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

DISEÑO E IMPLEMENTACIÓN DE UN LABORATORIO DE IPTV, MEDICIÓN Y GESTIÓN

MEMORÍA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL ELECTRICISTA

KURT RAINER ROTTMANN CHÁVEZ

PROFESOR GUÍA:
ALFONSO EHIJO BENBOW

MIEMBROS DE LA COMISIÓN:
NESTOR BECERRA YOMA
JORGE SANDOVAL ARENAS

SANTIAGO DE CHILE
ENERO 2010

RESUMEN DE LA MEMORIA
PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL ELECTRICISTA
POR: KURT ROTTMANN CH.
FECHA: Enero 2010
PROF. GUÍA: Sr. ALFONSO EHIJO BENBOW

"DISEÑO E IMPLEMENTACIÓN DE UN LABORATORIO DE IPTV, MEDICIÓN Y GESTIÓN"

El objetivo general del presente trabajo de título es diseñar e implementar un Laboratorio de IPTV, de bajo costo y con fines docentes. Esto implica definir las entidades de red a utilizar, escoger los sistemas de administración y verificar la correcta operación del servicio final considerando la utilización de sistemas de uso libre.

El Departamento de Ingeniería Eléctrica de la Universidad de Chile aborda los servicios tecnológicos emergentes, posibilitando de esta manera la continua actualización de conocimientos requeridos por las innovaciones en el área de las telecomunicaciones. La implementación del Laboratorio de IPTV permite el estudio docente de manera práctica al ofrecer un sistema apto para la realización de diversas pruebas de funcionamiento. Esta memoria es una continuación necesaria de trabajos de título previos del Departamento de Ingeniería Eléctrica que han seguido la línea del estudio y ofrecimiento de servicios sobre redes convergentes, de amplia adopción hoy en día en el mercado de las telecomunicaciones.

El Laboratorio de IPTV está constituido sobre la arquitectura IMS lo que implica que el diseño sigue los estándares de servicios de IPTV basados en IMS. Comenzando por el núcleo de esta arquitectura, han sido incorporadas las entidades necesarias para el ofrecimiento de las prestaciones de IPTV, complementándose además, con un módulo de tarificación y un sistema de políticas de control de QoS.

La plataforma está construida a partir de diversos proyectos de software libre, los cuales conforman cada elemento de red utilizado en el Laboratorio de IPTV. La implementación final del servicio incluye las siguientes características: canales en vivo, contenido bajo demanda (VoD), un grabador digital de video (NDVR, Network Digital Video Recorder), una Guía de programación (EPG, Electronic Program Guide), un sistema de tarificación de prepago y postpago, interfaz web de administración del núcleo IMS y del sistema de políticas de control de QoS, además de la posibilidad de ocupar otros servicios comunes en IMS como llamadas VoIP, videoconferencias o mensajería instantánea.

Como resultado del trabajo de título se obtiene que el Laboratorio de IPTV constituye una útil plataforma de estudio y otorga la posibilidad de ser ocupada como base para la realización de diversas pruebas de concepto relacionadas con la entrega de servicios sobre la arquitectura IMS. Se incluye además una serie de guías prácticas con fines docentes realizadas a partir de las comprobaciones efectuadas al sistema en el que se analizan las comunicaciones de los principales protocolos involucrados que son: SIP, DIAMETER, RTSP, RTP y RTCP.

En términos de proyecciones, se da pie a nuevos trabajos de memoria en los que se pueden ampliar las características aquí desarrolladas y extender las limitaciones del Laboratorio de IPTV de modo de acercarlo más a las prestaciones que debe entregar una plataforma comercial de su tipo. En particular, incluir un set de herramientas de software que permita monitorear aspectos de QoS en tiempo real. Esta memoria sirve además de base y ejemplo para cualquier trabajo de título que desee implementar y gestionar nuevos servicios de valor agregado sobre redes IMS.

AGRADECIMIENTOS

Agradezco a las numerosas personas que me han acompañado durante estos años de travesía. Un cariño especial a los más cercanos, los que me brindaron el apoyo y las fuerzas de forma incondicional día tras día. Gracias.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I: INTRODUCCIÓN

1.1. Motivación

Los Proveedores de Servicios en el área de las Telecomunicaciones se han visto enfrentados a cambios sustanciales en el mercado. La fuerte irrupción de las TIC basadas en IP, así como la evolución que ha tenido Internet como plataforma de desarrollo de nuevos y variados servicios ha producido una explosión de Proveedores de Servicios distintos a los ya existentes. En este escenario, dichos operadores han comenzado a diversificar su negocio en términos comerciales ofreciendo paquetes de servicios. Es así como por ejemplo operadores de cable ahora ofrecen servicios de telefonía fija, acceso a Internet y televisión. Dentro de esta iniciativa por posicionarse en el mercado las empresas tienen que ofrecer servicios atractivos para el cliente final como lo es IPTV.

Entonces la pregunta de: ¿Por qué IPTV? se responde desde el ámbito comercial debido a que existe una alta competitividad en el área de las telecomunicaciones la cual está dada por varios proveedores de servicios de telecomunicaciones con ofertas similares. Luego por esta causa, es que existen dos grandes motivos para entrar en el negocio de IPTV. El primero, es la oportuna necesidad de diferenciarse del resto de los proveedores. En segundo lugar, el proveer mayor cantidad y mejores servicios que la competencia [27]. Por estos motivos, ya existen implementaciones de IPTV comercial en el mundo, en donde son ofrecidos como parte de un paquete que incluye Telefonía IP y acceso a Internet con importantes anchos de banda.

El Departamento de Ingeniería Eléctrica de la Universidad de Chile debe abordar este tipo de servicios tecnológicos emergentes, posibilitando una continua actualización de los conocimientos requeridos por el mercado de las telecomunicaciones. El desarrollo de este trabajo de título implementará un Laboratorio de IPTV que permitirá el estudio docente de manera práctica al ofrecer como resultado un sistema apto para pruebas. Esta Memoria es una continuación necesaria de trabajos de titulo previos del Departamento de Ingeniería Eléctrica que han seguido la línea del estudio y ofrecimiento de servicios sobre redes convergentes de amplia adopción en el mercado de las telecomunicaciones hoy en día.

1.2. Objetivos

1.2.1. Objetivo general

El objetivo general del trabajo de título es diseñar e implementar un Laboratorio de IPTV. La plataforma de IPTV será de bajo costo y con fines docentes. Esto implicará definir las entidades de red a implementar, escoger los sistemas de administración de la red y establecer las pruebas para su estudio.

1.2.2. Objetivos específicos

Los objetivos específicos del trabajo de título son:

- Estudiar las principales arquitecturas de redes convergentes que existen en la actualidad, identificando los elementos que las componen de modo de hacer la plataforma de IPTV compatible con ellas y cumpliendo los estándares.
- Establecer los componentes que conformaran el sistema de IPTV y las características que ofrecerá el servicio.
- Estudiar los protocolos de comunicación involucrados en la plataforma de IPTV.
- Implementar el sistema de IPTV en el Laboratorio de Telecomunicaciones del Departamento de Ingeniería Eléctrica de la Universidad de Chile detallando los pasos para la puesta en marcha.
- Realizar pruebas de funcionamiento y capturas de tráfico en distintos escenarios de prueba con el fin de establecer las bases para el futuro desarrollo de experiencias docentes de laboratorio.

1.3. Hipótesis

La principal hipótesis de trabajo es que el Laboratorio de IPTV puede ser implementado en su totalidad a base de proyectos de código abierto existentes. Dentro de estos destacan el sistema operativo GNU/Linux, Open IMS Core que es una implementación del núcleo de la arquitectura IMS y la herramienta de análisis de tráfico de paquetes Wireshark.

1.4. Metodología

La metodología de trabajo comprende diversas etapas. La primera corresponde al estudio de los sistemas de IPTV, de las arquitecturas de redes convergentes existentes en la actualidad y de los protocolos de comunicaciones asociados en ellos. Posteriormente, una segunda etapa comienza con la generación de una propuesta de diseño basado en dichos mapas arquitectónicos y en los desarrollos de memoristas anteriores que han trabajado en temas relacionados con las arquitecturas de redes convergentes. En esta etapa se definen los elementos que participarán en la red, así como su estructura. Después de la exposición del diseño de la plataforma, se continúa con la etapa de implementación del Laboratorio de IPTV. En esta etapa se levantan las entidades de red que participan en el sistema. El procedimiento usado es el de comenzar por un sistema básico para luego ir incrementándolo en complejidad hasta la implementación completa, de este modo se pueden detectar posibles errores más fácilmente. Finalmente se validará el funcionamiento del Laboratorio de IPTV a través de pruebas que darán pie a experiencias de laboratorio.

1.5. Alcances

El servicio de IPTV pretende ser capaz de ofrecer las principales funcionalidades que constituyen un sistema de IPTV. El carácter de Laboratorio de IPTV hace alusión a que la plataforma debe posibilitar la realización de pruebas con fines docentes y ser lo suficientemente flexible como para ser útil frente a una nueva implementación de un sistema más complejo, por ejemplo en su incorporación dentro de un futuro trabajo de memoria.

Se espera que el Laboratorio de IPTV sea un servicio acorde a estándares en telecomunicaciones, inclusive siendo ideal el uso de redes convergentes, su potencialidad queda limitada por ser una implementación de bajo costo, basado exclusivamente de la disponibilidad de proyectos Open Source que se desarrollados externamente. Luego, es importante destacar que todas las funcionalidades son implementadas a través de software y que los equipos a utilizar son computadores de escritorio sin mayores prestaciones. Por lo tanto, más allá de perseguir como resultado una plataforma con características de sistemas comerciales como seguridad, escalabilidad o alta disponibilidad. Se busca que el Laboratorio de IPTV permita ser un centro de estudio y pruebas concepto.

1.6. Descripción de contenidos

A continuación se describen en términos generales los contenidos de los capítulos que comprenden el presente trabajo de título:

En el Capítulo 1 se exponen las bases del presente trabajo de título. Se introduce el estado actual del mercado de las telecomunicaciones y cómo la convergencia de redes y servicios representan una alternativa de evolución para esta industria. A partir de ello se enuncia la motivación del tema del trabajo de título, la justificación de su desarrollo y se definen los objetivos, alcances, hipótesis y la metodología a seguir en el desarrollo del mismo.

En el Capítulo 2 se exponen los antecedentes del trabajo a desarrollar. Se presenta el concepto detrás de IPTV, evidenciando la diferencia entre IPTV como un servicio comercial en contraste a una solución común de TV por Internet. Luego se estudian conceptos relacionados con arquitecturas de redes convergentes, tales como IMS, TISPAN y PacketCable. Luego se menciona como se puede ofrecer servicios sobre estas arquitecturas, para terminar con conceptos relacionados a la calidad y experiencia de servicio.

En el Capítulo 3 se establece la metodología para el diseño y la implementación del Laboratorio de IPTV. En primer lugar se exponen las consideraciones a tomar para el diseño del sistema. Posterior a esto se procede con la implementación gradual del Laboratorio de IPTV: Se comienza con el Núcleo y Cliente IMS, luego se continua levantando un sistema de IPTV básico, posteriormente se sigue adosando un sistema de tarificación, para terminar incluyendo un sistema de políticas de control. Finalmente se establecen las experiencias de laboratorio que permiten estudiar los distintos eventos que se dan dentro del Laboratorio de IPTV.

En el Capítulo 4 se describen los resultados obtenidos a partir del desarrollo del trabajo de título. Se entrega información sobre el diseño y la implementación del Laboratorio de IPTV y sobre las experiencias de laboratorio desarrolladas para establecer el comportamiento de los distintos componentes del sistema.

En el Capítulo 5 se expone la discusión sobre los resultados obtenidos. En términos generales se realizan observaciones y propuestas sobre los aspectos prácticos del sistema implementado y de las experiencias desarrolladas. Además se establecen posibles mejoras al sistema y se proponen

tareas futuras en base al potencial que entrega la implementación del Laboratorio de IPTV sobre IMS.

En el Capítulo 6 se entregan las conclusiones acerca del trabajo de título desarrollado. En base a la discusión generada en el capítulo anterior se establecen los logros obtenidos y el aporte realizado a través del diseño y la implementación del Laboratorio de IPTV. En este contexto se revisa la concreción de los objetivos planteados inicialmente.

CAPÍTULO II: ANTECEDENTES

2.1. Servicio de IPTV

2.2.1. Descripción de IPTV

IPTV (Internet Protocol Television) es una tecnología que día a día crece más en importancia, ya comenzando a interrumpir en los modelos de negocios existentes de los operadores de televisión de pago tradicionales. La definición oficial determinada por la ITU (ITU-T FG IPTV) [38] es la siguiente: "IPTV es definido como servicios multimedia tales como televisión/audio/texto/gráficos/datos transmitidos sobre una red IP gestionada para entregar los niveles requeridos de calidad y experiencia de servicio, así como también seguridad, interactividad y confiabilidad."

IPTV es un término usado para referirse a la transmisión de canales de televisión tradicional, películas, y video-on-demand sobre redes de datos privadas. Se tiene entonces que desde la mirada del usuario final, IPTV solamente se presenta como otro sistema más de televisión de pago. Bajo la perspectiva de un proveedor de servicios, IPTV comprende la adquisición, procesamiento, y transmisión segura y confiable de contenido de video sobre una infraestructura de red basada en IP. El tipo de proveedores de servicios involucrados en el desarrollo de servicios de IPTV abarca desde los operadores de cable y TV satelital, hasta las grandes compañías de telefonía y operadores de redes privadas en diferentes partes del planeta [2]. Algunas características destacadas de IPTV son:

Soporte para TV interactiva: Las habilidades de comunicación bidireccional de los sistemas de IPTV permiten a los proveedores de servicios entregar un amplio rango de aplicaciones de TV interactiva. Los tipos de servicios entregados a través de IPTV pueden ser televisión en vivo con sistemas de votación online, solicitud de contenido audiovisual específico (video on demand), juegos multimedia interactivos y navegación por Internet.

Cambiar horarios de transmisión: IPTV en combinación con un grabador de video digital permite cambiar los horarios en que el usuario final ve los contenidos de la programación. Es decir un sistema en que se graba y almacena contenido de IPTV para verlo posteriormente. Esta

idea no esta limitada a que sea un PVR (Personal Video Recorder) local, sino esto se puede lograr utilizándose una memoria caché centralizada y administrada por los proveedores de IPTV en donde los usuarios pueden solicitar contenidos en vivo transmitidos en el pasado con una antigüedad temporal solo limitada por el tamaño de este almacenamiento.

Personalizable: Un sistema de IPTV soporta comunicación bidireccional permitiendo que el usuario final pueda decidir que y cuando quiere ver televisión.

Bajo requerimiento de ancho de banda: En vez de transmitir cada canal a cada usuario, las tecnologías de IPTV permiten a los proveedores de servicio sólo transmitir el contenido que el usuario ha solicitado ver y no todos los canales. Esta característica permite a los operadores de red optimizar el uso del ancho de banda de sus redes.

Accesibles en múltiples dispositivos: La visualización del contenido de IPTV no esta limitado a los televisores, los consumidores pueden usar sus PCs o aparatos celulares para acceder a los servicios de IPTV.

2.2.2. Diferencias entre IPTV y TV por Internet

Existen algunas diferencias entre IPTV y TV por Internet o IP Video. Aunque ambos términos son muy similares, existe una clara distinción en como son usadas en el mercado. IPTV es usado para referirse a la comercialización por parte de proveedores de servicios hacia sus suscriptores de canales de televisión y contenidos multimedia con un aspecto similar a la televisión tradicional de pago. TV por Internet se usa comúnmente para referirse a páginas web o portales que ofrecen programas de televisión o películas on-demand [2]. Aunque ambos sistemas se basan en las mismas tecnologías, sus enfoques en como distribuyen el contenido de Video sobre IP difieren de las siguientes maneras:

Plataformas diferentes: Como su nombre lo sugiere, Internet TV utiliza la red de Internet pública para transmitir el contenido de video a los usuarios finales. IPTV, por el contrario, usa una segura red privada dedicada para transmitir el contenido de video a los consumidores. Estas redes privadas son manejadas y operadas por el proveedor del servicio de IPTV.

Alcance geográfico: Las redes pertenecen y son controladas por las compañías operadoras de telecomunicaciones siendo no accesibles por los usuarios de Internet y siendo localizadas en un lugar geográfico determinado. Internet, por el contrario, no posee limitaciones geográficas donde los servicios pueden ser accedidos desde cualquier parte del planeta.

Dueños de la infraestructura de red: Cuando el video es enviado sobre la red publica de Internet, algunos de los paquetes IP usados para transportar el video sufren retardos o se pierden completamente al atravesar las numerosas redes que componen la Internet. Como resultado, los proveedores de contenido de video sobre Internet no pueden garantizar una experiencia de ver televisión que se pueda comparar con la ver televisión tradicional. De hecho, el video transmitido sobre Internet puede a veces verse muchas veces con cortes o con una baja resolución de imagen. El contenido de video es generalmente transmitido al usuario final a través del mejor esfuerzo posible. En comparación a esto, IPTV es transmitido sobre una infraestructura de red, que pertenece típicamente al proveedor de servicios. Ser dueño de la infraestructura de red permite a las empresas proveedoras de telecomunicaciones poder gestionar sus sistemas de modo de hacer posible la entrega de video de alta calidad.

Mecanismo de acceso: Un Set-Top Box digital es generalmente usado para acceder y decodificar el contenido de video transmitido a través de un sistema de IPTV y reproducido típicamente en un televisor estándar, mientras que un PC es casi siempre utilizado para acceder a los servicios de Internet TV. El tipo de software usado en el PC va a depender del tipo de contenido de Internet TV que se desea. Por ejemplo, la descarga de contenidos desde un portal de Internet TV a veces requiere la instalación de un reproductor especializado para ver el contenido. Un sistema robusto de Digital Rights Management (DRM) es necesario también para este mecanismo de acceso.

Costos: Un porcentaje significante del contenido de video que es entregado sobre la red de Internet pública esta disponible gratuitamente. Aunque un creciente número de empresas de medios de comunicación han empezado a introducir servicios de Internet TV de pago. La estructura de costos aplicada a los servicios de IPTV es similar al modelo de suscripción mensual adoptada por los proveedores tradicionales de TV de pago. Con el tiempo, varios analistas esperan que la TV por Internet e IPTV converjan en un solo servicio de entretenimiento.

Metodologías de los generadores de contenidos: Un porcentaje significante del contenido de video que es entregado sobre la red de Internet pública esta disponible gratuitamente. Sin embargo un creciente número de empresas de medios de comunicación han empezado a introducir servicios de Internet TV de pago. La estructura de costos aplicada a los servicios de IPTV es similar al modelo de suscripción mensual adoptada por los proveedores tradicionales de TV de pago. Con el tiempo, varios analistas esperan que la TV por Internet e IPTV converjan en un solo servicio de entretenimiento.

2.2.3. Infraestructura general de una red de IPTV

La siguiente figura muestra los requerimientos funcionales de alto nivel típicos de un sistema de IPTV end-to-end [2].

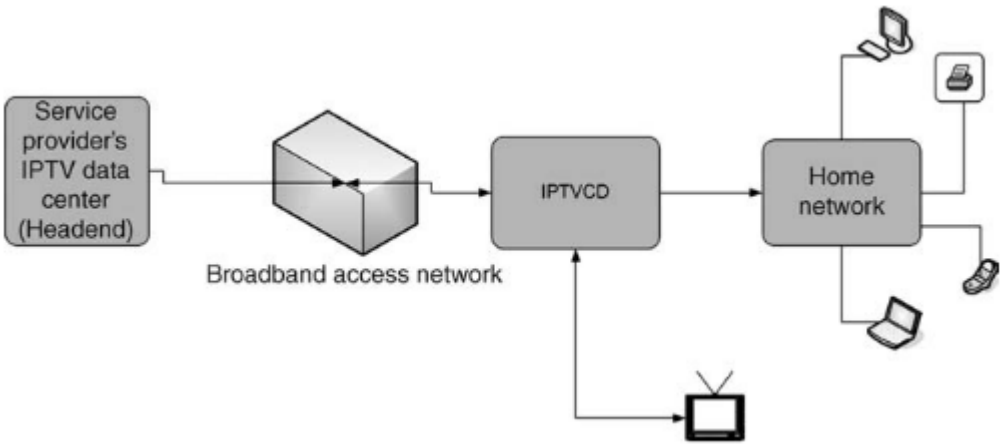

Figura 1: Diagrama de bloques de una red de IPTV.

IPTV Data Center: También conocido como "Headend", el IPTV Data Center recibe el contenido desde una diversidad de fuentes incluyendo todo tipo de generadores de contenido, productoras, canales de televisión gratuitos y de pago. Una vez recibida la información, diferentes equipos de hardware como encoders y servidores de video, así como también IP routers y hardware dedicado a la seguridad son usados para preparar el contenido de video que será transmitido sobre la red IP. Adicionalmente, es necesario un sistema de manejo de subscriptores para gestionar los datos de los clientes del servicio de IPTV y realizar labores de tarificación. La localización física del IPTV Data Center estará dada por la infraestructura de red usada por el proveedor de servicios.

Broadband Delivery Network: La entrega de servicios de IPTV requiere de conexiones uno a uno. En el caso de grandes despliegues de IPTV, el numero de conexiones uno a uno aumenta significativamente y la demanda en términos de ancho de banda para la infraestructura de la red puede ser bastante grande. Los avances tecnológicos en el último par de años permiten que los proveedores de telecomunicaciones puedan enfrentarse a la demanda. Infraestructuras hibridas de fibra óptica y redes coaxiales son particularmente convenientes para transportar contenido de IPTV.

IPTVCDs: Dispositivos de consumo de IPTV (IPTVCDs) son los componentes clave para permitir que la gente pueda acceder a servicios de IPTV. El IPTVCD conecta al usuario a la red IP y es responsable de decodificar y procesar el contenido de video entrante. Los IPTVCDs ayudan con tecnologías avanzadas que minimizan o eliminan completamente los efectos de los problemas en la red cuando se procesa el contenido de IPTV. Los IPTVCDs más populares son Gateways residenciales, IP Set-Top-Boxes, consolas de videojuegos y Media Servers los cuales aumentan cada vez en su sofisticación.

Home Network: Una red hogareña conecta dispositivos digitales en una pequeña área geográfica. Esto mejora la comunicación y permite el intercambio de grandes volúmenes de contenidos digitales entre miembros de una familia. El propósito de una red hogareña es proveer acceso a la información, como es voz, audio, datos y entretenimiento entre diferentes dispositivos digitales a lo largo de una casa. Con redes hogareñas locales, los consumidores pueden ahorrar dinero y tiempo porque los periféricos como impresoras y scanners, como también las conexiones de banda ancha, pueden ser fácilmente compartidos.

2.2. Convergencia de redes y servicios

Las redes de próxima generación tienen como principal objetivo ofrecer a los suscriptores una serie de aplicaciones que provean calidad de servicio (QoS) en un ambiente controlado en tiempo real. En la actualidad aparecen tres distintas arquitecturas que son: 3GPP IP Multimedia Subsystem destinada principalmente para acceso inalámbrico, ETSI TISPAN para arquitecturas fijas y PacketCable 2.0 para arquitecturas de cable.

2.2.1. Redes de próxima generación

Una Red de Próxima Generación (NGN, Next Generation Network), corresponde a una red convergente universal de telecomunicaciones. La ITU-T a través de la recomendación Y.2001 [39] establece las características básicas que esta debiera tener:

1. Ser una red basada en la conmutación de paquetes.
2. Agnóstica al acceso permitiendo el uso de diferentes redes de entrada.
3. Soporte de movilidad generalizada.
4. Red multiservicios.
5. Capas con funciones autónomas (estrato de transporte y de servicios autónomos).
6. Equipo de usuario final fijo y móvil.

La NGN tiene como principal objetivo ofrecer a los suscriptores una serie de aplicaciones que provean calidad de servicio (QoS) en un ambiente on-demand, sin importar la arquitectura de acceso o el dispositivo que se utilice. Las funciones de esta red se dividen en estratos de servicio y transporte como lo especifica la recomendación Y.2001 [39]. Las funciones del usuario final se conectan a la NGN a través de la interfaz UNI (User-to-Network Interface), mientras que las otras redes se encuentran interconectadas a través de la interfaz NNI (Network-to-Network Interface). Por último, la interfaz ANI (Application-to-Network Interface) demarca la frontera con los proveedores de aplicaciones.

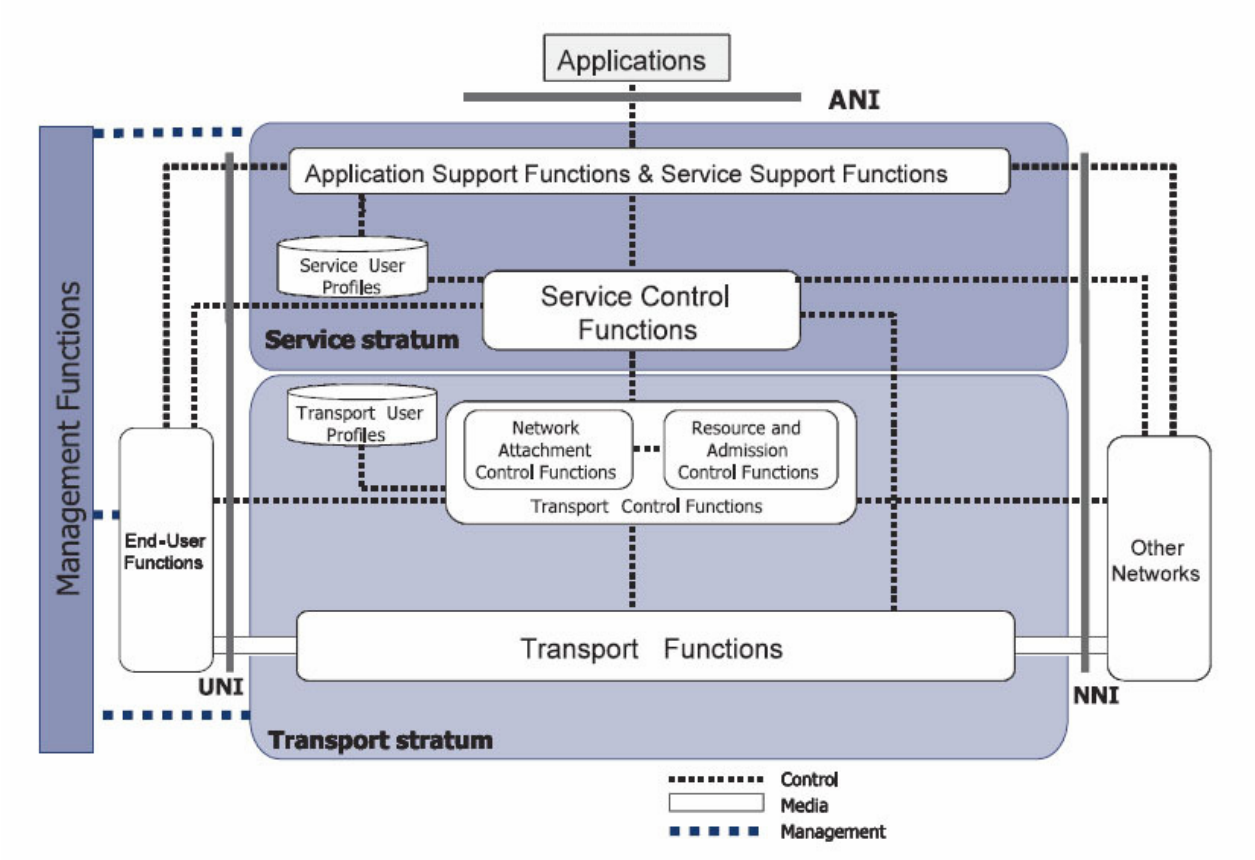

Figura 2: Arquitectura NGN.

Funciones del Estrato de Transporte: Las funciones del estrato de transporte permiten la conectividad entre todos los componentes y funcionalidades que están separadas físicamente. El estrato de transporte es el responsable de proveer QoS punto a punto. El estrato de transporte se divide en las redes de acceso y el Core de la red con una función de enlace entre las dos entidades.

Funciones del Estrato de Servicio: Estas funciones proveen servicios basados y no basados en la sesión, incluyendo suscripción o notificación de información de presencia y un método de mensajes para intercambio de mensajería instantánea. Las funciones del estrato de servicio también entregan todas las funcionalidades de red asociadas a los servicios existentes de la PSTN o ISDN y las capacidades e interfaces para los equipos antiguos de clientes.

Funciones de Administración: Las funciones de administración permiten a los operadores de una NGN administrar la red y entregar servicios que cumplan con la calidad, seguridad y fiabilidad esperadas. Estas funciones se localizan de forma distribuida a cada entidad e

interactúan con la administración de elementos de red, administración de red y entidades administradoras de servicios. Las funciones de administración incluyen funciones de precios y facturas. Estas funciones interactúan entre ellas dentro de la NGN para recolectar la información de cobranza y para permitir que los operadores de la red NGN cuenten con los recursos necesarios para cobrar apropiadamente a los clientes. Los cargos pueden realizarse tanto en aplicaciones fuera de línea como servicios en línea.

Funciones de Usuario Final: Las interfaces hacia el usuario final son tanto físicas como funcionales (control). En una red NGN se deben soportar todas las categorías de equipos de clientes, desde los teléfonos utilizados en una red PSTN a complejas redes corporativas. Pudiendo además el terminal de usuario ser fijo o móvil.

2.2.2. IP Multimedia Subsystem

IP Multimedia Subsystem (IMS) fue desarrollado por 3GPP (3rd Generation Partnership Project) como parte del trabajo de estandarización asociado a la Tercera Generación de Telefonía Celular (3G). En su primera versión (Release 5) se diseñó para la evolución de telefonía móvil 2G a 3G, soportando redes GSM y GPRS y siendo añadidos además el soporte de contenidos multimedia basados en SIP. Para el Release 6 se añadió el soporte para acceso vía redes inalámbricas (WLAN, WiMAX). Finalmente, en el Release 7 se incluyó el soporte para redes fijas (xDSL, cable modem, ethernet) [1]. Entre las aplicaciones más importantes que se puede soportar esta red están:

- Voz y videotelefonía
- Servicios presenciales
- Mensajería instantánea
- Mensajería unificada
- IPTV
- Audio y videoconferencia
- Servicios Push to talk

IMS corresponde a una arquitectura basada en estándares y compuesta por 3 capas que soporta un amplio rango de servicios basados en IP para tecnologías móviles y fijas, por lo tanto IMS

aparece como un escenario ideal para nuevos modelos de negocios y oportunidades a través de conectividad SIP y movilidad continua para sus usuarios. Su arquitectura está compuesta por tres capas.

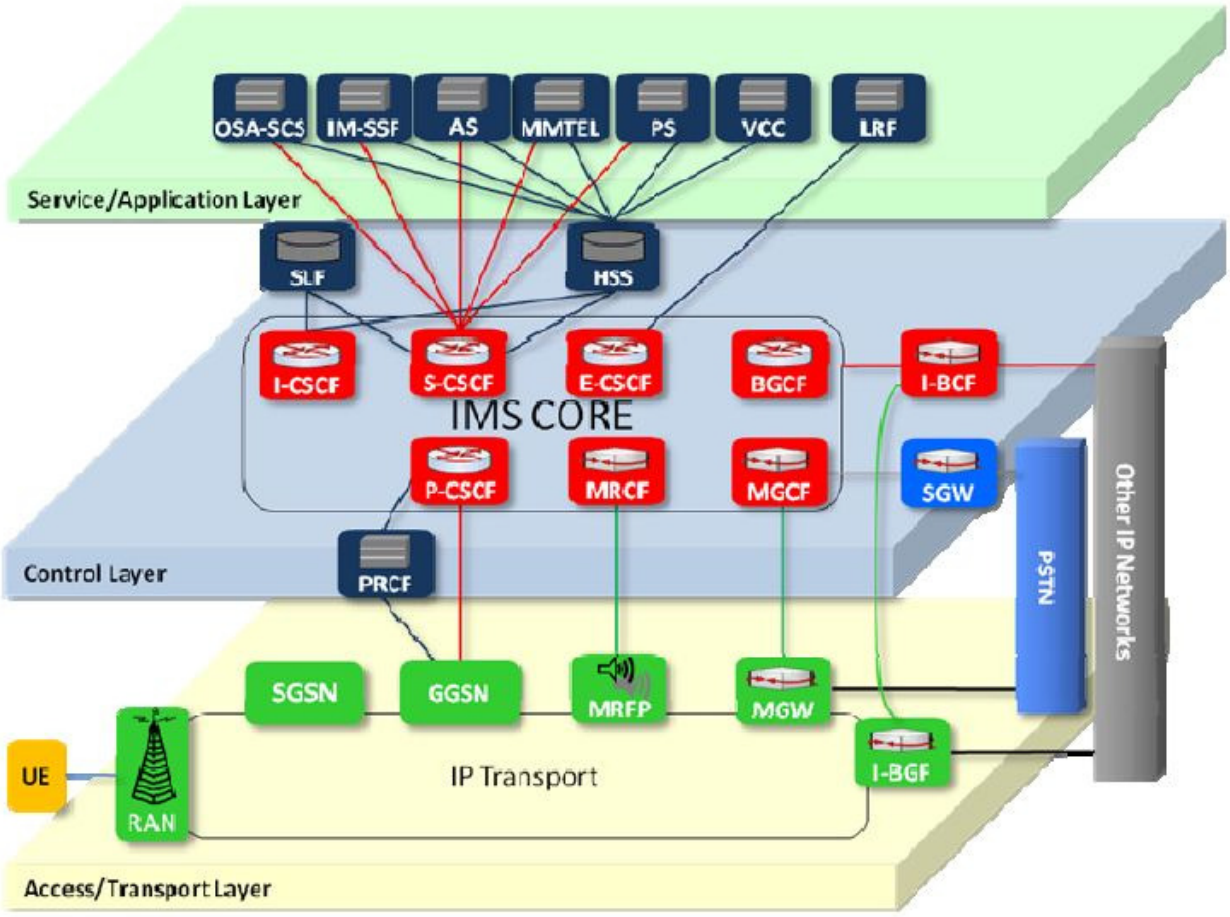

Figura 3: Arquitectura IMS.

