Universidad Nacional Autónoma de Nicaragua

UNAN – León

Departamento de Computación

Ingeniería en Telemática

Implementación de los servicios de control de sesión (IMS) para el soporte de telefonía y multimedia a través de IP con la herramienta OpenIMS

Integrantes:

Alejandro Antonio Mora Montes

Charles Shalim Mcfield Quinn

Reyna Susana Larios Centeno

Tutor:

- Msc.: Denis Leopoldo Espinoza Hernández

León, 2 de Julio de 2013

DEDICATORIA

A Dios y a la Virgen María:

Por darme la oportunidad de vivir y por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente.

A mi madre Sonia:

Porque es mi centro de inspiración y el principal cimiento para la construcción de mi vida profesional por darme tantos consejos y gracias a ellos puedo concluir mis estudios, por estar a mi lado siempre que la necesite apoyándome incondicionalmente a pesar de tanto sacrificio.

A mi padre Luis:

Por haberme apoyado en todo momento, por sus consejos y sus valores que me ha permitido ser una persona de bien. Sentó en mí las bases de responsabilidad y deseos de superación, en el tengo el espejo en el cual me quiero reflejar, pues sus virtudes infinitas, sus sacrificios y su gran corazón hacen que la admire cada día más.

A mis hermanos:

Por ser un ejemplo a seguir guiándome, apoyándome siempre en lo que pueden.

A mi novia Reyna García.

Por siempre estar a mi lado, brindándome dedicación y ser el pilar principal de mi vida con su apoyo constante, amor incondicional, ha sido amiga y compañera inseparable, fuente de sabiduría, calma y consejo en todo momento.

A mis maestros por haberme transmitido sus conocimientos y haberme llevado pasó a paso en el aprendizaje de mi vida universitaria.

Br.: Alejandro Antonio Mora Montes

DEDICATORIA

A mis padres por los inmensos sacrificios que han hecho por mí para ayudarme a alcanzar mis metas, a mi tía por el apoyo que me ha brindado durante el transcurso de todo este periodo y a mi novia por siempre estar a mi lado motivándome y aconsejándome para alcanzar mis sueños.

Br.: Charles Mcfield

DEDICATORIA

A mi Familia y Amigos.

Br.: Susana Larios

AGRADECIMIENTO

Principalmente a Dios quien me guía en todo momento y me da la fuerza de seguir adelante para cumplir una de mis metas

A nuestro tutor, Msc. Denis Leopoldo Espinoza Hernández maestro y amigo que guio este y muchos trabajos investigativos, gracias por compartir sus conocimientos para lograr cumplir una meta más en mi vida.

A nuestros maestros, en especial al Msc. Julio Gonzales, quienes nos inculcaron buenos valores y nos llenaron de conocimientos y experiencias que fortalecieron aún más el aprendizaje que día a día recibimos en los salones de estudio.

A mis padres por haberme apoyado siempre en la realización de mis sueños, por estar conmigo cuando más los he necesitado y por el inmenso amor que me han entregado.

Br: Alejandro Antonio Mora Montes

AGRADECIMIENTOS

A Dios por brindarme la vida, la sabiduría, la oportunidad y la ayuda de alcanzar una nueva meta.

A mis padres por sus sacrificios, amor, consejos y por estar siempre a mi lado apoyando a realizar mis sueños.

A mis profesores y compañeros de clase gracias por sus enseñanzas y amistad, a todo mi familia por sus apoyo amor y cariño.

Agradezco de una manera muy especial a dos de mis profesores quienes me han inspirado durante estos últimos años, me refiero al profesor Msc. Julio Cesar González y mi tutor Msc. Denis Leopoldo Espinoza gracias por ser mis ejemplos a seguir.

Br.: Charles Mcfield

AGRADECIMIENTOS

Quiero agradecer a mi familia, principalmente a mis padres Maritza Centeno y Félix Larios, por brindarme su apoyo durante el transcurso de mi formación, a mis amigos por darme ánimos para seguir adelante. Quiero además agradecer a mi tutor, Msc Denis Espinoza de gran ayuda para ser posible este trabajo.

Br.: Susana Larios

Índice

Índice de Figuras

Índice de Tabla

I. Introducción

El sector de las telecomunicaciones está sufriendo un cambio radical por la explosión de la banda ancha, el incremento de los terminales inteligentes, y la convergencia de las infraestructuras en torno a IP. Todo esto ha obligado a las operadoras a integrar las llamadas fijas con las móviles, la voz con el acceso a Internet de banda ancha, la televisión, el vídeo bajo demanda y las aplicaciones multimedia residenciales y empresariales.

La mayoría de las operadoras de telecomunicación ofrecen paquetes de servicios cada vez más atractivos para los usuarios, como demuestra el caso del servicio “casa claro” destinado a usuarios residenciales compuesto de una tarifa plana en llamadas nacionales de voz sobre la red fija, internet de banda ancha y televisión.

Estas ofertas empaquetadas responden por un lado a las necesidades de los clientes que piden ahorro en el consumo de varios servicios, previsión del gasto y comodidad de gestión con una factura única y un punto único de soporte, pero también son atractivas para las operadoras ya que les permite establecer una relación más estrecha y rica con sus clientes y aprovechar de una forma eficiente su costosa infraestructura de red.

La evolución de las redes y el desarrollo de nuevos servicios, con requisitos cada vez más exigentes en cuanto a ancho de banda y calidad, demandan importantes inversiones. Además, en los próximos años desaparecerá poco a poco la distinción entre telefonía fija y móvil, esto incrementará enormemente la competencia entre operadoras, provocando un abaratamiento de los costos y mejoras de las prestaciones. En pocos años, el cliente acabará pagando una tarifa plana por todas sus comunicaciones, independientemente del tipo, horario y destino.

Las redes de siguiente generación pretenden fusionar dos de los paradigmas más exitosos en las comunicaciones: redes móviles e Internet. El IP (Protocolo de Internet) Subsistema Multimedia (IMS) es el elemento clave en esta arquitectura que permite proporcionar acceso ubicuo a todos los servicios que ofrece internet tales como acceso web, leer el correo electrónico, ver una película, o participar en una videoconferencia desde cualquier parte haciendo uso de un dispositivo 3G.

Finalmente, cabe destacar que este nuevo entorno los terminales finales son cada vez más completos, pero a su vez más sencillos e intuitivos de utilizar. Llegará el momento en que el cliente emplee un único terminal para comunicaciones personales y profesionales, sin preocuparse de cuál es la red de acceso pues IMS reduce los costes de creación de servicios y facilita la integración con el usuario al ser accesible por una única dirección, similar a la del correo electrónico, independientemente del dispositivo (teléfono móvil, teléfono fijo, PC, PDA, televisor, etc.) y tipo de red de acceso (UMTS, HSDPA, DSL, Wi-Max, etc.) que emplee en ese momento.

II. Antecedentes

Por un lado, se ha mencionado que la idea de IMS es ofrecer servicios de internet en todas partes y en cualquier momento utilizando tecnologías celulares. Por otro lado, se sabe que las redes celulares ya ofrecen una amplia gama de servicios que incluyen algunos de los más empleados en internet, como es la mensajería instantánea. De hecho, cualquier usuario celular puede acceder a internet mediante una conexión de datos y de esta manera tener acceso a todos los servicios que internet le puede proporcionar. Si es posible el tener acceso a internet a través de dispositivos móviles en la actualidad, ¿cuál es la necesidad de IMS?

Se debe aclarar que para comprender las ventajas de la fusión de internet y el mundo de las comunicaciones móviles se deben introducir los conceptos de los diferentes dominios en redes 3G como son: el dominio de conmutación de circuitos y el dominio de conmutación de paquetes. El dominio de conmutación de circuitos es una evolución de la tecnología utilizada en las redes de segunda generación (2G). Los circuitos de este dominio están optimizados para el transporte de voz y video, aunque también se pueden utilizar para el transporte de mensajes instantáneos.

Aunque la tecnología de conmutación de circuitos ha estado en uso desde el nacimiento de la telefonía, la tendencia actual es sustituirla con una tecnología más eficiente como lo es la conmutación de paquetes empleada actualmente en las redes celulares. El dominio de conmutación de paquetes proporciona acceso a internet a través de IP.

Mientras que los terminales 2G pueden actuar como un módem para transmitir paquetes IP a través de un circuito, los terminales 3G utilizan la tecnología nativa de conmutación de paquetes para realizar comunicaciones de datos. De esta manera, las transmisiones de datos son mucho más rápidas y el ancho de banda disponible para el acceso a internet aumenta dramáticamente. Los usuarios pueden navegar por internet, leer el correo electrónico, descargar videos, y hacer prácticamente todo lo que pueden hacer por cualquier otro tipo de conexión a internet tales como ISDN (IntegratedServices Digital Network) o DSL (Digital Subscriber Line). Esto significa que cualquier usuario puede instalar un cliente de VoIP en sus terminales 3G y establecer llamadas VoIP sobre el dominio de conmutación de paquetes.

A pesar de la capacidad de acceso a internet que hoy en día poseen los dispositivos móviles gracias a las redes 3G, se tiene el problema que al estar basados en un dominio de conmutación de paquetes que realiza el mejor esfuerzo, estos no ofrecen calidad para los servicios multimedia en tiempo real, es decir, la red no ofrece garantías acerca de la cantidad de ancho de banda que un usuario obtiene para una conexión particular ni

sobre el retraso de los paquetes. En consecuencia, la calidad de una conversación VoIP puede variar dramáticamente a lo largo de su duración. En un momento dado la voz de la persona en el otro extremo del teléfono puede sonar perfectamente clara y un instante más tarde puede llegar a ser imposible de entender. Tratar de mantener una conversación (o una videoconferencia) con una mala calidad de servicio pronto puede convertirse en una pesadilla.

Por lo tanto, una de las razones para la creación de IMS es la calidad de servicio necesaria para disfrutar sesiones multimedia en tiempo real. IMS se encarga del establecimiento de la sesión de sincronización con la provisión de QoS para que los usuarios tengan una experiencia predecible. Sin embargo, muchos de estos servicios (voz, mensajería, datos, multimedia) pueden ser prestados fuera de IMS también. Dos usuarios pueden establecer una videoconferencia sobre el dominio de conmutación de circuitos y enviarse mensajes multimedia a través de MMS. Al mismo tiempo, pueden navegar por la web y consultar el correo electrónico en el dominio de conmutación de paquetes (por ejemplo, GPRS, General Packet Radio Service). Pueden incluso tener acceso a un servidor de presencia en internet para comprobar la disponibilidad de más personas que quieran unirse a la videoconferencia.

Dado que todos los servicios que se acaban de describir se pueden proporcionar con una excelente calidad de servicio sin IMS, entonces ¿qué ofrece realmente IMS? En primer lugar, el IMS proporciona todos los servicios que se utilizan sobre una tecnología de conmutación de paquetes, que es generalmente más eficiente que la tecnología de conmutación de circuitos. Sin embargo, la verdadera fuerza de IMS en comparación con la situación anterior es que el IMS crea un entorno de servicio donde cualquier servicio puede acceder a cualquier aspecto de la sesión. Esto permite a los proveedores crear servicios mucho más ricos que en un entorno donde todos los servicios son independientes el uno del otro. Por ejemplo, un servicio puede insertar un anuncio en una conferencia basada en un acontecimiento que sucede en internet, al igual que el cambio de estado de presencia de un colega de ocupado a disponible. Otro de los servicios podría ser, por ejemplo, aparecerán en la pantalla del usuario la página web de la persona que está llamando cada vez que se recibe una llamada. Por otra parte, el mismo servicio puede establecer automáticamente el estado de presencia del usuario a ocupado y desviar las llamadas entrantes a una dirección de correo electrónico en lugar del correo de voz normal.

III. Planteamiento del problema

No obstante todas las bondades que IMS ofrece a operadores y usuarios esta continúa siendo aún una tecnología bastante novedosa por lo cual se hace necesario el estudio de dicha arquitectura así como un análisis de la interacción que los usuarios y servicios tienen con el núcleo de IMS.

A raíz de esto nos planteamos las siguientes interrogantes:

- ¿Cuál sería la infraestructura de red apropiada para desplegar IMS de tal forma que se facilite el estudio de los mensajes que se intercambian entre el núcleo, los clientes y los servicios?
- ¿Qué mensajes son intercambiados entre los clientes y el núcleo de IMS en los procesos de autenticación de usuario y acceso a servicios nativos y cuál es el significado de los mismos?
- ¿Qué diferencia existe en el acceso a servicios por parte de los usuarios cuando estos son externos al núcleo de IMS tomando en cuenta ejemplos de servicios en que utilizan el protocolo SIP y servicios que no?

IV. Justificación

Hoy en día las comunicaciones son muy indispensables en todo ámbito, pues facilitan los negocios y las relaciones personales. Sin embargo vivimos en un mundo que día tras día evoluciona tecnológicamente buscando la satisfacción de las necesidades humanas, por lo cual es necesario realizar un estudio de nuevas arquitecturas que permitan ofrecer servicios unificados a fin de mejorar el servicio multimedia y de datos para así solucionar problemas de comunicación como la poca interoperabilidad entre las diferentes redes existentes actualmente.

4.1. Originalidad

Anteriormente en la UNAN – León, no se ha realizado ningún estudio acerca de este tema. Es importante destacar que a nivel mundial es un tema bastante novedoso y que IMS es una arquitectura que aún se encuentra en desarrollo no obstante existen algunas implementaciones en ambientes controlados que han permitido observar las enormes ventajas que dicha arquitectura es capaz de ofrecer.

4.2. Alcance

En este proyecto no se abordaron todas las funcionalidades aportadas por la arquitectura IMS pues eso requería de un estudio mucho más exhaustivo. Dicho trabajo se enfocó en implementar un escenario de pruebas empleando para ello la herramienta OpenIMS a fin de estudiar los mensajes intercambiados en los procesos de:

- Autenticación de usuarios con el núcleo IMS.
- Acceso por parte de los usuarios a servicios ofrecidos nativamente por el núcleo.
- Acceso por parte de los usuarios a servicios externos al núcleo tomando en cuenta los casos en que estos servicios utilizan el protocolo SIP para la comunicación y cuando no.

4.3. El producto

El producto entregado es un análisis teórico de la comunicación llevada a cabo entre los clientes y el núcleo de IMS en los procesos de autenticación de usuario y acceso a servicios. Dicho análisis incluye:

- Gráfico de cada uno de los procesos estudiados.
- Captura de los mensajes intercambiados.

- Explicación de cada uno de dichos mensajes.

4.4. Impacto

Este análisis pretende ser la punta de lanza en el estudio de arquitecturas de redes de siguiente generación (NGN) que permitan la integración de los servicios de telefonía fija y celular con servicios multimedia a través de IP.

V. Objetivos

5.1. Objetivo general

Analizar los mensajes intercambiados en los procesos de autenticación de usuario y acceso a servicios en la arquitectura IMS para una mejor comprensión de su funcionamiento a través de la creación de un escenario de pruebas con la herramienta OpenIMS.

5.2. Objetivos específicos

- Proponer una infraestructura de red para el despliegue de OpenIMS que permita estudiar los procesos de autenticación de usuarios y acceso a servicios internos y externos al núcleo.
- Describir los mensajes intercambiados entre los clientes y el núcleo de OpenIMS en los procesos de autenticación de usuario y acceso a servicios nativos.
- Explicar la diferencia en el acceso a servicios por parte de los usuarios cuando estos son externos al núcleo de OpenIMS tomando en cuenta ejemplos de servicios en que utilizan el protocolo SIP y servicios que no.

VI. Marco Referencial

Esta sección presenta un bosquejo relacionado a IMS, así como los componentes más importantes que lo conforman como son CSCF, P-CSCF, I-CSCF, S-CSCF, también se encuentran definidos algunos de los conceptos generales de los servicios y estándares que en conjunto conforman el IMS. Dos de los elementos importantes que también están definidos son OpenIMS y HSS un elemento importante dentro del IMS.

6.1. TISPAN

TISPAN (Telecoms& Internet converged Services & Protocolfor Advanced Networks) fue desarrollado por el EIST (Instituto Europeo de Estándares de telecomunicaciones) especializada para la convergencia de redes fijas e Internet, donde asegura que los usuarios conectados a las redes basadas en IP puedan comunicarse con usuarios en redes tradicionales de circuitos tales como: PSTN, ISDN, GSM.

TISPAN es el responsable de todos los aspectos de estandarización para el presente y futuro de las redes combinadas incluyendo las redes NGN(NextGenerationNetworking o Red Próxima Generación)contemplando aspectos de: servicios, arquitectura, protocolo, estudios de QoS, estudios relacionados con la seguridad, aspectos de movilidad dentro de redes fijas, utilizando tecnologías existentes.

TISPAN está estructurado como un solo comité técnico, conformados por Grupos de Trabajo (WorkingGroups) y Equipos de Proyectos (Project Teams). (José Antonio Pajuelo Martín, 2010)

6.2. IMS

IMS es un sistema de control de sesión diseñado con tecnologías de Internet adaptadas al mundo móvil que hace posible la provisión de servicios móviles multimedia sobre conmutación de paquetes, servicios IP multimedia en general. Los servicios IMS tienden a ser implementados en una sola aplicación de tal manera que el usuario final pueda dar un uso coordinado y simultáneo de servicios multimedia como lo son las videoconferencias y el streaming, la difusión multimedia, la descarga de contenidos, los juegos en línea y cualquier otro servicio de Internet basado en TCP/IP (Transmission Control Protocol/Internet Protocol). Sin embargo, IMS no define las aplicaciones o servicios que pueden brindarse al usuario final, sino la infraestructura y capacidades del servicio que los operadores o proveedores de servicio pueden emplear para construir sus

propias aplicaciones y producir su oferta de servicios. Dentro de la arquitectura de IMS se encuentran cuatro componentes principales: (José Antonio Pajuelo Martín, 2010)

- CSCF (Call Session Control functions) es aquel que durante el registro y el período de establecimiento de sesiones realiza el enrutamiento SIP. (Miikka Poikselka, 2009)
- P-CSCF (Proxy Call Session Control Functions) es el primer punto de contacto para los usuarios dentro de IMS. Esto significa que todo el tráfico de señalización de SIP desde el usuario será enviado al P-CSCF. (Miikka Poikselka, 2009)
- I-CSCF (Interrogating Call Session Control Functions) es un punto de contacto dentro de la red para todas las conexiones con destino a un abonado específico de la red. (Miikka Poikselka, 2009)
- S-CSCF (Serving Call Session Control Function) es el punto focal de IMS, dado que es el responsable de manejar los procesos de registro, haciendo que las decisiones de enrutamiento y el mantenimiento se almacenen en el perfil de servicio. (Miikka Poikselka, 2009)

6.3. NGN

Red de Próxima Generación (NGN por su sigla en inglés) es “una red basada en la conmutación de paquetes capaz de proveer servicios de telecomunicaciones y aprovechar el uso de banda ancha y QoS, donde las funciones de servicio sean independientes de las tecnologías de transporte. Ofrece el acceso sin restricciones a distintos proveedores de servicios. Soporta movilidad donde los usuarios cuentan con servicios ubicuos y continuos provenientes desde sus proveedores de servicios.” (La Unión Internacional de Telecomunicaciones (International Telecommunications Union: ITU)). (ITU-T Rec. Y.2001, “General Overview of)

6.4. QoS

QoS o calidad de servicio (Quality of Service)” Es el efecto colectivo del rendimiento de un servicio que determina el grado de sastifacion del usuario de dicho servicio.” (ITU E.800: Terms and definitions related to quality of service and network performance including dependability, 1994).
“Conjunto de requisitos del servicio que debe de cumplir la red en el transporte de un flujo”. (IETF RFC 2386)

6.5. SIP

Session Initiation Protocol (SIP o Protocolo de Inicio de Sesiones) es un protocolo desarrollado por el IETF con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual. ((RFC 2543))

6.6. VoIP

Voz sobre Protocolo de Internet, también llamado Voz IP, es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN (sigla de Public Switched Telephone Network, Red Telefónica Pública Conmutada) (José Antonio Pajuelo Martín, 2010).

6.7. GSM

El sistema global para las comunicaciones móviles (GSM, proviene del francés group especial mobile) es un sistema estándar, libre de regalías, de telefonía móvil digital.
Un cliente GSM puede conectarse a través de su teléfono con su computador y enviar y recibir mensajes por correo electrónico, navegar por internet (José Antonio Pajuelo Martín, 2010).

6.8. GPRS

General Packet Radio Service (GPRS) o servicio general de paquetes vía radio es una extensión del Sistema Global para Comunicaciones Móviles (Global System for Mobile Communications o GSM) para la transmisión de datos no conmutada (o por paquetes).

Con GPRS se pueden utilizar servicios como Wireless Application Protocol (WAP) , servicio de mensajes cortos (SMS), servicio de mensajería multimedia (MMS), Internet y para los servicios de comunicación, como el correo electrónico y la World Wide Web (WWW) (José Antonio Pajuelo Martín, 2010).

6.9. 3G

3G es la abreviación de tercera generación de transmisión de voz y datos a través de telefonía móvil mediante UMTS (Universal Mobile Telecommunications System o servicio universal de telecomunicaciones móviles) (José Antonio Pajuelo Martín, 2010).

6.10. 3GPP

El Proyecto de Asociación de Tercera Generación o más conocido por el acrónimo inglés 3GPP 3rd Generation Partnership Project es una colaboración de grupos de asociaciones de telecomunicaciones, conocidos como Miembros Organizativos.

El proyecto 3GPP sigue una metodología basada en tres fases, tal y cómo se define en la recomendación I.130 del ITU-T:

- **Fase 1**: Se definen los servicios requeridos desde el punto de vista del usuario
- **Fase 2**: Se define una arquitectura para dar solución a los servicios requeridos.

