejo de las cabeceras IMS. También se pudo observar que aun no existe desarrollo de aplicaciones orientadas a IMS que hagan uso de esta herramienta, por lo cual el proyecto se convierte en pionero dentro de esta área.

3.2.4 Fase 4: Validación de la solución

La validación del prototipo del módulo de control de sesiones de usuario implementado se realizó verificando que los mensajes recibidos por el módulo reciban el procesamiento adecuado, según las especificaciones técnicas TS.24.228 y TS.24.229 del 3GPP, donde se encuentra de forma detallada los procedimientos realizados por los tres servidores P-CSCF, I-CSCF Y S-CSCF para el control de las sesiones de usuarios.

La figura 14 muestra la arquitectura de referencia para la fase de validación, en ella se pueden identificar los tres servidores que hacen parte del módulo, el servidor P-CSCF, el I-CSCF y el S-CSCF, una base de datos y los clientes SIP entre los cuales se va a establecer la comunicación.

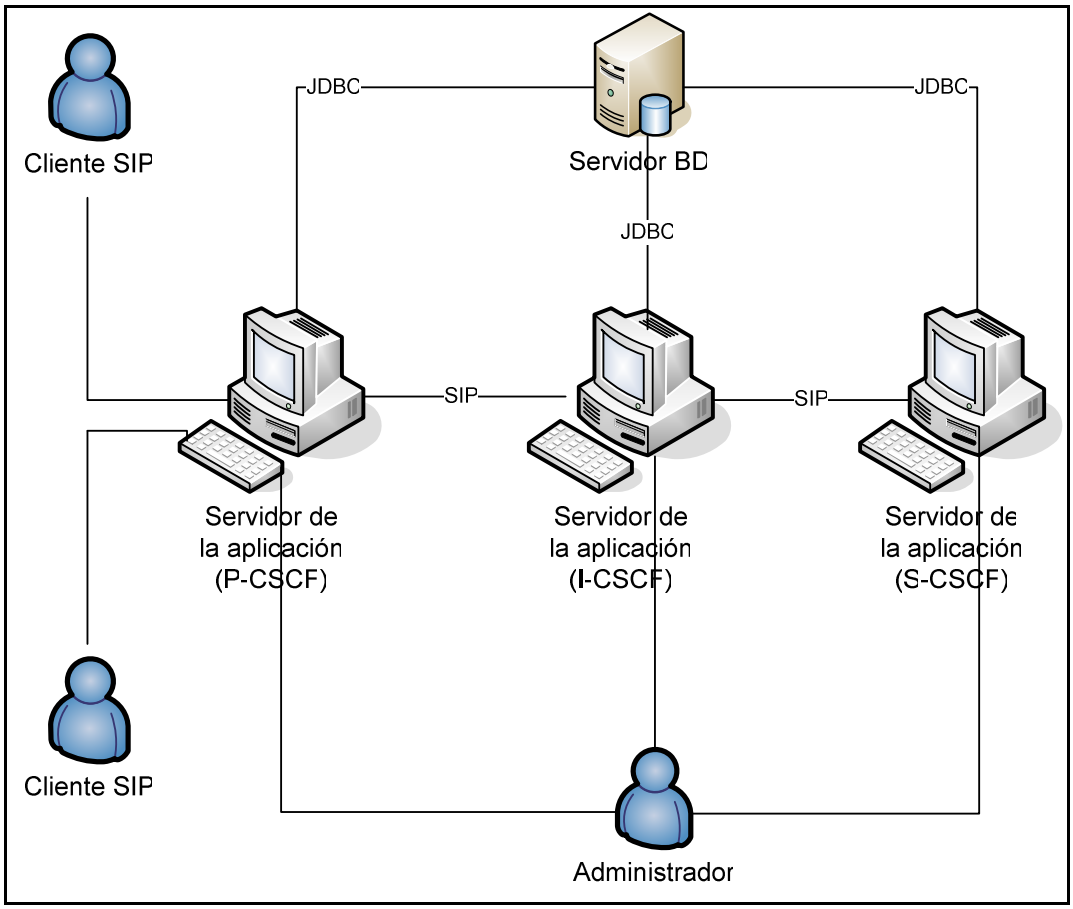


Figura 20. Arquitectura de referencia para la fase de validación

La validación del prototipo se ha dividido en tres etapas que serán explicadas a continuación:

3.2.4.1 Primera etapa: Verificación del proceso de señalización según las especificaciones del 3GPP

Para la verificación de los mensajes se desarrolló el prototipo de un cliente SIP desde donde se envían los mensajes SIP REGISTER, SIP INVITE Y SIP BYE al servidor P-CSCF para que los procese y los transmita a su próximo destino.

El prototipo de cliente también es el encargado de generar las respuestas correspondientes a las solicitudes que le llegan.

Los mensajes son observados y analizados antes y después de ser procesados por cada unos de los servidores que hacen parte del módulo de control de sesiones, es decir por el P-CSCF, el I-CSCF y el S-CSCF.