CAPA DE APLICACIÓN/SERVICIO

Esta capa maneja toda la lógica de servicios y aplicaciones. Las principales componentes se describen a continuación:

Applicaction Server (AS): Corresponde a la entidad SIP que ejecutará los servicios de valor agregado. Los SIP Application Servers pueden simplificar enormemente la construcción de aplicaciones a través del uso de Service Creation Environments (SCEs) que permiten a los desarrolladores concentrarse en el sistema de negocio abstrayéndose de toda la infraestructura.

El resto de componentes se requieren para el servicio de telefonía multimedia IMS.

MMTEL (IMS Multimedia Telephony Service): Fija la cantidad de recursos necesarios para establecer interoperabilidad entre telefonía multimedia y servicios anexos.

OSA-SCS (Open Service Access-Service Capability Server): Permite a los suscriptores acceso seguro a las nuevas aplicaciones.

VCC (Voice Call Continuity): Ofrece continuidad de llamadas entre redes fijas y móviles.

LRF (Location Retrieval Function): Determina la locación del usuario.

CAPA DE CONTROL

Es principalmente compuesto por el denominado "núcleo IMS" el cual contiene los elementos de señalización y control.

HSS (Home Subscriber Service): Base de datos de usuarios dentro de la red. Contiene perfiles, credenciales de autenticación, locación física de usuarios y datos relevantes para cada usuario hacia un particular AS:

SLF (Subscriber Locator Function): Base de datos que mapea los usuarios a un HSS.

CSCF (Call Session Control Function): Proxies SIP que autentifican y rutean a los usuarios dentro de las distintas redes. Se clasifican en:

P-CSCF (Proxy CSCF): Es el punto de entrada, valida mensajes SIP para rutearlos hacia el resto de los CSCF y establece QoS.

I-CSCF (Interrogating CSCF): Determina a que S-CSCF enviar la información, de acuerdo al usuario en cuestión.

S-CSCF (Serving CSCF): Es el elemento central de la capa de control, pues realiza el registro de usuario y el control de sesión.

BGCF (Breakout Gateway Control Function): Rutea las llamadas hacia las redes conmutadas, ejemplo PSTN:

IBCF (Interconnection Border Control Function): Punto intermediario entre redes IMS o con alguna otra red basada en SIP. Provee información como la topología de red.

CAPA DE TRANSPORTE Y ACCESO

Contiene los elementos de transporte de elementos IP. Sus principales componentes son:

MGW (Media Gateway): Convierte RTP (Real Time Protocol) en PCM (Pulse Code Modulation).

GGSN (Gateway GPRS Support Node): provee conectividad a redes externas de datos, ya sea IMS o Internet.

RAN (Radio Access Network): Establece el tipo de red de acceso ya sea: GSM, UMTS o GSM/EDGE.

User Equipment (UE): Terminal de usuario que permite acceder a servicios y aplicaciones de la red IMS (teléfono celular, laptop, pda, teléfono 3G, softphone, etc.).

2.2.3. TISPAN

TISPAN fue desarrollado por ETSI (European Telecommunications Standards Institute). La Next-Generation Network (NGN) release 1 fue liberado por TISPAN en Diciembre de 2005. Ella proveía estándares abiertos y robustos para el desarrollo e implementación de la primera generación de redes de siguiente generación. TISPAN es una arquitectura diseñada para la entrega de voz en tiempo real, video y servicios multimedia utilizando SIP y otros estándares para su control sobre redes de paquetes conmutados, pero basándose en líneas físicas fijas [12].

Como se mencionó, TISPAN admite SIP, pero además incorpora servicios no basados en SIP, aplicaciones HTTP, peer-to-peer, pensados básicamente en el legado su red fija. Para ello, TISPAN define 3 capas de arquitectura, muy similares a IMS, pero añade algunos bloques funcionales para poder manejar y administrar aplicaciones que no están basadas en SIP, y que no las incorpora IMS en su arquitectura. Al analizar esta primera unión de arquitecturas es posible

ver que se evitan muchas redundancias de software y hardware, habilitando una estructura común apara aplicaciones. Esto tiene un efecto económico importante, pues se reduce tanto el CAPEX como el OPEX. Para hacer una analogía de arquitecturas, se presenta un servicio en particular que puede ofrecer TISPAN: PSTN/ISDN emulation subsystem (PES). Este servicio tiene como objetivo proveer a los usuarios los mismos servicios desde los mismos terminales que pudieran recibir desde un PSTN. El modelo gráfico de capas se detalla a continuación:

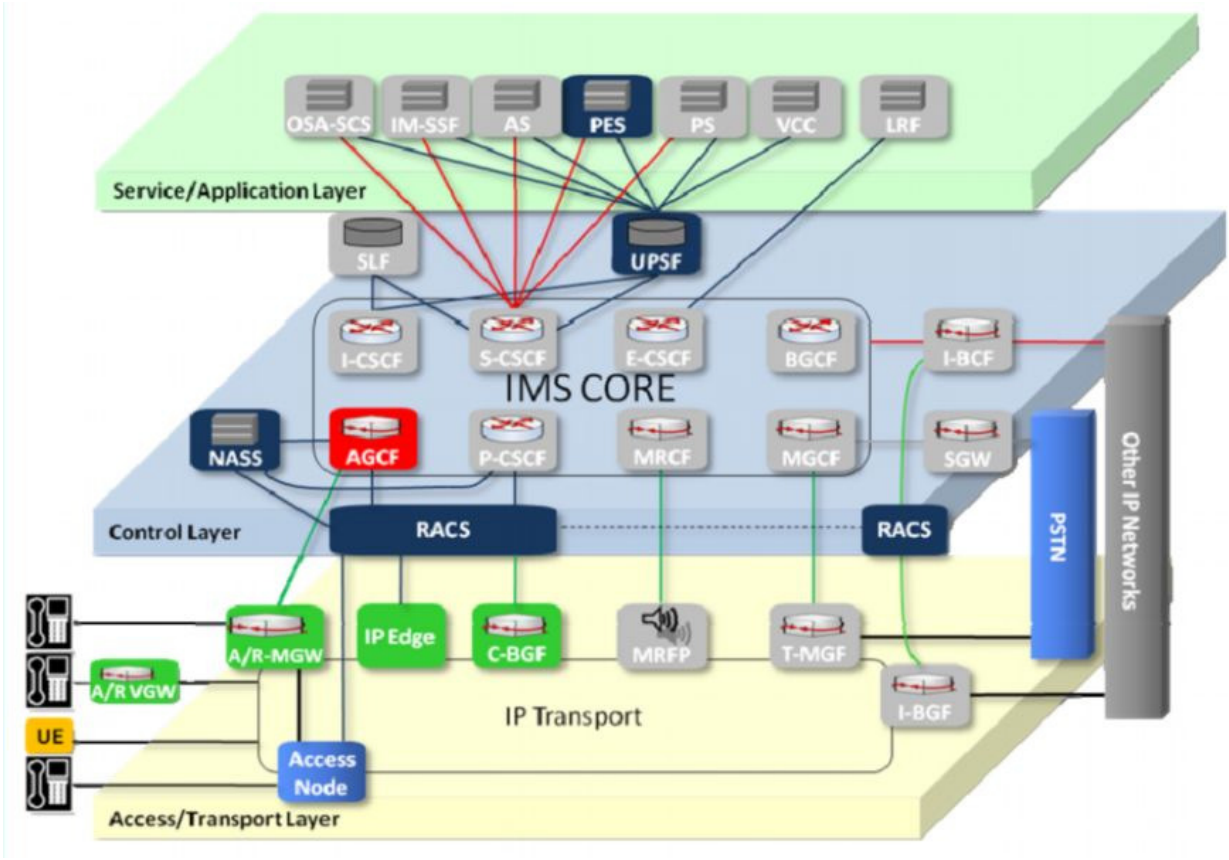

Figura 4: Arquitectura TISPAN.

Como se puede ver en la figura, el modelo es similar al de IMS, de hecho, comparte en común una serie de entidades y bloques (en color gris). La diferencia radica en los módulos encargados de suplir las falencias de IMS y que también se ajusten a la red a la cual fue diseñada, en este caso, red fija.

Los servicios ofrecidos por este simulador de PSTN/ISDN son básicamente los mismos que ofrece la telefonía normal. A ello, se deben agregar una serie de servicios suplementarios como por ejemplo:

OIP (Originating Identification Presentation): Permite que una persona presente su identidad cuando llama a otra.

OIR (Originating Identification Restriction): Capacidad de bloquear las llamadas entrantes de un usuario específico.

AOC (Advice of charge): Se le provee al usuario el costo de la llamada.

Los elementos nuevos que se aprecian en la capa de control son:

UPSF (User Profile Server Function): Base de datos que contiene información de usuarios, similar al HSS.

AGCF (Access Gateway Control Function): Es un Media Gateway Controller que convierte la señalización SIP en H.248.

NASS (Network Attachment Subsystem): Provee la inicialización y registro del terminal con la siguiente información: DHCP, autenticación de usuario, mapeo de locación por IP.

RACS (Resource and admisión control subsystem): Es el encargado de generar las políticas de QoS.

En la capa de transporte se encuentran los siguientes:

MGW (Media Gateway): Funcionalmente es similar al IMS MGW, pero éste está conectado a las líneas de acceso.

VGW (Voice over IP Gateway): Corresponde a un Media Gateway controlado por SIP:

Access Node: Es legado del equipamiento de acceso de PSTN.

2.2.4. PacketCable

PacketCable es una arquitectura definida por CableLabs para entregar servicios multimedia, y esta diseñado principalmente para redes de cable, dado que sigue con los lineamientos de DOCSIS cable módem. PacketCable fue desarrollado inicialmente por los operadores de cable

con la finalidad de definir una plataforma con QoS basada en IP y que utilizara las capacidades de red de acceso DOCSIS, para así acelerar la convergencia de video, voz, datos y tecnologías móviles. La arquitectura de PacketCable está basada en estándares comunes como SIP e IMS. Al utilizar un núcleo común, los servidores de aplicación están habilitados para entregar servicios a un amplio rango de clientes independiente de la topología utilizada en la red de acceso [12].

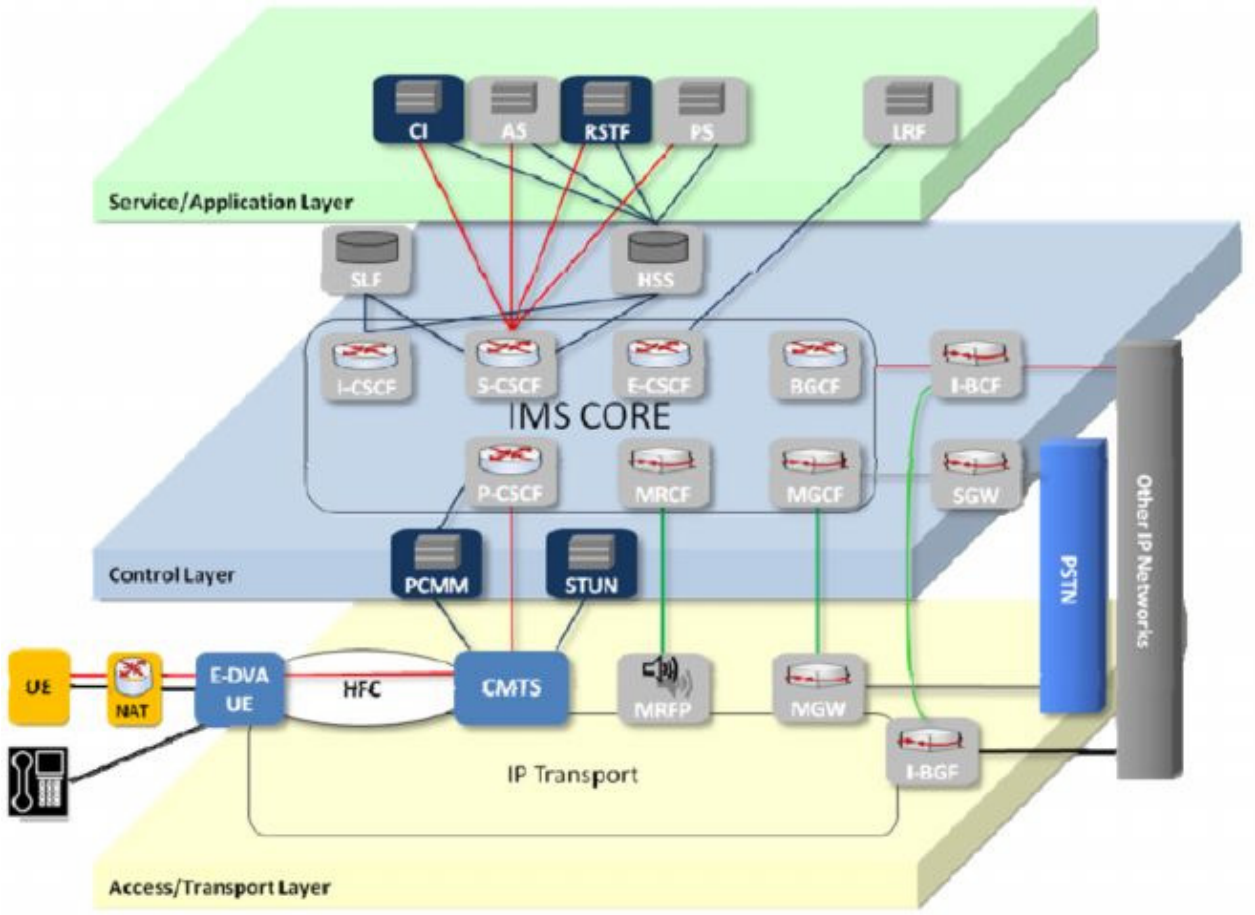

Figura 5: Arquitectura PacketCable.

Con PacketCable 2.0, CableLabs ha integrado algunas interfaces de IMS dentro de su arquitectura llamadas interfaces Rx. La interfase Rx es el punto de interconexión entre las aplicaciones de IMS y PCMM. Las interfaces Rx, permiten a las aplicaciones IMS a requerir controles de admisión mediante distintas políticas tales como permisos de usuario y recursos de red disponibles. Si la solicitud se acepta, una componente llamada Policy Server (PS) reservará los recursos e IMS procesará los requerimientos des sesión. Al integrar la capa de control de Packet Cable con la capa de control de IMS, se extiende el tiempo de uso de las actuales plantas

DOCSIS, y así se les permite a los operadores de cables ofrecer servicios de siguiente generación a sus abonados.

Al igual que TISPAN, PacketCable esta construido sobre un núcleo IMS, pero su capa de transporte está enfocado en una red HFC (Hybrid Fibre-Coaxial). Éste incluye especificaciones para transporte de voz y multimedia a través de un CMTS (Cable Modem Termination System). La arquitectura DOCSIS, permite hacer las reservaciones de recursos correspondientes durante cada sesión. Los componentes fundamentales en está operación son CMTS y Cable Modem (CM). Esta combinación, provee seguridad integrada además de permitir la definición y asignación de recursos durante cada sesión, lo cual hace ideal esta estructura para asegurar QoS.

2.3. Provisión de Servicios en IMS

En la arquitectura IMS, como se detalló anteriormente, los servicios son alojados y ejecutados en servidores de aplicación, por lo que se hace necesario tener un punto de referencia para poder enviar y recibir mensajes SIP entre estas entidades y los CSCFs. Esta interfaz se denomina ISC (IMS Service Control) y el protocolo seleccionado para su implementación es SIP. Los procedimientos de la interfaz ISC pueden corresponder al enrutamiento de un mensaje SIP hacia un servidor de aplicación, o bien al enrutamiento de una solicitud SIP iniciada por un servidor de aplicación, por ejemplo, en nombre de un usuario [6].

IMS provee los métodos necesarios para invocar y proveer servicios, lo que lleva a precisar tres pasos fundamentales:

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

Los iFC son propios del perfil del usuario, y representan información específica de éste con respecto a la aplicación. Dichos datos son necesarios cuando la suscripción IMS del usuario contiene servicios de valor agregado a utilizar, o bien cuando un operador requiere utilizar servidores de aplicación como parte de su infraestructura IMS.

Un TP (Trigger Point) es un componente del iFC que es utilizado para decidir cómo es contactado un servidor de aplicación; es decir, a qué AS contactar y cómo se gatilla su intervención en la sesión. El TP contiene una o más instancias de SPT (Service Point Trigger), que comprenden los tipos condicionales que se detallan a continuación:

- *Request-URI*: corresponde a una identidad o dirección única del AS, por ejemplo, servidor@operador.com.
- *SIP Method*: indica el tipo de requerimiento, por ejemplo, mensajes del tipo INVITE.
- *SIP Header*: contiene información relativa al requerimiento, por lo que un SPT puede corresponder a la presencia o ausencia de dichos datos específicos, los cuales son interpretados como una expresión regular.
- *Session Case*: indica si el filtro debe ser utilizado por el S-CSCF que atiende a la llamada originada (Originating, del usuario que llama), terminada (Terminating, del usuario que es llamado), o terminada en un usuario no registrado en el core (Terminating Unregistered).
- *Session Description*: el SPT se define en base al contenido de cualquier campo SDP en el cuerpo del mensaje SIP, evaluado como una expresión regular.

Basado en lo anterior, el operador puede definir iFC para manejar a ciertos tipos de usuarios. Por ejemplo, para aquellos usuarios que no se han registrado contra el core, se puede definir que cuando el SIP Method sea del tipo INVITE y el Session Case corresponda a Terminating Unregistered (lo que correspondería a una llamada hacia ese tipo de usuario), la llamada se desvíe hacia un buzón de voz localizado en una URI particular o simplemente se cancele la llamada. Los iFC son codificados en lenguaje XML. Esta información se descarga del HSS hacia el S-CSCF cuando el usuario se registra o cuando el requerimiento va hacia un usuario no registrado. El S-CSCF evalúa los iFC de acuerdo a los siguientes pasos:

1. Chequear si al usuario se le está prohibido utilizar el servicio; si no, proceder.
2. Chequear si es un requerimiento iniciado por el usuario o terminado en éste, seleccionando los iFC para el caso correspondiente.
3. Chequear si el requerimiento coincide con los iFC registrados en el perfil del usuario de acuerdo a un orden estricto de prioridad. Es decir, si el requerimiento coincide con las reglas del iFC de más alta prioridad, se contacta al AS respectivo; si no coincide se sigue

con el iFC de prioridad siguiente, y así sucesivamente hasta que se contacta al AS requerido.

4. Si el requerimiento no corresponde a ningún iFC y por lo tanto a ningún AS, enviar el requerimiento al siguiente nodo de acuerdo a las reglas de enrutamiento por defecto.

El AS recibe el requerimiento filtrado por la información establecida en los iFC, actuando como uno de los siguientes:

- *Terminating UA*: el AS actúa como UE, por ejemplo para proveer un servicio de Voice Mail.
- *Redirect Server*: servidor de redireccionamiento; el AS informa a quien originó el requerimiento sobre la nueva ubicación del usuario o sobre nuevos servicios, por ejemplo redireccionándolo a una página web específica.
- *SIP Proxy*: el AS procesa el requerimiento y lo envía de vuelta al S-CSCF, cambiando o agregando información en las cabeceras del mensaje SIP si es necesario.

Es preciso mencionar que el AS también puede actuar como Originating UA, siendo capaz de enviar requerimientos a los usuarios.

2.4. Medición de calidad

2.4.1. Calidad de servicio

Midiendo la calidad de servicio (QoS) en la red es posible ofrecer prioridad a determinados tipos de tráfico, independientemente de la tecnología de red utilizada. Estos mecanismos son inherentemente necesarios para la red cuando ésta ofrece diversos servicios de tiempo real como VoIP o transmisión de video sobre IP. Sería muy fácil dar calidad de servicio si las redes nunca se congestionaran, pero para ello habría que sobredimensionar todos los enlaces, cosa que no siempre es posible de realizar, ya sea por recursos necesarios para lograrlo o por costos involucrados. Por lo tanto, para dar calidad de servicio a gran escala y en redes con posibilidades de congestión, es preciso tener mecanismos que permitan dar al tráfico un trato diferenciado acorde con el SLA (Service Level Agreement). De todas formas, aunque el estado de congestión pueda ser una decisión de compromiso (Tradeoff) entre el sobre dimensionamiento de la red y su posible saturación, generalmente en las redes reales se tiene que una situación

permanente de congestión es inabordable y por lo tanto su única solución es la sobreestimación. Es decir, los mecanismos de calidad de servicio no son inútiles en una red saturada permanentemente. En general, todos estos conceptos quedan dentro de lo que se le denomina como "ingeniería de tráfico", la cual pretende analizar el tráfico para ofrecer servicios mejores y más predecibles, mediante: soporte de ancho de banda dedicado, mejorando las características de pérdida de paquetes, evitando y manejando la congestión de la red, organizando y priorizando el tráfico [8]. Se puede decir que los parámetros que definen la calidad de servicio son:

Dropped packets: Este concepto trata de la posibilidad existente que tiene un router de fallar o perder (drop, en inglés) paquetes, si ellos llegasen al router cuando el buffer de éste está completo. Algunos, ninguno o todos ellos se podrían perder, dependiendo del estado de la red, donde es imposible determinar que ocurrirá con anticipación. La aplicación del cliente (quién recibe el flujo de paquetes) debe comunicar que esta información debe ser retransmitida, lo cual provoca graves demoras en toda la transmisión.

Delay: Este concepto hace referencia a la diferencia de tiempo transcurrido, desde que el paquete es enviado desde su lugar de origen, hasta llegar a su lugar de destino. La ruta que el paquete siga en su trayecto es impredecible, ésta puede ser expedita o estar ampliamente congestionada, ser directa o simplemente no serlo.

Jitter: Este concepto hace referencia a los distintos delays que pueden tener distintos paquetes enviados desde un mismo origen, hacia un mismo destino. Este concepto describe la diferencia entre los delays de uno y otros, generalmente ésta es una de las principales causas de bajas en la calidad de un sistema de audio y/o video continúo.

Out of order delivery: Cuando un conjunto de paquetes relacionados son ruteados en Internet, distintos paquetes de este grupo pueden tomar distintas rutas, donde en cada una se presenta un delay distinto. El resultado es un estado de asincronía, donde los paquetes llegan en un orden distinto al destino, según el cual fueron enviados. Para poder solucionar el problema es necesario hacer uso de protocolos adicionales, los cuales son responsables de reordenar los paquetes en el lugar de destino. Este concepto es especialmente importante en streams de video o VoIP, puesto que en estos casos la calidad se ve dramáticamente impactada cuando actúan tanto los delays como el asincronismo.

Error: Algunas veces los paquetes son mal enviados, enviados juntos, o simplemente en el transcurso se dañan quedando corruptos. Esto implica que en el extremo receptor se debe detectar, de modo de pedir al emisor que reenvíe la información faltante. Para poder gestionar los parámetros de forma eficiente se debe hacer uso de la prioridad y gestión del tráfico por medio de colas. En comunicaciones IP, esto se traduce en dos modelos de trabajo, los cuales serán descritos a continuación.

2.4.2. Calidad de experiencia

La calidad de experiencia (QoE) es medida a menudo mediante pruebas subjetivas controladas cuidadosamente en los que se reproducen muestras de video a espectadores, a quienes se les pide que las califiquen según una escala. Uno de los sistemas más utilizados es el de puntuación media (MOS, Mean Opinion Score), el cual se basa en la reproducción de unas muestras (ya sean de video o de voz) a una serie de personas, las cuales se puntúan en una escala del 1 al 5 (siendo el 5 la mejor puntuación) en términos de calidad de experiencia.

Otro mecanismo es el MDI (Media Delivery Index) que permite a los proveedores de servicios medir tanto los servicios de IPTV como los de VoIP. El MDI da una indicación sobre la calidad esperada del video y, por lo tanto del QoE del usuario, basado en medidas sobre el nivel de red. Las medidas del MDI son acumulativas a través de la red y pueden ser medidas desde cualquier punto entre los proveedores de contenidos y los receptores de televisión. El MDI se expresa típicamente como dos números: el factor de retardo (delay factor) y la tasa media de pérdidas (media loss rate).

Existe una métrica avanzada de medición llamada V-Factor la cual es ofrecida comercialmente por la empresa Symmetricom. Esta es una solución robusta de control de la calidad de vídeo que permite a los de servicios de Internet y MSO comprender su calidad de servicio, en tiempo real y la calidad experimentada por los usuarios finales. V-Factor ha sido diseñada para ofrecer evaluaciones precisas de calidad por parte del usuario final. A diferencia de otras soluciones que se basan en vigilar la red de datos y tratan de predecir la experiencia del usuario, V-Factor se basa en analizar la calidad del vídeo, utilizando un sofisticado modelo del Sistema de Visión Humana (HVS) y ofreciendo un preciso MOS de la calidad del vídeo, entregando datos simples que el operador de cable pueda entender fácilmente. V-Factor informa al operador si hay un problemas

en la señal de video y si es o no importante para los usuarios finales. Permite informar que tipo de problema es el que están sufriendo los usuarios y la causa exacta de tal deterioro. V-Factor consta de las siguientes partes: Analizadores, instalados en la cabecera: Red de Sondas, recopilan la información y las cifras de rendimiento de la red; Agentes de Software, ubicados en los STB, PC o reproductores multimedia; y el Software de administración, encargado de la gestión de la calidad y supervisión de estado de extremo a extremo.

CAPÍTULO III: METODOLOGÍA

3.1. Diseño del Laboratorio de IPTV

A continuación se desarrolla el diseño del Laboratorio de IPTV, estableciéndose sus características y presentándose cada elemento que lo conformará con el fin de satisfacer los objetivos planteados en este trabajo de título.

3.1.1. Alcances del diseño

Esta memoria continúa ciertos trabajos de título realizados por alumnos del Departamento de Eléctrica en años anteriores. En ellos se ha incorporado la presencia de arquitecturas de redes convergentes como el camino a seguir en el ofrecimiento de servicios multimedia. Dado que las NGN son parte del actual proceso de adopción de nuevas tecnologías que están aplicando las empresas de telecomunicaciones, se vuelve necesario que la implementación del Laboratorio de IPTV se realice sobre una arquitectura de red convergente que cumpla con los estándares de una NGN. Las arquitecturas estudiadas en este caso fueron IMS, TISPAN y PacketCable, sin embargo TISPAN tiene la posibilidad de ofrecer el servicio de IPTV tanto basado como no basado en IMS y PacketCable incorpora el núcleo IMS dentro de su arquitectura [12]. De esto se deriva que si la plataforma de IPTV es basada en IMS se tendría que el Laboratorio de IPTV podría ser utilizado en cualquiera de las tres arquitecturas antes mencionadas. Considerándose además que la arquitectura IMS ha sido utilizada en trabajos de título anteriores, se procederá a utilizar la arquitectura IMS como base para el Laboratorio de IPTV extendiéndose de esta manera los esfuerzos ya realizados por otros memoristas.

En el capítulo previo, se estudió la arquitectura IMS encontrándose múltiples entidades necesarias para permitir el establecimiento de sesiones de usuarios que provienen de diferentes redes de acceso. Dada además la existencia de un sin numero de servicios de valor agregado que pueden incorporarse en la plataforma IMS, es necesario establecer los alcances del Laboratorio de IPTV acotando su funcionalidad acorde a los recursos y tiempo disponible para su desarrollo en el marco de este trabajo de título. A continuación se establecen los alcances del Laboratorio de IPTV considerando la arquitectura IMS como base para ello.

El Laboratorio de IPTV sobre arquitectura IMS constituye una plataforma que permitirá el establecimiento de sesiones de transmisión de video, existiendo múltiples canales que pueden ser solicitados por el cliente para ser recibidos, ya sea contenido de video-on-demand o en modo live streaming. También la plataforma ofrecerá la capacidad de tarificación y contará con un sistema de políticas de control de servicios. El Laboratorio de IPTV respetará los estándares establecidos para un servicio de IPTV basado en IMS, sin embargo dado que los fines de este trabajo son realizar pruebas con fines académicos se limitarán los componentes de la infraestructura IMS a los estrictamente necesarios para ofrecer el servicio de IPTV. Por lo tanto queda descartado como resultado obtener una plataforma de IPTV que posea desempeño y prestaciones aptas para ser utilizado con fines comerciales. Sin embargo el sistema debe posibilitar el estudio de los principales protocolos del núcleo de la arquitectura IMS, así como del servicio de IPTV montado sobre él y la posibilidad de analizar todo el funcionamiento que cumplen las entidades involucradas.

Se consideran aspectos docentes en el proceso de diseño al estructurar las actividades de forma evolutiva, desde un diseño básico hasta conformar una arquitectura de red más compleja. Por último cabe destacar que dado el carácter de bajo costo de la implementación, es que nace la restricción de que todos los componentes que conforman el Laboratorio de IPTV deberán ser constituidos idealmente a partir de proyectos de software libre ya existentes.

3.1.2. Diseño de la arquitectura del sistema

Considerando los alcances descritos anteriormente, se definen las características de diseño del Laboratorio de IPTV el cual debe cumplir con los lineamientos de la arquitectura IMS. En primer lugar se establece la necesidad de disponer de una arquitectura IMS bajo un ambiente controlado. En este sentido, las componentes conviven en una red privada de paquetes IP y se comunican a través de los protocolos establecidos en el estándar de la 3GPP para IMS. Para escoger que entidades IMS se deberán adoptar para implementar el servicio de IPTV será considerado que el acceso al sistema por parte de los usuarios se realiza exclusivamente a través de otros computadores de la misma red de área local, luego el servicio de IPTV actúa de forma aislada por lo que no existe interacción con otros tipos de redes y por lo tanto las comunicaciones se establecen exclusivamente entre componentes de la misma la red. Por esto serán obviados elementos de la arquitectura IMS que permitan la interoperabilidad con otras redes, por ejemplo

la PSTN. Se tiene entonces que para la plataforma de IPTV sólo es interesante implementar el núcleo funcional de la arquitectura IMS escogiéndose un grupo acotado de entidades de dicha arquitectura. Las entidades escogidas son: HSS, P-CSCF, I-CSCF y S-CSCF. Estas cuatro componentes son necesarias para el funcionamiento de una red IMS. El HSS (Home Suscriber Server) representa la base de datos que permite el registro de usuarios y la información asociada a los servicios disponibles para ellos. El P-CSCF (Proxy Call Session Control Function) es el primer punto de contacto de un usuario con la red IMS. El I-CSCF (Interrogating Call Session Control Function) decide que S-CSCF debe atender a cada usuario. Por último, el S-CSCF (Serving Call Session Control Function) es el servidor SIP que sirve los requerimientos de un usuario. Tomando en cuenta todas estas funciones se justifica el uso de estos elementos dentro de la construcción del núcleo IMS que servirá de base para la implementación del Laboratorio de IPTV. Las siguientes entidades que componen una arquitectura IMS se descartan por diversos motivos mencionados a continuación:

- E-CSCF: Servidor asociado a llamadas de emergencia. Considerando que es un servicio no necesario en este contexto, fue descartado.
- SLF: En caso de que exista más de un HSS, el SLF se hace necesario para determinar a cual HSS acceder según el perfil de usuario. En este caso existirá un único HSS por lo que no se requiere implementar el SLF.
- IMS-MGW: Esta entidad permite unir la terminación TDM y la terminación RTP posibilitando la comunicación hacia la PSTN. Dado que no se considera interoperabilidad del sistema con la red de telefonía conmutada no se requiere su uso.
- MGCF: Se encarga del control del IMS-MGW, luego se descarta su uso por las razones anteriores.
- T-SGW: Elemento que permite intercambiar el transporte de los protocolos de señalización SS7 sobre la red TDM y la red IP. Como no se considera la salida a la PSTN no se requiere su implementación.
- BGCF: Se encarga de seleccionar la red para el paso a la PSTN. Por las razones expuestas anteriormente no debe implementarse.