- **Fase 3:** Se define una implementación de la arquitectura especificando los protocolos en detalle.

Se podría considerar la existencia de una fase 4 del proceso que consistiría en analizar y comprobar el funcionamiento de la especificación. Las especificaciones se agrupan en versiones. Una versión consiste en un conjunto consistente y completo de características y especificaciones. El calendario es definido para cada versión especificando y dejando marcada una fecha para cada una de las fases así como una fecha final de lanzamiento. Una vez la fecha está marcada sólo se permiten correcciones esenciales, estando prohibido añadir o modificar funciones (José Antonio Pajuelo Martín, 2010).

6.11. OpenIMS

OpenIMS/OpenIMScore, es una implementación Open Source (código abierto) de las funciones de control de sesión de llamada (CSCF) del IMS y un servidor principal suscriptor (HSS) lightweight (ligero), que en conjunto forman los elementos básicos de todas las arquitecturas IMS/NGN como se especifica actualmente en 3GPP, 3GPP2, ETSI TISPAN y la INICIATIVA Packet Cable. Los cuatro componentes están todas basadas en software de código abierto (por ejemplo, el SIP Express Router (SER) o MySQL). (Fraunhofer FOKUS, OpenSourceIms core, 2004-2008)

6.12. HSS

HSS (Home SubScriber Server) registra toda la información acerca de los usuarios y servicios dentro de un dominio IMS. El HSS registra todos los distintos perfiles, identidades y credenciales que conforman los usuarios para realizar AAA (Autenticación, Autorización y Contabilización); además contiene información acerca de los distintos servicios que tienen habilitados así como el Serving-CSCF (S-CSCF) al que se registraron, permitiendo saber su punto de conexión y habilitar servicios de itinerancia (roaming). (Miikka Poikselka, 2009)

VIII. Tecnologías Empleadas

Para realizar las pruebas e implementaciones de esta tesis se dispuso de una serie de tecnologías que en conjuntos conforman el núcleo de la arquitectura IMS. A continuación se presenta una breve descripción de cada una de ellas.

8.1. OpenIMScore

Es utilizado para implementar las funciones CSCFs (Call Session Control Functions) del IMS, compuesto también por un servidor suscriptor ligero (HSS), es de código abierto y permite hacer una simulación de la arquitectura IMS para lograr la convergencia entre redes de conmutación de paquetes y redes de conmutación de circuito. (Fraunhofer FOKUS, OpenSourceIms core, 2004-2008)

8.2. P-CSCF o Proxy-CSCF

Es el primer punto de contacto entre un terminal IMS y la red. Puede estar colocado tanto en la red local como en una red de otra compañía. Sirve para enrutar la conexión hacia los I-CSCF. (José Antonio Pajuelo Martín, 2010). (José Antonio Pajuelo Martín, 2010)

8.3. S-CSCF o Serving-CSCF

Es el nodo central en el plano de señalización de IMS. Es un servidor SIP, pero también se encarga de controlar sesiones. Simplificando un poco, es el nodo en la arquitectura IMS que se encarga de conectarse con el HSS, para descargarse o actualizar perfiles de usuarios. En la conexión con el HSS, se usa el protocolo DIAMETER, específicamente usado para funcionalidades de AAA (“Authentication, Authorization and Accounting”). (José Antonio Pajuelo Martín, 2010)

8.4. I-CSCF o Interrogating-CSCF

Es un servidor SIP que se coloca en el “borde” del dominio administrativo. La dirección IP de este servidor se agrega al registro del DNS (“Domain Name System”) al dominio que pertenece. De esta manera, otros servidores remotos pueden encontrarlo y usarlo como punto de reenvió de paquetes SIP hacia dicho dominio. (José Antonio Pajuelo Martín, 2010)

8.5. HSS

El HSS (home suscriber server) es la base de datos principal que contiene las entidades de red que están actualmente utilizando la red. Contiene información de los perfiles de los usuarios, se encarga de su autentificación y autorización, puede dar información sobre la localización física de los mismos. Es similar al GSM. Está programado en lenguaje JAVA y utiliza MySQL como sistema gestor de base de datos de código abierto. (José Antonio Pajuelo Martín, 2010)

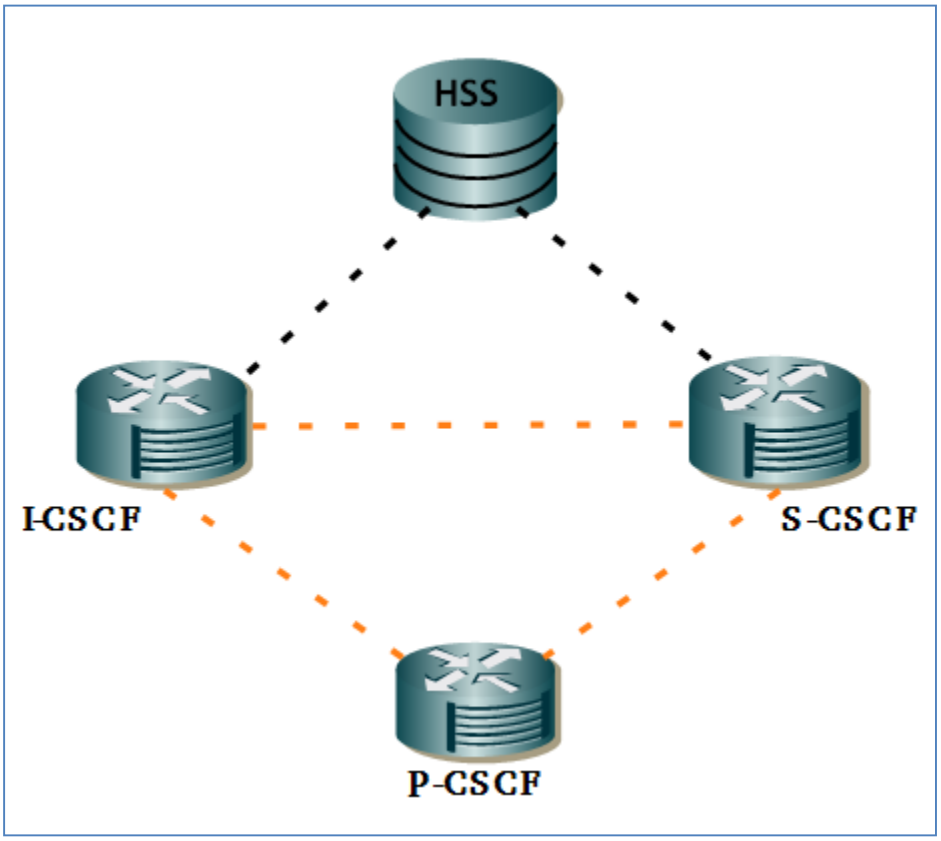


Figura 1: Núcleo IMS. (FOKUS, 2004-2008)

8.6. Protocolo de Inicio de Sesión (SIP)

SIP es un protocolo de señalización a nivel de la capa de aplicación para crear, modificar y terminar sesiones de comunicación entre uno o más participantes. Estas sesiones de comunicación incluyen: llamadas, telefonía, distribución multimedia y conferencia multimedia. (RFC 3261)

8.7. Protocolo de descripción de sesión (SDP)

SDP es un protocolo a nivel de aplicación encargado de describir sesiones multimedia. Incluye toda la información necesaria para establecer una sesión entre usuarios, como son las capacidades de los dispositivos, los protocolos empleados para entregar multimedia y los puertos de comunicación.

Por si solo SDP no puede ser un protocolo ya que únicamente es una descripción de propiedades de sesión en forma de texto, por eso se incorpora dentro del cuerpo de los mensajes INVITE de SIP que establecen la sesión.RFC (RFC 4566)

8.8. Protocolo Diameter

Diameter es desarrollado por el IETF para lograr las funciones de AAA. En IMS es usado para garantizar una comunicación y señalización confiable entre algunas funciones de IMS. También se emplea por el S-CSCF para realizar funciones AAA con el UE. SIP junto con Diameter forman el plano de control de IMS, encargados de negociar la QoS, autenticación del usuario y control de sesiones. (RFC 3588)

Las interfaces Cx y Dx son estándares que se describen en las especificaciones 3GPP TS29.228 y TS29.229 son los puntos de referencia entre los siguientes servidores:

- Home Subscriber Server (HSS): Le asigna un S-CSCF a un usuario cuando se realiza una petición mediante el I-CSCF.
- I-CSCF: Consulta al HSS utilizando la interfaz Cx para recuperar la ubicación (dominio) del usuario.
- S-CSCF: Utiliza la interfaz Cx y Dx para descargar y cargar perfiles de usuarios del HSS

8.9. RTP/RTCP

Real-Time TransportProtocol (RTP) y Real-Time Transport Control Protocol (RTCP) ambos son usados bajo IMS para transportar multimedia sobre IP. (RFC 3551)

8.10. IPSec

Internet Protocol Security usados dentro del dominio IMS para garantizar la seguridad del intercambio de mensajes entre el UE y el núcleo. (RFC 6071)

IX. La Herramienta OpenIMSCore

9.1. Escenario General de Funcionamiento

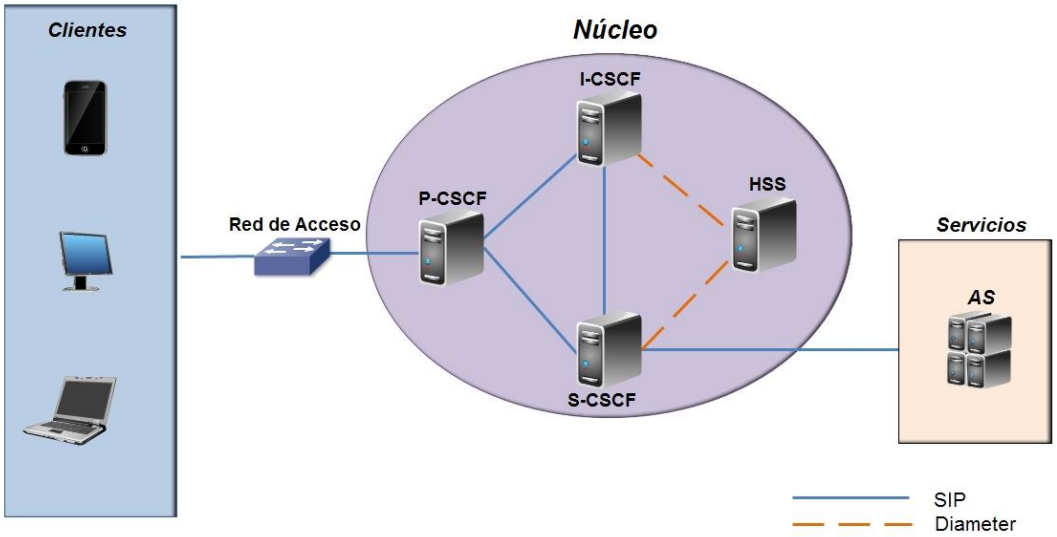


Figura 2: Escenario general. (FOKUS, 2004-2008)

Cada subcomponente tiene significado lógico, es decir pueden estar incluidos físicamente en el mismo equipo pero conectados por medio de las interfaces lógicas. En este plano se ejecutan todos los procesos necesarios para el intercambio de mensajes con el fin de ejecutar el registro de los usuarios en la red así como el establecimiento, mantenimiento y culminación de las sesiones.

El CSCF es el corazón del plano de control de IMS. Es en realidad un servidor SIP, que también implementa otros protocolos entre ellos DIAMETER. El CSCF está formado por tres componentes independientes: P-CSCF, I-CSCF y S-CSCF

El primer contacto de los clientes es a través del P-CSCF, este se comporta como un proxy de los usuarios SIP para enviar mensajes a los servidores de la red. Acepta solicitudes de los usuarios, las analiza para propósitos de enrutamiento y las retransmite, cabe destacar que el P-CSCF no modifica las solicitudes SIP del usuario sólo las retransmite.

El P-CSCF envía mensajes de registro, re-registro de sesión y de sesión INVITE a los correspondientes servidores, esto quiere decir que todas las solicitudes y respuestas desde o hacia el cliente pasan por el P-

CSCF. El P-CSCF asignado a un cliente durante el registro a nivel de IMS no cambia durante el registro, lo que significa que el cliente se comunica con un solo P-CSCF a la vez.

El HSS es una base de datos que almacena el perfil de todos los usuarios de un dominio. En la práctica pueden existir varios HSS, esto sucede cuando la capacidad de un solo HSS no es suficiente para la cantidad de usuarios de la red. El HSS implementa DIAMETER con aplicaciones específicas.

El perfil de usuario incluye información de seguridad como claves criptográficas, información relativa a los servicios asignados, el S-CSCF que ha sido asignado al usuario, entre otros.

El I-CSCF recibe mensajes SIP desde el P-CSCF y determina el S-CSCF asignado al cliente, esta asignación se realiza en función del tipo de usuario y servicios que ha contratado con el proveedor. Una vez que el I-CSCF sabe cuál es el S-CSCF asignado a un usuario re-direcciona el mensaje de registro ha dicho S-CSCF.
Cuando en una red IMS existe más de un HSS se necesita del componente SLF (Subscriber Location Function). El I-CSCF interroga al SLF indicándole el HSS donde está almacenado el perfil de usuario.

El otro componente es el S-CSCF, éste se encarga de manejar las sesiones de comunicación dentro de la red. Actúa como un Switch Center con acceso total a los perfiles de los usuarios, conecta las sesiones y administra el estado de las mismas; mantiene actualizado al HSS y es el que produce información para facturación.

El S-CSCF consulta al HSS por la información de autenticación correspondiente a un cliente que está tratando de registrarse en la red así como también el perfil de usuario de los servicios que el usuario ha acordado con el proveedor. También actúa como el nodo que almacena el enlace entre la ubicación del usuario (Dirección IP del usuario registrado en un momento dado) y el PUBLIC URI del usuario.

El S-CSCF es el encargado de suministrar servicios de enrutamiento hacia las aplicaciones; enruta las llamadas desde su origen al destino bien sea a través de otro S-CSCF, para una llamada dentro de la misma red, o a un I-CSCF si el destino de la llamada es otra red. El enrutamiento se hace de acuerdo con la dirección de destino: SIP URI o número de teléfono. También contribuye con el cumplimiento de las políticas del operador, por ejemplo negando al usuario la autorización para ciertos servicios.
Los Servidores de Aplicación son las entidades que almacenan, ejecutan servicios como: presencia, mensajería, llamadas etc. Para el núcleo IMS un AS es una entidad SIP que alberga y ejecuta servicios, pero IMS no estandariza ni describe el servicio ni la aplicación, lo que se definen son las interfaces entre el AS y el

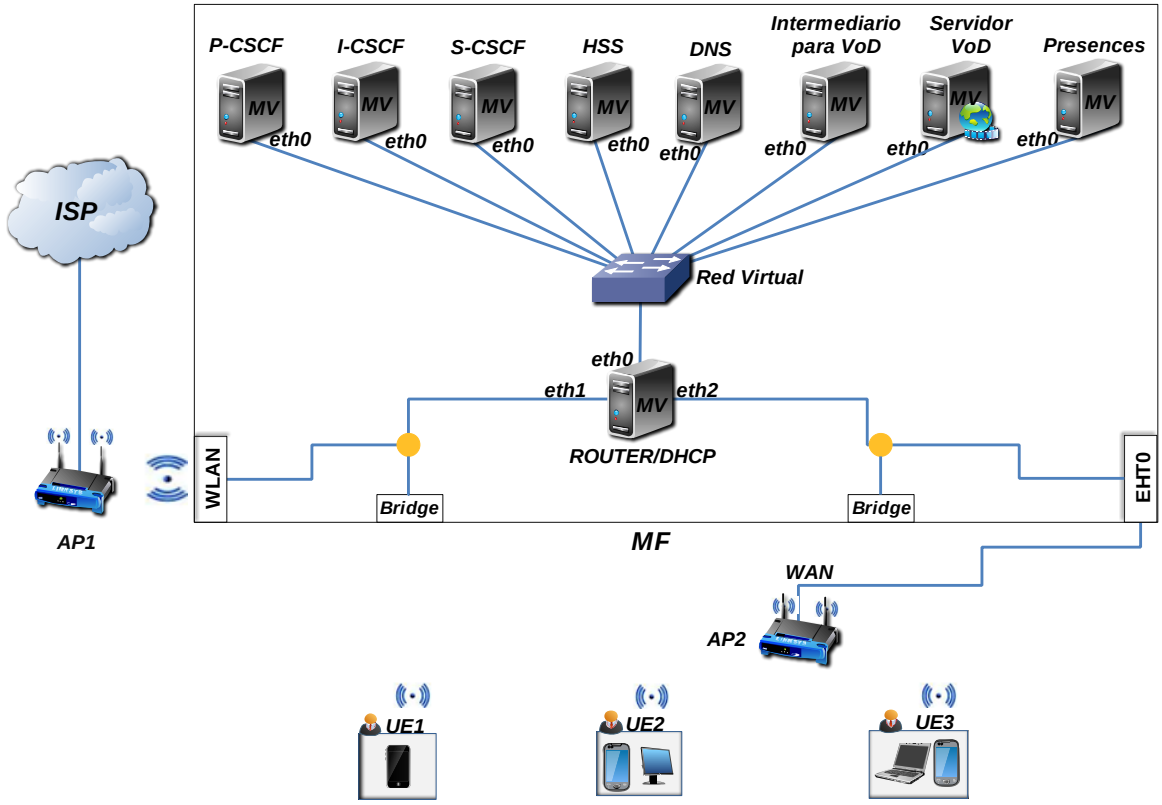
núcleo, dicha interfaz es el S-CSCF que permite el intercambio de mensajes SIP y se denomina IMS Service Control (ISC).

Los procedimientos de ISC se dividen en dos grandes categorías: aquellos que enrutan un SIP Request hacia un AS y aquellos que corresponden a un SIP Request originados en los ASs.

Las aplicaciones en IMS típicamente se implementarán en servidores nativos SIP sin embargo, muchos proveedores pueden decidir agregar ciertas funcionalidades a sus plataformas existentes que no son SIP para que se comuniquen con los servidores SIP a fin de minimizar los esfuerzos que requeriría el desarrollar todo de nuevo para una aplicación existente.

IMS permite ofrecer servicios individuales que se combinan en uno solo para que los usuarios puedan disfrutar de servicios multimedia entre diferentes dispositivos terminales. Tal es el caso del servicio VoD el cual necesita de dos entidades una que soporta el lenguaje SIP y otra que es propiamente el servicio.

9.2. Escenario de Prueba



	ROUTER/DHCP	eth0:192.170.1.2 eth1:192.168.0.29 eth2:192.170.1.129
	DNS	eth0:192.170.1.3
	Intermediario para VoD	eth0:192.170.1.4
	Servidor VoD	eth0:192.170.1.5
	Precenses	eth0:192.170.1.7
	P-CSCF	eth0:192.170.1.10
	I-CSCF	eth0:192.170.1.11
	S-CSCF	eth0:192.170.1.12
	HSS	eth0:192.170.1.13
	AP1	LAN:192.168.0.1
	AP2	LAN:192.168.1.1 WAN:DHCP

	Host o maquina Virtual (MV)
	Punto de Acceso (AP)
	Proveedor de Internet (ISP)

Figura 3 Escenario de prueba. **(Fuente Propia, 2012-2013)**

9.2.1 Equipos de usuarios

El usuario debe poseer un UE que soporte IMS o SIP y haber establecido un contrato de servicio con un proveedor. Luego debe conectarse a la red de acceso del operador sea fija o móvil con el fin de obtener una dirección IP siguiendo el procedimiento propio de la red de acceso, puede ser LTE, WiFi, WiMAX, ADSL, etc. Después que se han cumplido con estos dos requisitos, entonces se debe determinar la dirección del proxy mediante un proceso llamado P-CSCF Discovery (Consulta al DNS). Este proceso puede realizarse junto a la obtención de la dirección IP como un todo, o pueden ser procesos independientes, depende de la red de acceso. Luego el UE puede registrarse en la red IMS a través del P-CSCF

9.2.2 Servidor DHCP y Router:

Este equipo tiene 3 interfaces:

- **eth0**: Interfaz conectada a la Red virtual donde se encuentran todos los componentes necesarios del nucleo así como las AS.
- **eth1:** Interfaz conectada en modo puente con la interfaz de red Wifi de la máquina física a través de la cual se obtiene acceso a internet.
- **eth2:** Interfaz conectado en modo puente con la interfaz de red Ethernet de la máquina física, este está conectado a nuestro Access Point. En esta interfaz se ofrece el servicio de DHCP.

Este equipo también es el encargado de enrutar todos los paquetes hacia las distintas subredes.

9.2.3 Servidor DNS

Es el encargado de brindar todas las resoluciones de nombres del dominio (imscore.tesis). También realiza la traducción inversa del mismo RFC 2915. En nuestro dominio se ofrecen servicios multimedia y todos estos están encapsulado casi siempre en el protocolo SIP, para poder dar soporta a dicho protocolo, se necesitaron tipos de registros SRV (SeRVicio), también llamados registros de recursos, Este nos permite indicar el servicio que ofrece nuestro dominio. RFC 2782

9.2.4 Servidor VOD

Una maqueta IMS no puede estar completa sin tener la capacidad de ofrecer servicios multimedia, por lo cual es necesario incluir un servidor responsable de la entrega de este tipo de contenido. Dicho servidor, además de soportar tecnologías de entrega de multimedia como son RTP, RTCP y RTSP, debe ser capaz de comunicarse con el núcleo IMS vía mensajes SIP con el fin de establecer sesiones multimedia. En lugar de buscar una herramienta que cuente con ambas funcionalidades se optó por juntar dos herramientas para formar un AS que forma el servidor de VoD.