El repositorio de los datos para el procesamiento de mensajes es una base de datos en la cual está almacenada la información necesaria para la validación del prototipo. Esta información corresponde a los datos de perfil del usuario.

3.2.4.2 Segunda etapa: Implementación de un servicio de mensajería corta

Se implementó el servicio de mensajería corta empleando la petición MESSAGE que se encuentra definida en el RFC 3428. Mediante este servicio se puede apreciar de forma mas clara la comunicación establecida entre dos Clientes SIP después de haberse registrado ante la red.

3.2.4.3 Tercera etapa: Uso de un analizador de protocolos

Validación de los procesos de señalización entre los servidores y clientes con el analizador de protocolos ETHEREAL, que permite observar las rutas de los mensajes y verificar que la señalización se realiza de forma adecuada.

En la figura 21 se puede observar los mensajes de registro y de invitación a iniciar una sesión, REGISTER e INIVITE respectivamente, que se están intercambiando entre los tres servidores, donde las direcciones IP 172.16.131.2, 172.16.130.181 y 172.16.131.1 corresponden a los equipos en los cuales se están ejecutando los sub-módulos P-CSCF, I-CSCF y S-CSCF que hacen parte del módulo de control de sesiones de usuario MCSU.

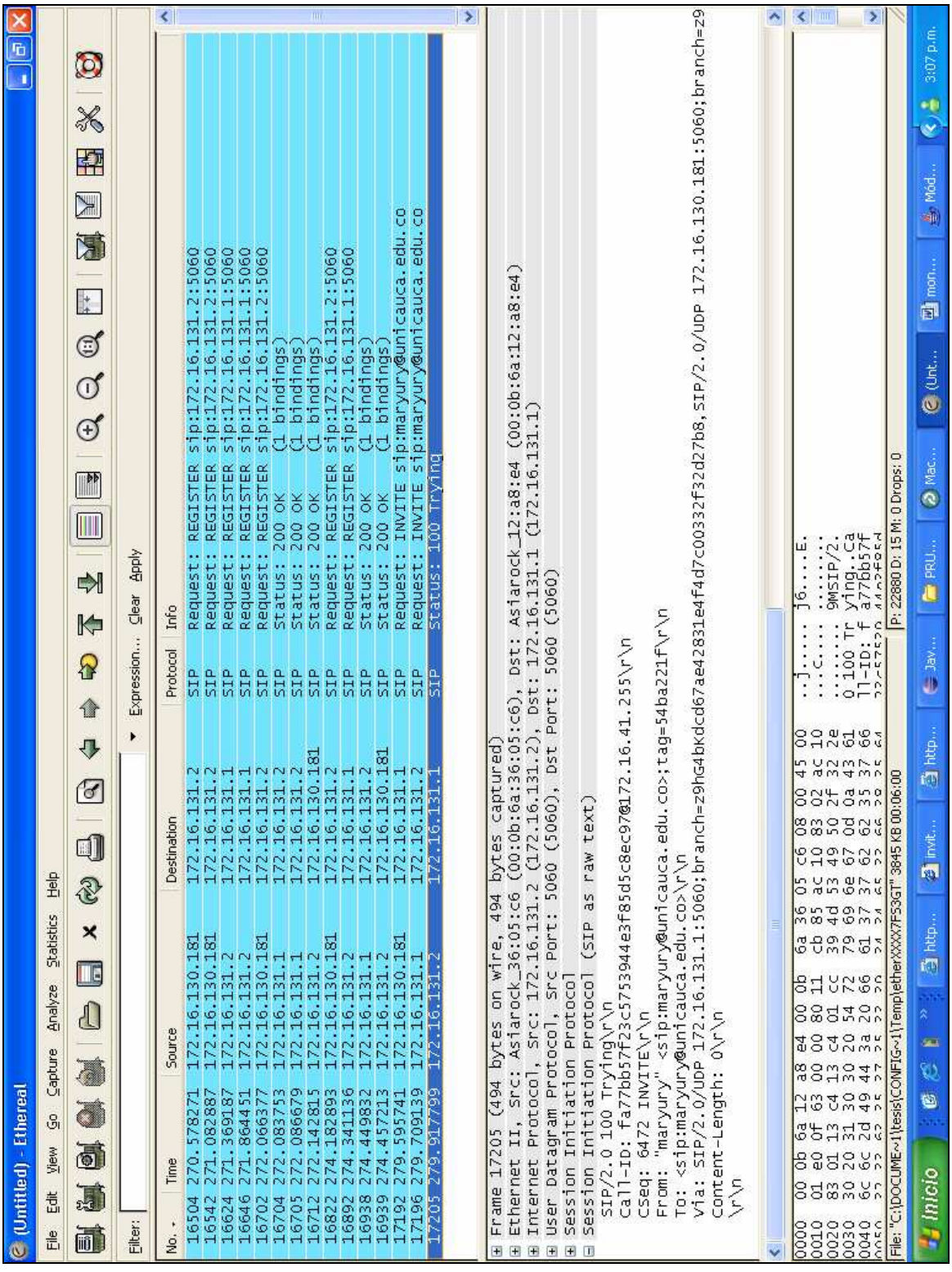


Figura 21. Prueba realizada con Ethereal

3.2.5 Restricciones del sistema

El prototipo implementado presenta algunas limitaciones, listadas a continuación:

- No se maneja compresión de los mensajes.
- Las pruebas se realizan en redes locales y dentro de la Universidad del Cauca y con las limitaciones que esto conlleva, como el uso de direcciones IP no reales.
- No se hace uso del protocolo DIAMETER para la obtención del perfil del usuario. El uso de este protocolo no influye en el comportamiento del sistema realizado, el módulo cumple con los requisitos necesarios para el control de sesiones y como no existe en la actualidad un HSS para poder realizar pruebas, el manejo del protocolo DIAMETER no es necesario para el funcionamiento de este sistema realizado.
- No implementa algoritmos de autenticación.
- No se realiza la función de ocultamiento de red. Esta función es realizada por el servidor I-CSCF, según los especifican los documentos del 3GPP, para proteger la integridad de la información que maneja el servidor S.-CSCF dentro de la red de un operador, pero esto tampoco influye en el control de la sesión de un usuario.

4 MODULO DE CONTROL DE SESIONES DE USUARIO MCSU EN LA RED

4.1 EL MÓDULO MCSU Y LAS REDES DE TELECOMUNICACIONES ACTUALES

En un entorno donde todas las sesiones se dieran entre dispositivos de usuario con capacidad IP, no se necesitaría otra cosa que los CSCFs y el HSS. Pero en la actualidad eso no es así, y teniendo en cuenta que las redes de conmutación de circuitos no están capacitadas para proporcionar servicios multimedia, como Push to Talk, servicios de presencia, entre otros, IMS soporta varios nodos para interconectarse con las redes tradicionales. Éstos son el Media Gateway -pasarela de medios- (MGW), Media Gateway Control Function –Función de Control de la Pasarela de Medios- (MGCF), y el Signaling Gateway -Pasarela de Señalización- (SGW).

La solución que se describe a continuación se hizo pensando en la convergencia de redes de telecomunicaciones que se puede lograr mediante IMS. En este caso se propone la interconexión del modulo desarrollado y de los componentes de interconexión de IMS con las redes actuales, tanto móviles como fijas.

4.2 GATEWAYS PARA LA INTERACCIÓN DEL MCSU CON LAS REDES ACTUALES

Las gateway son las encargadas de la interacción entre el módulo de control de sesiones ubicado dentro de la arquitectura IMS y las redes de telecomunicaciones actuales, tanto móviles como fijas; es decir que las gateways deben permitir la interacción de la red PSTN y las redes móviles actuales con las redes de nueva generación.

Las gateways deben servir de puente entre redes de diferentes características, incluyendo PSTN, SS7 y redes IP. Esta función de puente incluye la validación e

iniciación del establecimiento de la llamada y responsabilidades de manejo del tráfico de voz y datos a través de varias redes.

Existen muchos tipos de gateways, pero se puede hace una división general según su funcionalidad en tres grupos: Gateway de señalización, Gateway de acceso y Gateway de seguridad. Estas gateways tienen funciones específicas como se explica a continuación:

4.2.1 Gateway de señalización

La gateway de señalización debe manejar por lo menos los protocolos: SIP/SIMPLE, H.323 y SS7 y realizar conversiones de la señalización de un protocolo a otro. Por ejemplo, esta gateway debe crear un puente entre la red SS7 y la red de paquetes y controlar los circuitos de voz establecidos por el mecanismo de señalización convirtiendo los mensajes de señalización SS7 (CCN7) en señalización SIP y viceversa y transmitirlos entre la red PSTN y la red IMS.

4.2.2 Gateway de acceso

Las gateways de acceso deben soportar los servicios de telefonía, servicios suplementarios y tráfico de Internet, que actualmente poseen los usuarios de PSTN y las redes móviles actuales. Adicionalmente, deben permitir la prestación de servicios soportados por la red IMS y otros servicios suplementarios. Dentro de estas gateways se puede encontrar las AGW, de las cuales se habla en el anexo A.

4.2.3 Gateway de seguridad

Son gateways que protegen a la red IMS contra accesos maliciosos, previniendo los ataques que pueden producirse por el acceso de redes que no tienen buenas políticas de seguridad, de esta forma se asegura que los servicios IMS se vean siempre protegidos.

Cada una de estas gateways se interconectará con el MCSU y redes como, la red IP que también cuenta con una gateway encargada de la interacción entre redes IPv4 e IPV6, la PSTN con sus respectivas pasarelas, y otras redes, como se puede apreciar en la figura 21.