Para formar una plataforma de IPTV básica que funcione sobre IMS se necesitan al menos tres elementos: un Cliente IMS capaz de solicitar el servicio de IPTV, un IPTV Application Server y

un Media Server que idealmente soporte RTSP para poder controlar el flujo en transmisiones de VoD [14]. Todos ellos interactuarán directamente con el núcleo IMS. El funcionamiento es el siguiente, el cliente previamente registrado con el núcleo IMS realiza una petición de un canal al IPTV Application Server quien devuelve al cliente una dirección RTSP correspondiente al canal solicitado, luego el cliente utiliza esta dirección para establecer una sesión RTSP con el Media Server indicado. Para establecer las sesiones dentro de la plataforma de IPTV es necesario ocupar un Cliente IMS que permita acceder al sistema, esto posibilita también a los usuarios de la plataforma a una completa gama de servicios que pueda ofrecer el sistema IMS al mismo tiempo que ofrece los relacionados con IPTV, ejemplos de estos pueden ser: realizar videoconferencias, llamadas VoIP y uso de mensajería instantánea con otros usuarios conectados a la plataforma.

El servicio de IPTV también debe contar con un sistema de tarificación por lo cual tendrán que ser añadidos al sistema dos componentes. Antes de que el IPTV Application Server envíe la dirección RTSP al cliente IMS, se dispara el proceso de tarificación, enviándose una petición que activa al Charging Data Function (CDF) que es el encargado del sistema de tarificación offline, si es el caso en que se desea utilizar un método de post-pago del servicio, o al Online Charging System (OCS) que es el encargado en caso de que se desee utilizar la variante de prepago del servicio [4]. Por último la plataforma de IPTV contará con un framework de políticas de control en donde participan un Policy and Charging Rule Function (PCRF) y un Policy and Charging Enforcement Point (PCEF) que permitirán monitorear el uso de los servicios que ocurren sobre el núcleo IMS y aplicar decisiones de control sobre los servicios basados en reglas según QoS [4], en particular el PCEF posee un Proxy RTP por donde deberá pasar el contenido multimedia de los canales de IPTV.

Finalmente, en vez de que cada componente de la plataforma posea su propio servidor de resolución de nombres de dominio (DNS, Domain Name Server), se implementará uno único para todos los componentes, lo cual facilitará la administración de direcciones IPs y permitirá analizar más fácilmente todas las consultas de DNS.

3.1.3. Esquema de interconexiones

En el punto anterior se escogieron todas las componentes necesarias para la conformación del Laboratorio de IPTV basado en IMS. En resumen se tiene la siguiente lista de componentes:

1. Cliente IMS
2. DNS (Domain Name Server)
3. P-CSCF (Proxy – Call Session Control Function)
4. I-CSCF (Interrogating – Call Session Control Function)
5. S-CSCF (Serving – Call Session Control Function)
6. HSS (Home Suscriber Server)
7. IPTV AS (IPTV Application Server)
8. Media Server
9. CDF (Charging Data Function)
10. OCS (Online Charging System)
11. PCRF (Policy and Charging Rule Function)
12. PCEF (Policy and Charging Enforcement Point)

El esquema de comunicaciones diseñado para la plataforma de IPTV se aprecia en la siguiente figura:

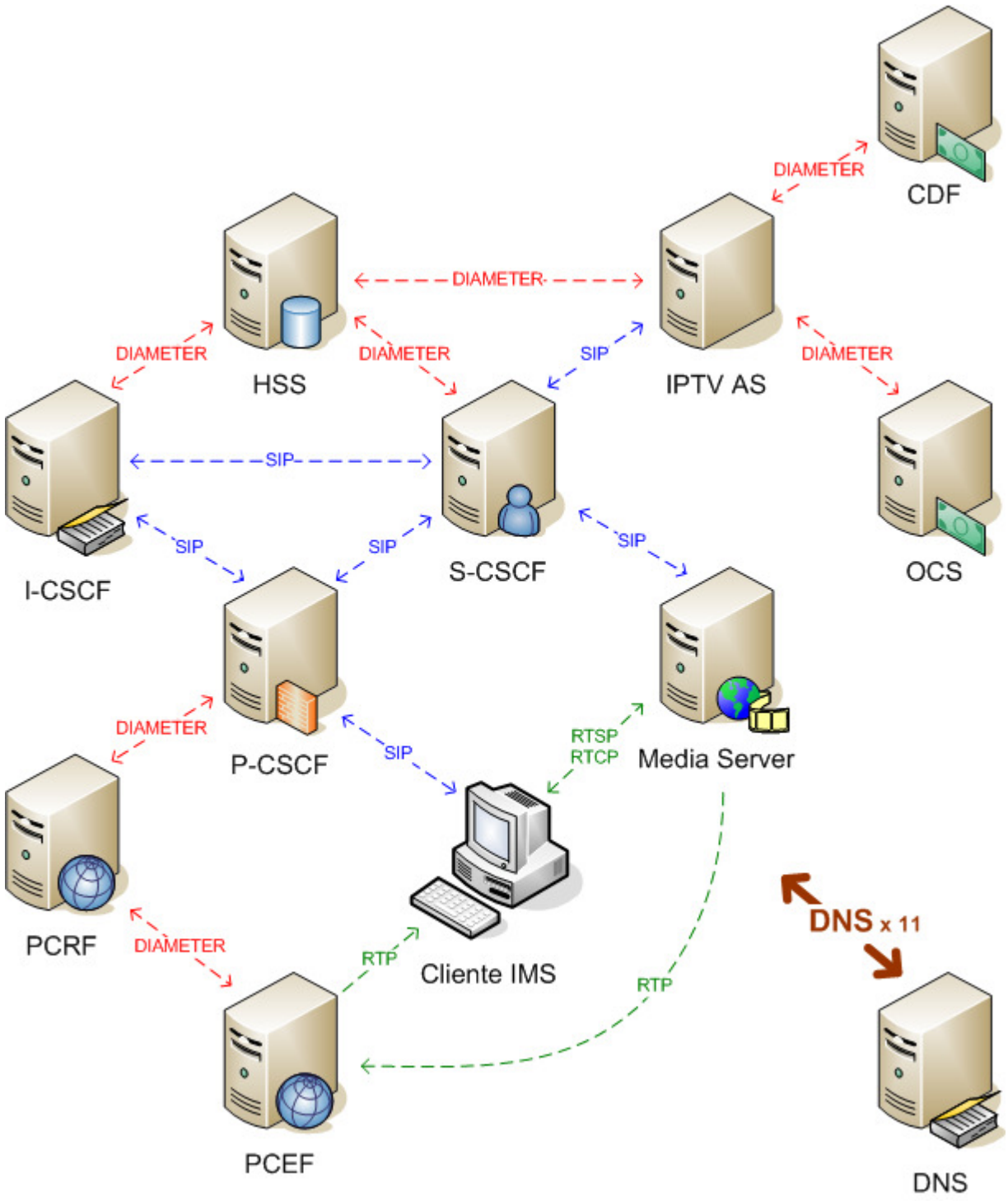

Figura 6: Diseño de interconexión de componentes del Laboratorio de IPTV.

La figura anterior corresponde a un esquema teórico cuya puesta en marcha se detalla en la sección de implementación, donde además se presentan las características especificas sobre cómo se llevó a la práctica el esquema presentado.

3.1.4. Servicios de usuario final

Dado el diseño final del Laboratorio de IPTV, se presentan los servicios que dispondrá el Laboratorio de IPTV para los usuarios y administradores del sistema:

- Capacidad de solicitud de canales en modo live streaming directamente desde el cliente IMS.
- Capacidad de solicitud de contenido VoD directamente desde el cliente IMS.
- Disponibilidad de un NDVR (Network DVR) [27] o también conocido como RS-DVR (Remote Storage Digital Video Recorder).
- Disponibilidad de una EPG (Electronic Program Guide).
- Capacidad de hacer uso de otros servicios como videoconferencias, llamadas VoIP y uso de mensajería instantánea con otro usuario conectado a la plataforma de IPTV directamente desde el cliente IMS.
- Sistema de tarificación del servicio de IPTV a través de asignación de créditos.
- Administración del núcleo IMS desde una interfaz web.
- Administración de un sistema de políticas de control para el núcleo IMS desde una interfaz web.

3.2. Implementación del Laboratorio de IPTV

La implementación del Laboratorio de IPTV implica levantar todas las componentes definidas durante el diseño dentro de una misma red de área local. Esta labor será realizada por etapas, definiéndose las siguientes: Levantamiento del Núcleo y Cliente IMS, Levantamiento de sistema de IPTV básico, Levantamiento de sistema de tarificación y Levantamiento de sistema de políticas de control. Considerando que la plataforma desarrollada tiene fines docentes se tiene que los componentes del sistema deben correr en equipos separados posibilitando de este modo un análisis más profundo de la comunicación entre cada uno de ellos y de los protocolos involucrados. Se comenzó con una implementación del Laboratorio de IPTV en computadores disponibles en el Laboratorio de Telecomunicaciones, sin embargo dado que se terminó necesitando un número mayor de computadores que el disponible en dicho Laboratorio, se decidió hacer una red de área local con máquinas virtuales que permitiera dejar cada componente en una sola máquina para realizar las pruebas. Utilizando virtualización en un computador con las

siguientes características: Procesador Intel Core 2 Duo de 2.00 Ghz y memoria RAM de 2 GB, se pudo crear adecuadamente todas las máquinas virtuales necesarias para tener los componentes separados, el programa de virtualización escogido es VirtualBox OSE por ser una solución de software libre ampliamente difundida y documentada. Fueron creadas 11 máquinas virtuales de 128 MB de RAM cada una, que sumadas al sistema operativo que hace de Host componen un total de 12 computadores en una LAN. Todo el desarrollo de esta memoria se realiza sobre el sistema operativo GNU/Linux, la distribución escogida ha sido Ubuntu 8.04 (Hardy Heron). Inicialmente se trató de hacer la implementación en Debian GNU/Linux, pero hubo dificultades con los paquetes de códecs que estaban disponibles en los repositorios de la distribución que causaron ciertas incompatibilidades en la comunicación entre el Media Server y el Cliente IMS. Finalmente se opto por utilizar Ubuntu dado que era la distribución utilizada por quienes desarrollan los proyectos de software libre relacionados con los componentes que proveerán al núcleo IMS el servicio de IPTV. Gracias a que el disco duro de una máquina virtual es solamente un archivo, es posible realizar una clonación de discos duros virtuales de modo que basta con instalar el sistema operativo en una máquina virtual para luego duplicarla y crear de esta manera todas las máquinas virtuales con el sistema operativo instalado junto con los requerimiento y configuraciones comunes a todos los computadores que albergarán las entidades del laboratorio de IPTV, de esta manera no fue necesario comenzar desde cero con todos los computadores que albergarán a cada elemento de la red.

3.2.1. Levantamiento de Núcleo y Cliente IMS

En primer lugar se debe levantar los componentes del núcleo IMS: P-CSCF, I-CSCF, S-CSCF y HSS. Dichas entidades han sido implementadas por el proyecto de código abierto Open IMS Core desarrollado por el Fraunhofer Institute for Open Communication Systems (FOKUS), y que es desarrollado con fines de investigación. Se utilizará este proyecto ya que es la única implementación de un núcleo IMS de código abierto que se encontró. Ella presenta todas las características y funciones requeridas para poder montar el resto de componentes que conformarán el futuro servicio de IPTV. Para la implementación del DNS se utilizará la aplicación BIND, se decidió por ella ya que es el software de su tipo más consolidado y el de más amplia utilización en desarrollos de este tipo.

A parte de los componentes que conforman el núcleo IMS es necesario levantar un cliente IMS que permita registrarse en el sistema y solicitar canales del futuro servicio de IPTV, el software elegido es UCT IMS Client desarrollado por el Communications Research Group de la Universidad de Cape Town. Este software es desarrollado con la característica de ser compatible con el proyecto Open IMS Core del Instituto FOKUS y de poseer bastantes características útiles para la implementación del Laboratorio de IPTV, como ser capaz de solicitar canales de IPTV, tener botones PLAY, PAUSE y STOP para controlar sesiones multimedia RTSP, poder mostrar una EPG, además de las prestaciones típicas de clientes SIP como videoconferencias, llamadas VoIP, mensajería instantánea, etc.

Una vez puesto en marcha todos los elementos mencionados, cuyo proceso se detalla en la sección de Anexos 9.3.2, se logra tener un núcleo IMS operativo junto con su respectivo Cliente IMS, lo cual servirá de base para el resto de la plataforma de IPTV. La topología de red resultante de la plataforma a este nivel se observa en la siguiente figura:

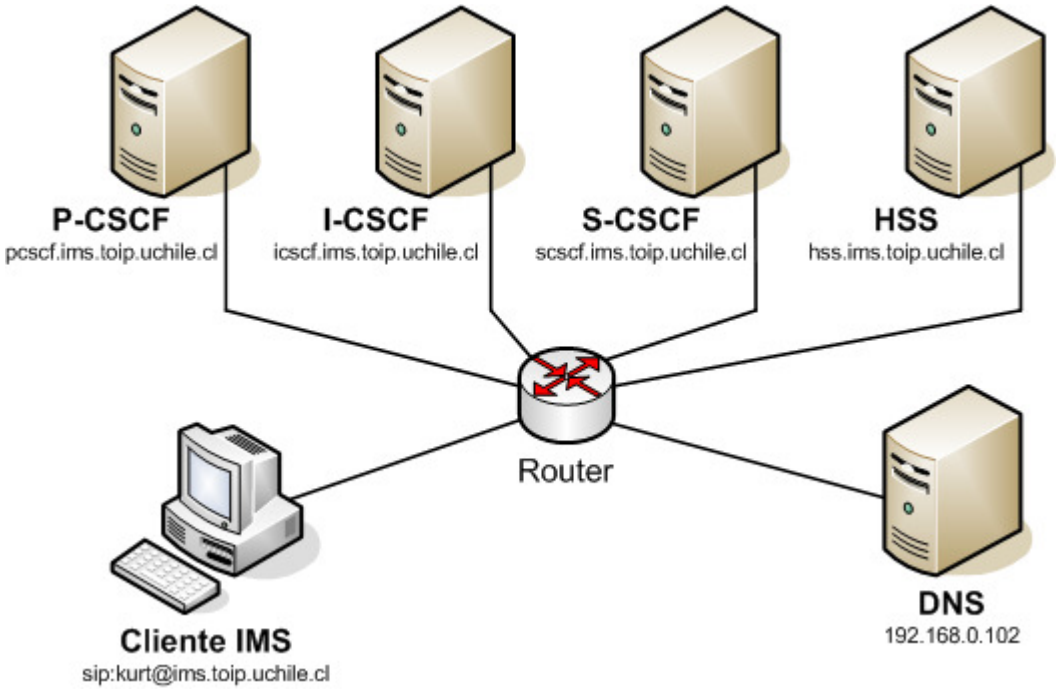

Figura 7: Diagrama de red de Cliente y Núcleo IMS.

Como se mencionó, tanto las entidades que componen el núcleo IMS, el servidor DNS y el Cliente IMS corren en distintos computadores. Luego, los elementos de la red, que se encuentran separados, pueden ser identificados por distintas direcciones IP. Los archivos de configuración

que vienen por defecto junto al código fuente de cada componente del núcleo IMS son para que todos ellos se ejecuten en un mismo computador teniendo todos los componentes la dirección localhost (127.0.0.1), por lo tanto se realizó las configuraciones pertinentes para que los elementos establecieran comunicación a través de las nuevas direcciones IP. Por otra parte, también se tiene que el nombre de dominio al que hacen referencia los archivos de configuración de los componentes del sistema está configurado con el nombre de dominio open-ims.test. Ésta fue cambiada con el interés de realizar una mayor personalización del sistema estableciendo un nuevo dominio llamado ims.toip.uchile.cl. Se eligió este nombre de manera de mantener compatibilidad con trabajos de memoristas anteriores del Team TOIP que trabajaron con IMS [5]. Estos cambios se realizaron no solo a través de la edición de archivos XML, sino que también fue necesario recargar las bases de datos MYSQL de algunos elementos con la nueva información.

A continuación se presenta una tabla con todos los elementos que componen el núcleo IMS que se utilizará en el resto de la implementación junto con el Cliente IMS y el servidor de resolución de nombres de dominio, en ella se ven las direcciones IP asignadas junto con sus nombres de dominio respectivos.

Tabla 1: Elementos, direcciones IP y nombres de dominio de Cliente y Núcleo IMS.

Elemento	Dirección IP	Nombre de dominio
Cliente IMS	192.168.0.101	ue.ims.toip.uchile.cl
DNS	192.168.0.102	ns.ims.toip.uchile.cl
P-CSCF	192.168.0.103	pcscf.ims.toip.uchile.cl
I-CSCF	192.168.0.104	icscf.ims.toip.uchile.cl
S-CSCF	192.168.0.105	scscf.ims.toip.uchile.cl
HSS	192.168.0.106	hss.ims.toip.uchile.cl

En cuanto al cliente, se ha configurado una cuenta SIP personalizada para acceder al Sistema IMS. Esto se hizo utilizando la interfaz web de configuración del HSS que fue levantada para estos fines, esto consistió en crear una suscripción IMS, luego una identidad privada de usuario y una identidad pública.

Tabla 2: Dirección SIP del Cliente IMS.

Cliente	Dirección IP
sip:kurt@ims.toip.uchile.cl	192.168.0.101

La implementación del núcleo IMS servirá de base para el resto de la plataforma de IPTV, la cual agregará componentes gradualmente a medida que se vayan incorporando nuevas características al sistema.

3.2.2. Levantamiento de Sistema de IPTV básico

Continuando con la implementación del Laboratorio de IPTV, cuyo detalle está contenido en Anexos 9.3.3. Se tiene que al núcleo IMS constituido se le debe incorporar dos componentes más que son de vital importancia para obtener un sistema de IPTV basado en IMS. El primero de ellos corresponde al IPTV Application Server, el cual será implementado a partir de un proyecto desarrollado por el Communications Research Group de la Universidad de Cape Town llamado UCT Advanced IPTV. Es necesario agregar al HSS la información necesaria para que el Núcleo IMS solicite correctamente los servicios del IPTV AS. Entre esto destaca la creación de un perfil para el Application Server en donde se incluyen la dirección SIP del servidor: iptv.ims.toip.uchile.cl, la función Trigger Point asociada y un Initial Filter Criteria. En cuanto a la configuración del IPTV AS, se le fue incorporada la tabla de Hash que relaciona la solicitud de canales de IPTV que dispone la plataforma con las direcciones RTSP del Media Server.

El segundo componente que se agregará en esta etapa es el Media Server. El software utilizado para esta instancia es VideoLan VLC Media Player, esta aplicación es elegida por ser software libre, ser altamente configurable y estar bien documentada. VLC es capaz de transmitir streaming de video a través del protocolo RTSP. Además es capaz de entregar video-on-demand como también ser una fuente de video en modo live streaming. Con el fin de agregar disponibilidad de canales al Laboratorio de IPTV fue dejado contenido multimedia en el Media Server para ambos tipos de modo de transmisión de canales. Tras haber incorporado a la red los dos elementos ya mencionados, se tiene la siguiente configuración de red en el sistema.

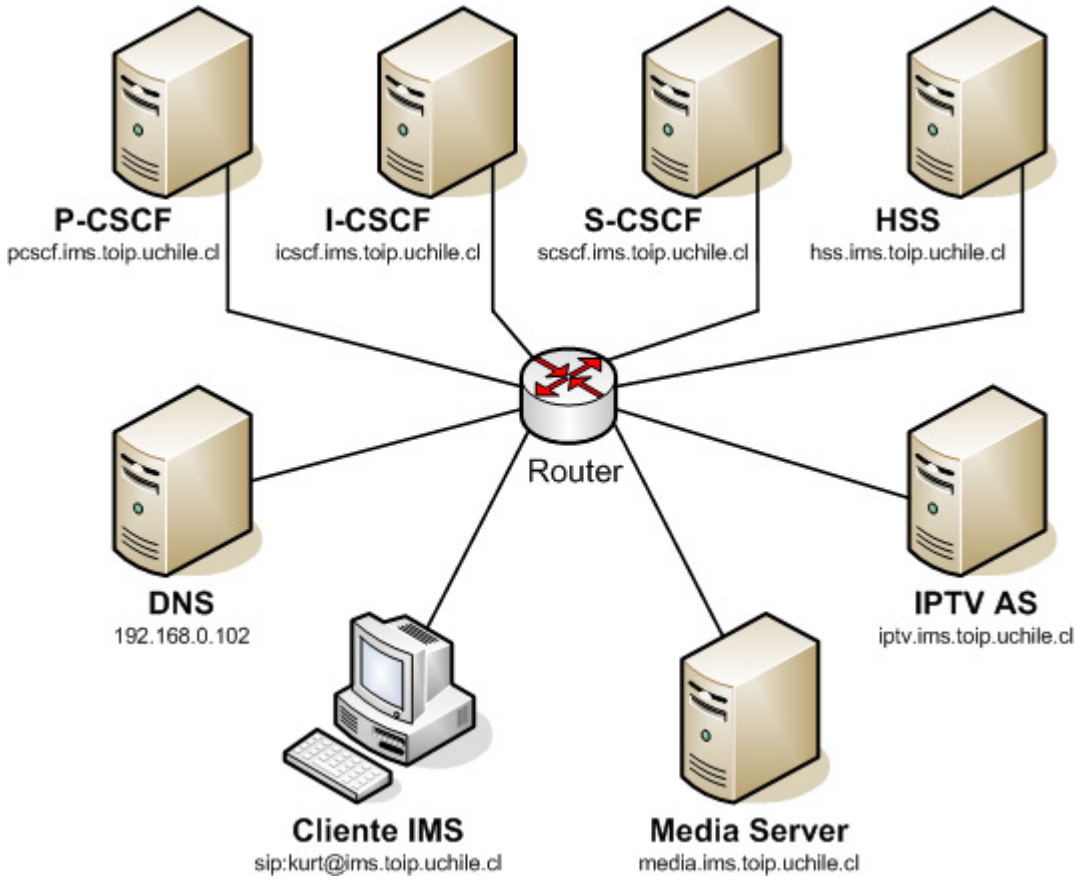

Figura 8: Diagrama de red de Sistema de IPTV básico.

Se presenta una tabla con los nuevos elementos incorporados al Laboratorio de IPTV.

Tabla 3: Elementos, direcciones IP y nombres de dominio de Sistema de IPTV básico.

Elemento	Dirección IP	Nombre de dominio
IPTV AS	192.168.0.107	iptv.ims.toip.uchile.cl
Media Server	192.168.0.108	media.ims.toip.uchile.cl

3.2.3. Levantamiento de Sistema de Tarificación

Continuando con la implementación gradual del Laboratorio de IPTV se incorporó un sistema de tarificación el cual es proporcionado por el proyecto UCT IMS IPTV Charging System desarrollado por la Universidad de Cape Town, el cual se presenta como una implementación que cumple con los estándares de un framework de tarificación de IMS. Este proyecto incluye los elementos IMS Charging Data Function y Online Charging System. El CDF

es una entidad IMS dedicada a la tarificación offline, la cual recolecta información del servicio consumido y lo guarda como un CDR (Charging Data Records), para posteriormente hacer un cobro de post-pago del servicio, como podría ser el cobro de un servicio a fin de mes. Por otra parte, el OCS realiza una tarificación online la cual permite un cobro de prepago del servicio asignando créditos al usuario y la eventual disminución de estos en tiempo real mientras se utiliza dicho servicio. Este software está todavía en un actual proceso de desarrollo y solo corresponde a una versión Beta, inclusive para realizar la comunicación de estos componentes a través de las direcciones de dominio cdf.ims.toip.uchile.cl y ocf.ims.toip.uchile.cl fue necesario modificar los códigos fuentes y compilarlos nuevamente, ya que los archivos de configuración XML no representaban todos las configuraciones necesarias para realizar las comunicaciones entre elementos. Por cierto este proyecto incluye un IPTV AS que reemplaza a la implementación anterior que se tenía en donde incluye la capacidad de comunicación DIAMETER con el CDF y OCS, además de incluir el Charging Trigger Function que inicia y termina el proceso de tarificación. Tras la inclusión en el sistema de estos dos nuevos componentes la topología de la red queda configurada de la siguiente manera.

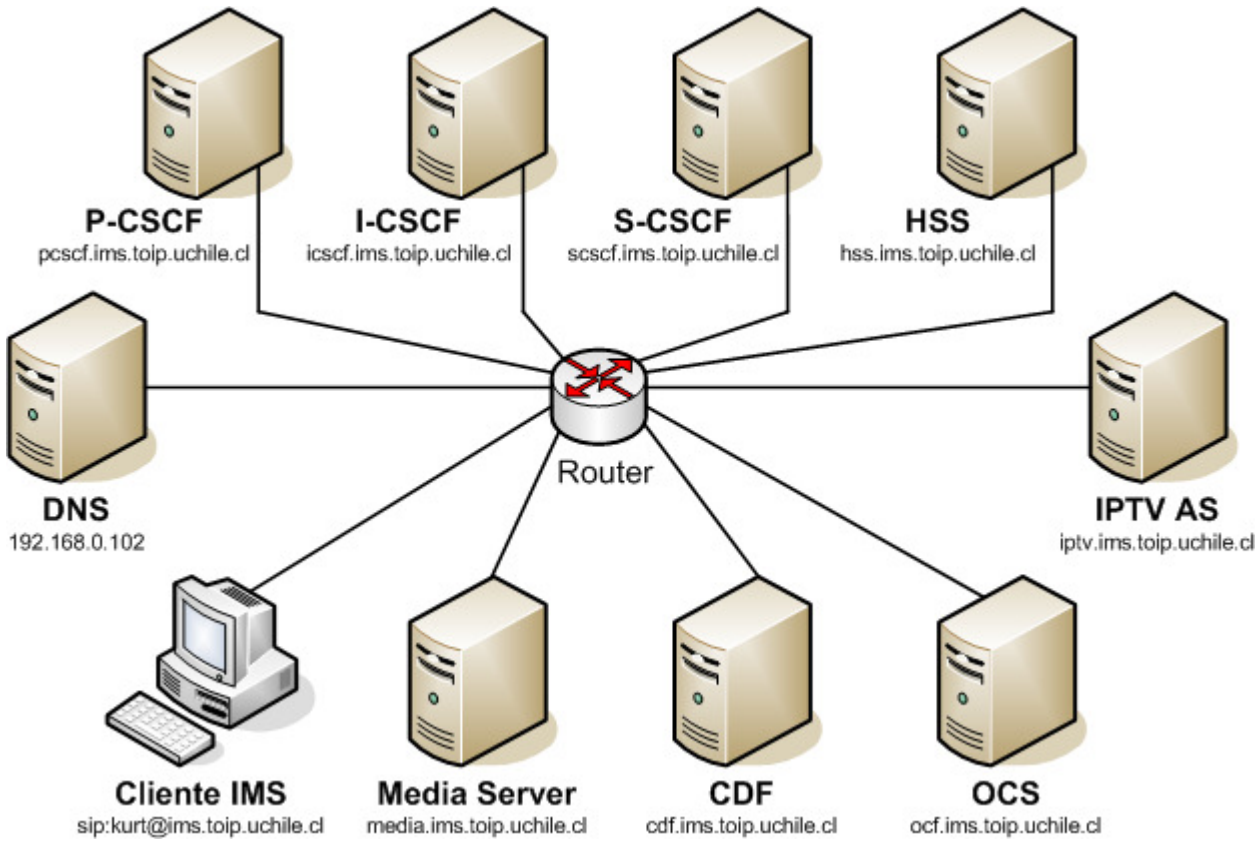

Figura 9: Diagrama de red del Sistema de Tarificación

Se presenta una tabla con los nuevos elementos incorporados al Laboratorio de IPTV.

Tabla 4: Elementos, direcciones IP y nombres de dominio de Sistema de Tarificación.

Elemento	Dirección IP	Nombre de dominio
CDF	192.168.0.109	cdf.ims.toip.uchile.cl
OCS	192.168.0.110	ocf.ims.toip.uchile.cl

3.2.4. Levantamiento de Sistema de Políticas de Control

Para incorporar un sistema de políticas de control se utilizó el desarrollado del proyecto UCT IMS Policy Control Framework. Este framework de políticas de control posee un Policy and Charging Rule Function (PCRF), un Policy and Charging Enforcement Point (PCEF) y un repositorio de políticas en XML que incluye una interfaz web para su manejo. Sin embargo estas

implementaciones de PCRF y PCEF que están en actual desarrollo no incluyen al día de hoy lo relacionado con la parte de tarificación. El PCRF implementado utiliza políticas de control en formato XML que son guardadas localmente, de igual manera también tiene la capacidad de utilizar un servidor XDM para guardar las políticas de control remotamente, sin embargo esta última cualidad no fue implementada en este trabajo de memoria. Además tampoco se implementó un Proxy RTP para que el PCEF pudiera tener control real sobre el ancho de banda del tráfico RTP que ocurre en el Laboratorio de IPTV.

Para que el PCRF pueda comunicarse a través de DIAMETER con el P-CSCF, de modo de que el P-CSCF reporte la información relevante de los mensajes SIP con contenido SDP que pasan por él, para que posteriormente el PCRF le responda con la toma de decisiones según políticas de control, fue necesario reemplazar el P-CSCF implementado inicialmente junto con el resto del núcleo IMS por otro P-CSCF que tiene mayores prestaciones que el que viene por defecto. Este P-CSCF se obtuvo desde una rama alternativa de desarrollo de Open IMS Core, en donde este P-CSCF trae la capacidad de operar con un PCRF a través de DIAMETER para poder aplicar las políticas de control en la plataforma IMS.

Al incluir nuevos elementos en el sistema, sus nombres de dominio deben ser incorporados en la lista con las direcciones IP que posee el DNS. Tras la incorporación de estos últimos elementos, finalmente se tiene la topología final del Laboratorio de IPTV:

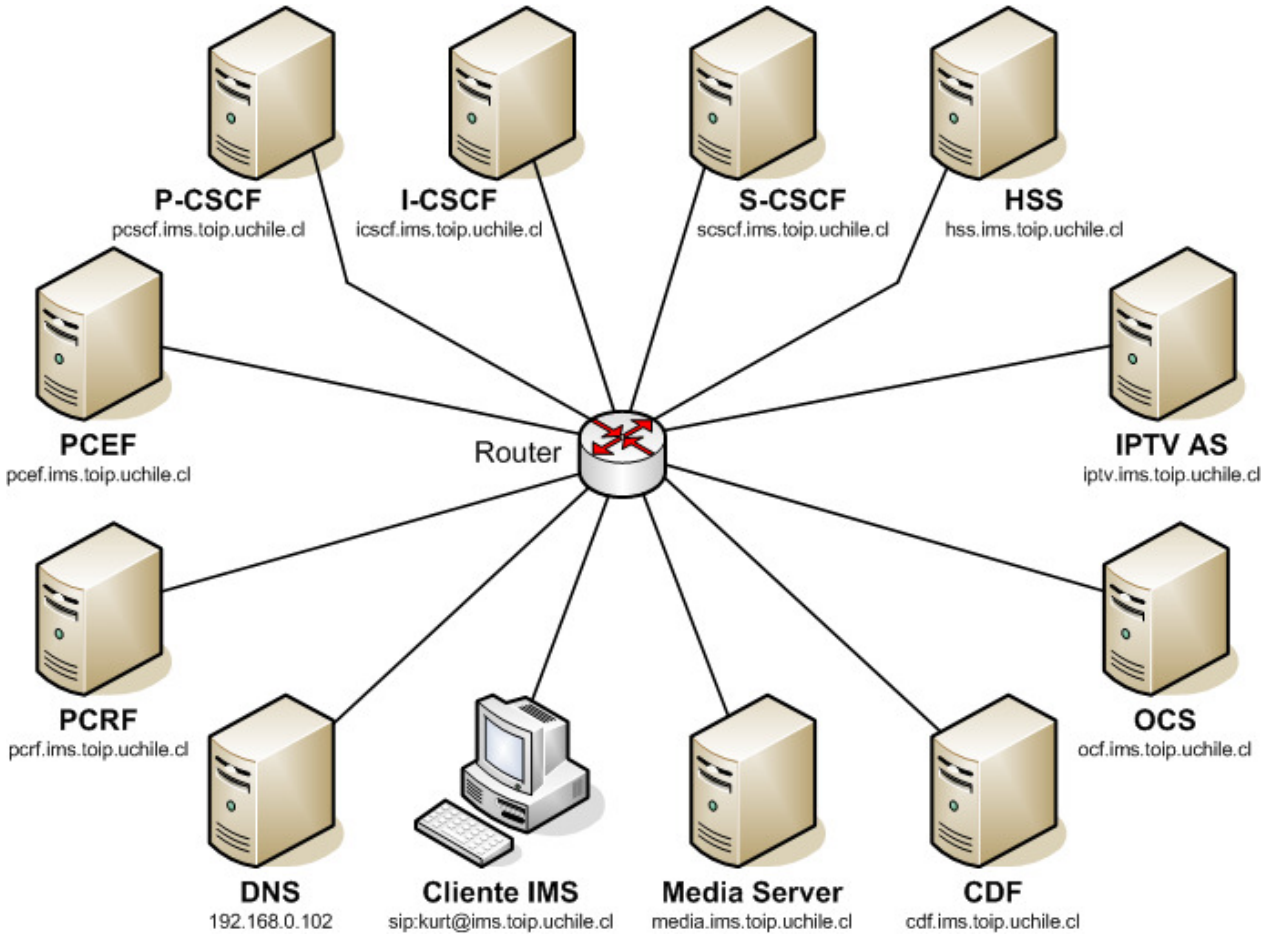

Figura 10: Diagrama de red de Sistema de Políticas de Control

Se presenta también una tabla que resume todos los componentes del Laboratorio de IPTV incluidas sus direcciones en la red.