9.2.5 Servidor de presencia

Los servidores de presencia fueron introducidos originalmente por el 3GPP como un servidor independiente, definido como un sistema que permite a los usuarios suscribirse a una entidad encargada de publicar el estado de los mismos

El servicio de presencia está basado en dos grandes premisas:

- Que mi estado pueda ser visto por otro usuario agregado previamente en su lista de contactos.
- Que yo pueda ver el estado de otros usuarios agregados a mi lista de contactos

El motivador principal de los servicios de presencia es la mensajería instantánea (IM). IM se ha usado por mucho tiempo en internet y el usuario de esta forma sabrá de antemano si está o no disponible para el envió de un mensaje, en el caso de nuestro núcleo estará disponible con la herramienta OpenSips.

9.3 Requerimientos

9.3.1 Software

Cada dominio IMS se compone de un núcleo IMS que se puede implementar con la herramienta OpenIMScore creado por FOKUS. Estos dominios forman el corazón del modelo, ya que son quienes controlan las sesiones y flujos entre los usuarios. Para la implementación de estos modelos de redes se requieren instalar y configurar cada uno de los dominios para lo cual se debe descargar el código fuente de las herramientas y compilarlo para obtener los paquetes.

Para el dominio implementado en este trabajo, el código fuente de las herramientas fue compilado a fin de obtener los paquetes Debian (.deb), que fueron instalados y configurados de forma exitosa bajo DebianSqueeze6.0.1 en un entorno virtual creado con VMware Workstation 9 instalado en Ubuntu 12.10.

La figura 4 muestra de forma lógica las máquinas virtuales empleadas:

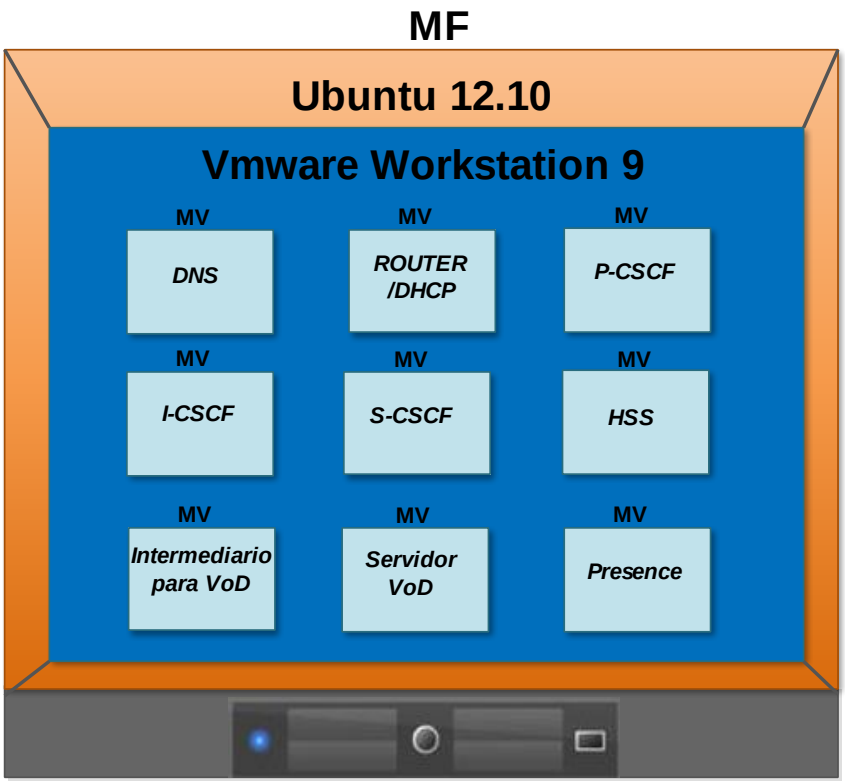


Figura 4: Entorno virtual de los Servidores. (Fuente Propia, 2012-2013)

Para lograr las instalaciones correctas primero debemos de actualizar nuestros repositorios poniendo lo siguiente:

```
deb-srchttp://ftp.antik.sk/debian/ squeezemain non-free.
debhttp://ftp.antik.sk/debian/squeeze main non-free
```

Lista de paquetes necesarios:

Tabla 9.1: Paquetes requeridos.

Paquetes para el DNS		bind9 bind9utils dnsutils
Paquetes para el DHCP		isc-dhcp-server
OpenIMScore	**Paquetes pre-requisitos para la instalación del Núcleo IMS**	subversion, bison, libcurl4-dev, debhelper, cdbs, lintian, build-essential, fakeroot, devscripts, pbuilder, dh-make, debootstrap, dpatch, flex, libxml2-dev, libmysqlclient15-dev, sun-java6-jdk, ant, docbook-to-man.
	Paquetes para la instalación del Núcleo IMS	FHoSS Ser_ims
Paquetes para los AS	**Paquetes pre-requisitos para la instalación del Presence (OpenSips)**	Gcc, bison, flex, make, openssl, libmysqlclient-dev, libradiusclient-ng2, libradiusclient-ng-dev, mysql-server, libxmlrpc-c3-dev.

	Módulos para el Presence(OpenSips)	opensips-mysql-module,opensips-jabber-module,opensips-presence-modules,opensips-xmlrpc-module,opensips-xmpp-module.
	Presence(OpenSips)	opensips
	Intermediado Para VoD (IPTV)	uctiptv_advanced1.0.0.deb
	ServidorVoD (DSS)	DarwinStreamingSrvr6.0.3-Source.tar Darwin_6.0.3_patches.zip
Paquetes para los Clientes	**Para Windows**	myMONSTER-TCS_WIN_PC_v0_9_25.exe X-Lite_Win32_1104o_56125_100106.exe (Versión 3.0)
	Para Linux	uctimsclient1.0.14.tar.gz myMONSTER-TCS_Linux32_v0.9.25.tar.gz
	Para Android	imsdroid-2.0.481.apk
	Para IPhone	Join1.0.ipa

El código fuente se pueden obtener en el siguiente enlace:

Para el hss de FOKUS (FHoSS)

```
http://svn.berlios.de/svnroot/repos/openimscore/FHoSS/trunk
```

Para el ser_ims

```
http://svn.berlios.de/svnroot/repos/openimscore/ser_ims/trunk
```

9.3.2 Hardware

Las especificaciones hardware que necesitamos para llevar acabo la implementación del dominio IMS son las siguientes:

9.3.2.1 Para la Maquina Fisica:

- Disco duro de 500GB
- RAM de7GB
- Interfaz Ethernet
- Wifi.

9.3.2.2 Para la conexión a Internet:

- Dos AP (Punto de Acceso).

Para las máquinas virtuales, cada uno cuenta con 8GB de Disco Duro y 512MB de RAM, tanto el Disco Duro como la RAM están asignada dinámicamente.

9.4 Instalación y configuración del núcleo de la red

La instalación de los dominios IMS requiere descargar el código fuente de las herramientas y compilarlos justo como lo habíamos mencionado en el apartado anterior. En este apartado haremos mención sobre cómo llegamos a construir el núcleo de nuestro dominio IMS así como los servicios agregados al mismo.

Antes de continuar y primero que todo debemos tener ya instalado y corriendo en una máquina (en nuestro caso DebianSqueeze 6.0.1) las herramientas necesarias para la compilación de los paquetes del núcleo IMS [Ver Tabla 9.1].*cabe* mencionar que para llevar a cabo estas instalaciones (únicamente el núcleo de nuestro dominio IMS.) nos apoyamos en la guía de instalación oficial de Open IMS Core que se puede encontrar en la página http://www.openimscore.org/installation_guide, y aunque esta guía explica la instalación del dominio en una sola maquina en este proyecto las instalaciones fueron hechas en máquinas virtuales separadas, cuatro para el núcleo del dominio IMS, uno para enrutador y DHCP, una para DNS y dos para AS (Application server, servidor de aplicación).

9.4.1 Instalación y configuración de Nuestro Dominio

Para crear el dominio IMS utilizamos el nombre de dominio llamado imscore.tesis, el cual se implementó en el servidor DNS local (Bind9).

9.4.1.1 ¿Qué es Bind9?

BIND (acrónimo de Berkeley Internet Name Domain) es una implementación del protocolo DNS y provee una implementación libre de los principales componentes del Sistema de Nombres de Dominio, los cuales incluyen:

- Un servidor de sistema de nombres de dominio (named).
- Una biblioteca resolutoria de sistema de nombres de dominio.
- Herramientas para verificar la operación adecuada del servidor DNS (bind-utils).

El Servidor DNS BIND es ampliamente utilizado en la Internet (99% de los servidores DNS) proporcionando una robusta y estable solución.

9.4.1.2 Instalando bind9 en el Servidor DNS

```
apt-get install bind9 bind9utils dnsutils
```

Una vez instalado, bind9 y sus archivos de configuración se alojaran en */etc/bind*por defecto. El paquete dnsutils brinda algunas funcionalidades y herramientas para el trabajo con servidores DNS, para hacer comprobaciones y demás.

9.4.1.3 Interfaz de Red e IP asignada al Servidor DNS

El servidor DNS cuenta con una interfaz de red eth0 que está conectado a la LAN con la dirección IP de 192.170.1.3 asignada estáticamente.

9.4.1.4 Configuraciones Realizadas en el Servidor DNS

El servidor de nombre está configurado para cumplir con la tarea de resolver los nombres de cada uno de los componentes del núcleo y los AS que están conectados al mismo dentro de nuestro dominio IMS.

Para lograr que este funcione de manera adecuada creamos un archivo llamado db.open-ims.testen donde creamos los registros de la zona y otra llamado db.192.170.1.0 en donde creamos los registros inversos de la zona. Luego creamos un archivo nuevo llamado named.conf.openimscore en el cual definimos nuestras zonas con el siguiente contenido:

named.conf.openimscore

```
zone "imscore.tesis" {
        type master;
        file "/etc/bind/db.open-ims.test";
};
zone "1.170.192.in-addr.arpa"{
        type master;
        file "/etc/bind/db.192.170.1.0";
};
zone "open-ims6.test" {
        type master;
        file "/etc/bind/db.open-ims6.test";
};
```

A continuación incluimos el archivo *named.conf.openimscore* en el archivo de configuración primario de bind9 *named.conf* de la siguiente manera:

```
include "/etc/bind/named.conf.openimscore";
```

Editamos el archivo *named.conf.options* y asigna los IPs de ISP, también tendremos que decirle a bind9 en que red se debe escuchar.

9.4.2.1 Instalación del Servidor de ROUTER/DHCP

El servidor DHCP cumple también con las funcionalidades de un router, este servidor además de ser el encargado de asignarlas direcciones IP a nuestros clientes, realiza el enrutamiento entre las subredes y el NAT hacia internet.

Para la instalación del servidor DHCP usaremos el paquete *isc-dhcp-server*, ejecutaremos el siguiente comando:

```
apt-get install isc-dhcp-server
```

9.4.2.2 Interfaces de Red e IP asignados al Servidor de ROUTER/DHCP

El servidor cuenta con tres interfaces de red, el eth0 que está conectado a la LAN con la dirección IP de 192.170.1.2 asignada estáticamente, el eth1 que tiene una IP 192.168.0.29 asignado dinámicamente, y el eth2 tiene la dirección IP de 192.170.1.129 asignada estáticamente.

9.4.2.3 Configuración del Servidor de ROUTER/DHCP

Ya instalado lo primero que haremos es establecer la interfaz en el cual el servidor dhcp va a estar escuchando, para ello editamos el archivo *isc-dhcp-server* en */etc/default* y ponemos como interfaz el eth2.

```
INTERFACES="eth2"
```

Ahora editamos el archivo *dhcpd.conf*que está en la ruta /etc/dhcppara establecer la dirección IP del servidor DNS, la subred, la máscara de la sub red, el rango de las direcciones IP a asignar, el nombre del dominio y el Gateway.

```
option domain-name-server 192.170.1.3;
subnet 192.170.1.128 netmask 255.255.255.128 {
range 192.170.1.130 192.170.1.254;
option domain-name "imscore.tesis";
option routers 192.170.1.129;
}
```

Reinicia el servicio ejecutando “/etc/init.d/isc-dhcp-server restart”.

9.4.2.4 Activando la funcionalidad de router

Para que el servidor funcione como router, tendremos que habilitar el enrutamiento dentro del archivo */etc/sysctl.conf*, para esto haremos lo siguiente:

```
nano /etc/sysctl.conf
```

Y des comentar la siguiente línea.

```
net.ipv4.ip_forward = 1
```

9.4.2.5 Habilitando NAT

Para habilitar el funcionamiento del NAT en el servidor haremos uso de dos reglas iptables, los cuales son:

```
iptables -A FORWARD -j ACCEPT
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

Con esto tenemos listo y corriendo nuestro servidor de ROUTER/DHCP.

9.5 Empaquetamiento de los códigos fuente para los CSCF y el HSS

Una vez obtenidos los paquetes procedemos a hacer el empaquetamiento para generar los paquetes **.deb** necesarios para las instalaciones. Para ello realizamos lo siguiente:

Creamos un directorio para los CSCF y otro para el FHoSS en los cuales descargamos los códigos fuentes.

```
mkdir openims
mkdir openims-fhoss
```

Ahora con el comando *svncheckout* descargaremos los códigos fuentes.

```
cd openims
svn checkout http://svn.berlios.de/svnroot/repos/openimscore/ser_ims/trunkopenims
cd openims-fhoss
svn checkout http://svn.berlios.de/svnroot/repos/openimscore/FHoSS/trunkopenims-fhoss
```

Una vez obtenidas los paquetes nos colocaremos en *openims* (o en *openims-fhoss*) y copiamos la carpeta llamada **debían** de la siguiente manera:

```
cd openims
cp -a pkg/debian ./debían
```

Antes de empezar a empaquetar debemos de hacer una actualización para los archivos de changelog, esto es para generar paquetes actualizados, usaremos el siguiente comando:

```
dch -v $(svnversión) "..."
```

9.5.1 Generando paquetes para los CSCF

Esto se logra con el siguiente comando.

```
cd openismcore
dpkg-buildpackage –rfakeroot
```

9.5.2 Generando paquetes para el HSS

Igual que para los CSCF solo tenemos que acordar de actualizar los archivos de changelog para genera los paquetes más actualizados.

```
cd openismcore-fhoss
dch -v $(svnversion) "..."
dpkg-buildpackage–rfakeroot
```

9.6 Instalación de los CSCF y el HSS

En este acápite listaremos los procedimientos para la instalación y configuración tanto para los CSCF así como para el HSS.

9.6.1 Interfaz de Red e IP asignada al P-CSCF

El P-CSCF cuenta con una interfaz de red y una dirección IP de 192.170.1.10 asignada estáticamente.

9.6.2 Instalación del P-CSCF

Para instalar el P-CSCF hay que utilizar los paquetes *openimscore-pcscf_1182_i386.deb* y el *openimscore_1182_i386.deb* (este último es un paquete de dependencia de todos los CSCF por lo que se utilizara en la instalación de cada uno de ellos) generados durante el empaquetamiento de los CSCF.
Ejecutamos el comando siguiente:

```
dpkg -i openimscore-pcscf_1182_i386.deb  openimscore_1182_i386.deb
```

Durante su instalación nos aparecerán unas ventanas en donde tendremos que indicar el nombre de nuestro DNS, la dirección IP de la máquina, luego la dirección IP del DNS, el nivel de depuración (en nuestro caso escogemos el nivel 3).

Por último iniciamos el servicio ejecutando:

```
/etc/init.d/openimscore-pcscf start
```

9.6.3 Configuración del P-CSCF

Hay que realizar los siguientes cambios para que todo funcione bien.

```
nano /etc/openimscore/pcscf.cfg
```

Cambiar del puerto 4060 al puerto 5060 de manera que el archivo pcscf.cfg queda así:

```
port=5060
alias="pcscf.imscore.tesis":5060
```

En el mismo archivo *pcscf.cfg* cambiamos en el modparam de:

```
modparam ("pcscf","name","sip:pcscf.imscore.tesis:4060")
```

A

```
modparam ("pcscf","name","sip:pcscf.imscore.tesis:5060")
```

Cambiar también los siguientes puertos para IPsec.

```
modparam("pcscf","ipsec_port_c",5060)
modparam("pcscf","ipsec_port_s",5060)
```

Reinicia el servicio.

```
/etc/init.d/openimscore-pcscf restart
```

9.6.4 Interfaz de Red e IP asignada al I-CSCF

En el I-CSCF asignaremos la dirección IP 192.170.1.11 en su interfaz eth0 de forma estática.

9.6.5 Instalación del I-CSCF

Antes de la instalación de los paquetes openimscore-icscf_1182_i386.deb y el openimscore_1182_i386.deb debemos instalar los siguientes paquetes del que el I-CSCF dependerá.

```
apt-get install mysql-server mysql-client libcurl3-gnutls libmysqlclient16
```

Procede a instalar el servicio del ICSCF:

```
dpkg -i openimscore_1182_i386.deb openimscore-icscf_1182_i386.deb
```

Durante la instalación de estos paquetes nos preguntara para algunas información como se muestra a continuación deberemos de brindarle los correctos para que todo funcione correctamente.

```
domain name:Imscore.tesis
public IP address for this machine:192.170.1.11
IP address for your Domain Name Server:192.170.1.3
Do you want to configure MySQL:yes
What is the MySQL password for root: ....
What debug level do you want:3
Do you want to start I-CSCF automatically?yes
```

Inicia los servicios:

```
/etc/init.d/openimscore-icscf start
```

9.6.6 Configuración del I-CSCF

Para la configuración de este servicio nos resta nada más hacer una modificación en la Base de Datos para esto haremos uso de lo siguiente.

```
mysql -uroot -p icscf
UPDATE `icscf`.`s_cscf` SET `s_cscf_uri` = 'sip:scscf.imscore.tesis:5060' WHERE `s_cscf`.`id` =1;
```

Estos se hace debido a que el archivo icscf.sql que es utilizado para insertar datos en mysql tiene el puerto por defecto del S-CSCF a 6060, así que lo tenemos que modificar para que utilice el puerto 5060. Ahora solo nos toca reiniciar el servicio.

```
/etc/init.d/openimscore-icscf restart
```

9.6.7 Interfaz de Red e IP asignada al S-CSCF

La máquina del SCSCF tiene la dirección IP 192.170.1.12 estáticamente asignado en la interfaz eth0.

9.6.8 Instalación del S-CSCF

Para proceder con la instalación del S-CSCF tendremos que resolver las dependencias instalando los siguientes paquetes para esto hacemos lo siguiente:

```
apt-get install libcurl3-gnutls libmysqlclient16 mysql-common
```

Una vez instaladas los paquetes procedamos a instalar el S-CSCF.

```
dpkg -i openimscore_1182_i386.deb openimscore-scscf_1182_i386.deb
```

Tendremos que brindar algunas informaciones para la instalación correcta del S-CSCF.

```
domain name:imscore.tesis
public IP address for this machine: 192.170.1.12
IP address for your Domain Name Server: 192.170.1.3
What debug level do you want: 3
Do you want to start S-CSCF automatically? Yes
```

9.6.9 Configuración del S-CSCF

Para la configuración del S-CSCF tendremos que editar el archivo scscf.cfg para cambiar el puerto de 6060 al puerto 5060 para esto haremos lo siguiente:

```
nano /etc/openimscore/scscf.cfgport=5060
alias="scscf.imscore.tesis":5060
t_relay_to_udp("192.170.1.12",5060);
```

9.6.10 Interfaz de Red e IP asignada al HSS

El servidor HSS cuenta con una interfaz de red eth0 con la dirección IP de 192.170.1.13 asignado estáticamente.

9.6.11 Instalación del HSS

Para instalar el HSS nos es obligatorio instala algunos paquetes de dependencias como son sun-java6, mysql-server, mysql-client y mysql-common para poder instalar el paquete openimscore-fhoss_1182_i386.deb.

Primero resolveremos las dependencias instalando los paquetes de la siguiente manera:

```
apt-get install sun-java6-jre mysql-server mysql-client mysql-common
```

Luego instalaremos el paquete que tiene el servicio HSS.

```
dpkg -i openimscore-fhoss_1182_i386.deb
```

Pedirá las siguientes informaciones.

```
What is the domain name?imscore.tesis
What is the IP address for this domain name? 192.170.1.13
What is the public IP address for your Domain Name Server? 192.170.1.3
Do you want to configure MySQL? yes
You can add user to the HSS database. If no more user to add, left empty. Separate different users by
<space>. Users name?
What is the MySQL password for root? …
Do you want to start HSS automatically? Yes
```

9.6.12 Configuración del HSS

Para la configuración del HSS será necesario crear un directorio de configuración en */etc/* como es normal en Linux y hacer un enlace de */usr/share/java/fhoss-0.2* hasta el directorio creado, el directorio que vamos a crear se va a llamar *fhoss.* Para lograr esto hacemos lo siguiente.