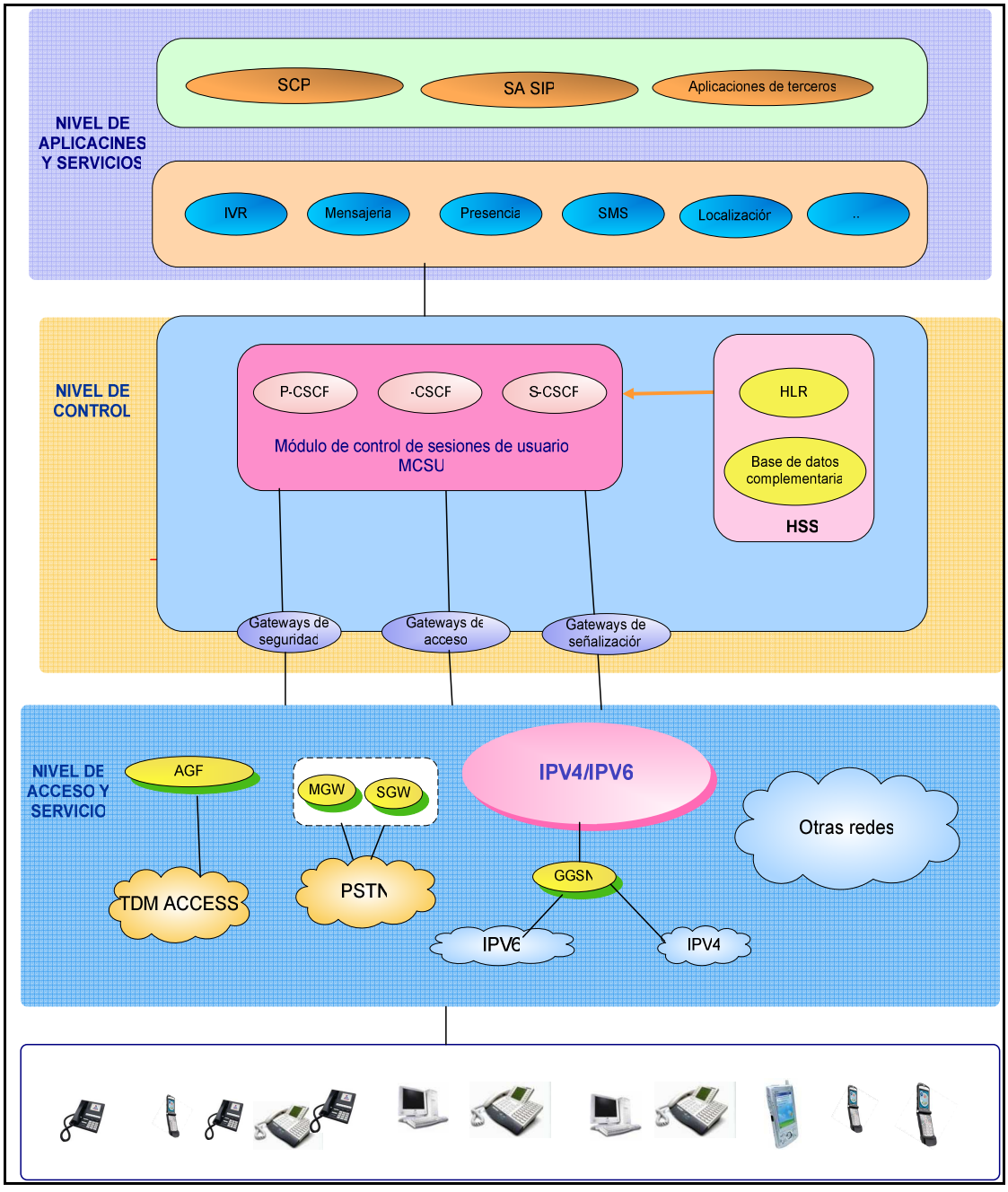


Figura 22. Integración del módulo MCSU con las redes actuales

4.3 EL MCSU Y LA PSTN

Actualmente la PSTN usa como protocolo de señalización SS7, protocolo que tiene algunas limitaciones y no es tan flexible como IP. Para evitar la necesidad de que el MGCF soporte SS7, existe dentro de la arquitectura IMS una pasarela de señalización (Signaling Gateway, SGW). Su función es convertir SS7 a IP. El SGW convierte las capas más bajas de SS7 en 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.

4.4 EL MCSU Y EL HSS

En este trabajo el MCSU no interactúa con un HSS, sino con una base de datos que contiene algunas características del HSS, algunas de esas características son complementarias a las que le hacen falta a un HLR para convertirse en un HSS.

El HSS es un elemento clave en la arquitectura IMS y de la convergencia de redes. Este es una ampliación del HLR actual, entonces es la evolución del HLR un elemento importante a la hora de buscar la compatibilidad entre redes.
En este momento no se cuenta con un HSS funcionando, pero si existen un HLR al cual se le deben hacer algunas adiciones funcionales, como se puede ver en la figura 10, donde en el lado izquierdo se muestra el HLR de una red actual y en el lado derecho se muestra la un HLR con propiedades adicionales para que pueda convertirse en un HSS.