Tabla 5: Elementos, direcciones IP y nombres de dominio de Laboratorio de IPTV.

Elemento	Dirección IP	Nombre de dominio
Cliente IMS	192.168.0.101	ue.ims.toip.uchile.cl
DNS	192.168.0.102	ns.ims.toip.uchile.cl
P-CSCF	192.168.0.103	pcscf.ims.toip.uchile.cl
I-CSCF	192.168.0.104	icscf.ims.toip.uchile.cl
S-CSCF	192.168.0.105	scscf.ims.toip.uchile.cl
HSS	192.168.0.106	hss.ims.toip.uchile.cl

IPTV AS	192.168.0.107	iptv.ims.toip.uchile.cl
Media Server	192.168.0.108	media.ims.toip.uchile.cl
CDF	192.168.0.109	cdf.ims.toip.uchile.cl
OCS	192.168.0.110	ocf.ims.toip.uchile.cl
PCEF	192.168.0.111	pcef.ims.toip.uchile.cl
PCRF	192.168.0.112	pcrf.ims.toip.uchile.cl

3.3. Pruebas del Laboratorio de IPTV

Una vez implementada la versión final del Laboratorio de IPTV se establecieron pruebas experimentales para realizar capturas de tráfico de paquetes a través del analizador de protocolos Wireshark. Esto se realizó con el fin de estudiar las comunicaciones entre los elementos de red y establecer su comportamiento bajo los distintos escenarios de prueba. Cada captura se hace sobre una interfaz de red distinta correspondiente a cada elemento que se desea estudiar. Para la realización de cada captura se identifica la tarjeta de red que utiliza el computador para conectarse. El programa Wireshark se instala y ejecuta en cada computador de interés. Las capturas asociadas a cada componente del proveedor se realizaron en las siguientes interfaces de captura:

Tabla 6: Interfaces de captura de tráfico de paquetes de datos.

Elemento	Dirección de Interfaz de captura
Cliente IMS	192.168.0.101
DNS	192.168.0.102
P-CSCF	192.168.0.103
I-CSCF	192.168.0.104
S-CSCF	192.168.0.105
HSS	192.168.0.106
IPTV AS	192.168.0.107
Media Server	192.168.0.108
CDF	192.168.0.109
OCS	192.168.0.110

PCEF	192.168.0.111
PCRF	192.168.0.112

A continuación se describen las pruebas y las condiciones bajo las que se realizaron en el Laboratorio de IPTV.

3.3.1. Experiencia 1: Inicio del Laboratorio de IPTV

Esta primera prueba consiste en realizar una captura de tráfico al inicio del sistema, es decir, en el momento en que todas las entidades que conforman el Laboratorio de IPTV se inicializan. La prueba en cuestión permite conocer los mensajes que se intercambian las distintas entidades durante el inicio del sistema. Esto posibilita un primer análisis del establecimiento de comunicaciones entre componentes del Laboratorio de IPTV.

3.3.2. Experiencia 2: Inicio de sesión en el Laboratorio de IPTV

En esta prueba se realiza captura de tráfico durante el proceso de registro de un Cliente IMS, para esto se utilizará la cuenta SIP kurt@ims.toip.uchile.cl El objetivo es conocer los distintos tipos de mensajes intercambiados entre las entidades cuando se realiza el proceso de registro de un usuario en el sistema. Lo anterior permite establecer el tipo actividad de cada componente del sistema durante este proceso, en particular se espera la participación del I-CSCF, S-CSCF y del HSS elementos que realizan esta tarea en un núcleo IMS.

3.3.3. Experiencia 3: Solicitud de canal de IPTV e inicio de tarificación

Una vez analizado el comportamiento de las entidades en el registro de un usuario, el siguiente paso es estudiar la solicitud de un canal de IPTV desde un Cliente IMS que ya ha iniciado sesión dentro del Laboratorio de IPTV usando el sistema de tarificación online. Al realizar las capturas pertinentes se establece el rol que juega cada entidad en el proceso de la solicitud de un canal de IPTV. También se estudian los tipos de mensajes intercambiados entre los distintos elementos. Se pretende que en esta experiencia se pueda observar como el IPTV AS recibe la solicitud del canal de parte del Cliente IMS, que el IPTV AS inicie con el OCS la tarificación de prepago del servicio que se le brinda al usuario y que envíe al Cliente IMS la

dirección RTSP del canal que pidió ver. También se pretende observar la transmisión multimedia que se realiza bajo el protocolo RTSP.

3.3.4. Experiencia 4: Término de servicio por agotamiento de créditos

En esta prueba se realiza una captura de tráfico a un usuario que esta ocupando el servicio de IPTV y que de pronto se le acaban los créditos existentes en el sistema de tarificación online. Luego de que el OCS le informa sobre el agotamiento de créditos al IPTV AS, este deberá pedir el corte de la transmisión del canal de IPTV. Durante esta prueba se intenta capturar los mensajes de término del servicio y fin del sistema de tarificación.

3.3.5. Experiencia 5: Denegación de servicio efecto de políticas de control

Se ha construido un escenario en el que se aplique una restricción impuesta por el sistema de políticas de control. A través de la interfaz web de este sistema, se ha bloqueado la opción de utilizar el códec de audio gsm, el cual es usado por defecto en las llamadas de videoconferencias que realizan dos Clientes IMS en la implementación de este Laboratorio de IPTV. Al intentar realizar la llamada, el P-CSCF debe informar al PCRF los datos relacionados al servicio, es aquí donde el PCRF debe actuar y bloquear la llamada.

3.3.6. Experiencia 6: Término de sesión en el Laboratorio de IPTV

Finalmente, esta experiencia presenta todas las comunicaciones capturadas en la red durante el término de la sesión de un usuario en el Laboratorio de IPTV. La prueba en cuestión permite conocer los mensajes que se intercambian las distintas entidades durante la salida de un usuario del sistema, considerándose que la plataforma de IPTV continúa operativa esperando la nueva llegada de un usuario al sistema.

CAPÍTULO IV: RESULTADOS

A continuación se presentan los resultados obtenidos a partir del diseño, la implementación y las pruebas realizadas sobre el Laboratorio de IPTV. Considerando las distintas versiones obtenidas del sistema y las diferentes experiencias efectuadas, los resultados se presentan en tres secciones:

1. Resultados sobre la implementación del Laboratorio de IPTV: Análisis de la implementación final de las diversas funciones y servicios inicialmente propuestos durante la etapa de diseño del Laboratorio de IPTV.
2. Resultados de las pruebas: Resumen de lo obtenido en los escenarios de prueba establecidos para el Laboratorio de IPTV.
3. Fines docentes del trabajo de título: Resultados sobre los aspectos docentes que potencia el trabajo.

4.1. Resultados sobre la implementación del Laboratorio de IPTV

Lo primero en la implementación fue levantar un núcleo y un cliente IMS. Por si solo, este sistema ya ofrece bastantes características útiles. Primero se tiene que el HSS del Núcleo IMS posee una interfaz web que permitió agregar a los nuevos usuarios del sistema. Además desde esta misma interfaz se incorporó la configuración necesaria para sumar el IPTV AS como un nuevo servicio al núcleo IMS. Por su parte, el cliente proporcionado por el proyecto UCT IMS Client tiene bastantes funcionalidades para usar desde su misma interfaz. Esta permite un fácil registro de usuario en el sistema, y la capacidad de poder hacer mensajería de texto, y videoconferencia.

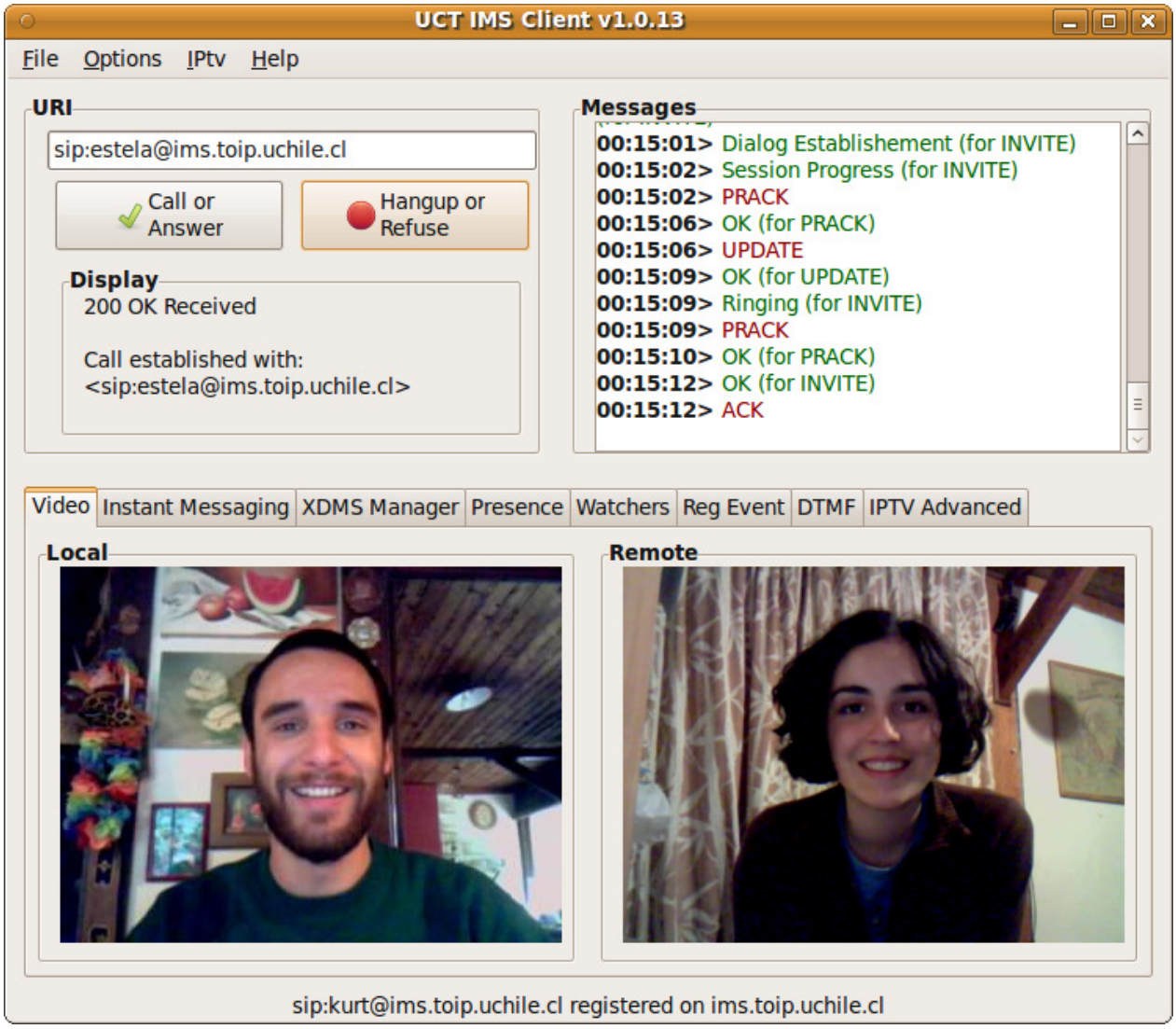

Figura 11: Ejemplo de videoconferencia en Cliente IMS.

La capacidad de solicitar canales de IPTV desde el mismo cliente si está implementada y se pudo utilizar en conjunto con el sistema de IPTV que consiste en un Media Server y un Application Server que opera con el núcleo IMS. La implementación de este sistema básico permitió que desde el Cliente IMS se pudieran solicitar contenido VoD o canales en modo live streaming. El contenido VoD es contenido multimedia que inicia su reproducción con su solicitud pudiendo detener o pausar su reproducción, al respecto, si fue posible pausar y detener la transmisión de contenido VoD, que hace provecho del protocolo RTSP, a través de botones que dispone la interfaz de reproducción del Cliente IMS. El modo live streaming se refiere a lo que se conoce comúnmente como canales de televisión, que es una reproducción continua en el lado del Media Server sin la posibilidad de controlarla. El cliente no hace la distinción entre estos dos tipos de

servicios, la diferencia sólo depende de cómo el Media Server dispone el contenido asociado a sus direcciones RTSP. No existió una limitante para el número de canales o contenido VoD, esto sólo depende de la capacidad de almacenamiento de los videos en el Media Server.

El cliente dispone un par de EPGs, una es para mostrar la lista de canales live streaming y la otra es para mostrar la lista de contenido VoD disponible. Estas guías electrónicas de programas permiten mostrar información relativa a cada contenido. El Cliente IMS carga los datos a partir de los archivos de configuración: tv_epguide.xml y tv_epguide.xml ubicados al interior de la carpeta del Cliente IMS. Estas EPGs permiten solicitar los canales o contenidos VoD directamente desde ellas, a continuación se pueden visualizar ambas EPGs.

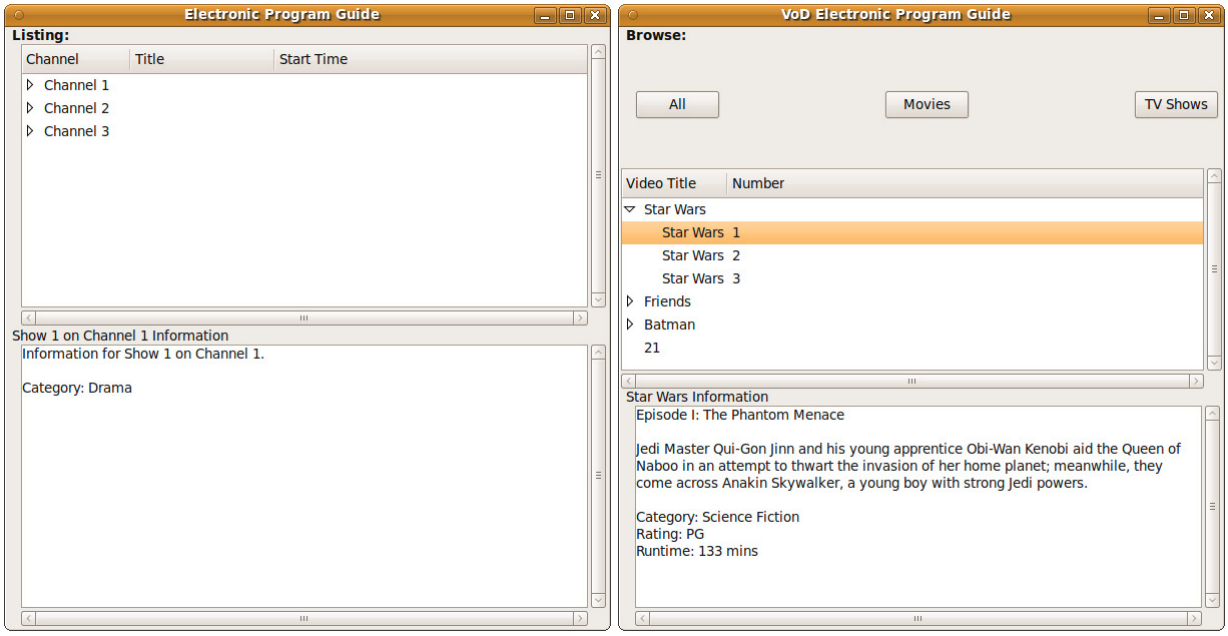

Figura 12: Electronic Program Guides.

En cuanto a la calidad de servicio del sistema, esta es aceptable debido a que el Laboratorio de IPTV fue montado en una red de área local dedicada para este fin, obteniendose de este modo transmisiones con muy bajos niveles de perdidas de paquetes y en consecuencia un contenido de video fluido. La calidad y resolución de imagen dependen principalmente de los códecs y características que se utilicen en el contenido multimedia de origen, en este estudio no se utilizó video en alta definición (sobre 1280x720 pixeles). Al hacer diversas pruebas de apreciación subjetiva de QoS, se determinó un puntaje MOS igual a 4 de un máximo de 5, esto significa que la calidad de la transmisión es buena, con un nivel de error perceptible pero no molesto no

ameritando el cambio de canal [28]. Se muestra a continuación una imagen del sistema funcionando bajo las circunstancias recién mencionadas.

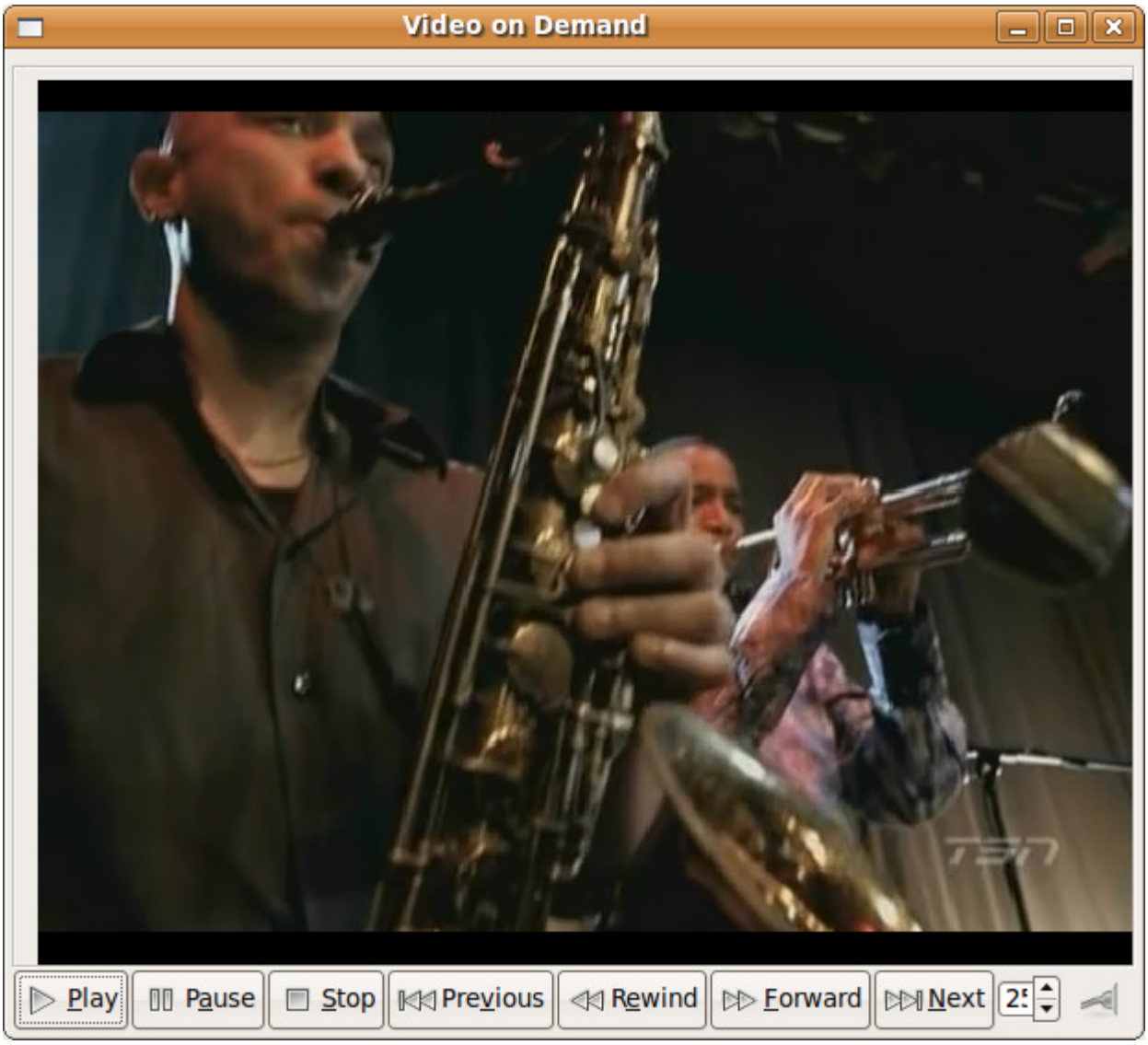

Figura 13: Servicio de Video-on-Demand.

Sin embargo, al iniciar una transmisión de un canal en modo live streaming o cuando se pone en marcha después de pausar la recepción de material VoD, se produce un pixelamiento muy molesto durante unos instantes hasta que se compone correctamente la imagen. Al realizar pruebas de apreciación subjetiva de QoS, se determinó un puntaje MOS igual a 2 de un máximo de 5, esto significa que la calidad de la transmisión es pobre, con un nivel de error molesto que amerita el cambio de canal de mantenerse [28]. A continuación se muestra una imagen de la

recepción de la transmisión con el problema recién comentado, el título de la ventana que contiene el video dice Video on Demand sin embargo en la imagen se muestra una transmisión live streaming, pues como se comentó el Cliente mismo no hace distinciones en cuanto a interfaz al solicitar uno u otro modo pues esto depende del Media Server.

Figura 14: Inicio de canales live streaming.

Otra característica que perjudica bastante la calidad de experiencia (QoE) es que en el Laboratorio de IPTV al cambiar de un canal a otro, lo cual significa detener la transmisión e iniciar otro canal manualmente, toma un mayor tiempo que lo debido. Esta demora durante el salto de canales es conocida como tiempo de zapping y es uno de los principales problemas a

tener en cuenta por quienes pretenden implementar una plataforma de IPTV a nivel comercial [28]. Cerrar un canal y abrir otro toma más de 3 segundos en esta implementación, sin considerar el retraso introducido en la manipulación que se debe realizar en la interfaz del Cliente IMS que no permite cambiar de canal con sólo un click. Para tener un buen servicio, el tiempo de zapping no debiera sobrepasar los 2 segundos según se comenta en el documento "Consideration on Channel Zapping Time in IPTV Performance Monitoring" desarrollado por el ITU-T FG IPTV [40].

El sistema NDVR fue implementado en el misma máquina que hace de Media Server. Este DVR remoto permite agendar una grabación de un canal live streaming, que llegado el momento previamente programado iniciará la grabación del material en un archivo de video para su posterior, o inclusive inmediata, solicitud como contenido VoD desde el Cliente IMS. Sin embargo la implementación de la interfaz del cliente con que se realiza la configuración del NDVR no está integrada como un servicio dentro de los ofrecidos por el Cliente IMS, sino que se implementó como un servicio por líneas de comando que se opera paralelamente al Cliente IMS.

Respecto al sistema de tarificación, se tiene que es un sistema exclusivo de cobro del servicio de IPTV y no de los otros servicios IMS que son ofrecidos dentro del Laboratorio de IPTV, por lo tanto no es posible tarificar los servicios de llamadas de videoconferencias o de VoIP, esto debido a que solo el IPTV AS contiene un Charging Trigger Function para estos fines. Como ya se ha comentado, la plataforma posee un OCS encargado de la tarificación online que opera bajo la lógica de sistema de prepago y un CDF encargado de la tarificación offline que permite realizar cobros de postpago del servicio. El proyecto de software libre desde el cual se basa la implementación de estos componentes está en una fase Beta, por lo cual es una solución muy precaria en cuanto a la posibilidad de configurar y sacar provecho sin necesidad de modificar sus códigos fuentes. Considerando todo esto, ambos módulos fueron ocupados en la medida de lo posible. Respecto a los resultados obtenidos con el sistema de tarificación Online se pudo distinguir que para la tarificación se utiliza un modelo de cobro conocido como Unit Reservation [4], esto significa que el IPTV AS solicita de forma periódica al OCS la asignación de créditos durante el uso del servicio. Si el usuario detiene manualmente la transmisión del canal de IPTV, el sistema de tarificación se detiene. En caso de que se le acaben los créditos al usuario, el sistema de tarificación pide el corte inmediato del servicio.

No existen archivos XML para la configuración tarifaria, toda esta información se encuentra contenida en los códigos fuentes del programa, por lo que cualquier cambio implica la nueva compilación del OCS. Por defecto se tiene que el número de créditos inicial es de 200, la tarificación es por tiempo de uso del servicio y el precio fijado es de un crédito por segundo. Al estudiar el código fuente de los elementos involucrados en la tarificación, se encontró que están las funciones asociadas a las otras modalidades de tarificación, que son el caso de Direct Debiting [4] que corresponde a un cobro único por uso del servicio y el caso de Unit Reservation según flujo de datos transmitido, con lo que se podría rarificar el MB consumido en vez del tiempo de uso de los servicios, sin embargo la utilización de estos dos tipos de métodos significaría un esfuerzo mayor de coordinación con el IPTV AS o el PCEF en el caso del cobro por flujo de datos. Al hacer pruebas con el sistema de tarificación offline se corroboró el envió del tiempo de uso del servicio con una periodicidad de 30 segundos desde el IPTV AS al CDF, sin embargo el CDF no almacena ni crea ningún Charging Data Record [4] con el cual se pueda facturar a los usuarios posteriormente, por lo que la información de uso del servicio se pierde.

El sistema de políticas de control permitió aplicar ciertas reglas para gestionar la calidad del servicio del sistema. A través de su interfaz web es posible por ejemplo definir cómodamente que códecs son permitidos en las comunicaciones. En caso de que una llamada intente ocupar un códec no permitido, el sistema de políticas de control a través del PCRF bloqueará la llamada.

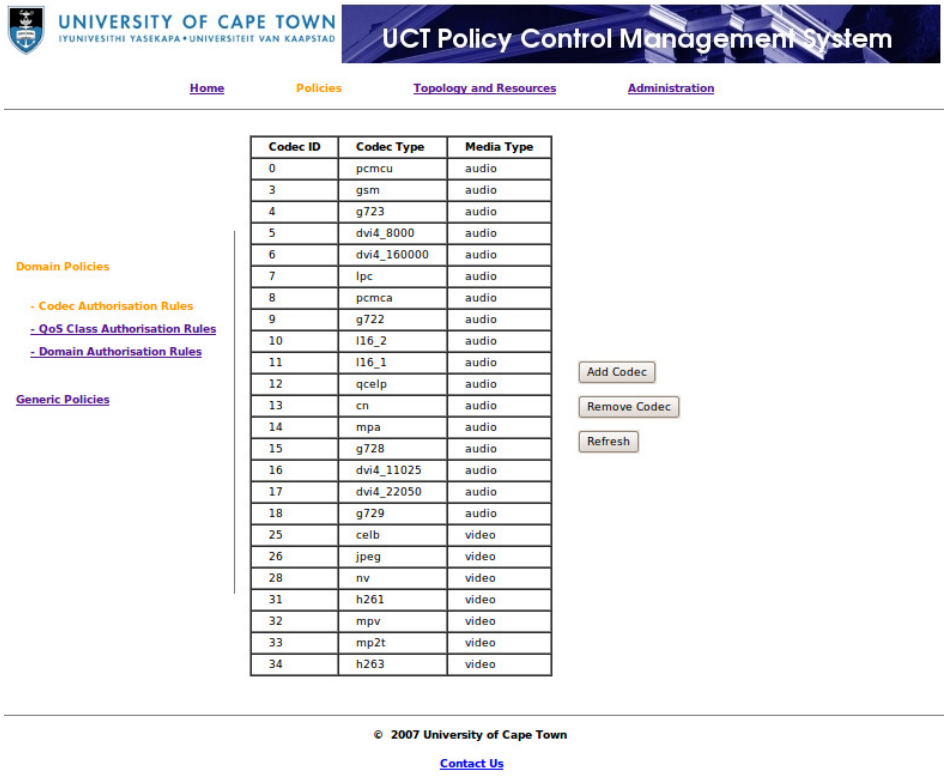

Figura 15: Sistema de políticas de control - Codec Authorizarion Rules.

También es posible definir clases de servicios con sus respectivos anchos de banda para cumplir con requisitos de QoS. Además, a través de la interfaz web es posible monitorear el consumo de ancho de banda de cada clase de servicio en tiempo real. En caso de que se alcance el límite para una clase, el sistema bloqueará una nueva llamada de aquella clase. Estas clases de QoS se aprecian en la siguiente imagen.

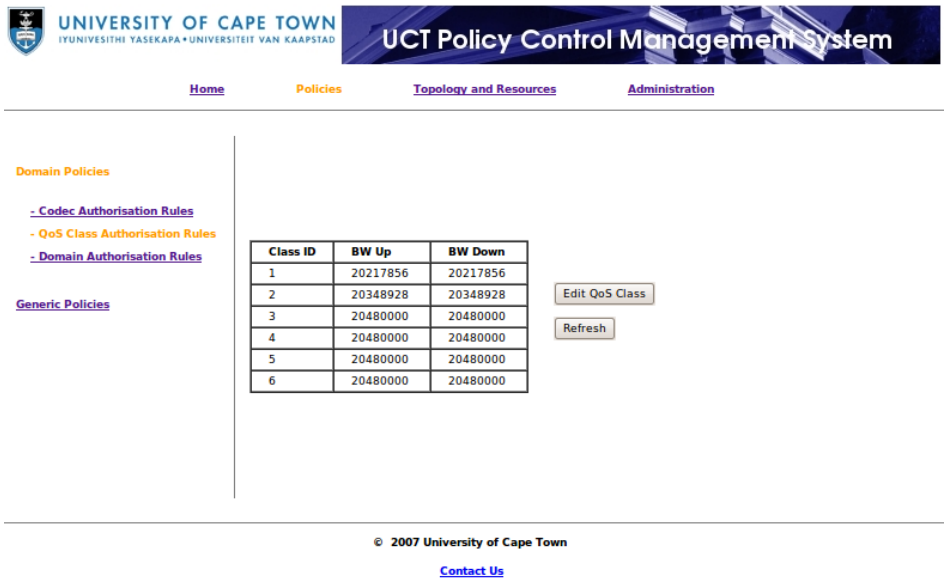

Figura 16: Sistema de políticas de control - QoS Class Authorizarion Rules.

La interfaz web permite también fijar los recursos máximos que pueden ser ocupados por el sistema completo, pudiéndose operar sobre más de un dominio IMS. Es posible visualizar a través de la interfaz del sistema de políticas de control los flujos para las llamadas que se cursan sobre el núcleo IMS en tiempo real. Por ejemplo en la figura 16 se aprecia como existen dos flujos de clase 2 que corresponde a transmisión de audio y dos flujos de clase 1 correspondiente a la transmisión de video. Estos cuatro flujos corresponden a los existentes durante una videoconferencia, considerando que existe flujo de audio y video en ambos sentidos. La implementación de este sistema de políticas de control no permitió poder aplicar reglas sobre el servicio de IPTV, esto debido a que las invitaciones SIP con descripción de sesión del servicio de IPTV no son informadas al PCRF como si lo son las llamadas de VoIP o videoconferencias. Dado que no fue implementado un servidor proxy RTP en el PCEF. Los monitorización de los flujos no es real, sino valor definidos previamente en los archivos XML de configuración del sistema de políticas de control en donde se definen las clases de QoS y los anchos de banda asociados a estas y al dominio ims.toip.uchile.cl completo.

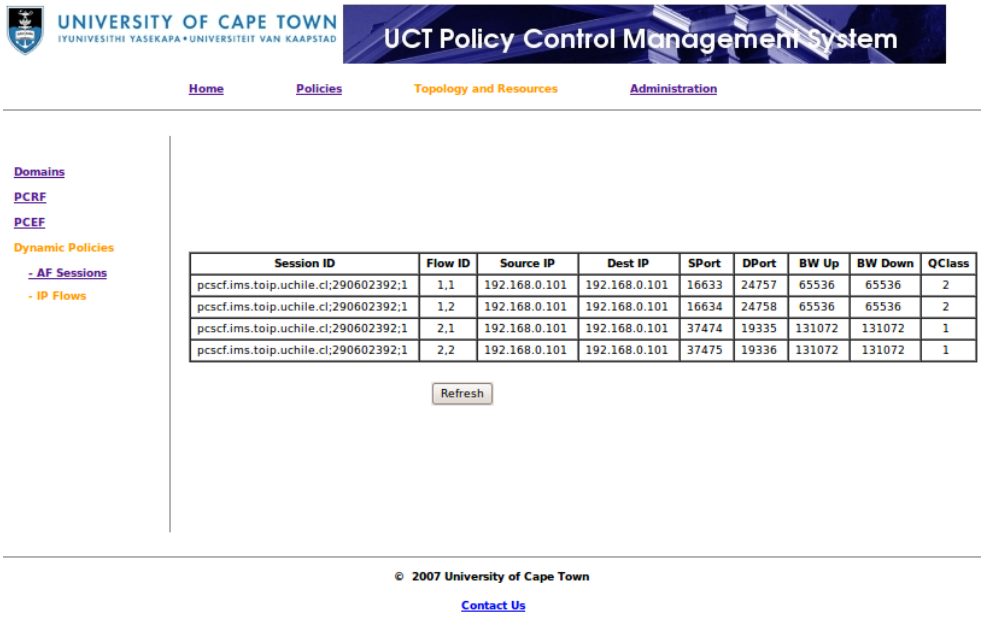

Figura 16: Sistema de políticas de control - IP Flows.