```
ln -s /usr/share/java/fhoss-0.2 /etc/fhoss
```

9.7 Administración de Usuarios.

IMS permite la identificación de los usuarios, servicios y nodos mediante un URI (Universal Resource Identifier), que evita que el usuario deba memorizar números de teléfono, pues se trata de nombres al estilo de servicios Internet. De esta forma, IMS ofrece para el acceso a otros usuarios o contenidos una interfaz gráfica similar a los actuales programas de mensajería instantánea (como MSN Messenger), con la ventaja de que integrará la telefonía fija y móvil multimedia, los accesos inalámbricos y cualquier sistema de comunicaciones que se implemente en el futuro. Es decir, una persona podrá ver desde su teléfono móvil qué contactos de su agenda están conectados, incluso dónde están en ese momento, y a través de qué medios es posible comunicarse con ellos.

9.7.1 Identificación de Usuarios

Hay dos maneras para la identificación de usuario: Privadas y Públicas.

9.7.1.1 Identificación Privadas

Es la identificación asignada por el operador y se guarda en el HSS esta se usa para el registro, la autenticación y facturación, no se usa con propósitos de enrutamiento. Tiene la forma de un NAI (Network Access Identifier). Estructura: nombre-de-usuario@dominio RFC 2486. El NAI es un método estandarizado para identificar al usuario de manera que se pueda hacer de forma interoperable el roaming y el tuneling.

9.7.1.2 Identificación Pública:

Se refiere a identificaciones que pueden ser comunicadas a los contactos de cada usuario y que pueden mostrarse públicamente, este tiene la forma de un SIP URI RFC 3261 o un URI para números telefónicos denominado “tel” URI RFC 3966.

Ejemplo:
SIP URI: sip:nombre-de-usuario@dominio
“tel” URI: tel:+505-21548-5425
Se pueden tener varios identificadores públicos pues un usuario puede tener varios dispositivos pero que soporten distintos servicios: número móvil, número de oficina, Televisión con soporte IPTV. Solo una identidad

privada puede ser asociada a varias identidades públicas y así el usuario puede suministrar una u otra identidad a sus contactos en función del tipo de comunicación que desea establecer con cada uno de ellos.

Haciendo la analogía con un teléfono celular el identificador público corresponde al número de teléfono, mientras que la identidad privada IMS equivale a un número especial guardado en el SIM que utiliza para autenticarse en la red móvil.

9.8 Comunicación del Cliente con el núcleo

9.8.1 Mensajes Intercambiados con el Núcleo: Señalización SIP en Open IMS

SIP utiliza el control de sesión junto con el usuario, esto permite modificar, configurar y cancelar las sesiones Hay 6 mensajes para llevar a cabo estas funciones.

- **INVITE:** Paquete enviado por el UE al núcleo para solicitar un servicio.
- **ACK:** Usado junto con el INVITE, el UE envía este mensaje para confirmar que ha recibido un mensaje.
- **BYE:** Método utilizado para liberar un servicio solicitado.
- **CANCEL:** Utilizado para cancelar una solicitud incompleta, no tiene nada que ver con solicitudes completadas.
- **REGISTER:** Método utilizado para registrar las direcciones en el servidor.
- **OPTIONS:** Utilizado para preguntar los servicios disponibles que ofrece el Núcleo.

En la figura 5 se muestra el procedimiento general del proceso de registro y autenticación de un UE.

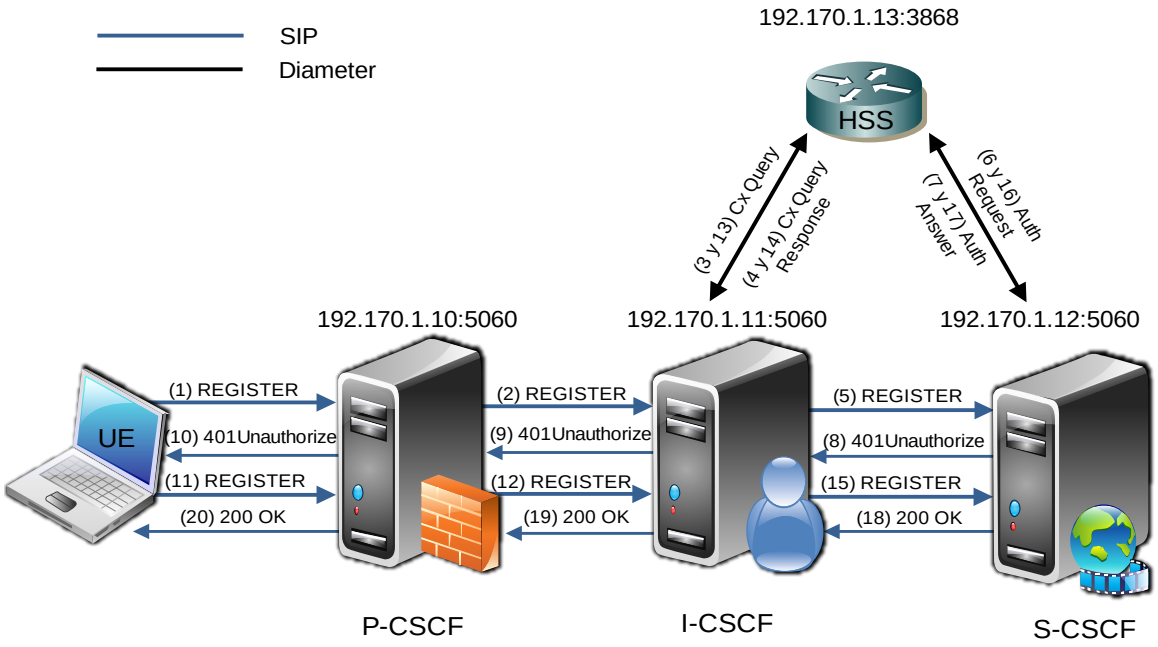


Figura 5: Procedimiento de registro. (Fuente Propia, 2012-2013)

El UE envía una solicitud de registro SIP al P-CSCF. P-CSCF envía un mensaje de registro al I-CSCF que contiene el nombre y la información del usuario. I-CSCF obtiene la dirección del HSS e intercambia información a través de la interfaz Cx, mientras que al mismo tiempo HSS elige el S-CSCF adecuado para el UE de acuerdo a la solicitud del I-CSCF y envía la información al mismo.

Luego el I-CSCF entregara la información al S-CSCF seleccionado. El HSS registra la información de identidad del usuario y su correspondiente S-CSCF y finalmente el S-CSCF envía la información de la conexión al I-CSCF y este libera toda la información de registro. En este momento el UE está listo para utilizar los servicios que tiene el núcleo.

a. Del UE al P-CSCF: Mensaje 1 –REGISTER

```
REGISTER sip:imscore.tesis SIP/2.0
Call-ID: b213969ad0dcdb75cb73d401f4f65dad@192.168.1.3
CSeq: 1 REGISTER
 From: "Shall" <sip:shall@imscore.tesis>;tag=1000
To: "Shall" <sip:shall@imscore.tesis>
Via: SIP/2.0/UDP 192.168.1.3:5060;branch=z9hG4bK5470c91bb58c21e1a9962e3fb953c44f3134
Max-Forwards: 20
```

```
Expires: 3600
Authorization: Digest
username="shall@imscore.tesis",realm="imscore.tesis",nonce="",response="",uri="sip:imscore.tesis"
Contact: "Shall" <sip:shall@192.168.1.3:5060>;+sip.instance=cd89c4aa-ca86-4daa-89a6-864d5dbb4d67
User-Agent: monster Version: 0.9.25
Content-Length: 0
```

El propósito de este mensaje es registrar el SIP URI del usuario con S-CSCF del núcleo. Esta solicitud se envía al P-CSCF ya que es el que está configurado en el UE.

- **Request-URI:** Especifica el método e indica el dominio de destino de esta petición, las reglas para enrutar una solicitud SIP para este dominio (imscore.tesis) están descrita en el Servidor DNS.
- **Call-ID:** Es un identificador único para agrupar una serie de mensajes. Este tiene que ser el mismo para todas las solicitudes y respuestas.
- **Cseq:** Sirve para especificar y ordenar. Se compone por un número de secuencia y un método, dicho método debe coincidir con el de la solicitud.
- **From:** Indica la identificación publica del usuario que origina la solicitud del REGISTER (registro).
- **To:** Indica la identidad de usuario pública que se registra, a través de este nombre se podrán comunicar los demás usuarios con este usuario.
- **Via:** protocolo de trasporte y direccion IPv4 asignada al UE.
- **Authorization:** Información de autenticación. Tipo de autenticación en este caso Digest md5, Identidad privada, el valor realm contiene el dominio de la red y el campo URI contiene el mismo valor que el Request URI. Los campos nonce y responce están vacíos ya que es la primera solicitud de registro y no hay información en cache de otra transacción.
- **Contact:** Esto indica el punto de presencia para el abonado - la dirección IP del UE. Este es el punto temporal de contacto para el suscriptor que se está registrando. Las solicitudes subsiguientes destinados a este abonado serán enviados a esta dirección. Esta información es almacenada en la S-CSCF.
- **UserAgent:** Nombre y versión del software del cliente.

b. Entre el P-CSCF y el DNS:

Consulta SRV:

```
Queries
    _sip._udp.imscore.tesis: type SRV, class IN
      Name: _sip._udp.imscore.tesis
      Type: SRV (Service location)
Class: IN (0x0001)
```

Respuesta SRV:

```
Queries
    _sip._udp.imscore.tesis: type SRV, class IN
      Name: _sip._udp.imscore.tesis
      Type: SRV (Service location)
      Class: IN (0x0001)
  Answers
    _sip._udp.imscore.tesis: type SRV, class IN, priority 0, weight 0, port 5060, target icscf.imscore.tesis
                                                    Service: sip
      Protocol: udp
      Name: imscore.tesis
      Type: SRV (Service location)
      Class: IN (0x0001)
      Time to live: 1 day
      Data length: 27
      Priority: 0
      Weight: 0
      Port: 5060
      Target: icscf.imscore.tesis
```

Basado en el URI del usuario, P-CSCF determina que este UE está intentando registrarse en un dominio visitante y solicita un servicio SIP realizando las consultas DNS necesarias para localizar el I-CSCF en la red.

Cuando el P-CSCF reenvía el paquete REGISTER debe especificar el protocolo, número de puerto y la dirección IP del servidor I-CSCF en la red local a la que enviar la solicitud de registro.

El P-CSCF realiza la consulta según los registros SRV en la respuesta el DNS utiliza una técnica de selección empleando los parámetros de prioridad y el tamaño (RR) (mejor especificados en el RFC 2782) de esta forma obtiene la dirección del I-CSCF que está brindando este recurso y enviado al P-CSCF.

c. Del P-CSCF al I-CSCF:Mensaje 2 –REGISTER

```
REGISTER sip:imscore.tesis SIP/2.0
Call-ID: b213969ad0dcdb75cb73d401f4f65dad@192.168.1.3
CSeq: 1 REGISTER
From: "Shall" <sip:shall@imscore.tesis>;tag=1000
To: "Shall" <sip:shall@imscore.tesis>
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK5ccc.04ad661.0
Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bK5470c91bb58c21e1a9962e3fb953c44f3134
Max-Forwards: 16
Expires: 3600
Contact: "Shall" <sip:shall@192.170.1.131:5060>;+sip.instance=cd89c4aa-ca86-4daa-89a6-
864d5dbb4d67
User-Agent: monster Version: 0.9.25
Content-Length: 0
Authorization: Digest
username="shall@imscore.tesis",realm="imscore.tesis",nonce="",response="",uri="sip:imscore.tesis",
integrity-protected="no"
Path: <sip:term@pcscf.imscore.tesis:5060;lr>
Require: path
P-Charging-Vector: icid-value="P-CSCFabcd514dcd8600000021";icid-generated-at=192.170.1.10;orig-
ioi="imscore.tesis"
P-Visited-Network-ID: imscore.tesis
```

El P-CSCF necesita estar en la ruta de acceso para todas las solicitudes de este usuario, para asegurar esto el P-CSCF se suma al valor de la cabecera para futuras solicitudes.

- El P-CSCF añade a la cabecera P-Visited-Network-ID: imscore.tesis, este es el valor del dominio visitado o cualquier otro nombre que identifique a la red.
- **Path:** esta es la dirección del P-CSCF y se incluye para informar al S-CSCF donde enrutar las solicitudes y posteriormente reenviarlas al UE.
- **Require:** esta se incluye para asegurar que el receptor use bien la nueva ruta que agrego el P-CSCF a la cabecera.
- **P-Charging-Vector:** lo agrega a la cabecera y rellena los parámetros del ICID con un valor único.

d. Entre el I-CSCF y el HSS: Mensaje 3 - Cx-Query y Mensaje 4 - Cx-Query response

Cx-Query, Diameter UAR o User-Authorization-Request: El I-CSCF hace una solicitud de información relacionada con el estado del registro del usuario mediante él envió de la identidad privada (shall@imscore.tesis), la identidad pública (sip:shall@imscore.tesis) y el nombre del dominio (imscore.tesis). Para más detalles ver Figura 6 del anexo.

Cx-Query response, Diameter UAA o User-Authorization-Answer: El HSS devuelve el S-CSCF requerido para este usuario, de esta forma el I-CSCF determina quién será el encargado de brindarle los servicios a dicho usuario. Para más detalles ver Figura 7 del anexo.

e. Del I-CSCF al S-CSCF: Mensaje 5 –REGISTER

```
REGISTER sip:scscf.imscore.tesis:5060 SIP/2.0
Call-ID: b213969ad0dcdb75cb73d401f4f65dad@192.168.1.3
CSeq: 1 REGISTER
From: "Shall" <sip:shall@imscore.tesis>;tag=1000
To: "Shall" <sip:shall@imscore.tesis>
Via: SIP/2.0/UDP 192.170.1.11;branch=z9hG4bK5ccc.6259c6e.0
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK5ccc.04ad661.0
Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bK5470c91bb58c21e1a9962e3fb953c44f3134
Max-Forwards: 15
Expires: 3600
Contact: "Shall" <sip:shall@192.170.1.131:5060>;+sip.instance=cd89c4aa-ca86-4daa-89a6-864d5dbb4d67
User-Agent: monster Version: 0.9.25
Content-Length: 0
Authorization: Digest
username="shall@imscore.tesis",realm="imscore.tesis",nonce="",response="",uri="sip:imscore.tesis",
integrity-protected="no"
Path: <sip:term@pcscf.imscore.tesis:5060;lr>
Require: path
P-Charging-Vector: icid-value="P-CSCFabcd514dcd8600000021";icid-generated-at=192.170.1.10;orig-
ioi="imscore.tesis"
```

```
P-Visited-Network-ID: imscore.tesis
```

El I-CSCF no modifica el Path pero almacena el contenido URI para enrutar peticiones con que correspondan al mismo dominio.

f. Entre el S-CSCF y el HSS: Mensaje 6 - AuthRequest y Mensaje 7 - AuthAnswer

Para esto el S-CSCF necesita al menos un vector de autenticación (AV) para ser utilizado en la comprobación del usuario. Para más detalle ver Figura 8 y Figura 9 del anexo

La solicitud REGISTER llega sin la protección de integridad del P-CSCF. El S-CSCF deberá comprobarlo.

g. Del S-CSCF al I-CSCF: Mensaje 8 - 401 Unauthorized

```
SIP/2.0 401 Unauthorized - Challenging the UE
Call-ID: b213969ad0dcdb75cb73d401f4f65dad@192.168.1.3
CSeq: 1 REGISTER
From: "Shall" <sip:shall@imscore.tesis>;tag=1000
To: "Shall" <sip:shall@imscore.tesis>;tag=60fa2418f8483d59c7f61e68e1212879-6dd0
Via: SIP/2.0/UDP 192.170.1.11;branch=z9hG4bK5ccc.6259c6e.0
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK5ccc.04ad661.0
Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bK5470c91bb58c21e1a9962e3fb953c44f3134
WWW-Authenticate: Digest realm="imscore.tesis", nonce="6c37d68da155f73bef4fa8038c3c5421",
algorithm=MD5, qop="auth,auth-int"
Path: <sip:term@pcscf.imscore.tesis:5060;lr>
Service-Route: <sip:orig@scscf.imscore.tesis:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE,
INFO
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0
```

Este mensaje *401 Unauthorized* obliga al usuario que envié sus credenciales para la autenticación.

- WWW-Authenticate: campo que contiene el tipo de autenticación y los parámetros necesarios para cumplir el reto.
- Service-Route: Nombre del S-CSCF que le brindara servicios ha dicho UE.

h. Del I-CSCF al P-CSCF: Mensaje 9 - 401 Unauthorized

```
SIP/2.0 401 Unauthorized - Challenging the UE
Call-ID: b213969ad0dcdb75cb73d401f4f65dad@192.168.1.3
CSeq: 1 REGISTER
From: "Shall" <sip:shall@imscore.tesis>;tag=1000
To: "Shall" <sip:shall@imscore.tesis>;tag=60fa2418f8483d59c7f61e68e1212879-6dd0
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK5ccc.04ad661.0
Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bK5470c91bb58c21e1a9962e3fb953c44f3134
WWW-Authenticate: Digest realm="imscore.tesis", nonce="6c37d68da155f73bef4fa8038c3c5421",
algorithm=MD5, qop="auth,auth-int"
Path: <sip:term@pcscf.imscore.tesis:5060;lr>
Service-Route: <sip:orig@scscf.imscore.tesis:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE,
INFO
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0
```

i. Del P-CSCF al UE: Mensaje 10 - 401 Unauthorized

```
SIP/2.0 401 Unauthorized - Challenging the UE
Call-ID: b213969ad0dcdb75cb73d401f4f65dad@192.168.1.3
CSeq: 1 REGISTER
From: "Shall" <sip:shall@imscore.tesis>;tag=1000
To: "Shall" <sip:shall@imscore.tesis>;tag=60fa2418f8483d59c7f61e68e1212879-6dd0
Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bK5470c91bb58c21e1a9962e3fb953c44f3134
Path: <sip:term@pcscf.imscore.tesis:5060;lr>
Service-Route: <sip:orig@scscf.imscore.tesis:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE,
INFO
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))\
Content-Length: 0
WWW-Authenticate: Digest realm="imscore.tesis", nonce="6c37d68da155f73bef4fa8038c3c5421",
algorithm=MD5, qop="auth,auth-int"
```

El P-CSCF elimina de la trama el campo *VIA* añadido por el mismo y reenvía el resto de la respuesta.

j. UE al P-CSCF: Mensaje – 11REGISTER

```
REGISTER sip:imscore.tesis SIP/2.0
Call-ID: b213969ad0dcdb75cb73d401f4f65dad@192.168.1.3
CSeq: 2 REGISTER
From: "Shall" <sip:shall@imscore.tesis>;tag=1001
To: "Shall" <sip:shall@imscore.tesis>
Via: SIP/2.0/UDP 192.168.1.3:5060;branch=z9hG4bKbf81d6bacb8b20605ab601d94bc1115e3134
Max-Forwards: 20
[truncated]Authorization: Digest
username="shall@imscore.tesis",realm="imscore.tesis",nonce="6c37d68da155f73bef4fa8038c3c5421",uri=
"sip:imscore.tesis",algoritm=MD5,response="41f9785b2152a807308d9a721f657d7e",qop=auth-
int,nc=00000001,cnonce="519950101101995050"
Expires: 3600
```

```
Contact: "Shall" <sip:shall@192.168.1.3:5060>;+sip.instance=cd89c4aa-ca86-4daa-89a6-864d5dbb4d67
User-Agent: monster Version: 0.9.25
Content-Length: 0
```

Authorization: este campo lleva la respuesta a la prueba de autenticación junto con la identidad de usuario privado, el realm, el nonce, el URI y el algoritmo de encriptación, este mensaje está protegido por IPSec (Asociación de seguridad).

k. Del P-CSCF al I-CSCF: Mensaje 12- REGISTER

```
REGISTER sip:imscore.tesis SIP/2.0
Call-ID: b213969ad0dcdb75cb73d401f4f65dad@192.168.1.3
CSeq: 2 REGISTER
From: "Shall" <sip:shall@imscore.tesis>;tag=1001
To: "Shall" <sip:shall@imscore.tesis>
Via: SIP/2.0/UDP 192.170.1.131:5060;branch=z9hG4bKbf81d6bacb8b20605ab601d94bc1115e3134
Max-Forwards: 20
[truncated]Authorization: Digest
username="shall@imscore.tesis",realm="imscore.tesis",nonce="6c37d68da155f73bef4fa8038c3c5421",uri=
"sip:imscore.tesis",algoritm=MD5,response="41f9785b2152a807308d9a721f657d7e",qop=auth-
int,nc=00000001,cnonce="519950101101995050"
Expires: 3600
Contact: "Shall" <sip:shall@192.170.1.131:5060>;+sip.instance=cd89c4aa-ca86-4daa-89a6-864d5dbb4d67
User-Agent: monster Version: 0.9.25
Content-Length: 0
```

l. Entre el I-CSCF y el HSS: Mensaje 13 - Cx-Query y Mensaje 14 - Cx-Query response

El I-CSCF solicita información relacionada con el estado del registro del suscriptor mediante él envió de la identidad privada, la identidad pública y el nombre de dominio de la red visitada. El HSS devuelve el nombre de S-CSCF que fue seleccionado previamente. Para más detalle del mensaje ver Figura 10 y Figura 11 del anexo.

m. Del I-CSCF al S-CSCF: Mensaje 15 –REGISTER