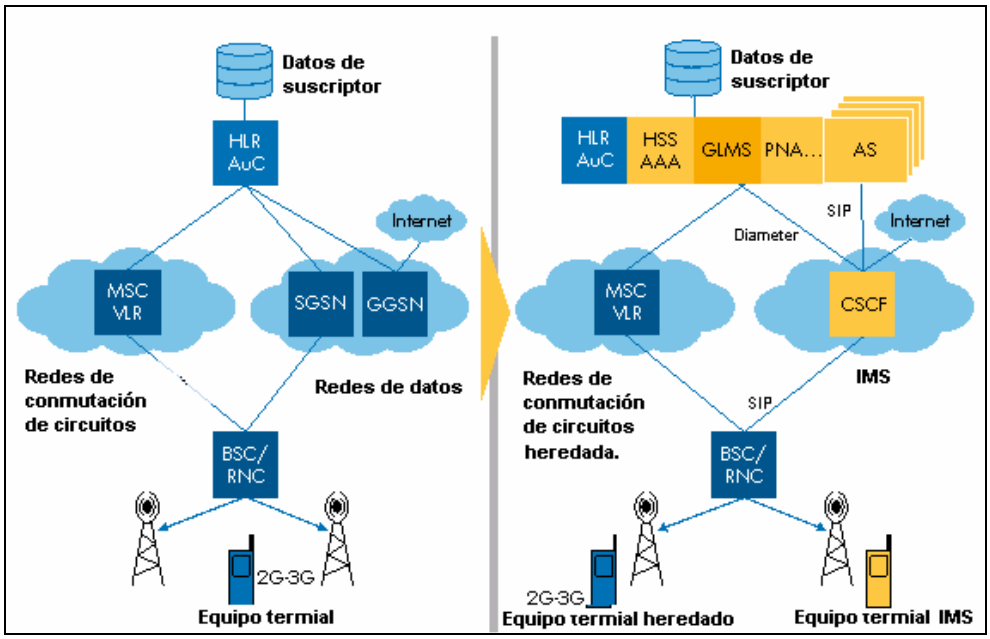


Figura 23. Cambio de HLR a HSS[35]

En las redes inalámbricas el HLR es un repositorio central de información de datos, donde se almacenan datos como, números, permisos etc. El HSS es una versión mejorada del HLR que tiene muchas mas características aparte de las heredadas del HLR y es el reposirotio principal de los datos más específicos de suscriptor y del servicio, el HSS combina el HLR el AuC (Authentication Center) funcionalidades de la red GSM y también provee información específica requerida para las redes IMS .

Información requerida por IMS:

Perfil de usuario del usuario:

- Una identidad privada y varias identidades públicas, una identidad publica para cada servicio que el usuario tenga en su perfil
- El estado del usuario
- El perfil de los servicios de cada usuario.

Hasta que no se cuente con toda la información que se requiere para el manejo de sesiones IMS será muy difícil poder gozar de todos los beneficios que esta arquitectura trae para la nueva era de las telecomunicaciones.

Existen muchos otros aspectos que se deben tener en cuenta para la interacción del MCSU en con las redes fijas y móviles actuales, pero esos detalles aún están siendo estandarizados por el 3GPP y TISPAN y se espera que el estándar de IMS para redes fijas este listo para finales del año 2007, no ocurre lo mismo con el estándar de IMS para redes móviles el cual se espera para finales del año 2008 o 2010.[36]

5 CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

5.1 CONCLUSIONES

- Este proyecto de investigación es pionero en Colombia; cuando se inició con la el desarrollo no se contaba con ningún antecedente que permitiera tener una base teórica o práctica realizada en el país y las investigaciones y desarrollo a nivel mundial se realizaron paralelamente a este trabajo, por esta razón el trabajo investigativo fue mucho mas extenso de lo que se había planeado. Por otro lado, en el mundo se han realizado o implementaciones propietarias pero en Colombia, aún no se ha encontrado registro de ningún trabajo de este tipo.

- Es muy difícil trabajar con tecnologías que todavía no se han estandarizado, los cambios que puede haber en el transcurso pueden ser de poca o de mucha trascendencia, pero eso es muy difícil de predecirlo y por dicha razón se puede presentar algunos inconvenientes en cuanto a los cambios repentinos que se deben hacer cuando se habla de un proceso de desarrollo software.

- El módulo de control de sesiones de usuario, a través de sus tres servidores el P-CSCF, El I-CSCF Y S-CSCF intercambia y procesa los tres mensajes de señalización indispensables para el control de la sesión de usuarios, SIP REGISTER, SIP INVITE Y SIP BYE, de esta forma se da solución al objetivo más importante de este trabajo de grado, el desarrollo de un prototipo de control de sesiones de usuarios según la arquitectura IMS. Resultados exitosos.