4.2. Resultados de las pruebas

En el Capítulo de Metodología se establece una serie de pruebas que permiten estudiar las funciones de los distintos componentes del Laboratorio de IPTV. El desarrollo y los resultados obtenidos mediante estas experiencias constituyen el aspecto docente de este trabajo de título. A continuación se presenta un resumen de los resultados obtenidos en el desarrollo de las experiencias. En la sección de Anexos 9.3 se encuentra una Guía de Laboratorio con el desarrollo detallado, junto con gráficos de flujo de los mensajes entre identidades y esquemas globales de las comunicaciones presentes en el sistema.

En la experiencia 1 se logra estudiar la interacción producida entre los distintos elementos del sistema durante el inicio de todos los componentes que conforman el servicio de IPTV. Es así como se comprueba que durante este proceso:

- El I-CSCF y el S-CSCF se comunican con el IPTV AS mediante comandos DIAMETER CER/CEA para reconocerse y mensajes DWR/DWA para monitorear la conexión, formando un trío de elementos aislados del resto del sistema.

- El P-CSCF y el PCEF se comunican con el IPTV AS mediante comandos DIAMETER CER/CEA para reconocerse y mensajes DWR/DWA para monitorear la conexión, formando un trío de elementos aislados del resto del sistema.
- El CDF y el OCS se comunican con el IPTV AS mediante comandos DIAMETER CER/CEA para reconocerse y mensajes DWR/DWA para monitorear la conexión, formando un trío de elementos aislados del resto del sistema.
- El Cliente IMS y el Media Server no realizan ninguna comunicación.
- No existe intercambio de mensajes SIP entre las entidades.

La experiencia 2 permite estudiar el proceso de registro del Cliente IMS en el Laboratorio de IPTV. Como resultado se establece la función de cada entidad IMS y se estudia la comunicación entre las distintas componentes durante este proceso:

- Todas las comunicaciones del Cliente IMS con el sistema son realizadas a través de la entidad P-CSCF utilizando el protocolo SIP.
- El Cliente IMS envía dos SIP REGISTER al S-CSCF. El primero para solicitar que se le envié un valor "nonce", luego el cliente IMS utiliza este valor único y las credenciales de usuario para generar a través de un algoritmo AKA una respuesta que es insertada en la segunda petición de REGISTER que envía al S-CSCF.
- Posteriormente el Cliente IMS envía el mensaje SIP SUBSCRIBE hacia el S-CSCF.
- El S-CSCF envía SIP NOTIFY al cliente que contiene en el campo Body del paquete información codificada en XML relativa al registro del usuario.
- Al final del proceso el S-CSCF envía un mensaje NOTIFY al P-CSCF, que luego es respondido con un 500 Error porque encuentra un error en el formato del mensaje en vez de responder con un 200 OK. Esto no afecta a los servicios posteriormente.
- El I-CSCF intercambió mensajes DIAMETER MAR/MAA, UAR/UAA y LIR/LIA con el HSS.
- EL S-CSCF intercambió mensajes DIAMETER SAR/SAA con el HSS.
- Mientras se realizó el registro del usuario, el IPTV AS junto con los módulos de tarificación CDF y OCS, así como también los elementos encargados de aplicar las políticas de control PCRF y PCEF sólo intercambian durante este proceso mensajes DIAMETER Device-Watchdog para mantener contacto entre peers.

La experiencia 3 permite estudiar las comunicaciones entre componentes durante la solicitud de un canal de IPTV, durante este evento se da inicio también al sistema de tarificación online. De los resultados de esta experiencia los principales obtenidos fueron:

- El cliente realiza una petición SIP INVITE al IPTV AS con la dirección del canal channel1@iptv.ims.toip.uchile.cl, a través del P-CSCF y el S-CSCF.
- En el IPTV AS el Charging Trigger Function provoca que se inicie la tarificación. El IPTV AS se comunica utilizando DIAMETER con el OCS a través de un comando DIAMETER Credit-Control-Request que incluye un AVP del tipo CC-Request-Type con el valor INITIAL_REQUEST para que se de inicio a la tarificación.
- Una vez que el IPTV AS recibe la respuesta del OCS con la asignación de créditos a través de un mensaje Credit-Control-Answer, el IPTV AS envía el mensaje SIP de 200 OK que contiene la dirección RTSP del Media Server al cual el Cliente IMS tendrá que solicitar el canal posteriormente.
- Para iniciar la transmisión del canal el cliente IMS envía un mensaje RTSP OPTIONS al Media Server.
- El cliente envía una petición RTSP DESCRIBE, que el Media Server responde con un mensaje RTSP/SDP 200 OK que contiene una descripción del recurso solicitado, en particular que se debe establecer dos flujos: uno para audio y otro para video.
- El cliente envía un par de mensajes RTCP SETUP al Media Server, uno para el audio y otro para el video que se transmitirán, informando al Media Server como será transportado el flujo de datos.
- El Cliente IMS envía una petición PLAY provocando que el servidor comience a enviar datos de los flujos especificados utilizando los puertos configurados previamente cuando se utilizó el comando SETUP.
- La transmisión del contenido multimedia se realiza unidireccionalmente desde el Media Server al Cliente IMS a través del protocolo RTP. Son distinguidos dos tipos de paquetes RTP, unos llevan el contenido del video y otros el del audio.
- Durante la transmisión de paquetes RTP, se envían y reciben periódicamente mensajes Reportes RTCP sobre el estado de la transmisión.
- El I-CSCF y HSS no se hacen presentes en esta prueba.

- En el proceso no participan activamente el PCRF, PCEF, I-CSCF ni HSS, los cuales solo comparten mensajes DIAMETER DWR/DWA.

En la experiencia 4 se logra estudiar la interacción producida entre los distintos elementos del sistema cuando ocurre el evento de agotamiento de créditos de un usuario que esta utilizando el servicio de IPTV bajo una tarificación online, es decir a través de un sistema de prepago. Durante este proceso se observó:

- Antes del corte, el IPTV AS hace periódicas consultas DIAMETER al OCS del tipo Credit-Control-Request con el contenido UPDATE_REQUEST en su AVP CC-Request-Type solicitando una nueva asignación de créditos para el servicio. Por su parte el OCS le devuelve cada vez un mensaje Credit-Control-Answer que contiene la cantidad de créditos en el AVP Check-Balance-Result.
- Cuando al usuario no le quedan créditos es informado por el OCS al IPTV AS a través de un mensaje DIAMETER Credit-Control-Answer con el valor NO_CREDIT en su AVP Check-Balance-Result.
- El IPTV AS envía un mensaje DIAMETER Credit-Control-Request con un AVP CC-Request-Type con el contenido TERMINATION_REQUEST al OCS que cierra la tarificación.
- El IPTV AS envía un mensaje SIP BYE por medio del S-CSCF y P-CSCF al Cliente IMS informándole el fin del uso del servicio de IPTV.
- El cliente envía un mensaje RTSP TEARDOWN al Media Server para detener la transmisión, el cual es respondido por un 200 OK.
- Se intercambian mensajes RTCP de Goodbye con lo que se cierra la transmisión.
- En el proceso no participan activamente el PCRF, PCEF, I-CSCF ni HSS, los cuales solo comparten mensajes DIAMETER DWR/DWA.

La experiencia 5 permite estudiar las comunicaciones entre componentes durante el bloqueo de una llamada de videoconferencia entre dos Clientes IMS por parte del PCRF al aplicar una política de control previamente establecida para este escenario. A partir de los resultados de esta experiencia se encontró que:

- El Cliente IMS 1 envía SIP INVITE al P-CSCF con la dirección SIP del Cliente IMS 2.

- El Cliente IMS 2 devuelve un SIP 100 Trying al P-CSCF, seguido de un 101 Dialog para el S-CSCF que viaja a través del P-CSCF con lo que se confirma que se estableció dialogo entre las partes.
- El Cliente IMS 2 envía un SIP183 Session Progress al S-CSCF a través del P-CSCF, este mensaje contiene información sobre las características de la sesión.
- El S-CSCF envía un SIP 183 Session Progress al P-CSCF con la información enviada por el Cliente IMS 2.
- Al recibir el P-CSCF el mensaje SIP 183 Progress, realiza una consulta DIAMETER AAR al PCRF, que responde con un DIAMETER AAA negando el servicio dado que en este ejemplo la comunicación entre clientes pretende ocupar el códec GSM para el audio el cual fue previamente sacado de la lista de códecs permitidos a través de la interfaz web del sistema de políticas de control.
- Inmediatamente el P-CSCF envía un mensaje DIAMETER Session-Termination Request al PCRF.
- Luego se desencadenan los mensajes para cancelar y terminar la comunicación entre clientes. El P-CSCF envía un mensaje SIP Status 488 Not Acceptable Here al Cliente IMS 1, que fue quien realizó la llamada negándosele el servicio. Y el Cliente IMS 1 responde con un ACK.
- El P-CSCF envía un SIP CANCEL al S-CSCF.
- El S-CSCF envía un SIP CANCEL al Cliente IMS 2 a través del P-CSCF.
- El Cliente IMS 2 envía un SIP 487 Request Cancelled al S-CSCF a través del P-CSCF.
- El S-CSCF envía un SIP 487 Request Cancelled al P-CSCF.
- Todo se termina con un 488 Not Acceptable Here del P-CSCF al Cliente IMS 1 que fue quien comenzó toda la comunicación.
- En el proceso no participan activamente el IPTV AS, CDF, ni OCS, los cuales solo comparten mensajes DIAMETER DWR/DWA.

La experiencia 6 permite estudiar el proceso de término de sesión del usuario en el Laboratorio de IPTV. Como resultado se establece la función de cada entidad IMS y se estudia la comunicación entre las distintas componentes durante esta labor:

- El Cliente IMS envía dos SIP REGISTER al S-CSCF. El primero para solicitar que se le envié un valor "nonce", luego el cliente IMS utiliza este valor único y las credenciales de usuario para generar a través de un algoritmo AKA una respuesta que es insertada en la segunda petición de REGISTER que envía al S-CSCF.
- El S-CSCF envía un mensaje NOTIFY al Cliente IMS a través del P-CSCF. El cual el P-CSCF reclama con un SIP Error 500 diciendo que la notificación contiene errores, lo cual no perjudicará posteriormente al Cliente IMS que responde con un SIP 200 OK.
- El I-CSCF intercambió mensajes DIAMETER UAR/UAA con el HSS.
- Mientras se realizó el registro del usuario, el IPTV AS junto con los módulos de tarificación CDF y OCS, así como también los elementos encargados de aplicar las políticas de control PCRF y PCEF sólo intercambian durante este proceso mensajes DIAMETER Device-Watchdog para mantener contacto entre peers.

4.3. Fines docentes del trabajo de título

En términos docentes, los resultados obtenidos sobre el diseño y la implementación del sistema revierten un fuerte potencial. Se logró estructurar un sistema que desplegado dentro de una red de computadores posibilita el estudio práctico de entidades de la arquitectura IMS. Además se generaron diferentes escenarios de prueba que permiten analizar los mensajes de los distintos protocolos envueltos en el sistema. Como resultado es posible establecer una lista genérica de temas prácticos que aborda el trabajo de título y que potencian el aspecto docente del mismo:

- Estudio e implementación de un Núcleo IMS extendido con entidades de tarificación y políticas de control.
- Incorporación de un Application Server a un Núcleo IMS.
- Configuración de red IP y familiarización con protocolos UDP, TCP, DNS.
- Creación de nuevos usuarios para Núcleo IMS.
- Uso y configuración de un programa Cliente IMS.
- Inicio y término de sesión de un Cliente IMS.
- Configuración de un Media Server con contenido de VoD o live streaming.
- Establecimiento de sesiones SIP entre dos Clientes IMS.

- Estudio práctico de protocolos SIP, DIAMETER, RTSP, RTP, RTCP.

Fueron definidas experiencias de Laboratorio que permiten estudiar los aspectos más importantes del Laboratorio de IPTV. Las experiencias establecidas y el desarrollo de las mismas se incluyen en una Guía de experiencias para el Laboratorio de IPTV en la sección de Anexos 9.4:

- Experiencia 1: Inicio del Laboratorio de IPTV.
- Experiencia 2: Inicio de sesión en el Laboratorio de IPTV.
- Experiencia 3: Solicitud de un canal de IPTV e inicio de tarificación.
- Experiencia 4: Término de servicio por agotamiento de créditos.
- Experiencia 5: Denegación de servicio efecto de políticas de control.
- Experiencia 6: Término de sesión en el Laboratorio de IPTV.

Estas guías se perfilan como base para el desarrollo de futuras actividades docentes de laboratorio en el ámbito de las tecnologías para la convergencia de redes en el área de Telecomunicaciones.

CAPÍTULO V: DISCUSIÓN

En este capítulo se establece la discusión sobre diferentes aspectos desarrollados y tratados en este trabajo de memoria. Se discutirá acerca del Laboratorio de IPTV y sus características implementadas, las pruebas realizadas, los fines docentes del trabajo de titulo y acerca de la arquitectura IMS.

El Laboratorio de IPTV implementó suficientes características de las que debiera poseer un servicio de IPTV basado en IMS, convirtiéndolo en una útil plataforma para futuros desarrollos que puedan agregar funcionalidades o mejorar las ya existentes. Al ser una implementación acorde con el estándar de IMS, el laboratorio se convierte en un ejemplo más de como es posible ofrecer servicios sobre una red convergente. Inclusive al utilizarse los servicios proporcionados por el Laboratorio de IPTV, este no interfiere más allá de consumir recursos con otros servicios que se puedan estar ofreciendo y/o usando sobre el núcleo IMS en el mismo instante. De hecho, el núcleo IMS utilizado para la implementación de IPTV es prácticamente el mismo que ha sido implementado en memorias anteriores del Departamento de Ingeniería Eléctrica, lo que demuestra la compatibilidad del Laboratorio de IPTV implementado. La única intervención que se realizó en el núcleo IMS fue un reemplazo del P-CSCF por uno perteneciente a una rama alternativa de desarrollo del proyecto Open IMS Core que contiene la capacidad de conectarse a un PCRF para realizar intervenciones de políticas de control y QoS. Sin embargo si no se quisiese hacer provecho del PCRF, se puede utilizar sin problemas el P-CSCF que trae el proyecto Open IMS Core por defecto.

El cliente IMS escogido para el desarrollo del Laboratorio de IPTV fue suficientemente apto para su uso en el servicio. Desde su interfaz existe la opción directa de iniciar una sesión IMS y solicitar canales de IPTV, posee una implementación rudimentaria para ofrecer EPGs, y mientras ocurre la reproducción de un canal, el cliente cuenta con controles de start, pause y stop que permiten sacar el máximo provecho de una transmisión bajo el protocolo RTSP. Además, este cliente IMS posee la habilidad de realizar tareas de mensajería instantánea, llamadas VoIP y videoconferencias con otro cliente IMS, por lo cual en la implementación del Laboratorio de IPTV no se pierden servicios agregados durante esfuerzos de memoristas anteriores que trabajaron con la arquitectura IMS. Si bien es cierto que el cliente IMS permite la visualización de los canales de IPTV en pantalla completa, el resto de la interacción con el cliente se realiza en

una interfaz poco atractiva en comparación a lo que se debiera ofrecer en un servicio de IPTV comercial. Idealmente, se debiera tener un aspecto de Media Center siguiendo los lineamientos de las interfaces generadas típicamente por Set-Top-Boxes que se ofrecen en servicios de televisión satelital o por cable.

En cuanto a los problemas detectados en el Laboratorio de IPTV se encuentra que el Media Server utilizado es una entidad que no mantiene comunicación con el núcleo IMS, por lo que cumple con la labor de transmitir audio y vídeo al Cliente IMS sin recibir ningún tipo de verificación desde el S-CSCF como debiera ocurrir [14]. Por lo tanto se deja constancia una vez más de que el Laboratorio de IPTV sólo es un intento de aproximación a un sistema de IPTV basado en IMS lo más completo posible. La falta de verificación recién mencionada se convierte en una falla de seguridad que permite que un cliente de vídeo que conoce la dirección RTSP asociada a un canal de IPTV pueda obtener el contenido saltándose el registro en el sistema IMS y el cobro por tarificación puesto que el Media Server está abierto a cualquier conexión desde un cliente RTSP sin realizar ningún tipo de discriminación.

Respecto al sistema de tarificación utilizado en el Laboratorio de IPTV, se tiene que es sólo aplicable para el servicio de IPTV, es decir no se permite tarificar los otros servicios disponibles en la plataforma IMS. La implementación del sistema de tarificación está hecha a partir de un software que está en estado de beta, por lo que es un proyecto muy precario a la fecha y sin documentación. Para sacarle un mejor provecho a este sistema, habría que estudiar detenidamente su código fuente, lo cual no se realizó por motivos de tiempo limitándose exclusivamente a modificar el código fuente para que funcionara bajo la implementación distribuida de los componentes que conforman el Laboratorio de IPTV.

Las pruebas realizadas en el Laboratorio de IPTV permitieron demostrar varios aspectos del funcionamiento, a nivel de protocolos de comunicación, entre componentes del sistema. Se pudo apreciar que los elementos se comunican a través de DIAMETER para intercambiar mensajes típicos de un protocolo AAA (authentication, authorization and accounting) cuando sucede un intercambio de mensajes relacionados a la autentificación y autorización del usuario, así como también para el intercambio de información durante la tarificación. Similarmente, se apreció que para la comunicación relacionada a la señalización de un servicio son intercambiados mensajes

SIP, y que para la transmisión de audio y video se usaron exclusivamente los protocolos RTSP, RTP y RTCP.

Con respecto a los fines docentes del trabajo de título se logró generar una serie de experiencias de laboratorio que establecen una base para el estudio del Laboratorio de IPTV sobre arquitectura IMS y de los principales protocolos de comunicación involucrados. Considerando los resultados obtenidos en cada experiencia, se extienden los esfuerzos previos de creación de material con fines docentes como los realizados en la memoria de Sebastian Peñaloza, que inicia un estudio práctico sobre la arquitectura IMS. El Laboratorio de IPTV finalmente implementado también podría ser utilizado de ejemplo para realizar cátedras prácticas sobre el funcionamiento de redes IMS. Por las razones anteriores este trabajo de título representa un apoyo importante a la docencia de temáticas actuales relacionadas a la convergencia de redes. Es claro que con iniciativas de este tipo se potencia la docencia sobre éste y otros temas innovadores dentro del Área de Telecomunicaciones del Departamento de Eléctrica.

Finalmente, tras haber implementado con éxito un servicio de IPTV sobre el mismo núcleo IMS que es capaz de ofrecer una amplia gama de otros servicios, se comprueba la existencia de las ventajas que conlleva adoptar IMS y que avalarían el desarrollo de aplicaciones y estudios como este trabajo de memoria. Esto debido a que desde el punto de vista del operador del sistema existen beneficios en cuanto al CAPEX, al no tener que invertir en múltiples redes sobrepuestas para ofrecer los distintos servicios, lo mismo se tiene para el OPEX considerando que se reutilizan recursos al integrar horizontalmente las funciones comunes a todos los servicios (autentificación, autorización, tarificación, etc.) [4]. Además, poniendo la atención en la implementación de los Application Servers se pueden reducir los tiempos en el ciclo de desarrollo de aplicaciones (time-to-market) permitiendo la entrega de servicios en menos tiempo y reduciendo los costos de soporte de dichas aplicaciones.

CAPÍTULO VI: CONCLUSIONES

Se cumplió el objetivo principal del trabajo de memoria que era diseñar e implementar un Laboratorio de IPTV. Un requisito es que debía ser de bajo costo, lo cual se cumplió a través del uso exclusivo de proyectos de software libre. A continuación se presenta una tabla que resume los proyectos usados, los componentes del sistema que ellos aportan y sus licencias de software.

Tabla 7: Proyectos de Software Libre utilizados.

Proyecto	Componentes aportados	Licencia
FOKUS Open IMS Core	HSS, P-CSCF, I-CSCF, S-CSCF	GPL v2
UCT IMS Client	Cliente IMS	GPL v3
UCT Advanced IPTV	IPTV AS básico	GPL v3
UCT IMS Charging Framework	IPTV AS, OCS, CDF	GPL v3
UCT Policy Control Framework	PCRF, PCEF	GPL v3
VideoLAN – VLC Media Player	Media Server	GPL v2
Bind DNS Server	DNS	BSD

La solución de IPTV implementada fue basada en IMS, por lo cual esta memoria extiende los esfuerzos ya realizados en trabajos de títulos previos relacionados al estudio de redes convergentes. El servicio de IPTV utiliza la misma implementación de núcleo IMS utilizado en trabajos de memoria anteriores como: “Diseño e implementación de un proveedor de servicios genérico con arquitectura IMS” de Sebastian Peñaloza. Por lo que se sumaría este servicio a los ya ofrecidos sobre el núcleo IMS.

Otro objetivo era que el Laboratorio de IPTV fuese con fines docentes. Al respecto este trabajo constituye una potente herramienta para la docencia sobre la arquitectura IMS, pudiendo ser aprovechado para definir actividades dentro de un curso sobre arquitecturas de redes convergentes. En el presente documento se entregan todas las instrucciones para levantar y configurar el sistema, así como también se estableció una serie de experiencias que posibilitan el estudio del comportamiento entre elementos de la plataforma y de los principales protocolos involucrados en el funcionamiento del servicio. A través de capturas de tráfico fueron estudiados

mensajes de los principales protocolos involucrados que son: SIP, DIAMETER, RTSP, RTP, RTCP y DNS.

Se realizó una doble implementación del sistema. La primera en una red de área local del Laboratorio de Telecomunicaciones del Departamento de Ingeniería Eléctrica utilizando 6 computadores de escritorio. La segunda, que fue la red de pruebas utilizada en el estudio de este trabajo de titulo, se hizo en un computador personal a través de 11 máquinas virtuales que junto con el sistema operativo host conformaron una red que albergaba los 12 elementos separados que conforman la plataforma de IPTV.

En relación a las características ofrecidas por el servicio, el Laboratorio de IPTV finalmente cuenta con las siguientes características generales que lo convierten en una sólida estación de pruebas de concepto asociadas al servicio de IPTV sobre IMS:

- Capacidad de solicitud de canales en modo live streaming directamente desde el cliente IMS.
- Capacidad de solicitud de contenido VoD directamente desde el cliente IMS.
- Disponibilidad de un NDVR (Network DVR) o también conocido como RS-DVR (Remote Storage Digital Video Recorder).
- Disponibilidad de una EPG (Electronic Program Guide).
- Capacidad de hacer uso de otros servicios como videoconferencias, llamadas VoIP y uso de mensajería instantánea con otro usuario conectado a la plataforma de IPTV directamente desde el cliente IMS.
- Sistema de tarificación del servicio de IPTV a través de asignación de créditos.
- Administración del núcleo IMS desde una interfaz web.
- Administración de un sistema de políticas de control para el núcleo IMS desde una interfaz web.

Este trabajo de memoria puede abrir ciertos trabajos futuros, o dar pie a nuevos trabajos de memoria que implementen más servicios relacionados, o que resuelvan las limitantes de ciertas características implementadas. Por ejemplo, añadir la funcionalidad de DVR al Cliente IMS lo cual permitiría la grabación local de contenido. Otra característica interesante sería que el Cliente IMS tenga el aspecto visual de un Media Center o la interfaz de menús desplegables que se ven a

pantalla completa típicos de los set-top-boxes utilizados en los servicios de televisión de pago, con lo que se conseguiría una agradable interfaz al traspasar la imagen a un televisor obteniéndose la apariencia de un verdadero servicio de IPTV. Entre los problemas relacionados a las características implementadas destacan que la implementación de la EPG es bastante precaria al no disponer de un sistema de actualización online, la interacción con el NDVR no es a través del Cliente IMS y el sistema de políticas de control del núcleo IMS no recibe información del servicio de IPTV, sino que sólo opera con los servicios de videoconferencias o VoIP. Por último mencionar lo vital que es para el Laboratorio de IPTV contar con un completo set de herramientas de software que permita monitorear aspectos de QoS en tiempo real, más allá de sólo ver anchos de banda.

CAPÍTULO VII: BIBLIOGRAFÍA

[1] HJELM, Johan: "Why IPTV? Interactivity, Technologies and Services". Wiley, 2008.

[2] O'DRISCOLL, Gerard: "Next Generation IPTV Services and Technologies". Wiley, 2008.

[3] RAMIREZ, David: "IPTV Security, Protecting High-Value Digital Contents". 2008.

[4] POIKSELKÄ, Miikka; MAYER, Georg: "The IMS, IP Multimedia Concepts and Services", 3rd Edition, Wiley, 2009.

[5] PEÑALOSA, Sebastián: "Diseño e implementación de un proveedor de servicios genérico con arquitectura IMS". Memoria de Título para optar a la carrera de Ingeniero Civil Electricista. Santiago, Chile. Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, Abril 2008.

[6] SAAVEDRA, Diego: "Arquitectura de aplicaciones para redes convergentes". Memoria de Título para optar a la carrera de Ingeniero Civil Electricista. Santiago, Chile. Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, Octubre 2008.

[7] MIRANDA, Javier: "Construcción de laboratorios docentes para arquitectura IMS". Memoria de Título para optar a la carrera de Ingeniero Civil Electricista. Santiago, Chile. Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, Octubre 2008.

[8] ORELLANA, Pablo: "Diseño e Implementación de una plataforma de servicios IP/TV, económica y con fines docentes". Memoria de Título para optar a la carrera de Ingeniero Civil Electricista. Santiago, Chile. Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, Enero 2007.

[9] ROBLES, Cristian: "Diseño e Implementación de una plataforma IP/TV tipo MythTV, económica y con fines docentes". Memoria de Título para optar a la carrera de Ingeniero Civil Electricista. Santiago, Chile. Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, Julio 2008.

[10] PEÑA, Paulina: "Estudio de arquitecturas para la convergencia de telefonía fija-móvil ". Memoria de Título para optar a la carrera de Ingeniero Civil Electricista. Santiago, Chile. Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, Abril 2007.

[11] CARRILLO, Paula: “Diseño de un laboratorio de televisión digital con fines docentes ”. Memoria de Título para optar a la carrera de Ingeniero Civil Electricista. Santiago, Chile. Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, Agosto 2008.

[12] QUIGLEY, Pete: “Separate But Not Equal: A Comparative Overview of PacketCableTM 2.0, IMS and TISPAN”.

[13] CARDONE, Richard: “PACKETCABLE 2.0 and TISPAN – Converging on IMS for a common QoS enabled application core”.

[14] MIKOCZY, Eugen; SIVCHENKO, Dmitry; RAKOCEVIC, Veselin: “IMS based IPTV services - Architecture and Implementation”.

[15] WAITING, David; GOOD, Richard; SPIERS, Richard: “Open Source Development Tools for IMS Research”

[16] DIKGOLE, Lesang; VENTURA, Neco: “Video on Demand Service for Next Generation Networks”.

[17] BERTRAND, Gilles: “The IP Multimedia Subsystem in Next Generation Networks”, Mayo, 2007.

[18] VAN GELDER, A.S.: “Media Security in Open IMS Core”, Julio, 2009.

[19] ÖZÇELEBI, Tanır; RADONOVIĆ, Igor; CHAUDRON, Michel: “Enhancing End-to-End QoS for Multimedia Streaming in IMS-Based Networks”.

[20] SPIERS, Richard; VENTURA, Neco: “An Evaluation of Architectures for IMS Based Video Conferencing”.

[21] NASSER, Nidal; SHANG, Ming: “Policy Control Framework for IP Multimedia Subsystem”.

[22] FRIEDRICH, Oliver; SEELIGER, Robert; ARBANOWSKI, Stefan: “Interactive and personalized Services for an open IMS-based IPTV infrastructure”.

[23] AL-HEZMI, Adel; CARVALHO DE GOUVEIA, Fabricio; MAGEDANZ, Thomas: “Provisioning of Multimedia Services over Open NGN Testbed”.

[24] BRAVO, Danny: “Desarrollo de servicios en IMS”, 2008.

[25] KUTHAN, Jiri; SISALEM, Dorgham: “SIP: More Than You Ever Wanted To Know About”, Marzo, 2007.

[26] PEÑALOZA, Sebastián: “Introducción a IMS: IP Multimedia Subsystem”, Seminario en Tecnologías de TV Digital - HyC Campus LatAm, Diciembre, 2008.

[27] CASTRO, Cesar: “Introducción a IPTV”, Seminario en Tecnologías de TV Digital - HyC Campus LatAm, Diciembre, 2008.

[28] HUERTA, Mario: “Introducción a la TV Digital”, Seminario en Tecnologías de TV Digital - HyC Campus LatAm, Diciembre, 2008.

[29] WELDON, Marcus: “IMS and IPTV, Perfect Together”, Enero, 2006.

[30] 3GPP website: http://www.3gpp.org

[31] IETF website: http://www.ietf.org

[32] Fraunhofer Institute FOKUS. Open IMS Core: http://www.openimscore.org

[33] University of Cape Town. UCT IMS Client: http://uctimsclient.berlios.de

[34] Wikipedia: http://www.wikipedia.org

[35] SIP RFC: http://tools.ietf.org/html/rfc3261

[36] RTSP RFC: http://www.ietf.org/rfc/rfc2326.txt

[37] RTCP RFC: http://tools.ietf.org/html/rfc3550

[38] Mandate and Terms of Reference of FG IPTV Working Groups: http://www.itu.int/ITU-T/IPTV/events/072006/docs/OD/FGIPTV-OD-0001e.doc

[39] Y.2001: General overview of NGN: http://www.itu.int/rec/T-REC-Y.2001-200412-I/en

[40] Consideration on Channel Zapping Time in IPTV Performance Monitoring: http://www.itu.int/md/T05-FG.IPTV-C-0545/en

CAPÍTULO VIII: ACRÓNIMOS

3G	3rd Generation
3GPP	3rd Generation Partnership Project
AAA	AAAnswer
AAA	Authentication, Authorization and Accounting
AAR	AARequest
AGCF	Access Gateway Control Function
ANI	Application-to-Network Interface
AOC	Advice of charge
AS	Application Server
BGCF	Breakout Gateway Control Function
BIND	Berkeley Internet Name Domain
CAPEX	Capital expenditures
CCA	Credit-Control-Answer
CCR	Credit-Control-Request
CDF	Charging Data Function
CDR	Charging Data Record
CEA	Capabilities-Exchange-Answer
CER	Capabilities-Exchange-Request
CM	Cable Modem
CMTS	Cable Modem Termination System
CSCF	Call Session Control Function
DNS	Domain Name Server
DOCSIS	Data Over Cable Service Interface Specification
DRM	Digital Rights Management
DVR	Digital Video Recorder
DWA	Device-Watchdog-Answer
DWA	Device-Watchdog-Answer
DWR	Device-Watchdog-Request
DWR	Device-Watchdog-Request
E-CSCF	Emergency – Call Session Control Function
EDGE	Enhanced Data Rates for Global Evolution
EPG	Electronic Program Guide
ETSI	European Telecommunications Standards Institute
FOKUS	Fraunhofer Institute for Open Communication Systems
GGSN	Gateway GPRS Support Node
GNOME	GNU Network Object Model Environment
GNU	GNU's not Unix!
GSM	Global System for Mobile communications
HFC	Hybrid Fibre-Coaxial
HSS	Home Suscriber Server
HVS	Human Visual System Model
IBCF	Interconnection Border Contol Function
I-CSCF	Interrogating – Call Session Control Function
iFC	Initial Filter Criteria
IMS	IP Multimedia Subsystem
IMS-MGW	IP Multimedia Subsystem – Media Gateway Function
IP	Internet Protocol
IPTV	Internet Protocol Television
IPTVCD	Internet Protocol Televisión Consumer Device
ISDN	Integrated Services Digital Network.
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
ITU-T FG PTV	ITU-T Focus Group on IPTV standardization
LIA	Location-Info-Answer

LIR	Location-Info-Request
LRF	Location Retrieval Function
MAA	Multimedia-Auth-Answer
MAR	Multimedia-Auth-Request
MDI	Media Delivery Index
MGCF	Media Gateway Control Function
MGW	Media Gateway
MMTEL	IMS Multimedia Telephony Service
MOS	Mean Opinion Score
MSO	Multiple System Operator
NASS	Network Attachment Subsystem
NDVR	Network Digital Video Recorder
NGN	Next-Generation Network
OCS	Online Charging System
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
OPEX	Operational Expenditures
OSA-SCS	Open Service Access-Service Capability Server
OSE	Open Source Edition
PC	Personal Computer
PCEF	Policy and Charging Enforcement Point
PCM	Pulse Code Modulation
PCRF	Policy and Charging Rule Function
P-CSCF	Proxy – Call Session Control Function
PES	PSTN/ISDN Emulation Subsystem
PS	Policy Server
PSTN	Public Switched Telephone Network
PVR	Personal Video Recorder
QoE	Quality of Experience
QoS	Quality os Service
RACS	Resource and admisión control subsystem
RAM	Random-access Memory
RAN	Radio Access Network
RS-DVR	Remote Storage Digital Video Recorder
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SAA	Server-Assignment-Answer
SAR	Server-Assignment-Request
SCE	Service Creation Environments
S-CSCF	Serving – Call Session Control Function
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLF	Subscriber Locator Function
SPT	Service Point Trigger
STB	Set-top-box
STR	Session-Termination-Request
TIC	Tecnología de la Información y la Comunicación
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TP	Trigger Point
T-SGW	Trunking Signaling Gateway
TV	Television
UE	User Equipment
UA	User Agent
UAA	User-Authorization-Answer
UAR	User-Authorization-Request

UCT	University of Cape Town
UMTS	Universal Mobile Telecommunications System
UNI	User-to-Network Interface
UPSF	User Profile Server Function
URI	Uniform Resource Identifier
VCC	Voice Call Continuity
VGW	Voice over IP Gateway
VLC	VideoLAN Client
VoD	Video on Demand
VoIP	Voice over Internet Protocol
XML	eXtensible Markup Language

CAPÍTULO IX: ANEXOS

9.1. Descripción de principales protocolos

9.1.1. SIP

SIP (Session Initiation Protocol) es el protocolo de señalización estándar de la IETF (Internet Engineering Task Force) para el manejo de sesiones multimedia cliente-servidor. Sirve para establecer sesiones, modificarlas o terminarlas. Además puede proveer presencia y movilidad. No esta limitado solamente a telefonía sobre Internet, sino que sirve para toda aplicación que tenga noción de sesión como mensajería instantánea o juegos en línea. SIP puede ser usado para iniciar sesiones de voz, video y multimedia para aplicaciones interactivas (llamada de un teléfono IP o una videoconferencia) y no interactivas (video streaming). Existen diversos tipos de mensajes SIP que representan solicitudes y respuestas [35]. Los principales mensajes de petición son:

- INVITE: Solicitud de establecimiento de conexión.
- ACK: Mensaje de acuso de recibo de mensaje.
- BYE: Solicitud de término de sesión.
- CANCEL: Mensaje para cancelar inicio de conexión.
- REGISTER: Solicitud de registro en el servidor Proxy.
- OPTIONS: Consulta de las opciones del servidor.