```
REGISTER sip:scscf.imscore.tesis:5060 SIP/2.0
Call-ID: b213969ad0dcdb75cb73d401f4f65dad@192.168.1.3
CSeq: 2 REGISTER
From: "Shall" <sip:shall@imscore.tesis>;tag=1001
To: "Shall" <sip:shall@imscore.tesis>
Via: SIP/2.0/UDP 192.170.1.11;branch=z9hG4bK2ccc.1f3b4487.0
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK2ccc.253696e2.0
Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bKbf81d6bacb8b20605ab601d94bc1115e3134
Max-Forwards: 15
Expires: 3600
Contact: "Shall" <sip:shall@192.170.1.131:5060>;+sip.instance=cd89c4aa-ca86-4daa-89a6-864d5dbb4d67
User-Agent: monster Version: 0.9.25
Content-Length: 0
[truncated]Authorization: Digest
username="shall@imscore.tesis",realm="imscore.tesis",nonce="6c37d68da155f73bef4fa8038c3c5421",uri=
"sip:imscore.tesis",algoritm=MD5,response="41f9785b2152a807308d9a721f657d7e",qop=auth-
int,nc=00000001,cnonce="519950101101995050", integrity-protected="no"
Path: <sip:term@pcscf.imscore.tesis:5060;lr>
Require: path
P-Charging-Vector: icid-value="P-CSCFabcd514dcd8700000022";icid-generated-at=192.170.1.10;orig-
ioi="imscore.tesis"
P-Visited-Network-ID: imscore.tesis
```

n. Entre el S-CSCF y el HSS: Mensaje 16 – Cx-Put y Mensaje 17 – Cx-Put Response

- Cx-Put, o Diameter SAR (Server AssigmentRequest): informa del registro de un usuario al HSS.
- Cx-Put Response o Diameter SAA (Server AssigmentAnswer): el HSS en la respuesta también incluye el perfil del usuario autorizado.
- Authentication: Al recibir un mensaje request REGISTER con la protección de integridad lleva la respuesta a la prueba de autenticación, este comprueba la respuesta (calculado por S-CSCF utilizando XRES y otros parametros definidos en RFC 3310) si este coincide el usuario ha sido autenticado y la identidad de usuario público se ha registrado en el S-CSCF.

o. Del S-CSCF al I-CSCF: Mensaje 18 - 200 OK

```
SIP/2.0 200 OK - SAR succesful and registrar saved
Call-ID: b213969ad0dcdb75cb73d401f4f65dad@192.168.1.3
CSeq: 2 REGISTER
From: "Shall" <sip:shall@imscore.tesis>;tag=1001
To: "Shall" <sip:shall@imscore.tesis>;tag=60fa2418f8483d59c7f61e68e1212879-a3b7
Via: SIP/2.0/UDP 192.170.1.11;branch=z9hG4bK2ccc.1f3b4487.0
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK2ccc.253696e2.0
Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bKbf81d6bacb8b20605ab601d94bc1115e3134
P-Associated-URI: <sip:shall@imscore.tesis>
Contact: <sip:shall@192.170.1.131:5060>;expires=3600;pub-gruu="sip:shall@imscore.tesis;gr=cd89c4aa-
ca86-4daa-89a6-864d5dbb4d67"
Path: <sip:term@pcscf.imscore.tesis:5060;lr>
Service-Route: <sip:orig@scscf.imscore.tesis:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE,
INFO
P-Charging-Function-Addresses: ccf=pri_ccf_address
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0
```

S-CSCF envía una respuesta 200 OK para el I-CSCF que indica que el registro fue exitoso.

p. Del I-CSCF al P-CSCF: Mensaje 19 - 200 OK

SIP/2.0 200 OK - SAR succesful and registrar saved
Call-ID: b213969ad0dcdb75cb73d401f4f65dad@192.168.1.3
CSeq: 2 REGISTER
From: "Shall" <sip:shall@imscore.tesis>;tag=1001
To: "Shall" <sip:shall@imscore.tesis>;tag=60fa2418f8483d59c7f61e68e1212879-a3b7
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK2ccc.253696e2.0
Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bKbf81d6bacb8b20605ab601d94bc1115e3134
P-Associated-URI: <sip:shall@imscore.tesis>
Contact: <sip:shall@192.170.1.131:5060>;expires=3600;pub-gruu="sip:shall@imscore.tesis;gr=cd89c4aa-ca86-4daa-89a6-864d5dbb4d67"
Path: <sip:term@pcscf.imscore.tesis:5060;lr>
Service-Route: <sip:orig@scscf.imscore.tesis:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
P-Charging-Function-Addresses: ccf=pri_ccf_address
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0

El I-CSCF envía la respuesta 200 OK de el S-CSCF se ha realizado correctamente. El P-CSCF guarda el valor del Service-Route y lo asocia con el UE.

q. Del P-CSCF al UE:Mensaje 20 - 200 OK

SIP/2.0 200 OK - SAR succesful and registrar saved
Call-ID: b213969ad0dcdb75cb73d401f4f65dad@192.168.1.3
CSeq: 2 REGISTER
From: "Shall" <sip:shall@imscore.tesis>;tag=1001
To: "Shall" <sip:shall@imscore.tesis>;tag=60fa2418f8483d59c7f61e68e1212879-a3b7
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK2ccc.253696e2.0
Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bKbf81d6bacb8b20605ab601d94bc1115e3134
P-Associated-URI: <sip:shall@imscore.tesis>
Contact: <sip:shall@192.170.1.131:5060>;expires=3600;pub-gruu="sip:shall@imscore.tesis;gr=cd89c4aa-ca86-4daa-89a6-864d5dbb4d67"
Path: <sip:term@pcscf.imscore.tesis:5060;lr>
Service-Route: <sip:orig@scscf.imscore.tesis:5060;lr>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, INFO
P-Charging-Function-Addresses: ccf=pri_ccf_address
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0

9.9 Clientes

Los Clientes son usados para realizar pruebas en la red IMS y pueden ser de dos tipos:

- Clientes SIP
- Clientes IMS

9.9.1 Clientes SIP

Estos son basados en el protocolo SIP y no necesariamente son usados solo en las redes IMS. Estos son aplicaciones que emulan un teléfono generalmente usando VOIP.
Normas que son específicas de IMS pero que no son soportadas por estos clientes:

- No soportan el método de autenticación AKA MD5.
- No requieren de identidad de usuario privado (IMS los define por separados).

Para conseguir que este tipo de cliente se autentique con el Núcleo IMS, el S-CSCF necesita ser modificado para admitir la autenticación MD5 en vez del AKA MD5. Los perfiles de usuario en el HSS también deben tener como mecanismo de Autenticación el Digest MD5 en lugar de AKA-MD5.

Dado que no tienen una identidad de usuario privada definida por separado estos clientes no pueden utilizarse en el caso cuando hay múltiples identidades de usuarios públicos definidos para una única identidad de usuario privado.

Clientes de este tipo utilizados en esta implementación:

9.9.1.1 X-lite

Es un Softphone (Teléfono de Aplicación) de Counterpath. Este es un cliente SIP, por cuestiones de compatibilidad utilizamos la versión 3.0. Esta versión de X-lite es libre no es de código abierto pero incluye todas las funcionalidades básicas, da soporte para el servicio Presence (Presencia), para envió y recepción de mensajes.

Figura 12: Cliente SIP XLite.

9.9.1.2 Join (Iphone)

Teléfono de Aplicación de VoipSwitch Inc. Cliente SIP con la versión 1.0 para IPhone. Permite utilizar las funcionalidades básicas, compatible con el servicio de presencia, envió y recepción de mensajes.

Figura 13: Cliente SIP Join.

9.9.2 Clientes IMS

Son los clientes específicos diseñados para la red IMS. Estos clientes soportan el tipo de autenticación AKA MD5. También requiere obligatoriamente una identidad de usuario privado definida para registrarse. Esto es lo que permite el registro con múltiples identidades públicas asociadas a una sola identidad privada.
Clientes de este tipo utilizados en esta implementación:

9.9.2.1 UCT IMS Client

Es un cliente IMS desarrollado por la Universidad de Cape Town, fue diseñado para ser usado solo para OpenIMSCore. Este soporta el tipo de autenticación AKA y emula la señalización en IMS.

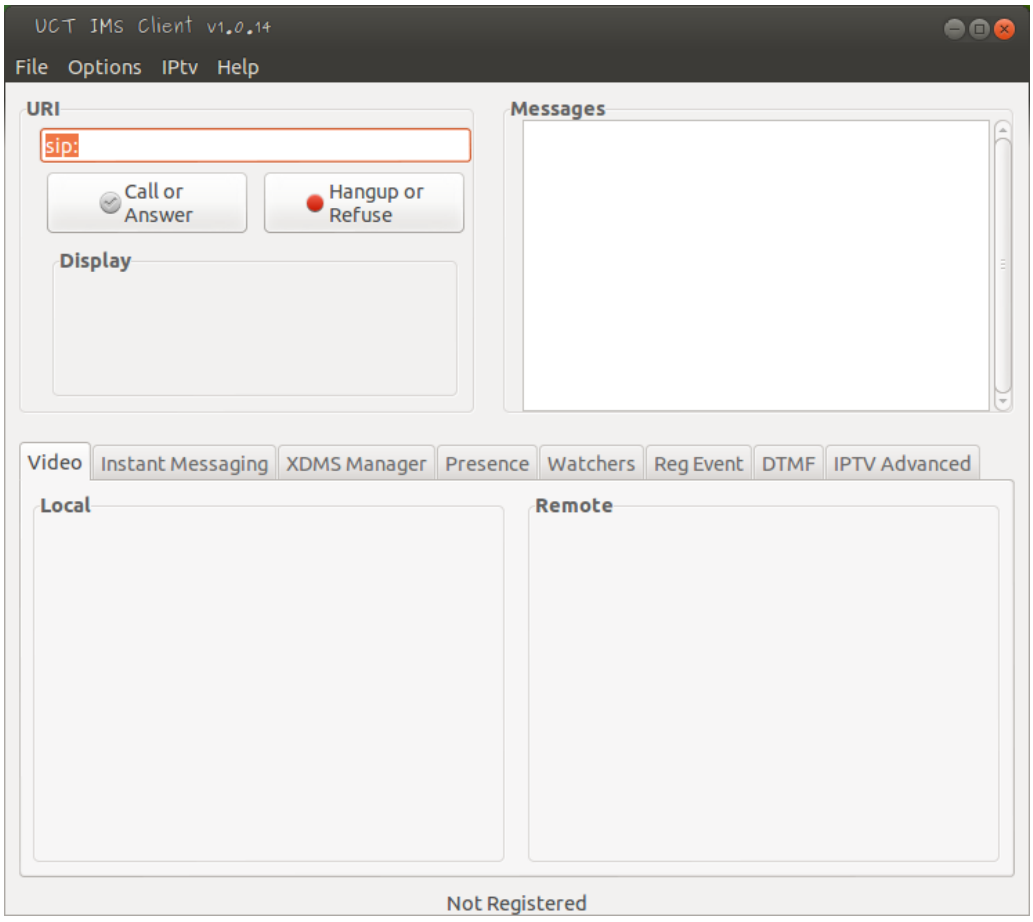


Figura 14: Cliente IMS UCT.

9.9.2.2 myMonster

myMONSTER (Multimedia Open InterNet Services and Telecommunication EnviRonment). Es un Cliente IMS desarrollado por Fraunhover FOKUS compatibles con las normas de IMS.

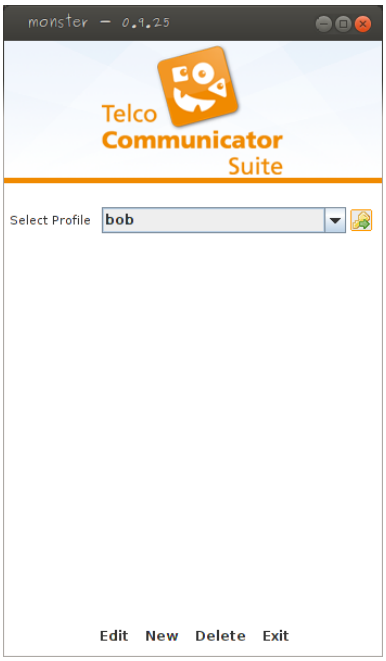


Figura 15: Cliente IMS MyMonster.

9.9.2.3 IMSDroid

Es el primero de todas las aplicaciones IMS de código abierto para Android desarrollado por Dubango compatible con todas las normas IMS.

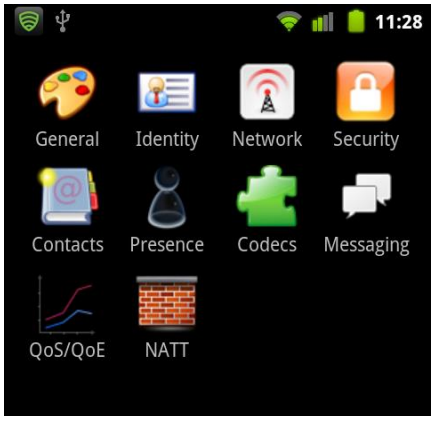


Figura 16: Cliente IMS IMSDroid.

9.10 Gestión de servicios del núcleo

A continuación discutiremos acerca de los servicios tanto nativos como servicios agregados que estaremos brindando dentro de nuestro dominio IMS.

9.10.1 Servicios ofrecidos nativamente por el núcleo

Los servicios nativos que ofrece el núcleo de IMS, como las llamadas y la mensajería, son los mismos ofrecidos por la tecnología VoIP utilizando el protocolo SIP de tal forma que un cliente que se quiere comunicar con otro a través de estos servicios (llamadas o mensajería), antes tiene que mandar una solicitud de “INVITE” o “MESSAGE” asía la red, la cabecera de la solicitud de INVITE o MESSAGE (en caso de mensajería) contiene los siguientes campos:

- **Campo Request-URI:** Este campo contiene la identidad pública que muestra el ID del usuario más el dominio en el que está, por ejemplo, sip:iphone@imscore.tesis junto con el puerto del host destino.

- **Campo Via:** Dentro de este campo está la dirección IP y el número de puerto mostrando donde el terminal IMS responde a la solicitud de “INVITE” o “MESSAGE”, el campo muestra también que protocolo de transporte será utilizado para transportar el mensaje SIP, en este caso será el protocolo UDP.

- **Campo Contact:** Este campo lleva los datos del emisor, es decir el campo contendrá el SIP URI del emisor por ejemplo: sip:android@192.168.1.3:5060, esto también ayuda al receptor para decirle que esta soportado las peticiones subsiguientes.

- **Campo Router:** El valor de este campo apunta al P-CSCF y/o al S-CSCF.

- **Campo P-Preferred-identity:** El valor de este campo de cabecera contiene el nombre del usuario y un SIP URI. Antes de que el P-CSCF reenvíe el mensaje de solicitud INVITE, cambiara este campo a un P-Asserted-identity manteniendo los mismos valores.

- **Campo P-Asserted-identity:** Los valores de este campo de cabecera son los mismos que los valores contenido en el campo de cabecera P-Preferred-identity los cuales son: el nombre del usuario, y un SIP URI el cual es una identidad publica del usuario [ver capítulo 11.1].

- **Campo P-Access-Network-info:** Este campo contiene información de la red de acceso (el tipo de red a la cual está conectado). El cuadro siguiente muestra una captura wireshark del campo P-Access-Network-Info y el valor del mismo de la cabecera del mensaje INVITE.

P-Access-Network-Info: IEEE-802.11a

- **Campo Privacy:** Este campo de cabecera es usado para mostrar que el agente de usuario que realiza la llamada, está dispuesto a indicar alguna información privada al agente de usuario al que está llamando.

- **Campo Content-Type:** Este campo describe el tipo de contenido que llevara el cuerpo del mensaje de solicitud INVITE. Normalmente el tipo es un “application/sdp”, denotando el protocolo de descripción de sesión (SDP Session Description Protocol).

- **Campo Content-Length:** Indica la longitud del cuerpo del mensaje INVITE. Este campo está presente siempre, pero su valor puede estar puesto a cero indicando que no existe cuerpo del mensaje en la petición INVITE.

La figura 11 muestra el proceso cuando un cliente (UE1) intenta establecer una comunicación con otro cliente (UE2) ya sea a través de una llamada VoIP o por mensajería instantánea (IM).

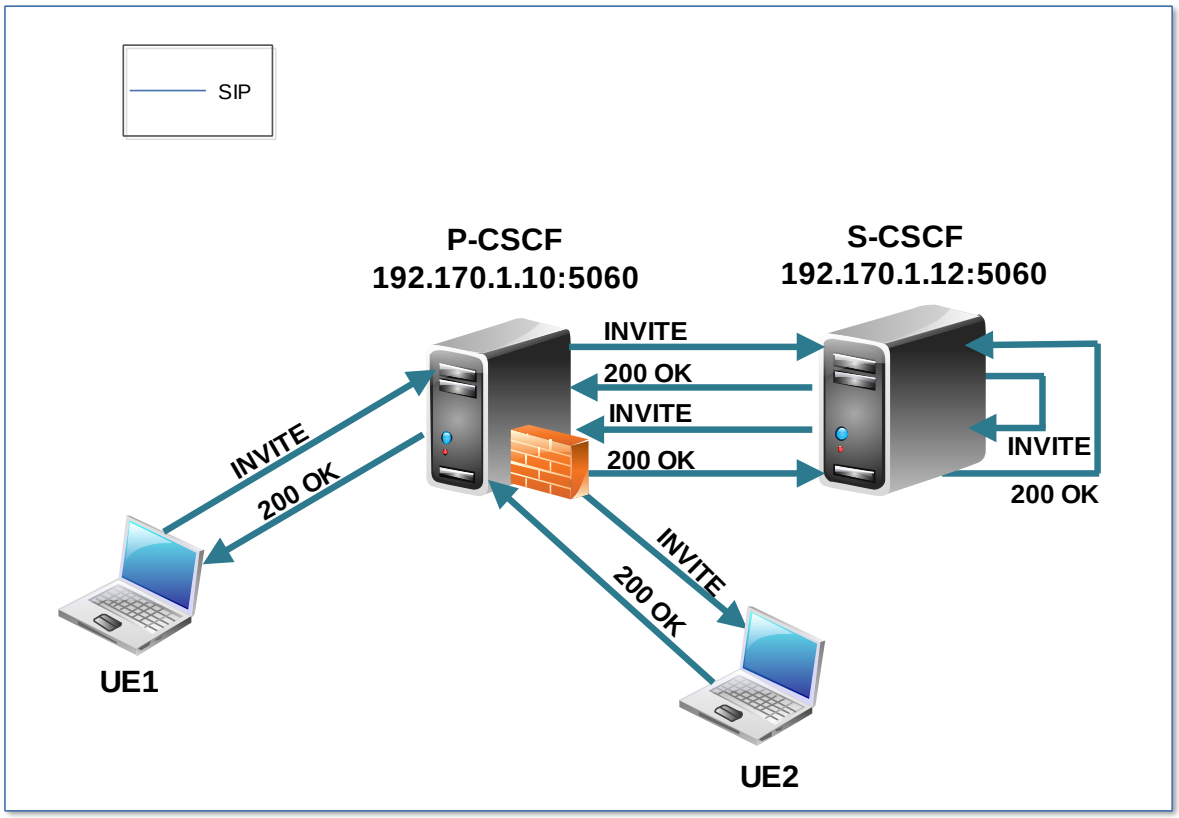


Figura 17: Solicitud de un servicio nativo dentro del IMS core. (Fuente Propia, 2012-2013)

El cliente origen manda una solicitud "INVITE" si es para la realización de una llamada o una solicitud "MESSAGE" si es para mensajería, con todos los valores puestos en los campos de la cabecera (como los mencionados anteriormente) al P-CSCF. El P-CSCF comprueba que si el campo "Router" contiene un valor (el cual es una ruta al S-CSCF) y elimina el campo "P-Preferred-identity" manteniendo su valor para asignarlos al nuevo campo P-Asserted-identity que este (el P-CSCF) agrega y reenvía la solicitud hasta el S-CSCF.

El S-CSCF intenta reenviar la solicitud INVITE basándose en el "Request-URI" del destino (por ejemplo: sip:iphone@imscore.tesis), así que el S-CSCF intenta localizar un servidor SIP dentro del dominio "imscore.tesis". Debido a que la solicitud será reenviada dentro del mismo dominio, el S-CSCF mantiene algunos datos del campo de cabecera como es el "P-Access-Network-Info".

Como El S-CSCF es usado también para encargarse de los servicios nativos (tanto llamadas como mensajería instantánea) dentro del dominio "imscore.tesis" recibe la solicitud INVITE que el mismo envió, verifica primero el "Request-URI" y agrega el contacto del usuario que está realizando la llamada al campo "Contact" luego reenvía la solicitud al P-CSCF.

El P-CSCF recibe la solicitud y extrae la identidad pública del usuario e identifica la identidad pública del destino, luego la solicitud es reenviado al cliente destino (esto es si el "Presence" detecta si está activo el cliente) en donde este decide si o no aceptar la solicitud (en caso de las llamadas). El terminal del usuario revisa el campo P-Asserted-identity para obtener la identidad del cliente que está realizando la llamada. Si la solicitud es aceptada entonces se genera un 200 OK que es reenviado de vuelta al núcleo.

9.10.2 Agregar nuevos servicios al núcleo

A continuación detallaremos la forma en que agregamos dos nuevos servicios a nuestro dominio IMS indicando para ello las instalaciones y configuraciones necesarias para su integración con el núcleo IMS.

9.10.2.1 Servicios de Presencia

a- Instalación del servidor de presencia (OpenSips)

El servidor Presence cuenta con una única interfaz (eth0) de red con la dirección IP 192.170.1.7 asignado estáticamente a él.

La instalación del Presence requiere que resuelva las dependencias del paquete opensips antes de instalarlo. Una vez instalados las dependencias se puede proceder sin problemas a instalar el paquete opensips junto con sus módulos, con solo ejecutar el comando "apt-getinstall", claro una vez que tengamos nuestro lista de repositorios actualizados. Solo basta con editar el "source.list" con lo siguiente:

```
deb http://www.opensips.org/apt/ squeeze main
deb http://ftp.sk.debian.org/debian/ squeeze main
deb-src http://ftp.sk.debian.org/debian/ squeeze main
```

b- Configuración del Servidor Presence (OpenSips)

Para la configuración del servidor Presence se debe realizar algunos cambios en los archivo de configuración opensips.cfg y opensipsctlrc ubicado en /etc/opensips/ así como también en el archivo opensips ubicado en /etc/default/. Luego se creara una base de datos en donde se guardara el estado de cada uno de los usuarios. La base de datos se puede crear con el comando “opensipsdbctlcreate”.

En el archivo opensips que se encuentra dentro del directorio /etc/default/ en donde dice “RUN_OPENSIPS” le ponemos el valor “yes” (si), esto es para habilitar opensips. Tanto en el archivo opensips.cfg como el archivo opensipsctlrc tenemos que indicar el nombre de nuestro dominio (para el primer archivo esta puesto como “alias = imscore.tesis” y en el segundo como “SIP_DOMAIN=imscore.tesis”).

/etc/opensips/opensipsctlrc

```
SIP_DOMAIN= imscore.tesis
DBENGINE=MYSQL
DBHOST=localhost
DBNAME=opensips
DBRWUSER=opensips
DBRWPW="opensipsrw"
DBROOTUSER="root"
USERCOL="username"
INSTALL_EXTRA_TABLES=ask
INSTALL_PRESENCE_TABLES=ask
CTLENGINE="FIFO"
OSIPS_FIFO="/tmp/opensips_fifo"
PID_FILE=/var/run/opensips.pid
```

c- Integra el Presence (OpenSips) al HSS

La instalación por defecto del HSS esta pre-configurado con un AS de ejemplo, para agregar el servicio "Presence" basta con modificar algunos valores de este AS. La primera modificación al AS pre-configurado consiste en cambiar las propiedades del servidor por las que posee el AS "Presence" que estamos agregando, se debe cambiar la dirección IP, el puerto y el nombre del AS registrado en "Application Servers" del menú "Services". La segunda modificación consiste en actualizar el "Trigger Point" del AS para que coincida con los valores mostrados en la Tabla13.1.

Sección	Campo	Valor
Principal	Name	default_tp
	ConditionType CNF	Disjuntive Normal Format
Trigger Point	SIP Method	PUBLISH
	SIP Method	SUBSCRIBE
	SIP Header	Evente
	SIP Header Content	.*presence.*

Tabla 13.1: Valores puestos en el HSS para el servidor Presence.

d- Mensajes intercambiados entre el cliente y el servidor de presencia

El servidor de presencia constituye la entidad central que recoge información acerca del estado del cliente, cada vez que este es autenticado en el núcleo, posteriormente podrá subscribirse al servidor, esto se guarda en una base datos y finalmente servir la información agregada para los observadores que la soliciten.

Los servidores de presencia se soportan sobre mensajes SIP esto para transportar los parámetros denominados Presence Information Data Format (PIDF) RFC 3863. Este definen el formato que utilizara para codificar la información, dicho formato es XML (eXtensible Markup Language) por tener una estructura jerárquica y ser totalmente extensible.

La figura 12 muestra básicamente el uso de tres mensajes SIP: PUBLISH, SUBSCRIBE y NOTIFY.

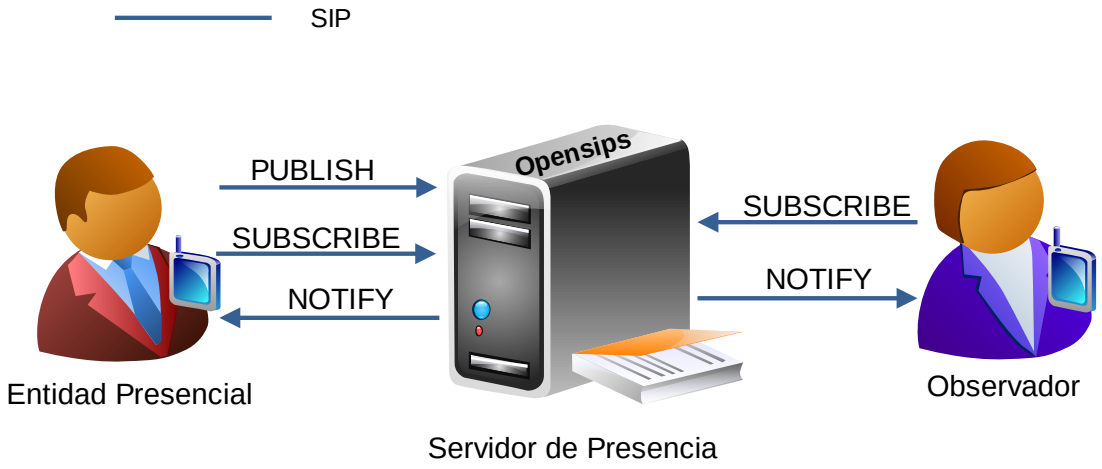


Figura 18: Mensajes de Presencia. (Fuente Propia, 2012-2013)

- Cada vez que hay un cambio en el estado de una entidad presencial (cliente) este envía un mensaje PUBLISH (publicar) al servidor de presencia.
- El observador (cliente) puede obtener información de presencia de otro cliente mediante envió de un mensaje SUBSCRIBE (subscripción). Los observadores también tienen que estar registrado en el servidor.
- El servidor de presencia envía un mensaje NOTIFY (notificación) a todos los observadores que han solicitado obtener información de una entidad.
- En reconocimiento de los mensajes recibidos se utiliza el 200 OK

La figura 13 ilustra el proceso de intercambio de estos mensajes.

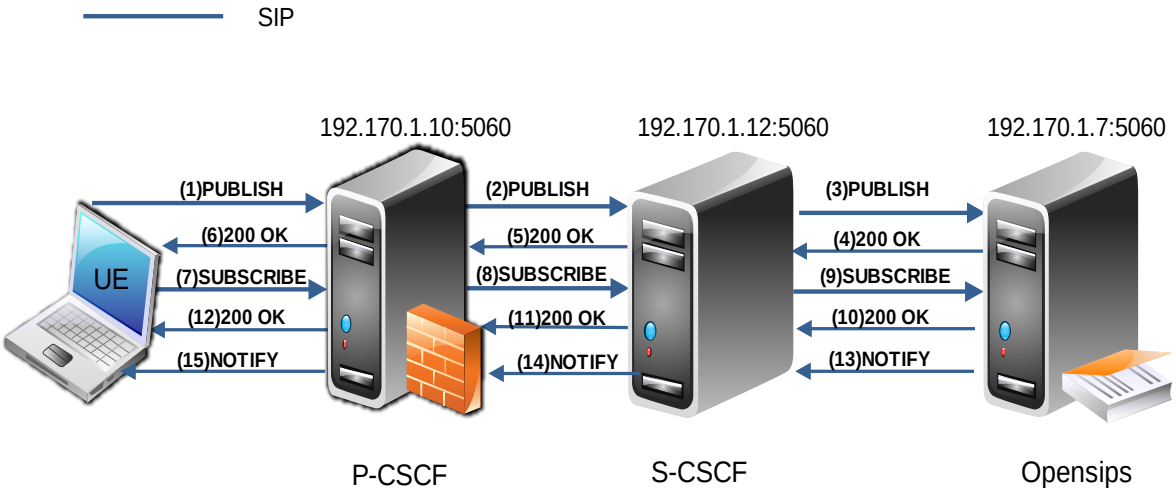


Figura 19: Mensajes de intercambio entre el UE y el servidor de presencia en el dominio IMS. (Fuente Propia, 2012-2013)

a. Del UE al P-CSCF: Mensaje 1 PUBLISH

```
Request-Line: PUBLISH sip:shall@imscore.tesis SIP/2.0
    Method: PUBLISH
    Request-URI: sip:shall@imscore.tesis
      Request-URI User Part: shall
      Request-URI Host Part: imscore.tesis
    [Resent Packet: False]
  Message Header
    Call-ID: 3e6eea5684cca605d6468f91b3432498@192.168.1.3
CSeq: 1 PUBLISH
    From: <sip:shall@imscore.tesis>;tag=1002
    To: <sip:shall@imscore.tesis>
    Via: SIP/2.0/UDP 192.168.1.3:5060;branch=z9hG4bK6f33704b436827d73183aa6620585ab63134
    Max-Forwards: 20
    Route: <sip:orig@scscf.imscore.tesis:5060;lr>
    Event: presence
    Accept: application/pidf+xml
```

```
Expires: 3600
Content-Type: application/pidf+xml
User-Agent: monster Version: 0.9.25
Content-Length: 387
```

El propósito de este mensaje es para proporcionarle al servidor de presencia (Opensips) el estado en el que se encuentra el usuario. Cuando el mensaje es recibido por el P-CSCF se encarga de enrutarlo al S-CSCF correspondiente, a continuación se muestra el cuerpo del mensaje.

```
Message Body
eXtensible Markup Language
<?xml
version='1.0'
encoding='utf-8'
        ?>
<presence
entity="sip:shall&#64;imscore.tesis"
xmlns="urn:ietf:params:xml:ns:pidf"
xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"
xmlns:rpidf="urn:ietf:params:xml:ns:pidf:rpid"
xmlns:op="urn:oma:xml:prs:pidf:oma-pres"
xmlns:opd="urn:oma:xml:pde:pidf:ext">
<tuple
id="com1">
<status>
<basic>
open
</basic>
</status>
<note>
jaja
</note>
</tuple>
</presence>
```

En el cuerpo del mensaje se encuentra las definiciones propias del lenguaje de los cuales solo comentaremos los más importantes:

- **status**: este define la disponibilidad que desea transmitir el cliente hacia sus observadores.
- **note**: este contiene una frase o estado de ánimo escrita por el cliente

b. Del P-CSCF al S-CSCF: Mensaje 2 PUBLISH

```
Request-Line: PUBLISH sip:shall@imscore.tesis SIP/2.0
    Call-ID: 3e6eea5684cca605d6468f91b3432498@192.168.1.3
CSeq: 1 PUBLISH
    From: <sip:shall@imscore.tesis>;tag=1002
    To: <sip:shall@imscore.tesis>
    Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK7514.be883c57.0
    Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bK6f33704b436827d73183aa6620585ab63134
    Max-Forwards: 16
    Route: <sip:orig@scscf.imscore.tesis:5060;lr>
    Event: presence
    Accept: application/pidf+xml
    Expires: 3600
    Content-Type: application/pidf+xml
    User-Agent: monster Version: 0.9.25
    Content-Length: 387
    P-Asserted-Identity: <sip:shall@imscore.tesis>
    P-Charging-Vector: icid-value="P-CSCFabcd514dcd8c00000023";icid-generated-
at=192.170.1.10;orig-ioi="imscore.tesis"
```

El P-CSCF agrega un nuevo campo Via para hacerla saber al S-CSCF a quien será devuelta la respuesta de la solicitud.

c. Del S-CSCF a Opensips: Mensaje 3 PUBLISH

```
Request-Line: PUBLISH sip:shall@imscore.tesis SIP/2.0
    Route: <sip:192.170.1.7:5060;lr>,
<sip:iscmark@scscf.imscore.tesis:5060;lr;s=1;h=0;d=0;a=7369703a7368616c6c40696d73636f72652e7465
736973>
    Call-ID: 3e6eea5684cca605d6468f91b3432498@192.168.1.3
CSeq: 1 PUBLISH
    From: <sip:shall@imscore.tesis>;tag=1002
    To: <sip:shall@imscore.tesis>
    Via: SIP/2.0/UDP 192.170.1.12;branch=z9hG4bK7514.70dd7742.0
    Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK7514.be883c57.0
    Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bK6f33704b436827d73183aa6620585ab63134
    Max-Forwards: 15
    Event: presence
    Accept: application/pidf+xml
    Expires: 3600
    Content-Type: application/pidf+xml
    User-Agent: monster Version: 0.9.25
    Content-Length: 387
    P-Asserted-Identity: <sip:shall@imscore.tesis>
    P-Charging-Vector: icid-value="P-CSCFabcd514dcd8c00000023";icid-generated-
at=192.170.1.10;orig-ioi="imscore.tesis"
```

El S-CSCF agrega un campo Route este para indicarle al opensips que todas las respuestas de todas las solicitudes que realice este cliente serán enviados a dicho S-CSCF.

d. Mensajes 4,5,6:200 OK

```
Session Initiation Protocol
   Status-Line: SIP/2.0 200 OK
      Call-ID: 3e6eea5684cca605d6468f91b3432498@192.168.1.3
CSeq: 1 PUBLISH
      From: <sip:shall@imscore.tesis>;tag=1002
      To: <sip:shall@imscore.tesis>;tag=155c340f586c28d0300cf5a6ccf90d99-580f
      Via: SIP/2.0/UDP 192.170.1.12;branch=z9hG4bK7514.70dd7742.0
      Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK7514.be883c57.0
      Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bK6f33704b436827d73183aa6620585ab63134
      Expires: 3600
      SIP-ETag: a.1364061500.2030.5.0
      Server: OpenSIPS (1.7.0-notls (i386/linux))
      Content-Length: 0
```

Debido a que este mensaje solo es ustilizado para notificar al origen que su mensaje a llegado exitosamente al destino solo sufre cambios en el campo Via.

e. Del UE al P-CSCF: Mensaje 7 SUBSCRIBE

```
Request-Line: SUBSCRIBE sip:alejo@imscore.tesis SIP/2.0
      Call-ID: 372d0f27fc89dfabae8cacfae6995e3c@192.168.1.3
CSeq: 3 SUBSCRIBE
      From: <sip:shall@imscore.tesis>;tag=1003
      To: <sip:alejo@imscore.tesis>
      Via: SIP/2.0/UDP 192.168.1.3:5060;branch=z9hG4bK37474138b2a1402a3a2fb8eefc22c3013134
      Max-Forwards: 20
      Route: <sip:orig@scscf.imscore.tesis:5060;lr>
      Event: presence
      Accept: application/pidf+xml
      Expires: 3600
      Contact: "Shall" <sip:shall@192.168.1.3:5060>
```

```
User-Agent: monster Version: 0.9.25
Content-Length: 0
```

Este mensaje es enviado desde el UE shall@imscore.tesis para hacerle saber al opensips que quiere obtener el estado de el usuario alejo@imscore.tesis

- Request-Line: metodo para subcribir a un usuario del cual se obtendra su informacion de estado.

f. Del P-CSCF al S-CSCF: Mensaje 8 SUBCRIBE

```
Request-Line: SUBSCRIBE sip:alejo@imscore.tesis SIP/2.0
Record-Route: <sip:mo@pcscf.imscore.tesis:5060;lr>
Call-ID: 372d0f27fc89dfabae8cacfae6995e3c@192.168.1.3
CSeq: 3 SUBSCRIBE
From: <sip:shall@imscore.tesis>;tag=1003
To: <sip:alejo@imscore.tesis>
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bKcb7f.abde07f7.0
Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bK37474138b2a1402a3a2fb8eefc22c3013134
Max-Forwards: 16
Route: <sip:orig@scscf.imscore.tesis:5060;lr>
Event: presence
Accept: application/pidf+xml
Expires: 3600
Contact: "Shall" <sip:shall@192.170.1.131:5060>
User-Agent: monster Version: 0.9.25
Content-Length: 0
P-Asserted-Identity: <sip:shall@imscore.tesis>
P-Charging-Vector: icid-value="P-CSCFabcd514dcd8c00000024";icid-generated-
at=192.170.1.10;orig-ioi="imscore.tesis"
```

g. Del S-CSCF al Opensips: Mensaje 9 SUBCRIBE

```
Request-Line: SUBSCRIBE sip:alejo@imscore.tesis SIP/2.0
    Record-Route: <sip:mo@scscf.imscore.tesis:5060;lr>
    Route: <sip:192.170.1.7:5060;lr>,
<sip:iscmark@scscf.imscore.tesis:5060;lr;s=1;h=0;d=0;a=7369703a7368616c6c40696d73636f72652e7465
736973>
    Record-Route: <sip:mo@pcscf.imscore.tesis:5060;lr>
    Call-ID: 372d0f27fc89dfabae8cacfae6995e3c@192.168.1.3
CSeq: 3 SUBSCRIBE
    From: <sip:shall@imscore.tesis>;tag=1003
    To: <sip:alejo@imscore.tesis>
    Via: SIP/2.0/UDP 192.170.1.12;branch=z9hG4bKcb7f.b04742d6.0
    Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bKcb7f.abde07f7.0
    Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bK37474138b2a1402a3a2fb8eefc22c3013134
    Event: presence
    Expires: 3600
    Contact: "Shall" <sip:shall@192.170.1.131:5060>
    User-Agent: monster Version: 0.9.25
    P-Asserted-Identity: <sip:shall@imscore.tesis>
    P-Charging-Vector: icid-value="P-CSCFabcd514dcd8c00000024";icid-generated-
at=192.170.1.10;orig-ioi="imscore.tesis"
```

h. Mensajes 10, 11, 12:200 OK

```
Session Initiation Protocol
  Status-Line: SIP/2.0 200 OK
  Message Header
    Record-Route: <sip:mo@scscf.imscore.tesis:5060;lr>
    Record-Route: <sip:mo@pcscf.imscore.tesis:5060;lr>
    Call-ID: 372d0f27fc89dfabae8cacfae6995e3c@192.168.1.3
CSeq: 3 SUBSCRIBE
    From: <sip:shall@imscore.tesis>;tag=1003
```

```
To: <sip:alejo@imscore.tesis>;tag=155c340f586c28d0300cf5a6ccf90d99-c5e3
Via: SIP/2.0/UDP 192.170.1.12;branch=z9hG4bKcb7f.b04742d6.0
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bKcb7f.abde07f7.0
Via: SIP/2.0/UDP
192.170.1.131:5060;rport=5060;branch=z9hG4bK37474138b2a1402a3a2fb8eefc22c3013134
Expires: 3600
Contact: <sip:192.170.1.7:5060>
Server: OpenSIPS (1.7.0-notls (i386/linux))
Content-Length: 0
```

i. Mensajes 13,14, 15: NOTIFY

```
Request-Line: NOTIFY sip:shall@192.170.1.131:5060 SIP/2.0
Via: SIP/2.0/UDP 192.170.1.7;branch=z9hG4bKeb7f.bb9ca2e2.0
To: <sip:shall@imscore.tesis>;tag=1003
From: <sip:alejo@imscore.tesis>;tag=155c340f586c28d0300cf5a6ccf90d99-c5e3
CSeq: 1 NOTIFY
Call-ID: 372d0f27fc89dfabae8cacfae6995e3c@192.168.1.3
Route: <sip:mo@scscf.imscore.tesis:5060;lr>,<sip:mo@pcscf.imscore.tesis:5060;lr>
Content-Length: 281
User-Agent: OpenSIPS (1.7.0-notls (i386/linux))
Max-Forwards: 70
Event: presence
Contact: <sip:192.170.1.7:5060>
Subscription-State: active;expires=3600
Content-Type: application/pidf+xml
```

Mensaje enviado por el servidor de presencia (opensips) a un clientes para notificar el estado de otros clientes previamente suscritos. A continuación se muestra el cuerpo del mensaje

```
Message Body
eXtensible Markup Language
<?xml
        version="1.0"
        encoding="UTF-8"
        ?>
<presence
xmlns="urn:ietf:params:xml:ns:pidf"
xmlns:im="urn:ietf:params:xml:ns:pidf:im"
        entity="sip:alejo@imscore.tesis">
<tuple
          id="UCTIMSClient">
<status>
<basic>
                open
</basic>
</status>
<note>
              Available
</note>
</tuple>
</presence>
```

De esta forma el UE shall@imscore.tesis puede interpretar que el usuario alejo@imscore.tesis esta disponible y tiene como nota Avaliable.

9.10.3 Servicio de Video

Para dar solución al servicio de contenido multimedia dentro de nuestro dominio IMS, es necesaria la utilización de dos herramientas, uno de ella es el UCT AdvancedIPtv que sirve de intermediario entre los clientes y el servidor de medios, y el otro es el Darwin Streaming Server (DSS) que será en si el servidor de medios.

La arquitectura que se muestra a continuación envuelve cuatro elementos para poder dar soporte a este servicio: OpenIMScore, UTC IMS client, Servidor de Aplicaciones Intermediario (VoD) y Servidor VoD.

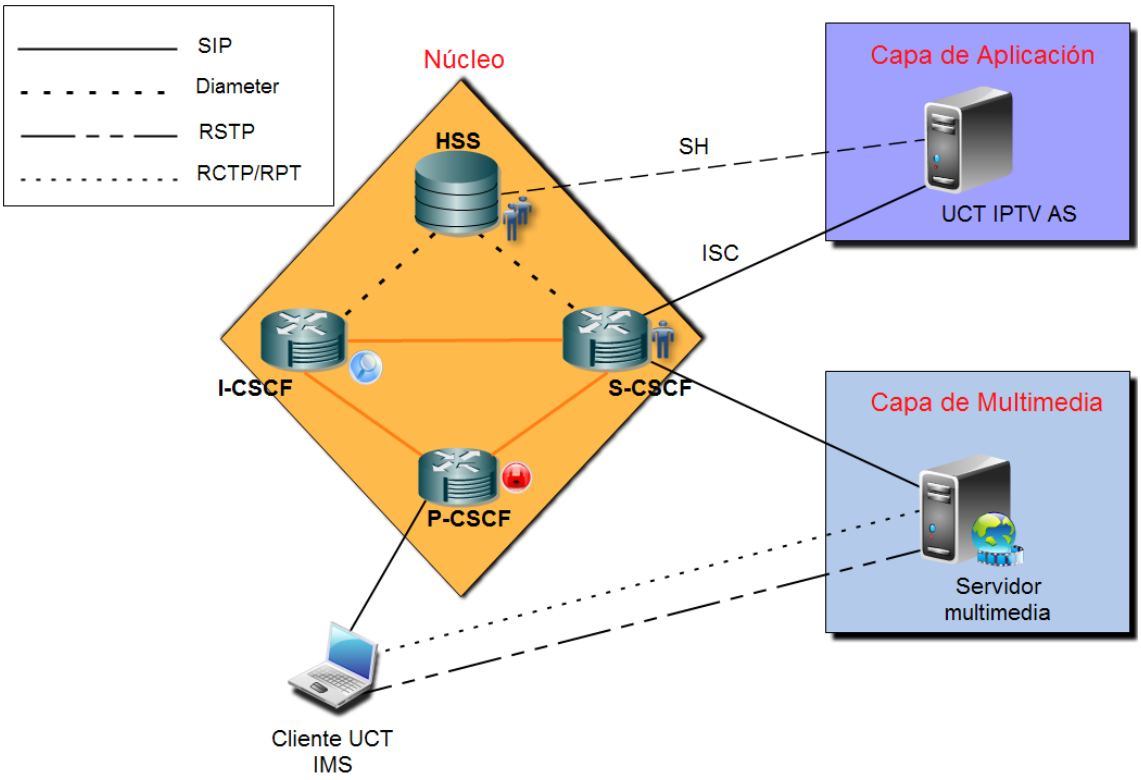


Figura 20: Arquitectura del servicio de video. (Town, n.d.)

Esta comunicación consta de 3 fases:

1- EL cliente realiza una solicitud INVITE a uno de los canales y es enviado al Servidor de Aplicación (Intermediario VoD).
2- El Servidor de Aplicación consulta una tabla HASH que contiene cada una de las direcciones de los respectivos canales y le devuelve al cliente la dirección RSTP del canal solicitado.
3- El cliente inicia una sesión RSTP con el servidor de Streaming (Servidor VoD).

Cabe destacar que la tabla HASH del Intermediario VoD es un archivo xml en el que tiene que tener los correspondientes canales asociados a un video en el Servidor VoD para realizar la traducciones satisfactoriamente.

9.10.3.1 Intermediario para VoD (IPTV)

El intermediario para VoD como mencionamos anteriormente, consiste en la herramienta UCT AdvancedIPtv creado por UTC (University of Cape Town), es un intento de una aplicación compatible con los estándares de IMS para el soporte de los servicios de IPtv. El proyecto está en las primeras etapas de desarrollo y todavía está en la fase Beta experimental, pero aun así podremos destacar que dicha herramienta se ajustó adecuadamente a nuestras necesidades. Para mayor información sobre este proyecto puede referirse a la web http://uctimsclient.berlios.de/uctiptv_advanced_howto.html.

9.10.3.2 Instalación del Intermediario para VoD (IPTV)

El servidor Intermediado para VoD cuenta con una interfaz de red eth0 en el cual está asignada la dirección IP de 192.170.1.4 estáticamente. Para la instalación del servidor de Intermediario para VoD es necesario tener instalado los paquetes libosip (2.2.3), libeXosip (2.2.3), libosip-dev, libexosip-dev y descargado el paquete uctiptv_advanced1.0.0.deb, una vez que tengamos esto listo utilizaremos el comando dpkg –i para instalar el paquete uctiptv_advanced1.0.0.deb.