- El prototipo de cliente desarrollado y el servicio de mensajería permiten validar de forma satisfactoria el módulo de control de sesiones, adicionalmente se utilizo un analizador de protocolos para verificar el trafico entre los tres servidores que hacen parte del módulo, de donde se pudo obtener los resultados esperados, concluyendo de esta forma que el trabajo realizado a cumplido con todos los objetivos generales y específicos propuestos.

5.2 RECOMENDACIONES Y TRABAJOS FUTUROS

- Usar el protocolo DIAMETER e implementar las interfaces correspondientes de comunicación a través del protocolo para lograr la interoperabilidad del CSCF con un HSS real.

- El prototipo desarrollado maneja la señalización de control para elementos que se encuentren dentro de la misma red o dominio, seria conveniente lograr la comunicación entre redes diferentes utilizando la resolución de nombres de dominio mediante un DNS.

- Implementar propiedades de ocultamiento de red en el servidor I-CSCF, para contar con una mayor seguridad a la hora de intercambiar mensajes de señalización entre los servidores.

- Realizar el estudio del protocolo IPV6 para agregar las funcionalidades de seguridad requeridas para la señalización entre las diferentes entidades de la arquitectura IMS con las que interactúa el CSCF.

- Realizar un HSS o un prototipo del mismo para el almacenamiento de los datos

- En una red puede existir uno o varios HSS, es conveniente que se haga un estudio detallado del SLF que es un nodo, dentro de la arquitectura IMS, encargado de buscar

dentro de un grupo de HSS, el HSS que contiene el perfil de determinado usuario. Para esto es necesario también agregar al módulo el manejo de la cabecera P-USER-DATABASE

- Se puede realizar un estudio del manejo de las capacidades que un operador móvil asignaría a un S-CSCF, es decir se puede mejorar los criterios de asignación de un S-CSCF a un usuario determinado.

- El módulo realizado se encarga únicamente del control de las sesiones, un buen trabajo futuro desarrollar un modulo de tarificación y facturación, y agregarle al módulo la funcionalidad de procesar las cabeceras P-CHARGING- FUNCTION y P-CHARGING-VECTOR, necesarias para esta función.

- Agregar la función de autenticación de usuario, por medio del algoritmo AKA.

- Realizar el estudio y realizar un prototipo de otras entidades de IMS e Integrarlas con el módulo de control de sesiones

BIBLIOGRAFÍA

[1]. División de Relaciones Corporativas y Comunicaciones de Telefónica I+D. [En línea]. Abril 2006, Número 38. Madrid, España. ISSN: 1130-4693. Disponible en web: http://www.tid.es/documentos/revista_comunicaciones_i+d/numero38.pdf [Consulta: Mayo 15 de 2006]

[2]. Navarro, Orlando; Urrutia, Carlos. "El siguiente paso en la evolución de las comunicaciones" Revista AHCIET Móvil [En línea]. Septiembre 2004, Número 1. Disponible en web: <http://www.ahcietmovil.com/comun/portales/1003/10029/10083/10452/docs/42.pdf> [Consulta: Octubre 1 de 2005]

[3]. ERICSSON. "IMS: hacia los servicios multimedia". [En línea]. <http://www.ericsson.com/es/novedades/ims.shtml> [Consulta: Agosto 10 de 2005]

[4]. 3GPP; TS 23.228. "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 6)" [En línea]. Valbonne, Francia: 3GPP, Septiembre 2005. Disponible en web: <http://www.3gpp.org/ftp/Specs/archive/23_series/23.228/23228-6b0.zip> [Consulta: Octubre 10 de 2005]

[5]. División de Relaciones Corporativas y Comunicación de Telefónica I+D (ed) "Las Telecomunicaciones y la Movilidad en la Sociedad de la Información" [En línea]. Primera Edición. Madrid: Telefónica I+D. AHCIET, 2005. 429p. ISBN: 84-89900-37-X. Disponible en web: <http://enter.ie.edu/enter/file/espanol/texto/ID_261.pdf> [Consulta: octubre 7 de 2005]

[6]. Attal, Dennis. Revista de telecomunicaciones de Alcatel. "IMS: La telefonía en la era Internet". [En línea]. Paris, Francia 2005. Disponible en web:

<http://www.alcatel.com/doctypes/articlepaperlibrary/pdf/ATR2005Q1/T0503-IMS-ES.pdf> [Consulta: Noviembre 11 de 2005]

[7]. División de Relaciones Corporativas y Comunicación de Telefónica I+D (ed) "Las Telecomunicaciones y la Movilidad en la Sociedad de la Información" [En línea]. Primera Edición. Madrid: Telefónica I+D. AHCIET, 2005. 429p. ISBN: 84-89900-37-X. Disponible en web: <http://enter.ie.edu/enter/file/espanol/texto/ID_261.pdf> [Consulta: octubre 7 de 2005]