En tanto, las respuestas a dichas consultas se codifican con números de tres dígitos en un formato similar al del protocolo HTTP:

- 1XX: Mensajes de información (100 Trying, 180 Ringing)
- 2XX: Solicitud exitosa (200 OK)
- 3XX: Reenvío de llamadas (302 temporarily moved, 305 use Proxy)
- 4XX: Mensaje de error (403 Forbidden)
- 5XX: Mensaje de error de servidor (500 Server Internal Error, 501 not implemented)
- 6XX: Falla global (606 Not Acceptable)

9.1.2. DIAMETER

DIAMETER es un protocolo desarrollado por la IETF que provee servicios AAA (Autentificación, Autorización, Accounting) para aplicaciones como el acceso a una red o la movilidad IP. Basado en el protocolo RADIUS, fue desarrollado para ofrecer servicios móviles, dinámicos y flexibles que puedan ser extendidos a nuevas tecnologías de acceso. En base a este protocolo es posible autentificar a un usuario, autorizar el uso de servicios y monitorear las cuenta utilizada [5].

DIAMETER constituye un protocolo peer-to-peer que permite la comunicación entre dos partes Una actúa como Servidor DIAMETER y la otra lo hace como Cliente DIAMETER. El intercambio de mensajes puede ser iniciado tanto por el cliente como por el servidor. Considerando esto, una sesión DIAMETER consiste en el intercambio de comandos y AVPs (Attribute Value Pair), donde los últimos corresponden a colecciones de atributos del mensaje DIAMETER.

Los mensajes DIAMETER definidos en la RFC 3588 son:

- Abort-Session-Request (ASR-274)
- Abort-Session-Answer (ASA-274)
- Accounting-Request (ACR271)
- Accounting-Answer (ACA271)
- Capabilities-Exchange-Request (CER-257)
- Capabilities-Exchange-Answer (CEA-257)
- Device-Watchdog-Request (DWR-280)
- Device-Watchdog-Answer (DWA-280)
- Disconnect-Peer-Request (DPR-282)
- Disconnect-Peer-Answer (DPA-282)
- Re-Auth-Request (RAR-258)
- Re-Auth-Answer (RAA-258)
- Session-Termination-Request (STR-275)
- Session-Termination-Answer (STA-275)

Así como se define el rol de cliente y servidor, DIAMETER establece además el uso de otros agentes:

Cliente: Entidad al borde de la red que ejecuta labores de control de acceso.

Servidor: Maneja la autentificación, autorización y accounting para una red en particular.

Relay Agent: Rutea mensajes DIAMETER basado en la información contenida en ellos. Puede alterar los mensajes únicamente agregando o quitando información de ruteo.

Proxy Agent: También rutea mensajes pero puede modificarlos para aplicar políticas directivas como el control de uso de recursos o de admisión.

Redirect Agent: Redirige mensajes pero lo hace indicando a la otra parte donde debe enviar directamente el mensaje.

Translation Agent: Traduce el protocolo RADIUS a DIAMETER.

El documento RFC 4740: "Diameter SIP Application" establece la aplicación del protocolo DIAMETER en sistemas basados en el protocolo de señalización SIP. Se define la interacción entre los clientes SIP, los servidores SIP y la entidad que actúa como Servidor DIAMETER.

Los comandos DIAMETER definidos en dicho RFC son los siguientes:

- User-Authorization-Request (UAR-283)
- User-Authorization-Answer (UAA-283)
- Server-Assignment-Request (SAR-284)
- Server-Assignment-Answer (SAA-284)
- Location-Info-Request (LIR-285)
- Location-Info-Answer (LIA-285)
- Multimedia-Auth-Request (MAR-286)
- Multimedia-Auth-Answer (MAA-286)
- Registration-Termination-Request (RTR-287)
- Registration-Termination-Answer (RTA-287)

- Push-Profile-Request (PPR-288)
- Push-Profile-Answer (PPA-288)

Cuando un cliente y un servidor establecen una conexión intercambian mensajes **Capabilities-Exchange-Request** y **Capabilities-Exchange-Answer** para conocer la identidad y capacidades de cada uno (versión del protocolo, aplicaciones Diameter soportadas, mecanismos de seguridad, etc.).

Los mensajes **Device-Watchdog-Request** y **Device-Watchdog-Answer** son utilizados para monitorear la conexión establecida y encontrar de forma proactiva posibles fallas en el transporte de datos para evitar el envío innecesario de información.

User-Authorization-Request: Este mensaje es enviado por el cliente Diameter (ubicado dentro de un servidor SIP) hacia el servidor Diameter para pedir autorización para rutear una petición de registro SIP (REGISTER). Debido a que la petición REGISTER implícitamente trae la dirección SIP del cliente para establecer el "binding", se utiliza el mensaje UAR para pedir al servidor Diameter que autorize dicho registro. El servidor puede verificar que dicho usuario es legítimo del sistema.

User-Authorization-Answer: Respuesta enviada por el servidor hacia el cliente Diameter. Indica el resultado de la autorización de registro requerida. Si tuvo éxito se incluye el código asociado a DIAMETER_SUCCESS.

Server-Assignment-Request: El cliente Diameter envía este mensaje para indicar el término del proceso de autentificación y para solicitar al Servidor Diameter que guarde (o elimine) la dirección URI del servidor SIP que este atendiendo al cliente durante el proceso de registro. Típicamente la recepción de un mensaje REGISTER en un servidor SIP provoca que el cliente Diameter en dicho servidor envíe un mensaje SAR.

Server-Assignment-Answer: Corresponde a la respuesta del mensaje SAR enviada desde el servidor hacia el cliente Diameter. Se envía un código que indica el éxito o fracaso de la petición.

Location-Info-Request: El cliente Diameter envía este comando al servidor Diameter solicitando información para el ruteo como la dirección URI del servidor SIP asignado.

Location-Info-Answer: Corresponde a la respuesta del comando anterior.

Multimedia-Auth-Request: El cliente Diameter envía este comando al servidor Diameter para que autentifique y autorize el uso de algún servicio SIP (por ej. una suscripción) por parte de un usuario.

Multimedia-Auth-Answer: Constituye la respuesta a la petición anterior.

9.1.3. RTSP

RTSP es un protocolo no orientado a conexión, en lugar de esto el servidor mantiene una sesión asociada a un identificador, en la mayoría de los casos RTSP usa TCP para datos de control del reproductor y UDP para los datos de audio y vídeo aunque también puede usar TCP en caso de que sea necesario. En el transcurso de una sesión RTSP, un cliente puede abrir y cerrar varías conexiones de transporte hacia el servidor por tal de satisfacer las necesidades del protocolo [36].

De forma intencionada, el protocolo es similar en sintaxis y operación a HTTP de forma que los mecanismos de expansión añadidos a HTTP pueden, en muchos casos, añadirse a RTSP. Sin embargo, RTSP difiere de HTTP en un número significativo de aspectos:

- RTSP introduce nuevos métodos y tiene un identificador de protocolo diferente.
- Un servidor RTSP necesita mantener el estado de la conexión al contrario de HTTP
- Tanto el servidor como el cliente pueden lanzar peticiones.
- Los datos son transportados por un protocolo diferente

Sesión RTSP

- El cliente accede a la URL RTSP para colocar el nombre del servidor y el puerto.
- Si el nombre del servidor no está en formato IP, el cliente hace una consulta DNS para obtener la dirección correspondiente.
- El cliente inicia una conexión TCP hacia el servidor.

- Cuando la conexión está establecida correctamente, el cliente envía al servidor una petición OPTIONS. EL servidor devuelve información que puede incluir la versión de RTSP, la fecha, el número de sesión, el nombre del servidor y los métodos soportados.
- 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.
- 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.
- El cliente inicializa los programas adecuados requeridos para reproducir la presentación.
- El cliente envía una petición PLAY que informa al servidor que ahora es el momento de comenzar a enviar datos.
- 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.
- Cuando la presentación termina o el usuario la para, el cliente envía un SET_PARAMETER que contiene las estadísticas de la sesión.
- El cliente envía TEARDOWN para dar por terminada la conexión con el servidor.

Peticiones RTSP

Las peticiones RTSP están basadas en peticiones HTTP y generalmente son enviadas del cliente al servidor. A continuación se describen las más típicas:

DESCRIBE: Este método obtiene una 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: Especifica como será transportado el flujo de datos, la petición contiene la url del flujo multimedia y una especificación de transporte, esta especificación típicamente incluye un puerto para recibir los datos (audio o video), y otro para los datos RTCP (meta-datos).

El servidor responde confirmando los parámetros escogidos y llena las partes restantes, como los puertos escogidos por el servidor. Cada flujo de datos debe ser configurado con SETUP antes de enviar una petición de PLAY.

PLAY: Una petición de PLAY provocará que el servidor comience a enviar datos de los flujos especificados utilizando los puertos configurados con 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.

9.1.4. RTP

RTP son las siglas de Real-time Transport Protocol (Protocolo de Transporte de Tiempo real). Es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una videoconferencia.

Está desarrollado por el grupo de trabajo de transporte de Audio y Video del IETF, publicado por primera vez como estándar en 1996 como la RFC 1889, y actualizado posteriormente en 2003 en la RFC 3550, que constituye el estándar de Internet STD 64.

Inicialmente se publicó como protocolo multicast, aunque se ha usado en varias aplicaciones unicast. Se usa frecuentemente en sistemas de streaming, junto a RTSP, videoconferencia y sistemas push to talk (en conjunción con H.323 o SIP). Representa también la base de la industria de VoIP [34].

La RFC 1890, obsoleta por la RFC 3551 (STD 65), define un perfil para conferencias de audio y vídeo con control mínimo. La RFC 3711, por otro lado, define SRTP (Secure Real-time Transport Protocol), una extensión del perfil de RTP para conferencias de audio y vídeo que puede usarse opcionalmente para proporcionar confidencialidad, autenticación de mensajes y protección de reenvío para flujos de audio y vídeo.

Va de la mano de RTCP (RTP Control Protocol) y se sitúa sobre UDP en el modelo OSI.

9.1.5. RTCP

RTP Control Protocol es un protocolo de comunicación que proporciona información de control que está asociado con un flujo de datos para una aplicación multimedia (flujo RTP). Trabaja junto con RTP en el transporte y empaquetado de datos multimedia, pero no transporta ningún dato por sí mismo. Se usa habitualmente para transmitir paquetes de control a los participantes de una sesión multimedia de streaming. La función principal de RTCP es informar de la calidad de servicio proporcionada por RTP. Este protocolo recoge estadísticas de la conexión y también información como por ejemplo bytes enviados, paquetes enviados, paquetes perdidos o jitter entre otros. Una aplicación puede usar esta información para incrementar la calidad de servicio (QoS), ya sea limitando el flujo o usando un códec de compresión más baja. En resumen. RTCP se usa para informar de la QoS (Quality of Service). RTCP por sí mismo no ofrece ninguna clase de cifrado de flujo o de autenticación. Para tales propósitos se puede usar SRTCP.

Funciones de RTCP

Información del desarrollo de una aplicación: Esta función es muy útil para aplicaciones de velocidad adaptativa. Un ejemplo de su utilidad seria reducir la congestión mediante el uso de un esquema de compresión más agresivo o enviar un stream de más alta calidad cuando hay poca congestión. También puede resultar útil para diagnosticar problemas de red [37].

Correlacionar y sincronizar diferentes media streams procedentes del emisor: Aquí es muy importante establecer la diferencia entre el identificador de fuente de sincronización de RTP, el SSRC y el CNAME del RTCP. Por ejemplo, un stream de audio y vídeo procedentes del mismo emisor utilizan diferentes SSRC, puesto que en el caso contrario se podrían dar colisiones de identificadores SSRC. Para solucionar este problema, RTCP utiliza el concepto de nombre canónico (CNAME) que se asigna al emisor. Este CNAME es asociado a varios valores SSRC. Así se garantiza que streams que no tienen el mismo SSRC se puedan sincronizar y ordenar correctamente.

Transferir la identidad de un emisor: Se transmite en el paquete de descripción de la fuente explicado más adelante en el apartado Tipo de paquetes.

9.2. Creación de una máquina virtual conectada a una LAN

Esta guía muestra como crear una máquina virtual con una dirección IP visible en la LAN a la que pertenece su host. El software de virtualización utilizado es VirtualBox OSE 3.0.8.

El contenido de esta guía se encuentra en el archivo “Extensión_Anexos.doc” al interior del disco que viene adjunto con esta memória.

9.3. Instalación y configuración del Laboratorio de IPTV

A continuación se presenta una guía para la instalación y puesta en marcha del Laboratorio de IPTV que utiliza la arquitectura IMS como base del sistema. Se incluyen los pasos a seguir para obtener un adecuado entorno de desarrollo, instalar los elementos que componen el sistema y realizar las configuraciones pertinentes de modo de disponer de una plataforma adecuada para el análisis y estudio que este trabajo de título busca realizar.

Todos los componentes que conforman el Laboratorio de IPTV se ejecutan sobre el sistema operativo GNU/Linux. Las instrucciones que en esta guía se enuncian fueron hechas para la distribución Ubuntu 8.04 (Hardy Heron), sin embargo son extensibles y aplicables a otras distribuciones de GNU/Linux si quien las ejecuta posee los conocimientos adecuados. La razón de elegir Ubuntu para la implementación por sobre otras distribuciones de GNU/Linux, como por ejemplo Debian GNU/Linux, es que el software que compone el sistema de IPTV, a excepción del núcleo IMS y el Media Server, ha sido exclusivamente probado y corroborado su funcionamiento en esta distribución por parte de sus desarrolladores. Es por lo tanto requisito para seguir las instrucciones tener conocimientos previos en el sistema operativo GNU/Linux, tales como saber sobre uso de terminales, instalar paquetes binarios, compilar programas y configurar el acceso a la red.

La instalación se hará por etapas, las primeras consistirán en el levantamiento gradual de todos los procesos corriendo en una misma máquina. Finalizado esta labor, se espera obtener un completo y correcto funcionamiento del sistema dadas las configuraciones por defecto que trae cada componente. De esta manera se evitan dificultades generadas por la personalización del

sistema o por la configuración de la red. Posteriormente se explicita como se debe replicar cada parte del sistema en una red de área local de modo de tener cada componente corriendo en computadores distintos. Se terminará con las configuraciones específicas de cada elemento que personalizarán la plataforma.

Las etapas son las siguientes:

9.3.1. Preparación del computador y sistema operativo

9.3.2. Instalación y configuración de Núcleo y Cliente IMS

9.3.3. Instalación y configuración de Sistema de IPTV básico

9.3.4. Instalación y configuración de Sistema de Tarificación

9.3.5. Instalación y configuración de Sistema de Políticas de Control

9.3.6. Implementación distribuida y personalización del Laboratorio de IPTV

El contenido de esta guía se encuentra en el archivo “Extensión_Anexos.doc” al interior del disco que viene adjunto con esta memória.

9.4. Guía de experiencias para el Laboratorio de IPTV

La siguiente guía de experiencias ha nacido a partir de las pruebas realizadas en el Laboratorio de IPTV. Su finalidad es servir de apoyo al estudio de los distintos componentes que constituyen el sistema y de los protocolos involucrados en la comunicación que se da bajo la arquitectura IMS. La topología de red implementada es la siguiente:

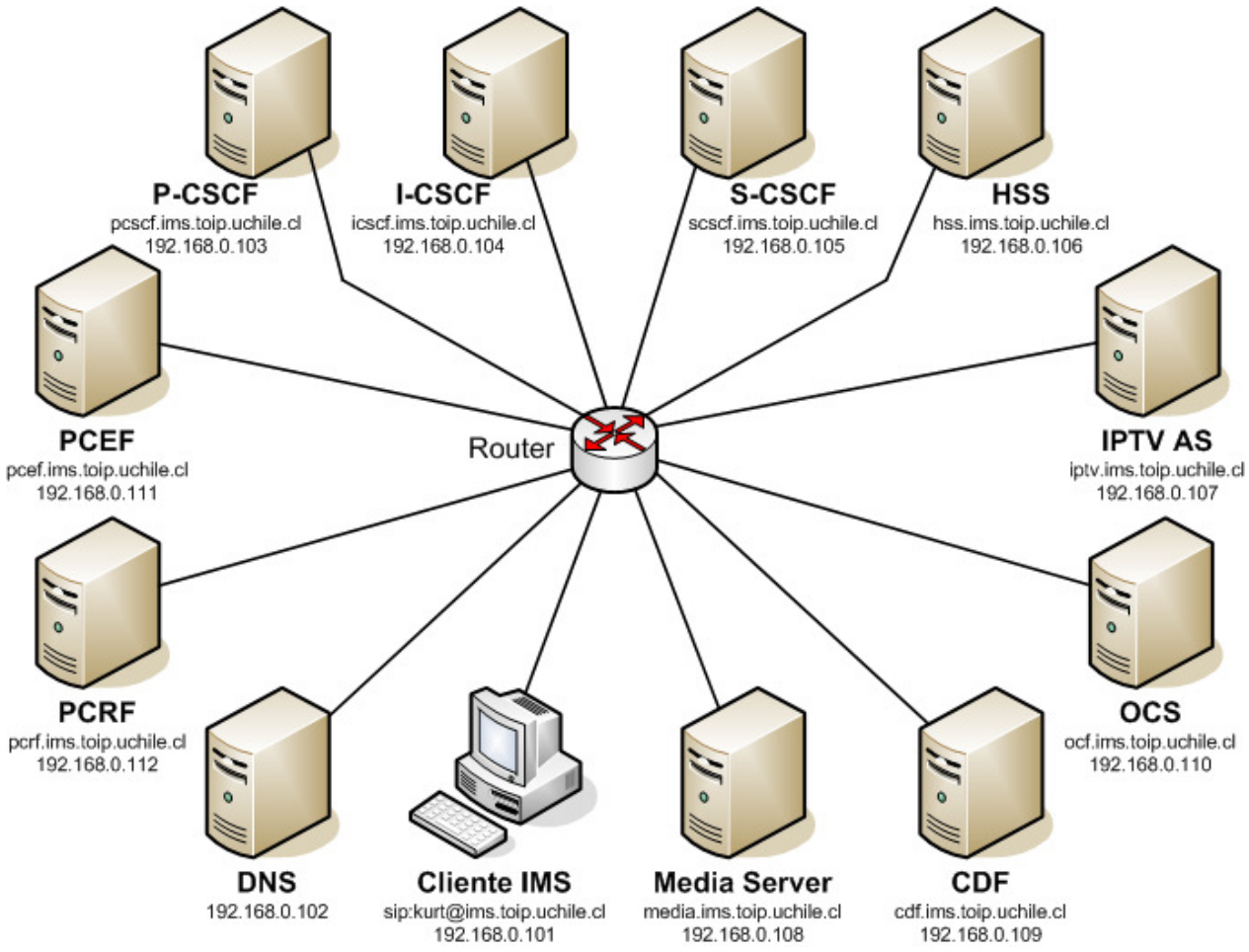

Figura 17: Topología de red del Laboratorio de IPTV.

El estudio de las comunicaciones entre componentes es realizado a partir de la captura y reconocimiento de paquetes que son enviados en la red. El software de análisis de protocolos utilizado en esta experiencia fue Wireshark versión 1.2.2. En el análisis de las capturas de paquetes han sido ignorados los relacionados con labores de administración de la red de área local como ARP, poniendo atención solo en los paquetes de los protocolos relevantes para el estudio, que son: DIAMETER, SIP, RSTP, RTCP y RTP.

9.4.1. Experiencia 1: Inicio del Laboratorio de IPTV

En esta experiencia se analiza el tráfico generado durante el inicio de los componentes que conforman el Laboratorio de IPTV. La siguiente tabla muestra las direcciones de las interfaces donde se realiza cada captura y los nombres de los archivos que contienen las capturas de tráfico de paquetes obtenidas para cada elemento:

Tabla 8: Archivos de captura para Experiencia 1.

Elemento	Dirección de interfaz de captura	Archivo de captura
Cliente IMS	192.168.0.101	exp1-client.pcap
DNS	192.168.0.102	exp1-dns.pcap
P-CSCF	192.168.0.103	exp1-pcscf.pcap
I-CSCF	192.168.0.104	exp1-icscf.pcap
S-CSCF	192.168.0.105	exp1-scscf.pcap
HSS	192.168.0.106	exp1-hss.pcap
IPTV AS	192.168.0.107	exp1-iptvas.pcap
Media Server	192.168.0.108	exp1-media.pcap
CDF	192.168.0.109	exp1-cdf.pcap
OCS	192.168.0.110	exp1-ocs.pcap
PCEF	192.168.0.111	exp1-pcef.pcap
PCRF	192.168.0.112	exp1-pcrf.pcap

En primer lugar se revisa la captura de la interfaz del servidor DNS (exp1-dns.pcap). A partir de dicha captura se genera un análisis gráfico de las peticiones que han sido recibidas por el servidor DNS.

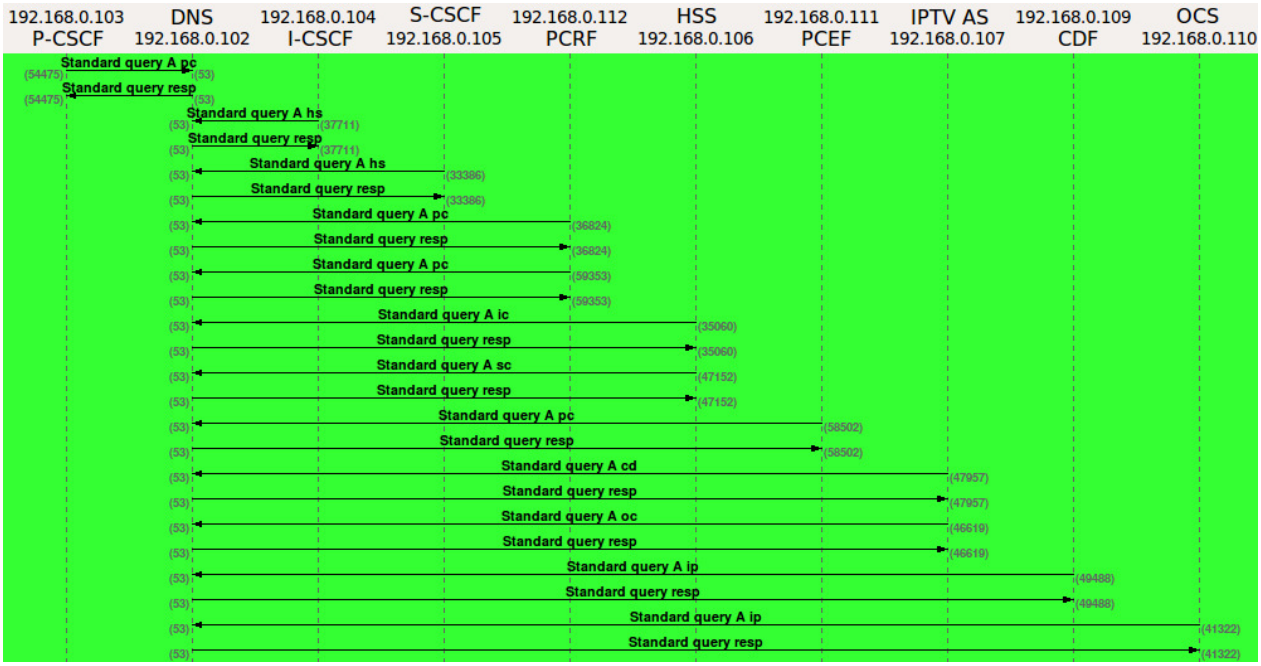

Figura 18: Gráfico de flujo de consultas de DNS en Experiencia 1.

En la figura anterior se observa que:

1. P-CSCF consulta al DNS la dirección IP asociada a pcrf.ims.toip.uchile.cl.
2. I-CSCF consulta al DNS la dirección IP asociada a hss.ims.toip.uchile.cl.
3. S-CSCF consulta al DNS la dirección IP asociada a hss.ims.toip.uchile.cl.
4. PCRF consulta al DNS la dirección IP asociada a pcef.ims.toip.uchile.cl y luego la asociada a pcscf.ims.toip.uchile.cl.
5. HSS consulta al DNS la dirección IP asociada a icscf.ims.toip.uchile.cl y luego la asociada a scscf.ims.toip.uchile.cl.
6. PCEF consulta al DNS la dirección IP asociada a pcrf.ims.toip.uchile.cl.
7. IPTV AS consulta al DNS la dirección IP asociada a cdf.ims.toip.uchile.cl y luego la asociada a ocf.ims.toip.uchile.cl.
8. CDF consulta al DNS la dirección IP asociada a iptv.ims.toip.uchile.cl.
9. OCS consulta al DNS la dirección IP asociada a iptv.ims.toip.uchile.cl.

Así mismo, al revisar la captura de la interfaz asociada al HSS (exp1-hss.pcap) se observa tráfico de mensajes DIAMETER. Si se genera un gráfico de flujo se obtiene lo siguiente:

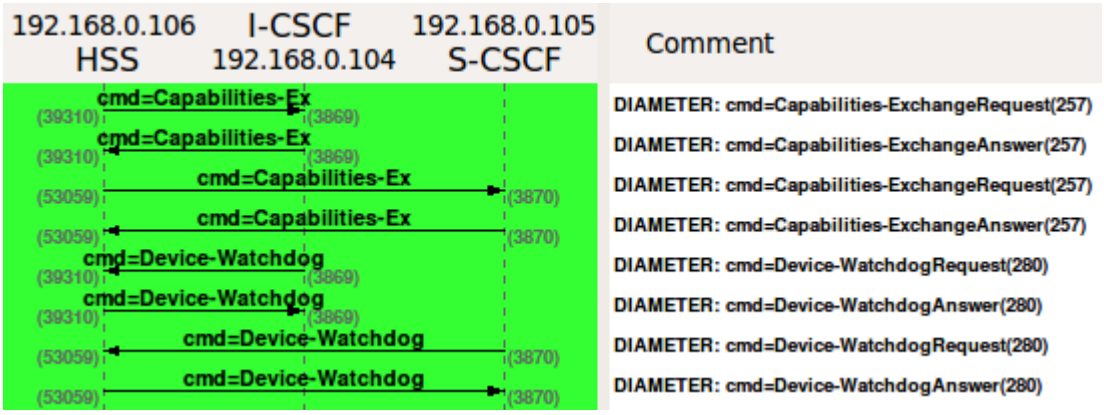

Figura 19: Gráfico de flujo basado en exp1-hss.pcap.

Con la gráfica anterior se comprueba que las entidades I-CSCF y S-CSCF se comunican mediante el protocolo DIAMETER con el HSS. Los tipos de comandos DIAMETER observados son los siguientes:

- Capabilities-Exchange-Request (CER)
- Capabilities-Exchange-Answer (CEA)
- Device-Watchdog-Request (DWR)
- Device-Watchdog-Answer (DWA)

Los comandos CER y CEA permiten al I-CSCF y S-CSCF identificarse con el HSS. De esta manera se identifican intercambiando información relativas a sus capacidades como la versión del protocolo utilizado, aplicaciones DIAMETER soportadas, etc., con el fin de establecer la comunicación entre ellos. Los comandos DWR y DWA permiten monitorear constantemente la comunicación entre peers DIAMETER con el fin de encontrar posibles fallas en el transporte de datos.

Al revisar la captura de la interfaz asociada al PCRF (exp1-pcrf.pcap) también se observa tráfico de mensajes DIAMETER. Al generar un gráfico de flujo se obtiene lo siguiente:

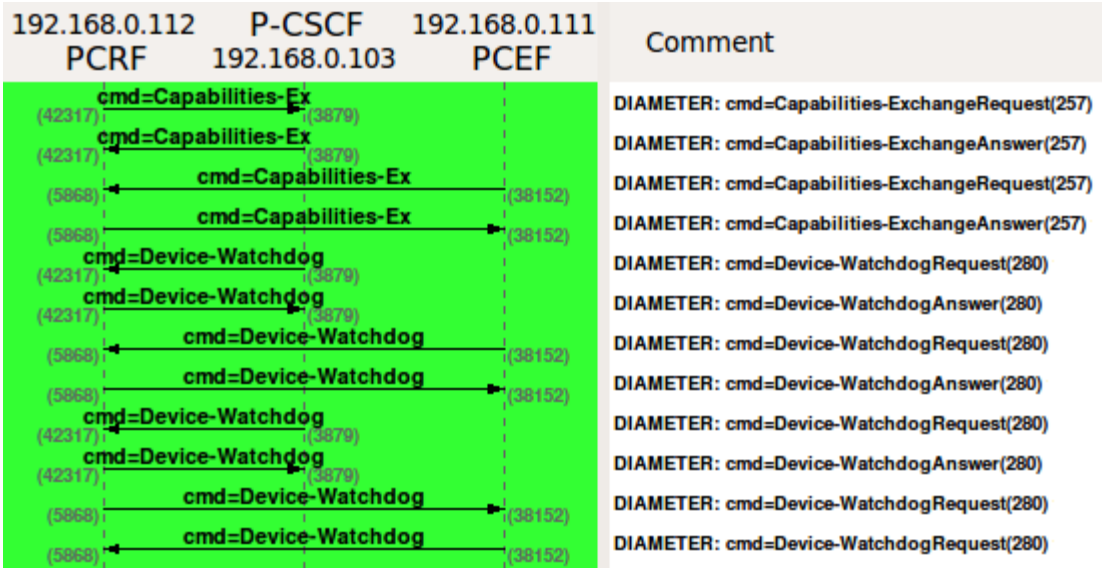

Figura 20: Gráfico de flujo basado en exp1-pcrf.pcap.

Al observar el gráfico anterior se observa el mismo comportamiento antes mencionado para el HSS, I-CSCF y S-CSCF. Al revisar la captura de la interfaz asociada al IPTV AS (exp1-iptv.pcap) también se observa tráfico de mensajes DIAMETER. Si se genera un gráfico de flujo se obtiene lo siguiente:

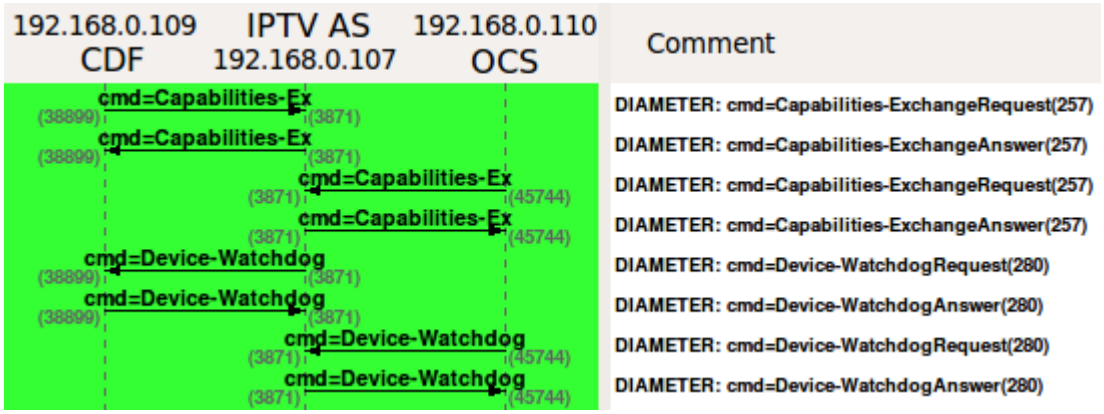

Figura 21: Gráfico de flujo basado en exp1-iptvas.pcap.