```
dpkg –i uctiptv_advanced1.0.0.deb
```

9.10.3.3 Configuración del Intermediario para VoD (IPTV)

El AS Intermediario para VoD hará un mapeo del canal solicitado (la primera parte del URI. Ejemplo: canal1@iptv.imscore.tesis) a una dirección RSTP en específica. Para esto tendremos que crear un archivo xml que contendrá una clave SIP URI (ejemplo canal1.) y el valor del RTSP (la dirección absoluta de un archivo multimedia dentro del servidor VoD).

```
<?xml version="1.0" encoding="UTF-8"?>
<key-value_pairs>
 <key-value_pair>
      <key>canal1</key>
      <value>rtsp://media-server-address.tudomain/requested_channel</value>
</key-value_pair>
</key-value_pairs>
```

Para ejecutar el archivo e iniciar el servicio usamos *"uct_iptv_as [key-value_file]"*.

9.10.3.4 Integrar el Intermediario para VoD (IPTV) al HSS

Para agregar un nuevo servicio al dominio IMS, primero se crea un AS con los valores del mismo, esto es: dirección IP, puerto y nombre. Posteriormente se va crear un Trigger Point. Finalmente se necesita crear un iFC uniendo la información creada en estos pasos. La creación del iFC consiste únicamente de asignarle un nombre único y definir el estatus de los usuarios que pueden tener acceso al servicio. La Tabla 13.2 muestra los valores en la creación del Trigger Point.

Sección	Campo	Valor
Principal	Name	iptv_trigger
	ConditionType CNF	Disjuntive Normal Format
Trigger Point	SIP Method	INVITE
	SIP Header	To
	SIP Header Content	.*iptv.imscore.tesis.*

Tabla 13.2: Valores puestos en el HSS para el Intermediario para VoD.

9.10.3.5 Servidor VoD (DSS)

La otra herramienta que forma parte del servicio de contenido utilizado en esta tesis, es el servidor de streaming llamado Darwin Streaming Server (DSS) creado por Apple, es la versión de código abierto del Quick Time Streaming Server de la tecnología de Apple que le permite enviar audio y video a los clientes a través de Internet utilizando los protocolos estándar RTP y RTSP. Darwin Streaming Server (DSS) proporciona un alto nivel de personalización y se ejecuta en una variedad de plataformas que le permiten manipular el código para satisfacer sus necesidades. Más información sobre este proyecto se puede encontrar en la página web http://dss.macosforge.org/.

9.10.3.6 Instalación del Servidor VoD (DSS)

En el servidor VoD asignaremos la dirección IP 192.170.1.5 en su interfaz eth0 de forma estática.

Para instalar el servidor de VoD bajo Linux tendremos que usar un patchllamadoDarwin_6.0.3_patches.zip junto con el servicio de VoD en este caso el paquete DarwinStreamingSrvr6.0.3-Source.tar, a continuación descomprimiremos estos dos paquetes, ejecutamos el patch con el comando “patch -p0”, ahora podremos hacer un “cd” hasta el directorio descomprimido del DSS (DarwinStreamingSrvr6.0.3-Source) y procedemos a instalarlo.

Una vez instalado el servicio de VoD ejecutamos los siguiente script para poner en marcha el servicio.

```
/usr/local/sbin/DarwinStreamingServer
/usr/local/sbin/streamingadminserver.pl
```

9.10.3.7 Configuración del Servidor VoD (DSS)

Para configurar el servidor de VoD solo es necesario dirigirse a la interfaz web por medio de la dirección http://streamer.imscore.tesis:1220. Ver Figura 16 y Figura 17 del anexo.

9.10.3.8 Mensajes intercambiados entre el cliente-núcleo-intermediario-servidor VoD.

En este apartado se describe los mensajes que intercambian el cliente, el P-CSCF, el S-CSCF, el Intermediado para VoD (IPTV), el DNS y el Servidor VoD (DSS) entre sí para establecer una sesión de video Streaming. La figura15 ilustra como es el proceso de intercambio de estos mensajes.

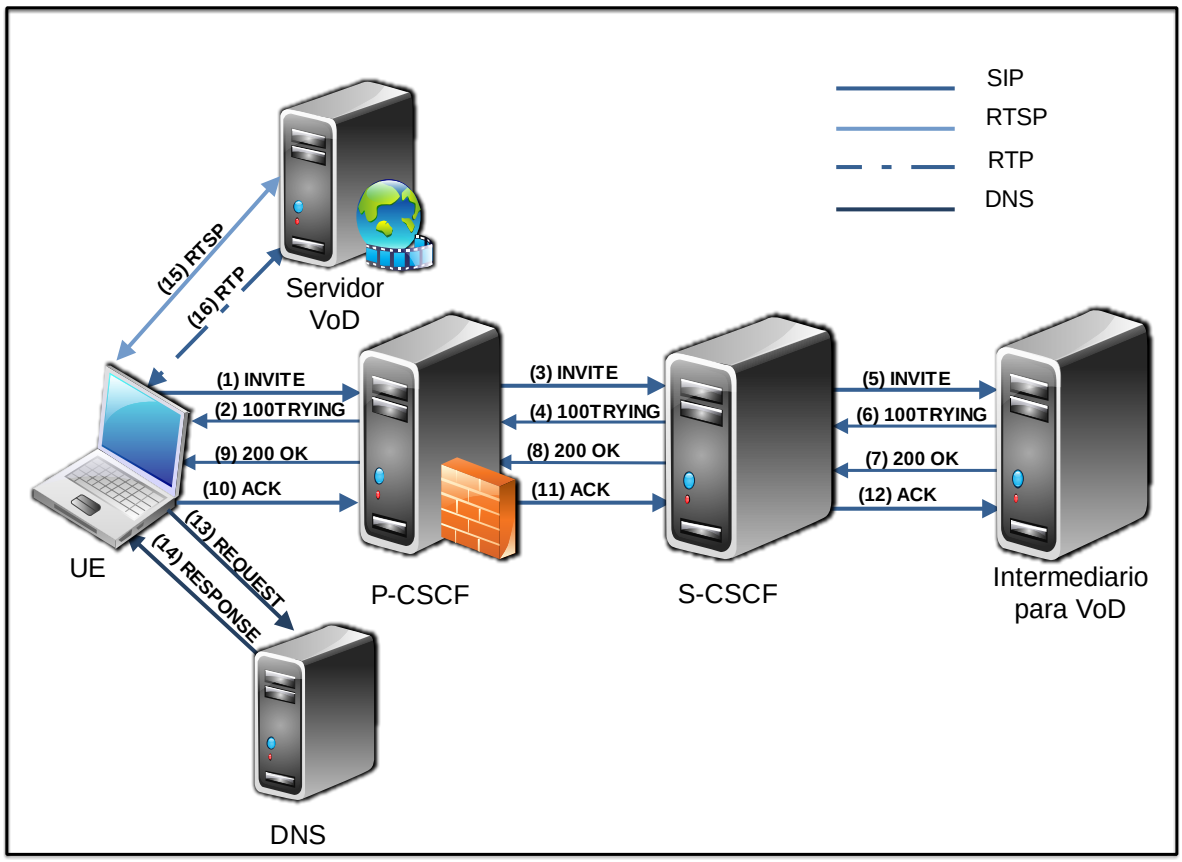


Figura 21: Proceso de intercambio de mensajes. (Fuente Propia, 2012-2013)

a. Mensaje 1: El cliente envía la solicitud INVITE al P-CSCF

Los campos de la cabecera del mensaje de solicitud INVITE son los mismos mencionado en el acápite Servicios ofrecidos nativamente por el núcleo pero con valores distintos, esto ocurrirá siempre y cuando un cliente requiere o solicita cierto servicio del dominio IMS (por ejemplo, cuando un cliente intenta llamar a otro o cuando un cliente solicita un video bajo demanda). Este paquete es enviado al P-CSCF ya que el agente de usuario que va a realizar la llamada no conoce la dirección IP del agente de usuario que recibirá la llamada o en este caso el agente de usuario que hace la solicitud al servicio de IPTV no conoce la dirección IP de dicho servidor, pero si conoce la dirección IP del P-CSCF que es el proxy de nuestro dominio IMS.

El agente de usuario construye el mensaje de solicitud INVITE con los siguientes valores puesto en los campos de cabecera como se muestra la siguiente cuadro.

Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:canal6@iptv.imscore.tesis SIP/2.0
Message Header
Via: SIP/2.0/UDP 192.168.1.3:5060;rport;branch=z9hG4bK1214415290
Route: <sip:orig@scscf.imscore.tesis:5060;lr>
From: "Shall" <sip:shall@imscore.tesis>;tag=862725853
To: <sip:canal6@iptv.imscore.tesis>
Call-ID: 1484722127
CSeq: 20 INVITE
Contact: <sip:shall@192.168.1.3:5060>
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Max-Forwards: 70
User-Agent: UCT IMS Client
Subject: IMS Call
P-Preferred-Identity: "Shall" <sip:shall@imscore.tesis>
P-Preferred-Service: urn:xxx:3gpp-service.ims.icsi.mmtel
Privacy: none
P-Access-Network-Info: IEEE-802.11a
Require: precondition
Require: sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Content-Length: 642

b. Mensaje 2: El P-CSCF responde con un "100 Trying" y reenvía la solicitud

El P-CSCF responde inmediatamente al cliente con un "100 Trying" con los valores puestos en los campos de la cabecera que a continuación se muestra en el siguiente cuadro.

```
Session Initiation Protocol (100)
Status-Line: SIP/2.0 100 trying -- your call is important to us
Message Header
Via: SIP/2.0/UDP 192.170.1.131:5060;rport=5060;branch=z9hG4bK1214415290
From: "Shall" <sip:shall@imscore.tesis>;tag=862725853

To: <sip:canal6@iptv.imscore.tesis>
Call-ID: 1484722127
CSeq: 20 INVITE
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
Content-Length: 0
Warning: 392 192.170.1.10:5060 "Noisy feedback tells:  pid=1523 req_src_ip=192.170.1.131
req_src_port=5060 in_uri=sip:canal6@iptv.imscore.tesis out_uri=sip:canal6@iptv.imscore.tesis via_cnt==1"
```

Este mensaje indica que la solicitud ha sido aceptada por el servidor y está siendo procesado para obtener una respuesta por lo que el cliente deberá esperar. Este mensaje de respuesta, así como todos los mensajes de respuestas provisionales, detiene la retransmisión de una solicitud INVITE por parte de un Agente de usuario (UAC: UserAgentClient). El P-CSCF agrega otro campo "Via" con su dirección IP como valor y elimina el campo P-Preferred-Identity pero mantiene su valor para agregarlo en un nuevo campo llamado P-Asserted-Identity agregado por él, luego reenvía la solicitud INVITE al S-CSCF.

En el siguiente cuadro se aprecia los valores que llevan los campos de la cabecera de la solicitud INVITE una vez que es reenviado al S-CSCF.

```
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:canal6@iptv.imscore.tesis SIP/2.0
Message Header
Record-Route: <sip:mo@pcscf.imscore.tesis:5060;lr>
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK091.23200923.0
Via: SIP/2.0/UDP 192.170.1.131:5060;rport=5060;branch=z9hG4bK1214415290
```

Route: <sip:orig@scscf.imscore.tesis:5060;lr>
From: "Shall" <sip:shall@imscore.tesis>;tag=862725853
To: <sip:canal6@iptv.imscore.tesis>
Call-ID: 1484722127
CSeq: 20 INVITE
Contact: <sip:shall@192.170.1.131:5060>
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Max-Forwards: 16
User-Agent: UCT IMS Client
Subject: IMS Call
P-Preferred-Service: urn:xxx:3gpp-service.ims.icsi.mmtel
Privacy: none
P-Access-Network-Info: IEEE-802.11a
Require: precondition
Supported: 100rel
Content-Length: 646
P-Asserted-Identity: "Shall" <sip:shall@imscore.tesis>
P-Charging-Vector: icid-value="P-CSCFabcd5153349600000065";icid-generated-at=192.170.1.10;orig-ioi="imscore.tesis"

c. Mensaje 3: El S-CSCF responde con un "100 Trying" y reenvía la solicitud

Una vez que el S-CSCF recibe la solicitud INVITE del P-CSCF este le responde con un "100 Trying" inmediatamente, este mensaje de respuesta es idéntica al "100 Trying" enviado al cliente por parte del P-CSCF, ahora el S-CSCF reenvía la solicitud INVITE al servidor Intermediado para VoD (IPTV) pero antes agrega un nuevo campo "Via" con su dirección IP como el valor de este campo. El siguiente cuadro muestra únicamente los campos "Via" de la solicitud INVITE en el S-CSCF antes de reenvíalo al servidor Intermediado para VoD (IPTV).

Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:canal6@iptv.imscore.tesis SIP/2.0
Message Header
Via: SIP/2.0/UDP 192.170.1.12;branch=z9hG4bK091.53fff932.0
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK091.23200923.0

Via: SIP/2.0/UDP 192.170.1.131:5060;rport=5060;branch=z9hG4bK1214415290

d. Mensaje 4: El servidor Intermediario para VoD (IPTV) responde y Procesa la solicitud

El servidor Intermediario para VoD (IPTV) responderá al S-CSCF con un mensaje "100 Trying" una vez que recibe la solicitud INVITE, continuamente procesara dicha mensaje para extraer los datos solicitados por el agente de usuario. Una vez obtenidos estos datos, el servidor Intermediario para VoD (IPTV) consultara su tabla hash (un archivo XML) el cual permite mapear el canal solicitado a una dirección RTSP. Esta dirección RTSP será devuelta al agente de usuario en un mensaje de respuesta "200 OK" el cual es pasado a través de las rutas establecidas por el campo "Via" (es decir que la respuesta "200 OK" es enviado al agente de usuario por el S-CSCF y luego por el P-CSCF). El cuadro siguiente muestra la respuesta "200 OK" que será reenviado al S-CSCF el cual lo reenviara al P-CSCF y este lo reenviara al agente de usuario.

Session Initiation Protocol (200)
Status-Line: SIP/2.0 200 OK
Message Header
Via: SIP/2.0/UDP 192.170.1.12;branch=z9hG4bK091.53fff932.0
Via: SIP/2.0/UDP 192.170.1.10;branch=z9hG4bK091.23200923.0
Via: SIP/2.0/UDP 192.170.1.131:5060;rport=5060;branch=z9hG4bK1214415290
Record-Route: <sip:mo@scscf.imscore.tesis:5060;lr>
Record-Route: <sip:mo@pcscf.imscore.tesis:5060;lr>
From: "Shall" <sip:shall@imscore.tesis>;tag=862725853
To: <sip:canal6@iptv.imscore.tesis>;tag=1887556322
Call-ID: 1484722127
CSeq: 20 INVITE
Contact: <sip:canal6@192.170.1.4:8010>
Content-Type: message/external-body; access-type="URL"; expiration="Sat, 30March2013 09:00:00 GMT";
URL="rtsp://streamer.imscore.tesis/Brave.m4v"
User-Agent: eXosip/3.3.0
Content-Length: 0

9.10.3.9 El cliente inicia una sesión RTSP con el Servidor VoD (DSS)

Antes de iniciar la sesión de RTSP con el servidor VoD (DSS) el agente de usuario manda un mensaje de

reconocimiento (ACK) al dominio IMS, este mensaje es enviado al P-CSCF quien se encarga a reenviarlo al S-CSCF y este último lo reenvía al servidor Intermediado para VoD (IPTV). Ahora el agente de usuario en este caso no conoce la dirección IP del servidor de VoD (DSS) por eso antes hay que realizar una consulta DNS para resolver el nombre de host, cuando el DNS responde al agente de usuario con la dirección del servidor de VoD (DSS) este puede iniciar la sesión RTSP. Los mensajes más importantes intercambiados entre el cliente y el servidor de VoD son:

- **Describe:** Este método obtiene la descripción de una presentación o del objeto multimedia apuntado por una URL RTSP situada en un servidor. El servidor responde a esta petición con una descripción del recurso solicitado, entre otros datos la descripción contiene una lista de los flujos multimedia que serán necesarios para la reproducción. Esta solicitud/respuesta constituye la fase de inicialización del RTSP.

- **Setup:** Hace que el servidor asigne los recursos para un stream y para comenzar una sesión de RTSP.

- **Play:** Comienza la transmisión de datos mediante un flujo asignado vía SETUP.

- **Pause:** Detiene temporalmente uno o todos los flujos, de manera que puedan ser recuperados con un PLAY posteriormente.

- **Teardown:** Detiene la entrega de datos para la URL indicada liberando los recursos asociados.

9.10.3.10 Inicialización de la sesión RTSP: El cliente y el servidor VoD (DSS)

Tomando en cuenta que el agente de usuario ya hizo los pasos mencionado anteriormente como son el proceso de solicitar el canal al dominio IMS y la resolución de nombre, ahora se procederá a hacer las peticiones RTSP necesarios para establecer e iniciar la sesión.

a. El cliente inicia una conexión TCP hacia el puerto 554 del servidor VoD (DSS).

b. Cuando la conexión está establecida correctamente, el cliente envía al servidor una petición “Options”. EL servidor devuelve información que incluye la versión de RTSP, el número de sesión, el nombre del servidor y los métodos soportados. Los siguientes cuadros muestran los valores del campo de cabecera del método “Options” y el método en respuesta al “Options” que es el “Replay 200 OK”.

```
Real Time Streaming Protocol
Request: OPTIONS rtsp://streamer.imscore.tesis/Brave.m4v RTSP/1.0
CSeq: 2
User-Agent: LibVLC/2.0.5 (LIVE555 Streaming Media v2012.05.17)
```

```
Real Time Streaming Protocol
Response: RTSP/1.0 200 OK
Server: DSS/6.0.3 (Build/526.3; Platform/Linux; Release/Darwin Streaming Server; State/Development; )
Cseq: 2\r\n
Public: DESCRIBE, SETUP, TEARDOWN, PLAY, PAUSE, OPTIONS, ANNOUNCE, RECORD
```

c. El cliente envía una petición “Describe” para obtener una descripción de la presentación. El servidor responde con todos los valores de inicialización necesarios para la presentación.

d. El cliente envía “Setup” para cada flujo de datos que se quiere reproducir. El “Setup” especifica los protocolos aceptados para el transporte de los datos.