[8]. INTEL, "Enhanced Service Delivery: IP Multimedia Subsystems and AdvancedTCA". [En línea]. 2005. Disponible en web: http://download.intel.com/network/csp/pdf/9342wp.pdf [Consulta: Noviembre de 2005

[9]. Byrd, **Matthew**. "An Introduction to the IP Multimedia Subsystem (IMS)" [En línea]. Enero de 2006 Disponible en web: <http://www.convergedigest.com/bp-c2p/bp1.asp?ID=295&ctgy> [Consulta: Febrero de 2006]

[10]. Burke, David; O'Flanagan, Darragh. "An IMS Application Example Based on SIP Servlets and VoiceXML". [En línea]. Junio de 2006 Disponible en web: <http://dev2dev.bea.com/pub/a/2006/06/ims-sip-voicexml.html>. [Consulta: Junio de 2006]

[11]. Radio electronics. "IMS, IP Multimedia Subsystem Tutorial". [En línea]. 2006 Disponible en web: http://www.radio-electronics.com/info/telecommunications_networks/applications/ims/ims.php

[12]. Commited 2U.TELCO. "NGN dan IMS Perbedaan Keduanya adalah". [En línea]. Junio de 2006 Disponible en web: http://www.ristishop.com/portal/portal_article_detail.php?id=344&lang [Consulta: 27 de Junio de 2006]

[13]. Alcatel. "Fixed - Mobile - IP Convergence". [En línea]. Disponible en web: <www.alcatel.com> .[Consulta: Julio de 2006]

[14]. ETSI TS 101 046 V7.1.0 (2000-07) Digital cellular telecommunications system (Phase 2+). "Customised Applications for Mobile network Enhanced Logic (CAMEL)"; CAMEL Application Part (CAP) specification (GSM 09.78 version 7.1.0 Release 1998). [En línea]. Disponible en web: <http://webapp.etsi.org/action/PU/20000808/ts_101046v070100p.pdf>

[15]. Carat, Gérard. "El papel potencial de las tecnologías móviles en los países candidatos" European Commission. The IPTS Report [En línea]. Sevilla, España. Disponible en web: <http://www.jrc.es/home/report/spanish/articles/vol77/ICT4S776.htm>

[16]. Fabini, Joachim; Reichl, Peter; Poropatich, Alexander; Huber, Rainer; Jordan, Norbert. "IMS in a Bottle: Initial Experiences from an OpenSER-based Prototype Implementation of the 3GPP IP Multimedia Subsystem". [En línea]. Vienna, Austria. Disponible en web: <http://userver.ftw.at/~reichl/publications/idpt06.pdf>.

[17]. Courau, F; Olsson, M. Erisson, Alcatel "Policy and Regulatory Requirements for Future Mobile Networks". [En línea]. Junio 22 de 2005. Disponible en web: <http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/public_consult/ngn/comments/coureau.ppt >. [Consulta: 27 de Noviembre de 2005]

[18]. Vera, Arturo. "Sistemas celulares de tercera generación". [En línea]. Venezuela. Disponible en web: <http://www.monografias.com/trabajos15/telefonia-celular/telefonia-celular.shtml#TERC>

[19]. Witzel, Andreas. Erisson Review número 4,2000. "Servidores de control de núcleo". [En línea]. Disponible en web: http://www1.ericsson.com/ericsson/corpinfo/publications/review/2000_04/files/es2000044.pdf

[20]. Teletec. "IMS: An Architectural Overview from a Signaling Perspective.pdf" [En línea]. Mayo de 2005. Disponible en web: <http://www.tekelec.com/rcenter/whitepapers/tklc_ims_architecture_wp.pdf>

[21]. http://www.radvision.com/NR/rdonlyres/FC60D840-1FE5-4F82-A6A2-088D2D4AADCB/0/IMSSIPWhitePaper.pdf

[22]. IETF. RFC 3261. "SIP: Session Initiation Protocol". [En línea]. Disponible en web: http://www.rfc-archive.org/getrfc.php?rfc=3261

[23]. Moreno Martín, Manuel. "Una primera aproximación al protocolo SIP". Revista de Telecomunicaciones AHCIET [En línea]. Abril 2002. Vol 91. p. 70-80. Disponible en web: <http://ahciet.net/comun/portales/1000/10002/10007/10302/docs/009.pdf>. [Consulta: Julio 13 de 2005]

[24]. Cruz, Yudivián. "Plataforma para el establecimiento y desarrollo de conferencias multimedia." [En línea]. Disponible en web: <deltha.uh.cu/~yudy/pdf/uhvc.pdf - Resultado Suplementario >

[25]. SIP Center. "Characteristics" [En línea]. Wales, UK. Disponible en web: <http://www.sipcenter.com/sip.nsf/html/Characteristics> [Consulta: Julio 29 de 2005]

[26]. Acosta, Diego Andrés. "SIP: Session Initiation Protocol" [En línea]. Madrid, España. Disponible en web: <http://greco.dit.upm.es/~david/TAR/trabajos2002/01-SIP-%20Diego-Acosta.pdf> [Consulta: Julio 29 de 2005]