Nuevamente se observa el mismo comportamiento para el flujo de mensajes DIAMETER. Al analizar el resto de las capturas es posible filtrar los mensajes DIAMETER que estas entidades intercambian con el HSS reflejando los mismos resultados que ya se han analizado. Así mismo se comprueba que no existe tráfico SIP por estas entidades durante el inicio del sistema. Finalmente

es posible realizar un esquema de los protocolos de comunicación relevantes que están presentes durante el inicio del sistema.

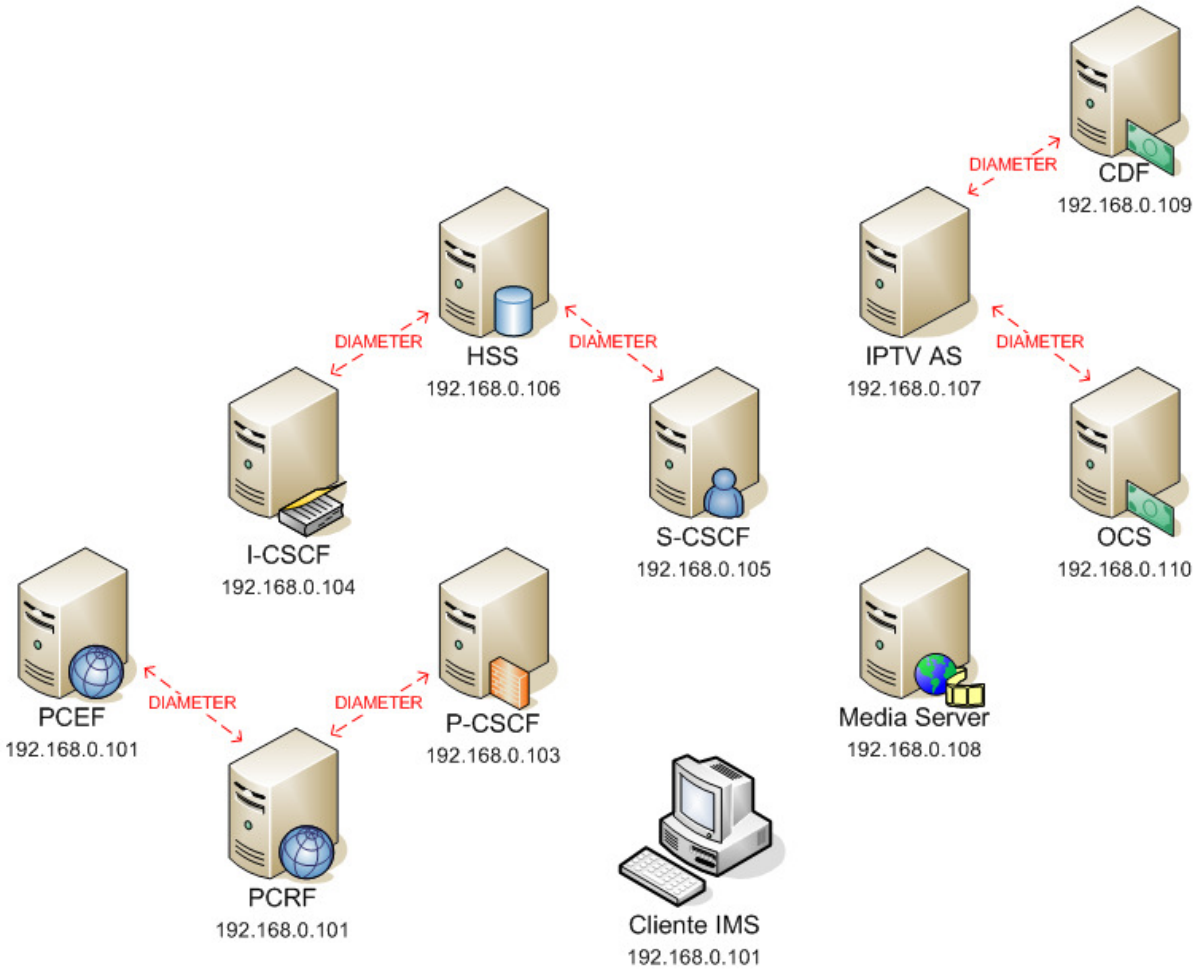

Figura 22: Presencia de protocolos en Experiencia 1.

En consecuencia, se tiene que al iniciarse el sistema solo intercambian mensajes los elementos que utilizan el protocolo DIAMETER estableciendo sus comunicaciones y luego manteniéndose a la espera de algún suceso como podría ser que un usuario se registre a través del Cliente IMS lo cual se analizará en la siguiente experiencia.

9.4.2. Experiencia 2: Inicio de sesión en el Laboratorio de IPTV

En esta experiencia se estudia el tráfico generado entre los elementos de la red durante el proceso de registro del Cliente IMS en el sistema. Las interfaces monitoreadas para esta prueba son las siguientes:

Tabla 9: Archivos de captura para Experiencia 2.

Elemento	Dirección de interfaz de captura	Archivo de captura
DNS	192.168.0.102	exp2-dns.pcap
Conexión Puente (Bridge)	192.168.0.108	exp2-bridge.pcap

Dado que se desea observar la secuencia con la que se intercambian mensajes las entidades durante el proceso de registro, se vuelve complicado intentar determinar el orden de los mensajes si se observan las capturas de cada elemento por separado. Es por esto que aprovechando que las tarjetas de red de las máquinas virtuales están configuradas utilizando la tarjeta del sistema operativo Host como adaptador puente (bridge), es que se vuelve muy útil hacer una captura utilizando Wireshark con la opción de "Captura de paquetes en modo promiscuo" sobre la interfaz de la tarjeta de red del Host. De esta manera se capturará todo el tráfico de paquetes de la red y se podrá graficar la secuencia de mensajes completa entre los elementos que conforman el Laboratorio de IPTV.

En primer lugar, al observar el archivo de captura exp2-dns.pcap se puede apreciar la secuencia de consultas al DNS que se presenta en el gráfico de flujo siguiente.

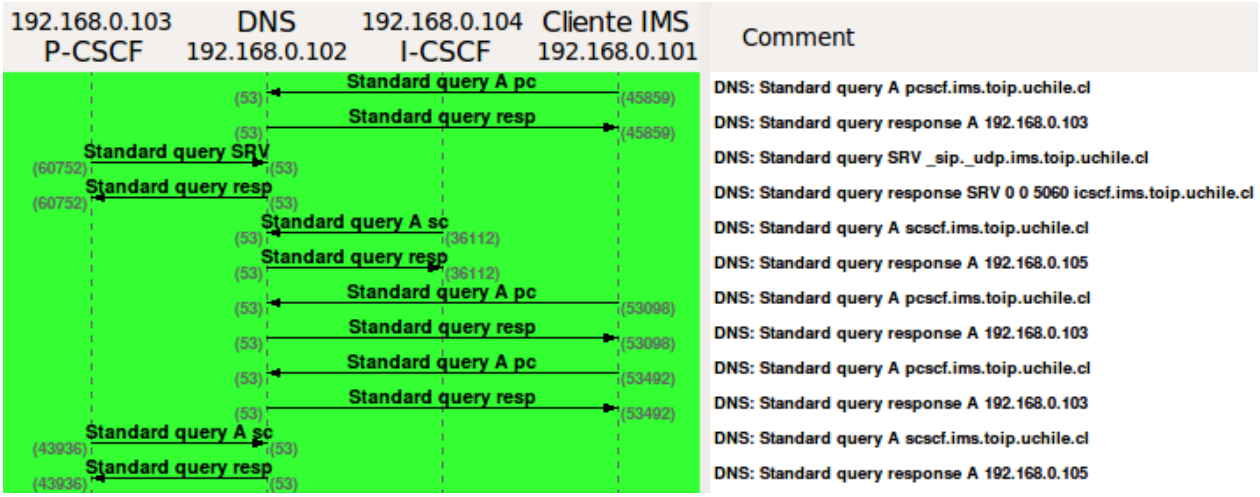

Figura 23: Gráfico de flujo de consultas de DNS en Experiencia 2.

El servidor DNS recibe las siguientes consultas durante el registro:

1. Cliente IMS consulta al DNS la dirección IP asociada a pcscf.ims.toip.uchile.cl
2. P-CSCF consulta al DNS por _sip._udp.ims.toip.uchile.cl, cuya respuesta es icscf.ims.toip.uchile.cl puerto 5060.
3. I-CSCF consulta al DNS la dirección IP asociada a scscf.ims.toip.uchile.cl
4. P-CSCF consulta al DNS la dirección IP asociada a scscf.ims.toip.uchile.cl

A diferencia del inicio del sistema, en el proceso de registro el HSS no realiza consultas DNS. El Cliente IMS Consulta por la dirección del P-CSCF porque es su punto de acceso al sistema. El I-CSCF consulta la dirección del S-CSCF para poder reenviar la petición de tipo SIP REGISTER. Con la última consulta el P-CSCF se prepara para el registro del cliente al identificar el servidor donde deberá redirigir el mensaje SIP SUSCRIBE.

A partir de la captura de tráfico de paquetes de la red obtenida en exp2-bridge.pcap se han graficado por etapas los mensajes que intercambian los elementos que participan en el registro del Cliente IMS. La primera etapa en que el Cliente IMS de autentifica se muestra a continuación:

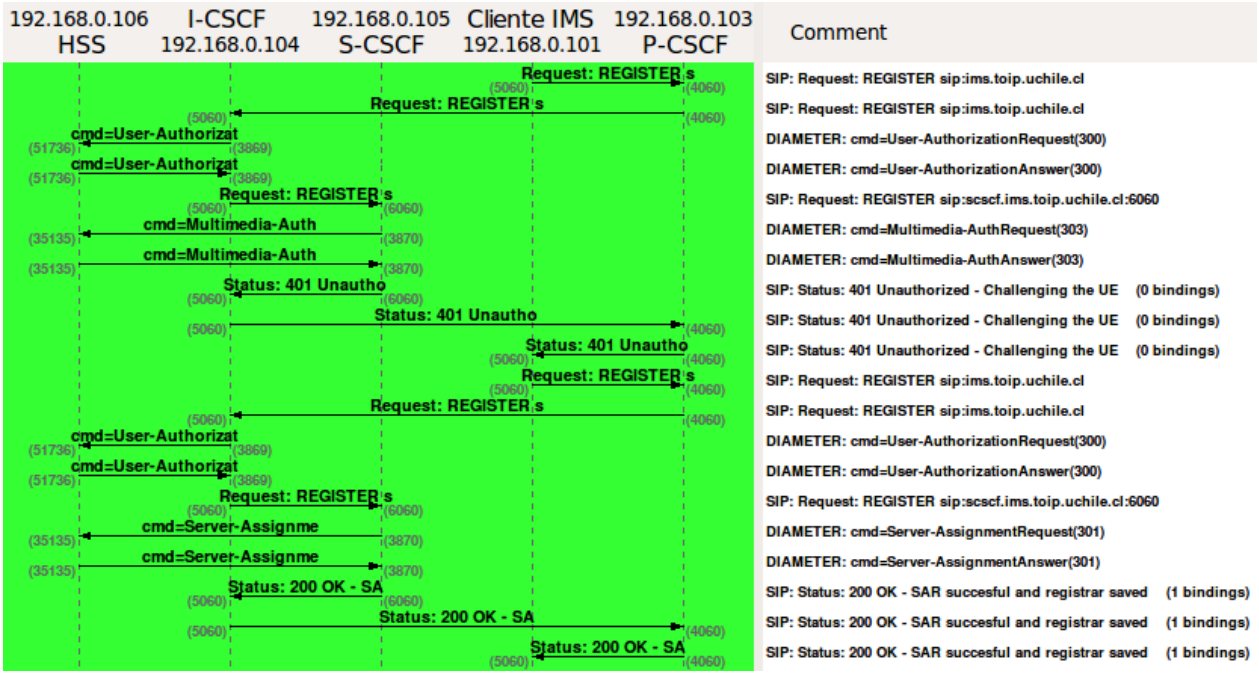

Figura 24: Gráfico de flujo de mensajes en Experiencia 2 - Primera etapa.

Considerando el intercambio de mensajes SIP y DIAMETER es posible explicar la primera etapa del proceso de registro:

1. El cliente envía SIP REGISTER al P-CSCF para iniciar el registro en el sistema.
2. El mensaje REGISTER es reenviado desde el P-CSCF hacia el I-CSCF.
3. El I-CSCF intercambia comandos DIAMETER UAR y UAA con el HSS para saber a que S-CSCF redirigir la petición SIP.
4. El mensaje REGISTER es reenviado desde el I-CSCF al S-CSCF.
5. El S-CSCF intercambia comandos MAR y MAA con el HSS para solicitar la autentificación de usuario.
6. El S-CSCF desafía al Cliente IMS a través del 401 Unauthorized enviando un valor "nonce".
7. El cliente IMS utiliza este valor único y las credenciales de usuario para generar a través de un algoritmo AKA la respuesta que es insertada en una segunda petición de REGISTER.
8. El mensaje REGISTER llega al I-CSCF a través del P-CSCF.
9. El I-CSCF intercambia nuevamente comandos UAR y UAA y se reenvía el REGISTER hacia el S-CSCF.

10. El S-CSCF intercambia comandos DIAMETER SAR y SAA donde se le solicita al HSS que guarde la dirección URI del Cliente IMS asociándola con su Public User Identity.
11. El S-CSCF envía un 200 OK a través del P-CSCF al Cliente IMS con lo que se termina la autentificación del usuario.

Siguiendo con el proceso de registro del Cliente IMS en el Laboratorio de IPTV, se presenta la continuación y segunda etapa de los mensajes enviados entre los elementos a través de un gráfico de flujo.

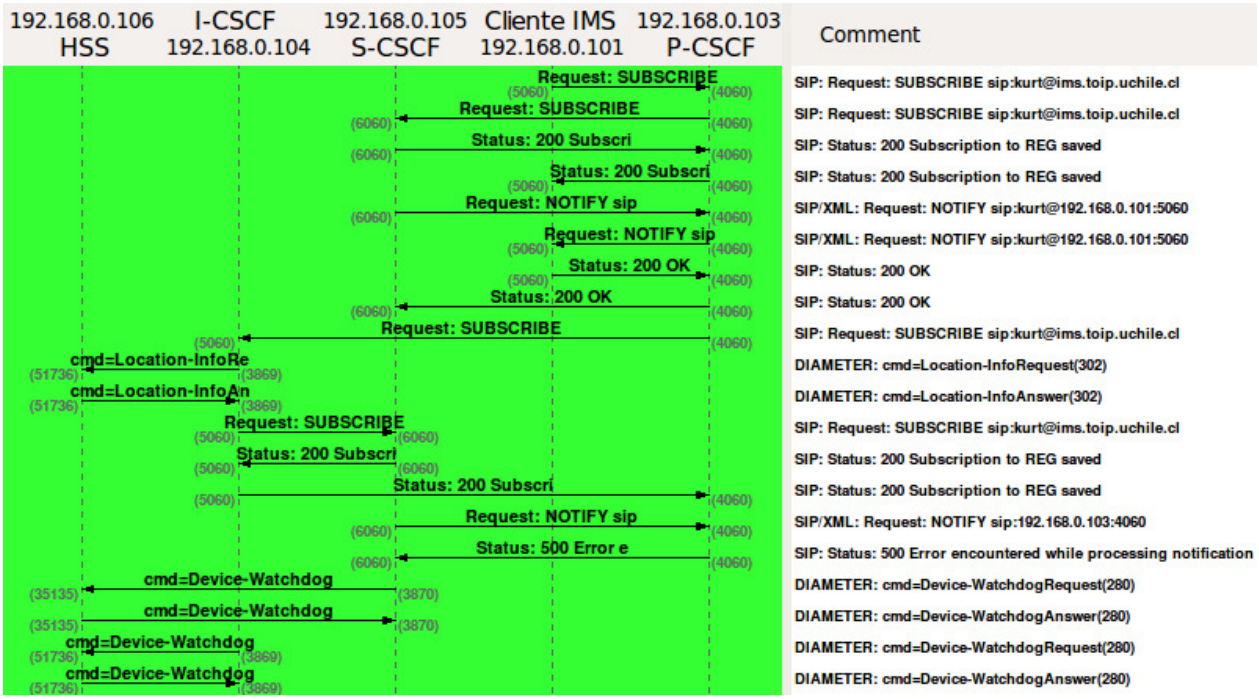

Figura 25: Gráfico de flujo de mensajes en Experiencia 2 - Segunda etapa.

Considerando el intercambio de mensajes SIP y DIAMETER es posible explicar la segunda etapa del proceso de registro:

1. Una vez efectuadas las peticiones SIP REGISTER, el cliente envía un mensaje SIP SUBSCRIBE hacia el P-CSCF.
2. El P-CSCF reenvía la petición al S-CSCF.
3. El S-CSCF responde con un 200 Subscription al Cliente IMS que viaja a través del P-CSCF con lo que se termina la suscripción.

4. El S-CSCF envía un mensaje SIP NOTIFY que contiene en el campo Body del paquete información codificada en XML relativa al registro del usuario.
5. El Cliente IMS responde con un 200 OK.
6. El P-CSCF envía un SIP SUBSCRIBE al I-CSCF.
7. Los comandos LIR y LIA se intercambian entre el I-CSCF y el HSS para consultar información de ruteo como la dirección URI del S-CSCF.
8. El I-CSCF reenvía la petición SUBSCRIBE al S-CSCF.
9. El S-CSCF responde al P-CSCF a través del I-CSCF con un 200 Subscription.
10. El S-CSCF envía un mensaje NOTIFY, que el P-CSCF responde con un 500 Error porque encuentra un error en el formato en vez de responder con un 200 OK. Esto no afecta el proceso.

En ocasiones que el I-CSCF y el S-CSCF reciben un mensaje SIP, estos realizan una consulta DIAMETER al HSS para poder contestar. Analizando el gráfico de flujo, se detectaron los siguientes tipos de comandos DIAMETER intercambiados:

- User-Authorization-Request (UAR)
- User-Authorization-Answer (UAA)
- Multimedia-Auth-Request (MAR)
- Multimedia-Auth-Answer (MAA)
- Server-Assignment-Request (SAR)
- Server-Assignment-Answer (SAA)
- Location-Info-Request (LIR)
- Location-Info-Answer (LIA)
- Device-Watchdog-Request (DWR)
- Device-Watchdog-Answer (DWA)

Finalmente se puede apreciar el esquema global de comunicaciones que se da en la plataforma durante este proceso.

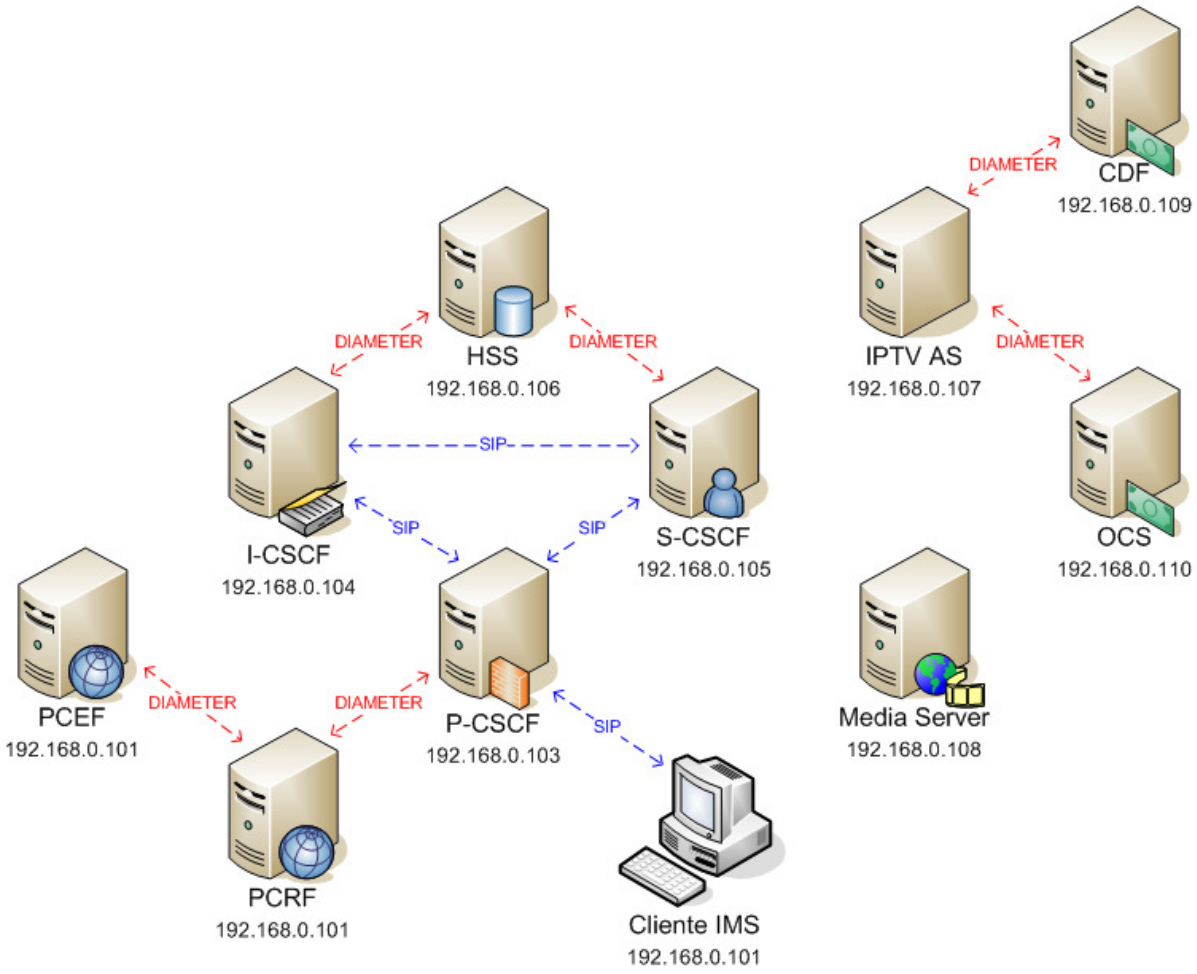

Figura 26: Presencia de protocolos en Experiencia 2.

A diferencia de la experiencia anterior, aquí se aprecia la aparición del protocolo SIP en las comunicaciones presentes en el Cliente IMS y el CSCF. Sin embargo el IPTV AS junto con los módulos de tarificación, así como también los elementos encargados de aplicar las políticas de control sólo intercambian durante este proceso mensajes DIAMETER Device-Watchdog para mantener contacto. También se aprecia como el Cliente IMS se comunica exclusivamente con el P- CSCF.

9.4.3. Experiencia 3: Solicitud de un canal de IPTV e inicio de tarificación.

En esta experiencia se estudiarán los protocolos involucrados en la solicitud de un canal de IPTV por parte del Cliente IMS y el consecuente inicio de tarificación. Durante este proceso se pondrá en marcha el sistema de tarificación online proporcionado por el OCS. A continuación se presentan las interfaces de captura de esta prueba.

Tabla 10: Archivos de captura para Experiencia 3.

Elemento	Dirección de interfaz de captura	Archivo de captura
DNS	192.168.0.102	exp3-dns.pcap
Conexión Puente (Bridge)	192.168.0.108	exp3-bridge.pcap

A partir del archivo de captura exp3-dns.pcap se puede apreciar la secuencia de consultas al DNS que se presenta en el gráfico de flujo siguiente.

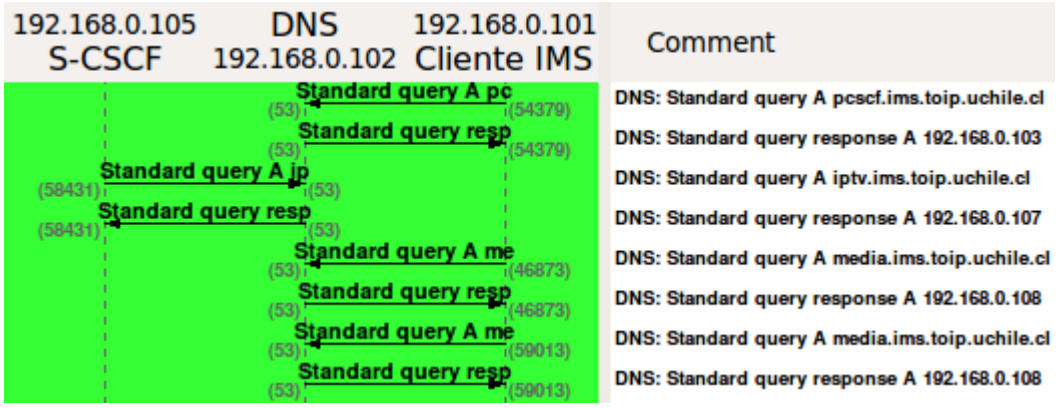

Figura 27: Gráfico de flujo de consultas de DNS en Experiencia 3.

El servidor DNS recibe las siguientes consultas durante la solicitud del canal de IPTV:

- Cliente IMS consulta al DNS la dirección IP asociada a pcscf.ims.toip.uchile.cl
- S-CSCF consulta al DNS la dirección IP asociada a iptv.ims.toip.uchile.cl
- Cliente IMS consulta al DNS la dirección IP asociada a media.ims.toip.uchile.cl en dos ocasiones.

Estas consultas de DNS comienzan con la solicitud del Cliente IMS que necesita comunicarse con el resto de la plataforma de IPTV, siendo su punto de acceso el P-CSCF. Por otra parte, se tiene que por primera vez el núcleo IMS necesita un servicio que proporciona el IPTV AS, razón por la que el S-CSCF necesita la dirección del IPTV AS. Por último se tiene que el Cliente IMS necesita la dirección del Media Server para poder hacer la solicitud del streaming de audio y video.

A partir de la captura de tráfico de paquetes obtenida en exp3-bridge.pcap se han realizado dos gráficos representando las etapas de la secuencia de mensajes que intercambian los elementos que participan en esta experiencia. La primera etapa se presenta a continuación:

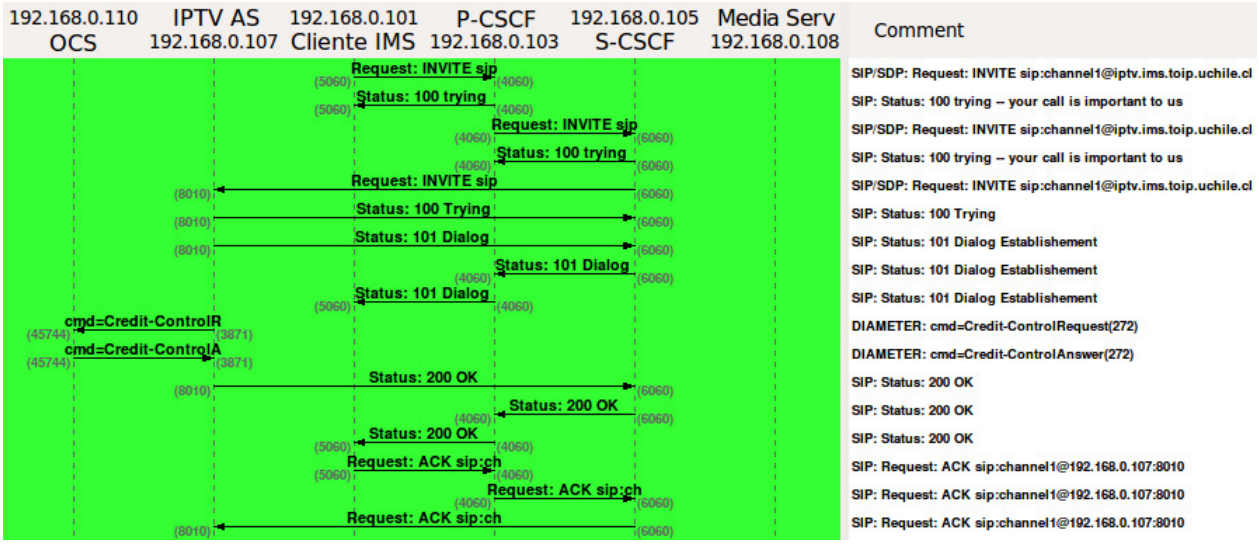

Figura 28: Gráfico de flujo de mensajes en Experiencia 3 - Primera etapa.

Considerando el intercambio de mensajes SIP y DIAMETER es posible explicar esta primera etapa en la solicitud de un canal de IPTV:

1. El cliente realiza una petición INVITE con la dirección del canal channel1@iptv.ims.toip.uchile.cl, a través del P-CSCF y el S-CSCF.
2. Mientras este mensaje SIP se transmite al IPTV AS por medio del S-CSCF, el P-CSCF devuelve al Cliente IMS un 100 Trying que indica que su solicitud está en proceso, y de la misma forma el S-CSCF lo hace con el P-CSCF.

3. Después de que el S-CSCF devuelve el mensaje de 100 Trying, este envía de vuelta un mensaje 101 Dialog que llega hasta el cliente IMS para que siga a la espera de la confirmación final.
4. Mientras tanto en el IPTV AS el Charging Trigger Function provoca que se inicie la tarificación. El IPTV AS se comunica utilizando DIAMETER con el OCS a través de un comando DIAMETER Credit-Control-Request que incluye un AVP del tipo CC-Request-Type con el valor INITIAL_REQUEST para que se de inicio a la tarificación.
5. Una vez que el IPTV AS recibe la respuesta del OCS a través de un mensaje Credit-Control-Answer que contiene en un AVP Check-Balance-Result la asignación de créditos iniciales, el IPTV AS envía el mensaje SIP de 200 OK que contiene la dirección RTSP del Media Server al cual el Cliente IMS tendrá que solicitar el canal posteriormente.
6. El mensaje de 200 OK pasa por el S-CSCF y el P-CSCF hasta el Cliente IMS dando por terminada esta primera etapa de solicitud del canal de IPTV.
7. El Cliente IMS envía un ACK al IPTV AS a través del P-CSCF.

Después de que se dio inicio a la tarificación y el Cliente IMS recibió la dirección RTSP del canal de IPTV, comienza la etapa en que el Cliente IMS se comunicará con el Media Server para que le envíe por protocolo RTP el contenido de audio y video. Esto se aprecia en el siguiente gráfico de flujo de paquetes de datos.

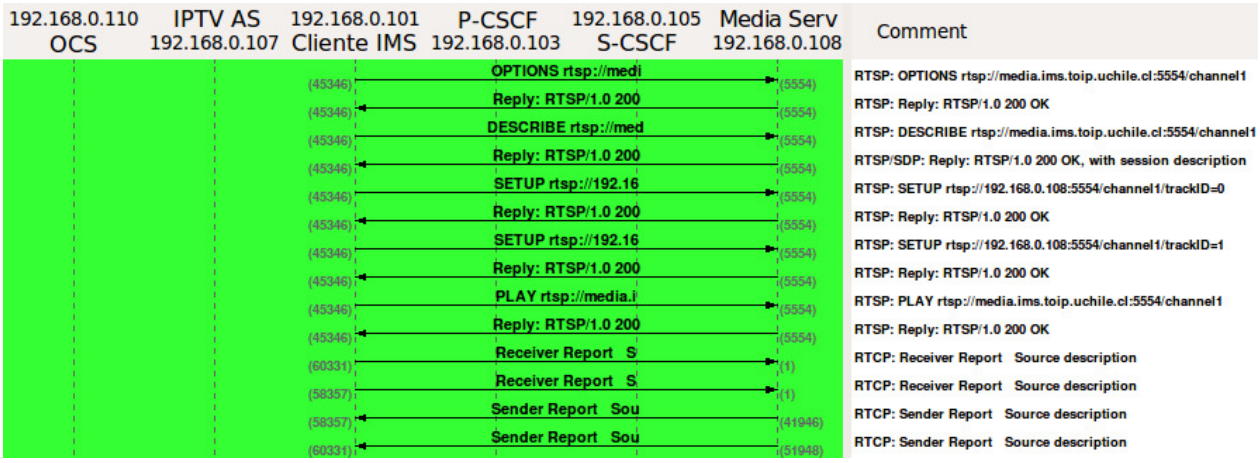

Figura 29: Gráfico de flujo de mensajes en Experiencia 3 - Segunda etapa.

Luego comienza la comunicación directamente con el servidor de contenidos, iniciándose la comunicación bajo el protocolo RTSP entre el Cliente IMS y el Media Server.

1. El cliente IMS comienza enviando un mensaje RTSP OPTIONS con el canal de IPTV
2. El cual es respondido por un 200 OK.
3. Inmediatamente después el cliente envía una petición DESCRIBE
4. El Media Server responde con un mensaje RTSP/SDP 200 OK que contiene una descripción del recurso solicitado, en particular que se debe establecer dos flujos: uno para audio y otro para video.
5. Después se envían un par de mensajes SETUP al Media Server, uno para el audio y otro para el video que se transmitirán, a los que son respondidos por un 200 OK de parte del Media Server. Este proceso se realiza para informar al Media Server como será transportado el flujo de datos.
6. Luego, para comenzar con la transmisión, el Cliente IMS envía una petición PLAY provocando que el servidor comience a enviar datos de los flujos especificados utilizando los puertos configurados previamente cuando se utilizó el comando SETUP.
7. Durante la transmisión de paquetes RTP, que han sido filtrados en el gráfico anterior para que no aparezcan, se envían y reciben periódicamente mensajes Reportes RTCP sobre el estado de la transmisión.