```
Real Time Streaming Protocol
Request: SETUP rtsp://streamer.imscore.tesis/Brave.m4v/trackID=65537 RTSP/1.0\r\n
Method: SETUP
URL: rtsp://streamer.imscore.tesis/Brave.m4v/trackID=65537
```

```
CSeq: 5\r\n
User-Agent: LibVLC/2.0.5 (LIVE555 Streaming Media v2012.05.17)\r\n
Transport: RTP/AVP;unicast;client_port=39490-39491
Session: 975379080323484227
```

e. Cinco: El cliente envía una petición “Play” que informa al servidor que ahora es el momento de comenzar a enviar datos.

f. Seis: Durante la sesión, el cliente periódicamente hace ping al servidor utilizando peticiones SET_PARAMETER. Aunque la respuesta sea errónea el cliente la ignora informando al cliente que el servidor todavía está activo.

g. Siete: Cuando la presentación termina o el usuario la detiene, el cliente envía un “SET_PARAMETER” que contiene las estadísticas de la sesión.

h. Ocho: El cliente envía “Teardown” para dar por terminada la conexión con el servidor.

9.11 Agregar un nuevo servicio a un usuario.

Cada usuario perteneciente a un dominio IMS puede tener uno o varios servicios asignados a él, como en nuestro caso, encontraran usuario que tendrá un único servicio agregado a él, mientras que habrá otros que tienen asignados todos los servicios ofrecidos por nuestro dominio. Para agregar un servicio a un usuario basta con entrar en la interfaz web del HSS e indicarles a los usuarios, los servicios a las cuales van a tener acceso. Los pasos son, ir a “USER IDENTITIES” ->“PublicUserIdentity” seleccionar el usuario a la cual va a agregar un servicio y en el campo “ServiceProfile*” seleccionamos el perfil del servicio a agregar.

X. Conclusiones y recomendaciones

Al finalizar la realización de este trabajo el cual tuvo como fin el análisis de los procesos de autenticación de usuario y acceso a servicios en la arquitectura IMS se llegó a las siguientes conclusiones:

- La infraestructura de red propuesta para el despliegue de la arquitectura IMS empleando la herramienta OpenIMS permitió crear los escenarios de prueba para el estudio de los diferentes procesos que se analizaron. Dicho escenario tuvo como base el esquema propuesto por los desarrolladores de OpenIMS en el cual cada elemento de la arquitectura se encuentra en una máquina distinta.
- Se logró realizar un análisis de los procesos de autenticación de usuario y el acceso a los servicios nativos ofrecidos por el núcleo IMS a través de la captura de los mensajes intercambiados con el núcleo lo que permitió encontrar diferencias entre las cabeceras SIP generadas por los clientes IMS y de las generadas por los clientes SIP. Esto ayudo a comprender el grado de compatibilidad que existe entre ambos tipos de clientes así como justificar las limitantes que los clientes SIP presentan.
- Por último se agregaron dos servicios externos a OpenIMS: un servidor de presencia el cual utiliza el protocolo SIP para la comunicación con el núcleo y un servidor de video bajo demanda (VOD) el cual al no utilizar el protocolo SIP, necesitó la configuración de un intermediario para su comunicación con el núcleo. Esto permitió estudiar la diferencia en el funcionamiento de OpenIMS cuando un cliente accede a los servicios nativos del núcleo de cuando éste accede a servicios externos así como la necesidad de emplear intermediarios cuando dichos servicios externos no utilizan el protocolo SIP para su comunicación.

Una vez finalizado este trabajo se proponen a continuación una serie de recomendaciones:

- Promover el estudio de tecnologías de redes de nueva generación (NGN) en los estudiantes de la carrera de Ingeniería en Telemática a través de trabajos investigativos, ponencias o seminarios que les permitan adentrarse en estas nuevas tendencias.
- Profundizar en el estudio de IPv6 para una mejor comprensión, IMS pues es sobre este protocolo sobre el cual se sustenta dicha arquitectura.
- Complementar escenario propuesto agregando un servidor que brinde a los usuarios calidad de servicio (QoS) ya que éste es uno de los principales objetivos de la arquitectura IMS, así como un servidor que permita la facturación a los clientes en el núcleo.

XI. Bibliografía

(RFC 2543). (s.f.).

Dueñas, J. B. (2013). *Configuración De Servidores Con GNU/Linux.*

FOKUS, N. F. (2004-2008). *N. Fraunhofer FOKUS*. Obtenido de http://www.openimscore.org/

Fraunhofer FOKUS, N. (2004-2008). Obtenido de OpenSourceIms core: http://www.openimscore.org/installation_guide#step8

Fraunhofer FOKUS, N. (2004-2008). Obtenido de OpenSourceIms core: http://www.openimscore.org/download

(2012-2013). *Fuente Propia.* Leon.

IETF RFC 2386. (s.f.).

ITU E.800: Terms and definitions related to quality of service and network performance including dependability, 1994. (s.f.).

ITU-T Rec. Y.2001, "General Overview of. (s.f.).

José Antonio Pajuelo Martín, L. T. (2010). Arquitectura TISPAN. Aplicaciones y desarrollos comerciales. *Arquitectura TISPAN, 1*(1), 16.

Miikka Poikselka, G. M. (2009). *THE IMS.* WILEY.

Propia, F. (s.f.).

Propia, F. (2012-2013). *Fuente Propia.*

propia, F. (s.f.). *FP.*

RFC 3261. (s.f.).

RFC 3551. (s.f.).

RFC 3588. (s.f.).

RFC 4566. (s.f.).

RFC 6071. (s.f.).

Town, U. o. (s.f.). *UCT IMS Client*. (University of Cape Town, South Africa) Obtenido de http://uctimsclient.berlios.de/uctiptv_advanced_howto.html

XII. Acrónimo

3G Tercera Generación de Telefonía Celular.
3GPP Third Generation Partnership Project.
3GPP2 Third Generation Partnership Project 2.
4G Cuarta Generación de Telefonía Celular.
AAA Autenticación, Autorización y Contabilización (Authentication, Authorizationand Accounting).
AP Access Point (AP).
AS Servidor de Aplicacion (Application Server).
DSS Darwin Streaming Server.
FOKUS Fraunhofer Institute for Open Communications Systems.
HSS Home Subscriber Server.
I-CSCF Interrogating-CSCF.
IETF Internet Engineering Task Force.
iFC Criterio de Filtrado Inicial (Initial Filter Criteria).
IMS IP Multimedia Subsystem.
IP Protocolo de Internet (Internet Protocol).
IPSec Internet Protocol Security.
IPTV Televisión vía IP (IP Television).
IPv4 Protocolo de Internet versión 4 (Internet Protocol v4).
IPv6 Protocolo de Internet versión 6 (Internet Protocol v6).
NAT Traducción de Direcciones de Red (Network AddressTranslation).
NGN Redes de Siguiente Generación (Next Generation Networks).
P-CSCF Proxy-CSCF.
PSTN Red TelefónicaTradicional (Public Switched Telephone Network).
QoS Calidad de Servicio (Quality of Service).
RFC Request for Comments.
RTCP Real-Time Transport Control Protocol.
RTP Real-Time Transport Protocol.
S-CSCF Serving-CSCF.
SDP Protocolo de Descripción de Sesión (Session DescriptionProtocol).
SIP Protocolo de Inicialización de Sesión (Session InitiationProtocol).
SIP-URI Session Initiation Protocol Universal Resource Identifier.
UCT Universidad de Cape Town.
UE Equipo Terminal del Usuario (User Equipment).
URI Identificador de Recurso Universal (Universal Resource Identifier).
VoD Video en Demanda (Video on Demand).
VoIP Vozsobre IP (Voice over IP).
XML eXtensible Markup Language.

XIII. Anexos

Interfaz web del servidor de VoD (DSS).

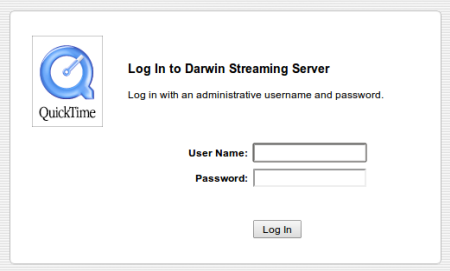


Figura 22: Panel de acceso.

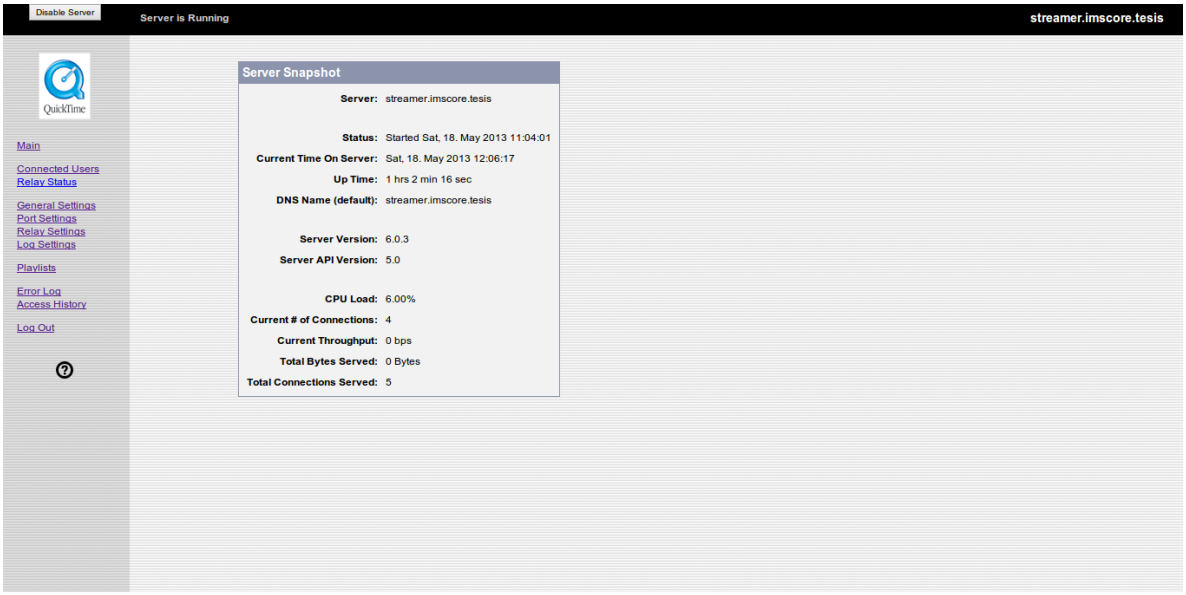


Figura 23: Panel de administración.

Diameter UAR o User-Authorization-Request.

Figura 24: Diameter UAR.

Diameter UAA o User-Authorization-Answer.

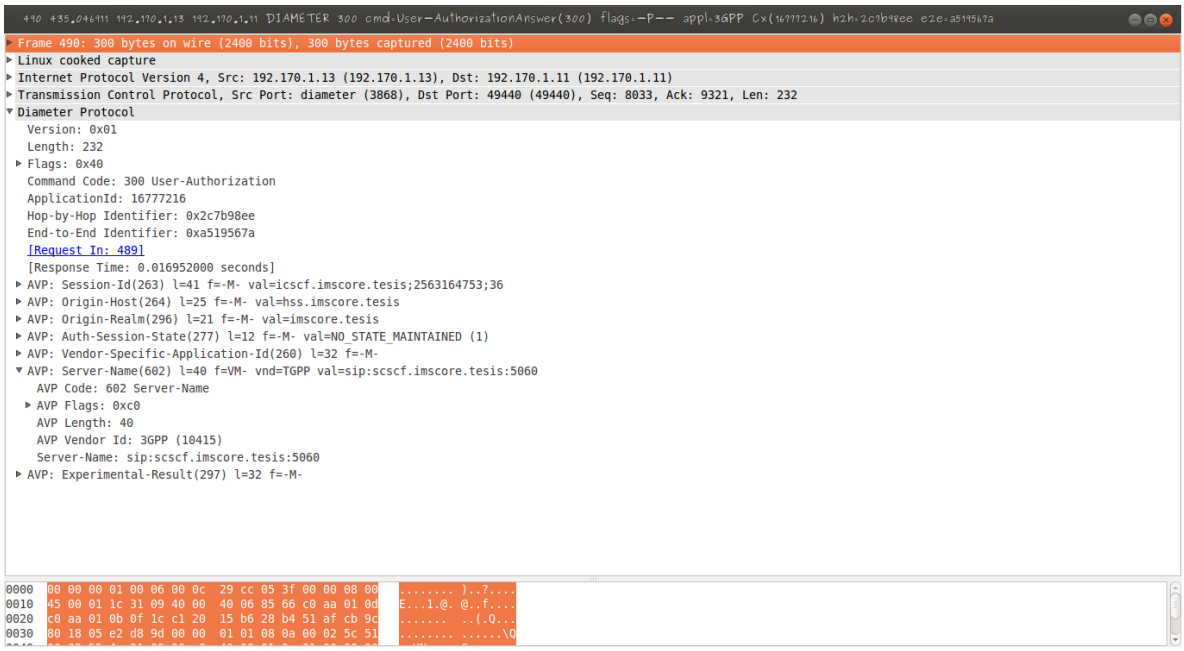


Figura 25: Diameter UAA

Captura de un mensaje de Solicitud en el proceso de Autenticación de un usuario al núcleo IMS.

Figura 26: Mensaje de solicitud para la autenticación a IMScore.

Captura de un mensaje de Respuesta en el proceso de Autenticación de un usuario al núcleo IMS.

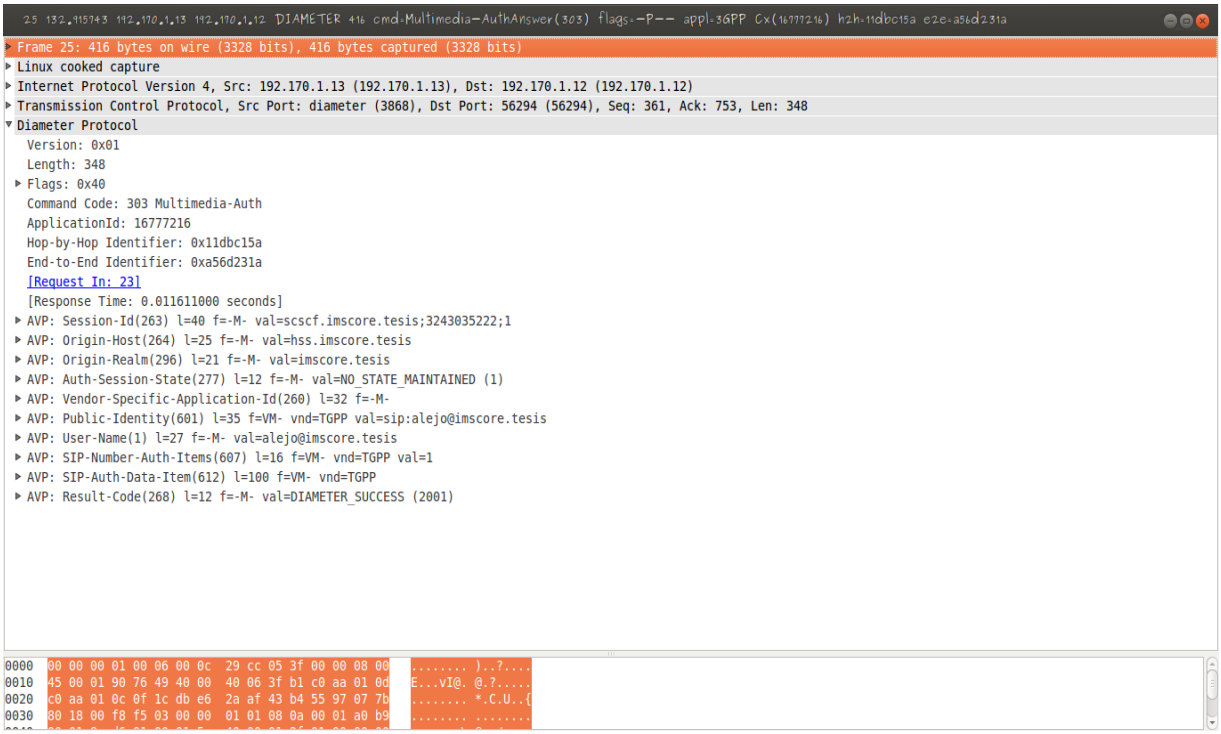


Figura 27: Mensaje de respuesta para la autenticación a IMScore.

Captura de un mensaje de solicitud de estado del registro del suscriptor entre el I-CSCF y el HSS.

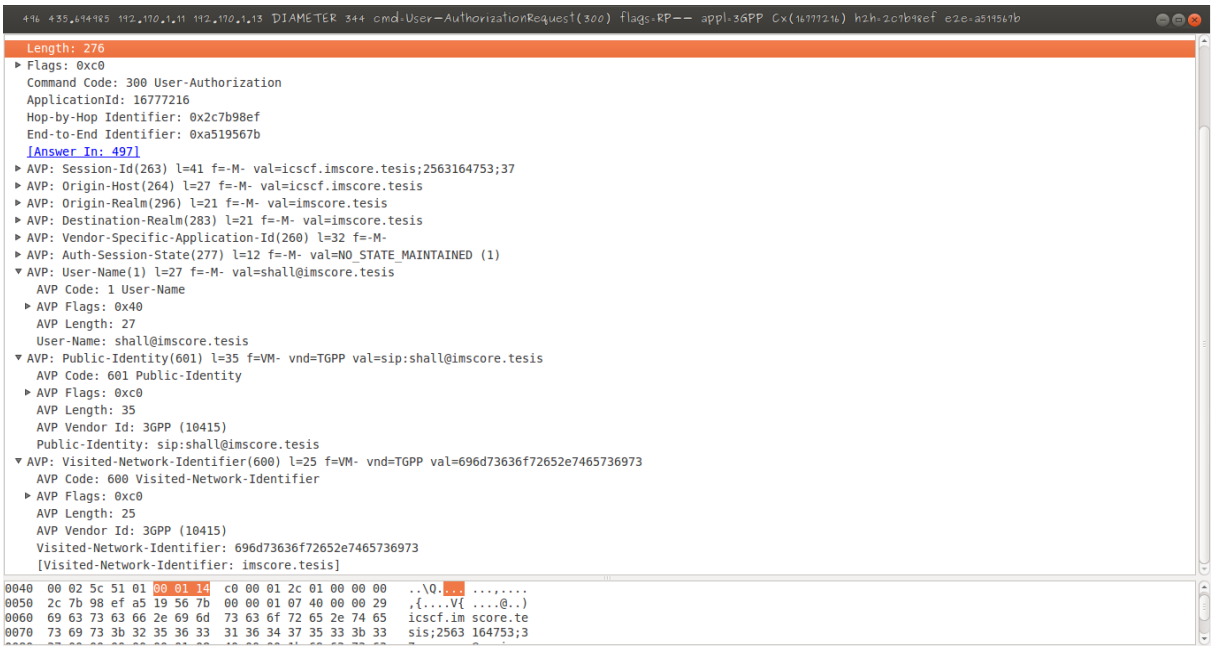


Figura 28: Estado de registro entre I-CSCF y HSS.

Captura de un mensaje de respuesta de estado del registro del suscriptor entre el HSS y el I-CSCF.

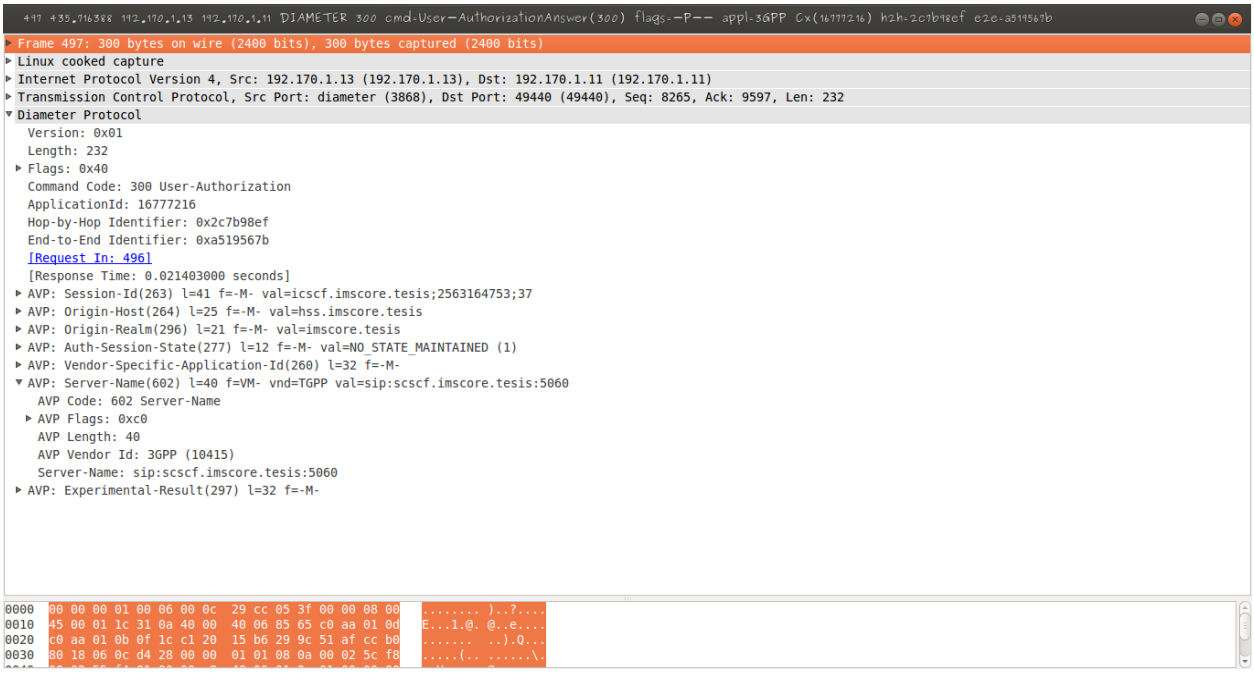


Figura 29: Estado de registro entre HSS y I-CSCF.