[27]. RFC 3455 "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)" [En línea]. Disponible en web: < http://www.rfc-archive.org/getrfc.php?rfc=3455 >

[28]. Telefónica. " Características técnicas de las interfaces de Telefónica España"[En línea]. Disponible en web: <http://www.recursosvoip.com/docs/spanish/ITE_BA_009_v1.pdf >

[29]. 3GPP. TSG-CN. Marzo de 2004. [En línea]. Disponible en web: <http://www.3gpp.org/ftp/tsg_cn/tsg_cn/TSGN_23/Docs/PDF/NP-040039.pdf.>

[30]. 3GPP. TR 45. "All-IP Core Network Multimedia Domain" [En línea]. Disponible en web: http://ftp.tiaonline.org/tr-45/tr452/Public/PN-3-4935.007_X.P0013.007_IMS_Charging_Architecture/PN-3-4935.07%20v033%20IMS%20Charg%20Arch%20Post%20Ballot.doc

[31]. 3GPP TS 32.200. "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging principles. Release 5. [En línea]. Disponible en web: http://www.3gpp.org/ftp/Specs/archive/32_series/32.200/32200-590.zip

[32]. TISPAN. Shopia Antipolis. [En línea]. Disponible en web: <http://portal.etsi.org/docbox/TISPAN/Open/Joint_Meetings/2005-07_3GPP_TISPAN_Sophia/CT1-WG3/07TD058%20Overlap_WI3019.doc >

[33]. SIP Center. "3G and SIP" [En línea]. Wales, UK. Disponible en web: <http://www.sipcenter.com/sip.nsf/html/3G+and+SIP> [Consulta: Julio 29 de 2005]

[34]. Cookson Martin, Smith David. "3G Service Control" [En línea]. Wales, UK. Disponible en web: <http://www.sipcenter.com/sip.nsf/html/WEBB5YH724/$FILE/3G_Service_Ctl.pdf> [Consulta: Enero 12 de 2006]

[35]. Webinar de Light Reading. "The Rol of IMS"in PSTN migration to VoIP"

[36]. Zinaty, Simón. EFORT. Conferencia de redes de Nueva Generación. Universidad del cauca. Agosto de 2006

GLOSARIO

3GPP: 3rd Generation Partnership Project

AAA: Authentication, Authorization, and Accounting

AAS: Associated Address Space

API: Application Programming Interface

AKA: Authentication and Key Agreement

AS: Application Server

BGCF: Breakout Gateway Control Function

BSC: Base Station Controller

CAMEL: Customized Applications for Mobile network Enhanced Logic

CAP: CAMEL Application Protocol

CSE: CAMEL Service Environment

CDMA: Code Division Multiple Access

CCF: Charging collection function

CORBA: Common Object Request Broker Architecture

CSCF: Call Session Control Function

ECF: Event Charging Function

EJB: Enterprise Java Beans

FMC : Fixed Mobile Convergence

GPRS: General Packet Radio Service

GSM: Global System for Mobile Communications

GSM: Global System for Mobile Communications

HSS: Home Subscriber Server

I-CSCF: Interrogating CSCF

IETF: Internet Engineering Task Force

IM-MGW: IP Multimedia Media Gateway

IM-SSF: IP Multimedia - Service Switching Function

IMS: IP Multimedia Subsystem

IP: Internet Protocol

ISIM: IP Multimedia Services Identity Module
ISUP: ISDN User Part
JAAS: Java Authentication and Authorization Service
JDBC: Java Database Connectivity
JMF: Java Media Framework
JNDI: Java Naming and Directory Interface
MGCF: Media Gateway Control Function
MGW: Media Gateway
NAI: Network Access Identifier
NAPT: Network Address and Port Translation
NAT: Network Address Translation
OSA-GW: Open Service Access - Gateway
PCMCIA: Personal Computer Memory Card Interface Adapter
P-CSCF: Proxy CSCF
PDA: Personal Digital Assistant
PDF: Policy Decision Function
OSA SCS: OSA Service Capability Server
RACS: Resource and Admission Control Subsystem
RTCP: Real Time Control Protocol
RTPC: Red Telefónica Pública Conmutada
RDSI: Red Digital de Servicios Integrados
RSVP: Resource Reservation Protocol
RTP: Real Time Protocol
SDP: Session Description Protocol
SOFDMA: Scalable Orthogonal Frequency Division Multiplexing Access
SSCF: Serving CSCF
SSL: Secure Socket Layer
TAS: Telephony Application Server
THIG: Topology-Hiding Inter-network Gateway
UAC: User Agent Client
UMTS: Terrestrial Radio Access Network

UAS: User Agent Server

UICC: Universal Integrated Circuit Card

USIM: Universal Subscriber Identity Module

URL: Uniform Resource Locator

WAP: Wireless Application Protocol

WWW: World Wide Web

XML: Extensible Markup Language