A continuación se presenta un gráfico exclusivo para el intercambio de mensajes RTP que se da entre el Cliente IMS y el Media Server.

Figura 30: Gráfico de flujo RTP en Experiencia 3.

Se aprecia en el gráfico anterior como son enviados los paquetes unidireccionalmente desde el Media Server al Cliente IMS. Los paquetes RTP marcados como PT=DynamicRTP-Type96 corresponden a los paquetes que contienen la información del contenido de video mientras que

los marcados como PT=MPEG-I/II Audio corresponden a la transmisión de audio en este ejemplo.

Cuando se inicia la tarificación para realizar la transmisión de audio y video, el IPTV AS intercambia con el OCS los siguientes tipos de comandos DIAMETER:

- Credit-Control-Request (CCR)
- Credit-Control-Answer (CCA)

Finalmente se puede apreciar el esquema global de comunicaciones que se da en la plataforma durante este proceso.

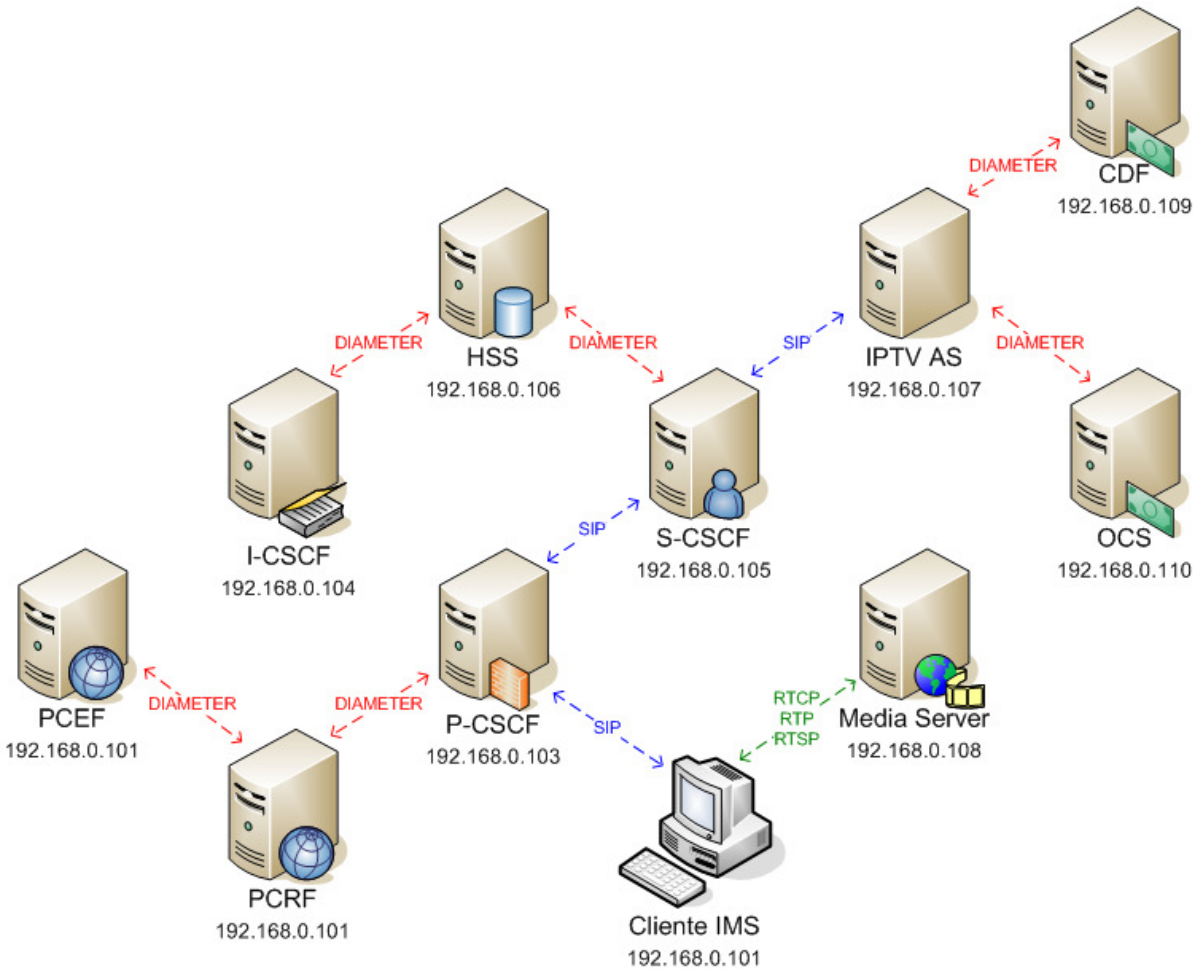

Figura 31: Presencia de protocolos en Experiencia 3.

En esta prueba aparecen por primera vez los protocolos RTSP, RTCP y RTP en el sistema, debido a que se transmite el contenido de audio y video desde el Media Server al Cliente IMS. El PCRF y PCEF no interactúan con el resto del sistema más allá de intercambiar mensajes DIAMETER del tipo Device-Watchdog. Además se apreció que el I-CSCF y el HSS tampoco se hacen presentes durante la prueba, sin embargo el IPTV AS si se comunicó con el núcleo IMS a través de SIP al ser solicitada la información del canal RTSP y realizando la petición del inicio de la tarificación al OCS a través de DIAMETER.

9.4.4. Experiencia 4: Término de servicio por agotamiento de créditos

En esta experiencia se capturaron los paquetes de datos de las comunicaciones existentes cuando se da término a una transmisión de un canal de IPTV dado que al usuario se le acabaron los créditos para el uso del servicio en el sistema de tarificación online. Las interfaces de captura fueron las siguientes.

Tabla 11: Archivos de captura para Experiencia 4.

Elemento	Dirección de interfaz de captura	Archivo de captura
DNS	192.168.0.102	exp4-dns.pcap
Conexión Puente (Bridge)	192.168.0.108	exp4-bridge.pcap

Las consultas al DNS se presentan en el siguiente gráfico:

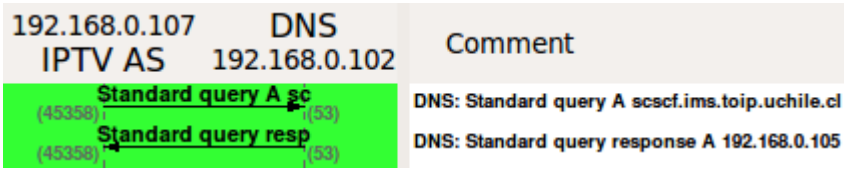

Figura 32: Gráfico de flujo de consultas de DNS en Experiencia 4.

Como se ve en el gráfico anterior, existe una única consulta de DNS que es cuando el IPTV AS necesita comunicarse con el S-CSCF para avisar que se debe cortar el servicio al usuario porque se acabaron sus créditos. A partir del archivo de captura exp4-dns.pcap se creó el siguiente gráfico de flujo de paquetes.

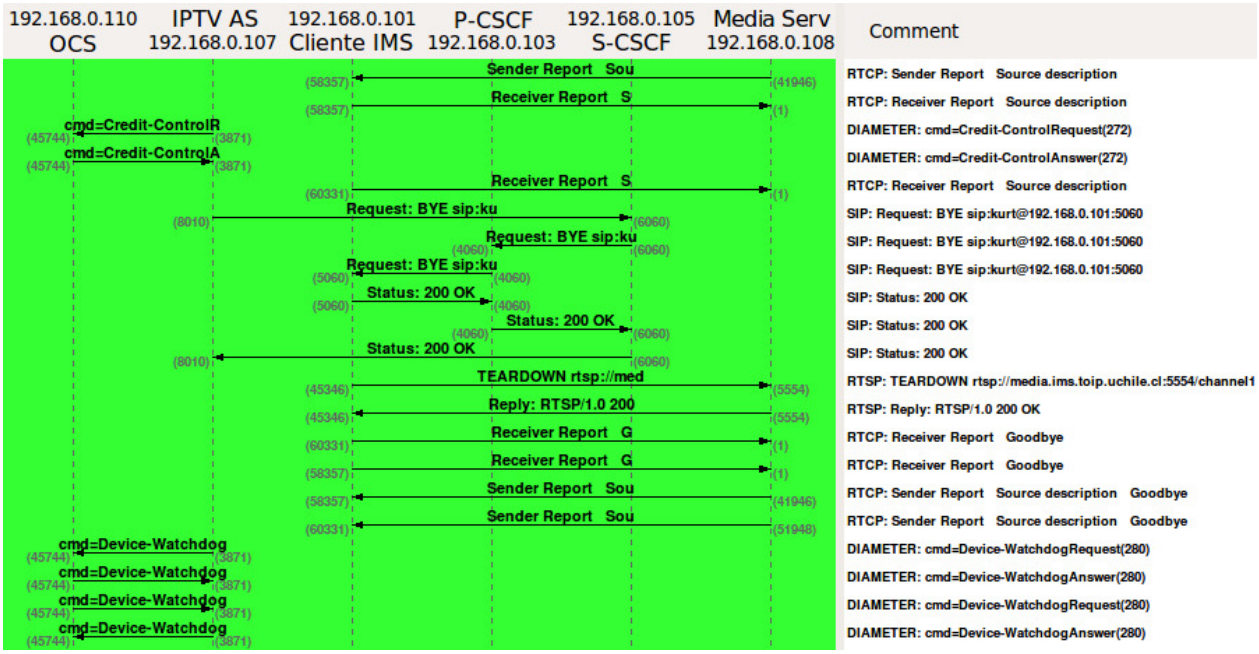

Figura 33: Gráfico de flujo de mensajes en Experiencia 4.

Continuando el intercambio de mensajes proveniente de la experiencia anterior en donde se estaba enviando la transmisión de audio y video en RTP, y existiendo un intercambio frecuente de mensajes RTCP. Sucede que durante la transmisión, el IPTV AS hace periódicas consultas DIAMETER al OCS del tipo Credit-Control-Request con un AVP CC-Request-Type con el contenido UPDATE_REQUEST en donde se le solicita nuevos créditos para seguir con la reproducción. Por su parte el OCS le devuelve cada vez un mensaje Credit-Control-Answer que contiene en un AVP Check-Balance-Result la nueva cantidad de créditos asignados para continuar con el servicio. En esta experiencia se da el caso en que al usuario no le quedan créditos lo cual es informado a través del AVP Check-Balance-Result con el valor NO_CREDIT.

1. Al ocurrir esto el IPTV AS envía un mensaje DIAMETER Credit-Control-Request con un AVP CC-Request-Type con el contenido TERMINATION_REQUEST para cerrar la tarificación.
2. Al ocurrir esto el IPTV AS envía un mensaje SIP BYE al S-CSCF, que pasa por el P-CSCF para luego llegar al Cliente IMS informándole el fin del uso del servicio.
3. Luego el Cliente IMS responde al IPTV AS por medio de las entidades ya mencionadas con un mensaje 200 OK.

4. Después el cliente envía un mensaje RTSP TEARDOWN al Media Server para detener la entrega de datos, el cual es respondido por un 200 OK.
5. Inmediatamente después se intercambian unos mensajes RTCP de Goodbye con lo que se cierra la transmisión.

Cuando el IPTV AS solicita poner fin al sistema de tarificación se intercambia con el OCS los siguientes tipos de comandos DIAMETER:

- Credit-Control-Request (CCR)
- Credit-Control-Answer (CCA)

El esquema global de comunicaciones que se da en la plataforma durante este proceso es el mismo que en la experiencia 3. Nuevamente sin participar en el proceso el PCEF, PCRF, I-CSCF, HSS y CDF. Solo se aprecian en estos los comandos DIAMETER Device-Watchdog entre los componentes que realizan comunicaciones DIAMETER para mantener contacto.

9.4.5. Experiencia 5: Denegación de servicio efecto de políticas de control

La siguiente experiencia estudia los mensajes intercambiados por los elementos durante el intento de una llamada de videoconferencia entre dos Clientes IMS previamente registrados, pero en donde el sistema de políticas de control interrumpe el proceso. Los archivos de captura de paquetes transmitidos en la red se presentan en la siguiente tabla.

Tabla 12: Archivos de captura para Experiencia 5.

Elemento	Dirección de interfaz de captura	Archivo de captura
DNS	192.168.0.102	exp4-dns.pcap
Conexión Puente (Bridge)	192.168.0.108	exp4-bridge.pcap

Al crear un gráfico a partir del archivo exp5-dns.pcap se puede apreciar que las únicas consultas provienen del Cliente IMS que realiza la llamada. El elemento que realiza la llamada será denominado Cliente IMS 1 quien esta ubicado en la dirección IP 192.168.0.101 y al que se pretende llamar será el Cliente IMS 2 con dirección IP 192.168.0.108 en este ejemplo.

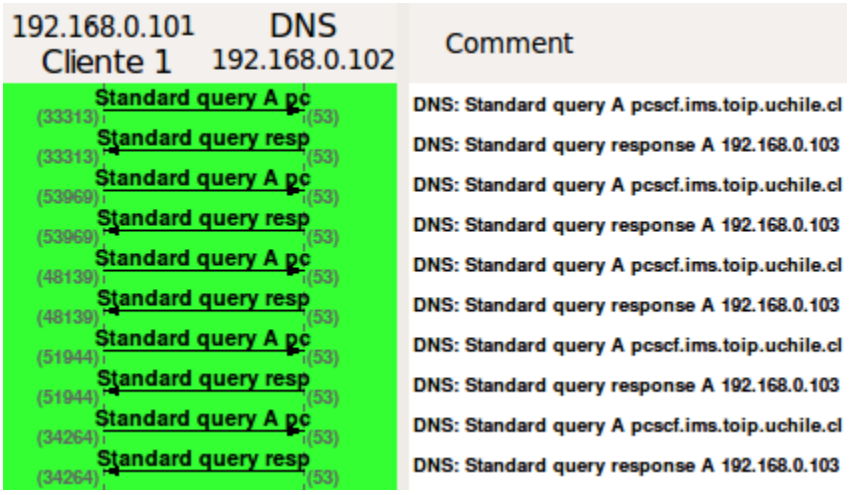

Figura 34: Gráfico de flujo de consultas de DNS en Experiencia 5.

A partir del archivo de captura exp5-bridge.pcap se creó el siguiente gráfico del tráfico de mensajes SIP y DIAMETER que se da en esta experiencia.

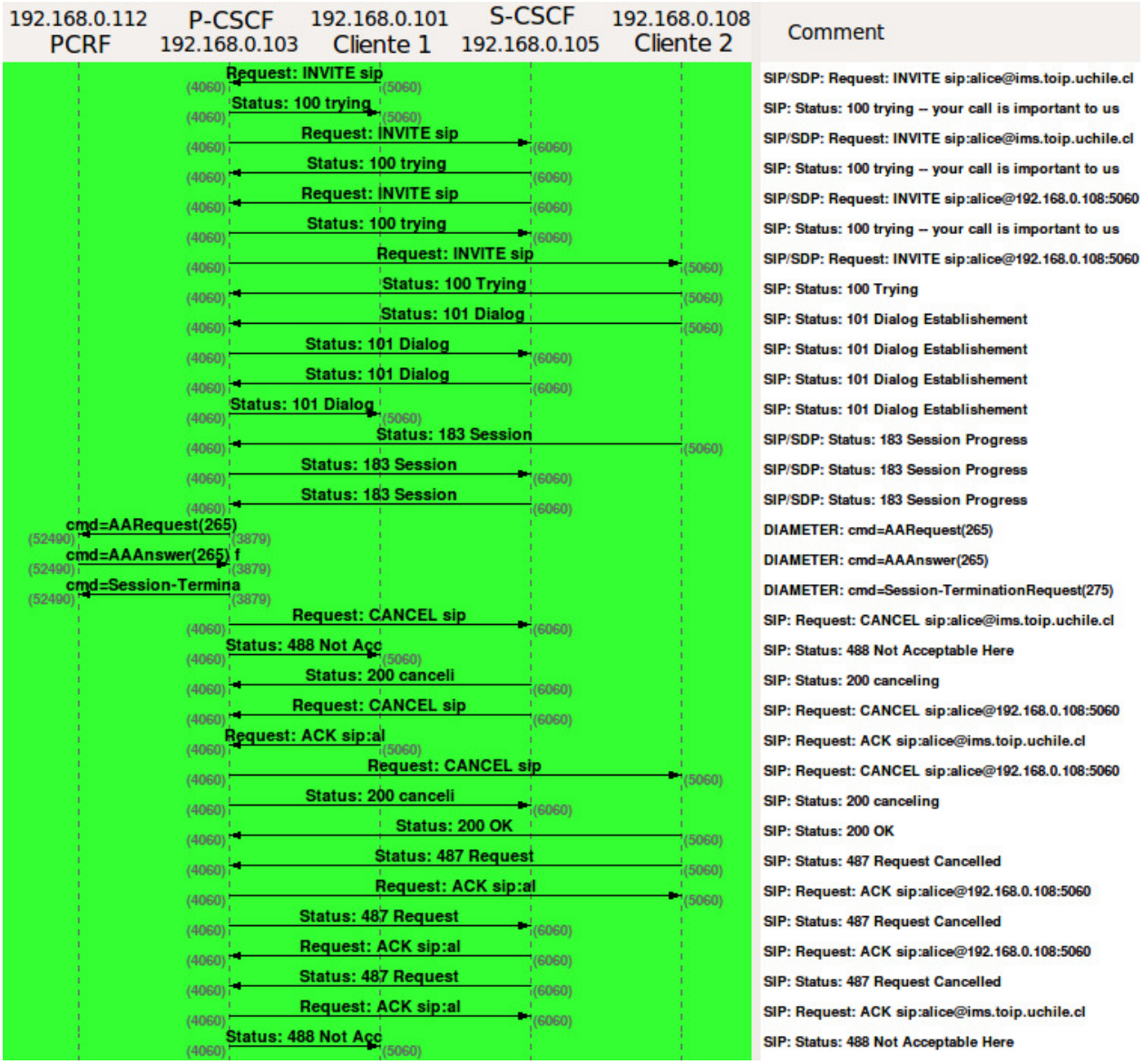

Figura 35: Gráfico de flujo de mensajes en Experiencia 5.

Considerando el intercambio de mensajes SIP y DIAMETER es posible explicar el proceso como sigue:

1. El Cliente IMS 1 envía INVITE al P-CSCF con la dirección SIP del Cliente IMS 2.
2. El P-CSCF le responde 100 Trying y reenvía la petición INVITE al S-CSCF.
3. El S-CSCF responde 100 Trying al P-CSCF y envía un INVITE al Cliente IMS 2 a través del P-CSCF.
4. Al pasar el INVITE por el P-CSCF este envía un 100 Trying al S-CSCF.

5. El Cliente IMS 2 devuelve un 100 Trying al P-CSCF, seguido de un 101 Dialog para el S-CSCF que viaja a través del P-CSCF con lo que se confirma que se estableció dialogo entre las partes.
6. El S-CSCF envía un 101 Dialog al Cliente IMS 1 a través del P-CSCF.
7. Luego el Cliente IMS 2 envía un 183 Session Progress al S-CSCF a través del P-CSCF, este mensaje contiene información sobre las características de la sesión.
8. El S-CSCF envía un 183 Session Progress al P-CSCF con la información enviada por el Cliente IMS 2.
9. Al recibir el P-CSCF el mensaje 183 Progress, realiza una consulta DIAMETER AAR al PCRF.
10. El PCRF responde con un DIAMETER AAA negando el servicio dado que en este ejemplo la comunicación entre clientes pretende ocupar el codec GSM para el audio el cual ha sido previamente sacado de la lista de códecs permitidos a través de la interfaz web del sistema de políticas de control.
11. Inmediatamente el P-CSCF envía un mensaje DIAMETER Session-Termination Request al PCRF.
12. Luego se desencadenan los mensajes para cancelar y terminar la comunicación entre clientes. El P-CSCF envía un mensaje SIP Status 488 Not Acceptable Here al Cliente IMS 1, que fue quien realizó la llamada negándosele el servicio. Y el Cliente IMS 1 responde con un ACK.
13. El P-CSCF envía un CANCEL al S-CSCF el cual es confirmado con un 200 Canceling.
14. Luego el S-CSCF envía un CANCEL al Cliente IMS 2 a través del P-CSCF. Al pasar por el P-CSCF este responde con un 200 Canceling al S-CSCF.
15. El P-CSCF envía el CANCEL al Cliente IMS 2 y este responde con un 200 OK.
16. Finalmente el Cliente IMS 2 envía un 487 Request Cancelled al S-CSCF a través del P-CSCF que es respondido con un ACK para cada elemento.
17. El S-CSCF envía un 487 Request Cancelled al P-CSCF que es confirmado con un ACK.
18. Todo se termina con un 488 Not Acceptable Here del P-CSCF al Cliente IMS 1 que fue quien comenzó toda la comunicación.

Al comunicarse el P-CSCF con el PCRF se intercambian los siguientes tipos de comandos DIAMETER:

- AARequest (AAR)
- AAAnswer (AAA)
- Session-Termination-Request (STR)

El esquema global de comunicaciones que se da en la plataforma durante este proceso es el siguiente.

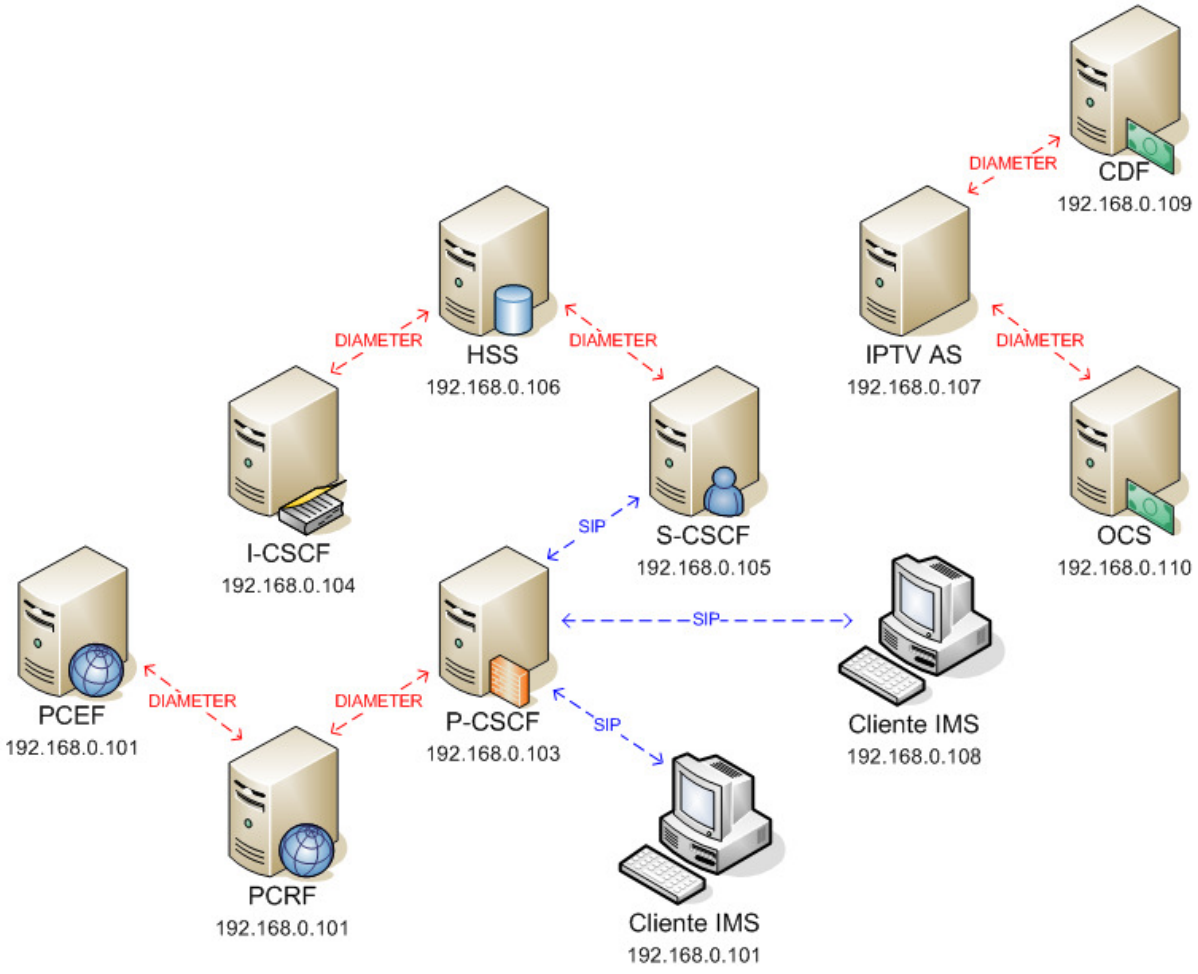

Figura 36: Presencia de protocolos en Experiencia 5.

Existe intercambio de mensajes SIP en las comunicaciones presentes en los Cliente IMS y el CSCF. El IPTV AS junto con los módulos de tarificación sólo intercambia mensajes DIAMETER

Device-Watchdog para mantener contacto. Sin embargo en esta experiencia el PCRF intercambia mensajes relevantes de DIAMETER al negar el permiso de la llamada por decisión de políticas de control.

9.4.6. Experiencia 6: Término de sesión en el Laboratorio de IPTV.

En esta experiencia se estudia los mensajes intercambiados por los elementos durante el término de la sesión en el sistema de IPTV por parte del Cliente IMS. Los archivos de captura de paquetes transmitidos en la red se presentan en la siguiente tabla.

Tabla 13: Archivos de captura para Experiencia 6.

Elemento	Dirección de interfaz de captura	Archivo de captura
DNS	192.168.0.102	exp6-dns.pcap
Conexión Puente (Bridge)	192.168.0.108	exp6-bridge.pcap

Al crear un gráfico a partir del archivo exp6-dns.pcap se puede apreciar que las únicas consultas provienen del Cliente IMS que desea conocer la dirección del P-CSCF pues es su único punto de acceso al sistema.

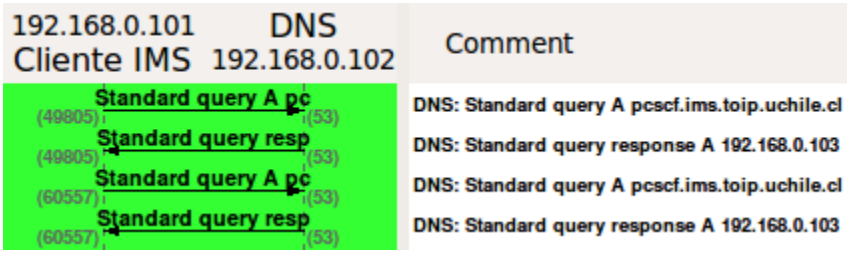

Figura 37: Gráfico de flujo de consultas de DNS en Experiencia 6.

A partir del archivo de captura exp6-bridge.pcap se creó el siguiente gráfico del tráfico de mensajes SIP y DIAMETER que se da en el Laboratorio de IPTV.

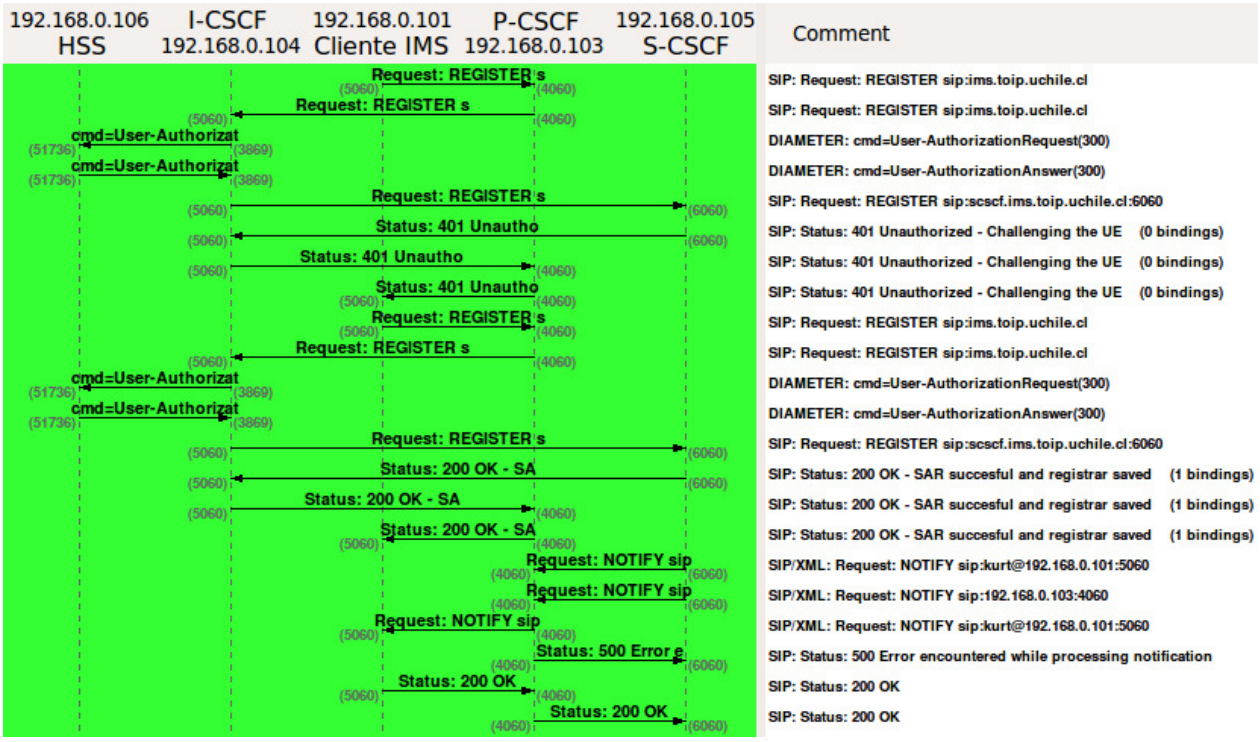

Figura 38: Gráfico de flujo de mensajes en Experiencia 6.

Considerando el intercambio de mensajes SIP y DIAMETER es posible explicar el proceso como sigue:

1. El cliente envía SIP REGISTER al P-CSCF para iniciar el registro en el sistema.
2. El mensaje REGISTER es reenviado desde el P-CSCF hacia el I-CSCF.
3. El I-CSCF intercambia comandos DIAMETER UAR y UAA con el HSS para saber a que S-CSCF redirigir la petición SIP.
4. El mensaje REGISTER es reenviado desde el I-CSCF al S-CSCF.
5. El S-CSCF desafía al Cliente IMS a través del 401 Unauthorized enviando un valor único.
6. El cliente IMS utiliza este valor único y las credenciales de usuario para generar a través de un algoritmo AKA la respuesta que es insertada en una segunda petición de REGISTER.
7. El mensaje REGISTER llega al I-CSCF a través del P-CSCF.
8. El I-CSCF intercambia nuevamente comandos UAR y UAA y se reenvía el REGISTER hacia el S-CSCF.
9. El S-CSCF envía un 200 OK a través del P-CSCF al Cliente IMS con lo que se termina la autentificación del usuario.

10. El S-CSCF envía un mensaje NOTIFY al Cliente IMS a través del P-CSCF. El cual el P-CSCF reclama con un Error 500 diciendo que la notificación contiene errores, lo cual no perjudicará posteriormente al Cliente IMS.
11. El Cliente IMS responde con un 200 OK al S-CSCF.

En un principio se aprecia el mismo flujo de mensajes existentes durante el proceso de inicio de un usuario en el sistema, es decir el cliente realiza dos peticiones de REGISTER con el desencadenamiento de los mensajes correspondientes en el P-CSCF que hace de punto de acceso del Cliente IMS con el sistema, el I-CSCF que intercambia mensajes DIAMETER User-Authorization con el HSS y las peticiones SIP REGISTER que envía el I-CSCF al S-CSCF. La diferencia está en que tras estas dos peticiones REGISTER, el S-CSCF envía un mensaje SIP NOTIFY al Cliente IMS a través de P-CSCF lo cual es devuelto por el cliente con un 200 OK que llega la S-CSCF para dar por terminada la sesión.

Al poner fin a la sesión en el Laboratorio de IPTV se intercambian los siguientes tipos de comandos DIAMETER:

- User-Authorization-Request (UAR)
- User-Authorization-Answer (UAA)

El esquema global de comunicaciones que se da en la plataforma durante este proceso es el mismo que en la experiencia 2.

Es decir intercambio de mensajes SIP en las comunicaciones presentes en el Cliente IMS y el CSCF. El IPTV AS junto con los módulos de tarificación, así como también los elementos encargados de aplicar las políticas de control sólo intercambian mensajes DIAMETER Device-Watchdog para mantener contacto.