TESIS DE MAGISTER
de Ing. Hernán Dima

"IMS a 16 años de su creación... resultó ser un ecosistema sustentable?"

INDICE

LISTADO DE ABREVIACIONES

2G	Second Generation Telecom System
3.5G	3.5 Generation Telecom System
3DES	Triple Data Encryption Standard
3GPP/3GPP2	3rd Generation Partnership Project (http://www.3gpp.org).
4G	4rd Generation Telecom System
AAA	Authentication, Authorization, and Accounting
AES	Advance Encryption Standards
AH	Authentication Header
AKA	Authentication and Key Agreement
AS	Application Server
BGCF	Breakout Gateway Control Function
CAMEL	Customized Applications for Mobile network Enhanced Logic
CDMA	Code Division Multiple Access
CDR	Charging Data Records
CN	Core Network
CS	Circuit Switched Domain
CSCF	Call Session Control Function
CSFB	Circuit Switch FallBack
DES	DES Data Encryption Standard
DNS	Domain Name Service
EPC	Evolved Packet Core
ESP	Encapsulated Security Payload
ETSI	European Telecommunications Standards Institute
FMC	Fixed Mobile Convergence
FQDN	Fully Qualified Domain Name
GGSN	Gateway GPRS Support Node
GPS	Geographical Positioning System
GSM	Global System for Mobile Communication
GUI	Graphical User Interface
HSS	Home Subscriber Server
IaaS	Infrastructure as a Service
ICS	IMS Centralized Services
ISO	International Organization for Standardization
IMS	P Multimedia Subsystem (3GPP standard)
IP	Internet Protocol
I-CSCF	Interrogating-Call Session Control Function
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKE v2	Internet Key Exchange version 2
IKE v1	Internet Key Exchange version 1
IMN	IMS Network
IMS	IP Multimedia Subsystem
IM-SSF	IP Multimedia Service Switching Function
IP Telephony	Internet Protocol Telephony
ISAKM	Internet Security Association Key Management
ISC	IMS Service Control
ISUP	Integrated Service Digital Network User Part
IWF	Inter Working Function
LAN	Local Area Network
LTE	Long Term Evolution
MD5	Message Digest Algorithm
MGCF	Media Gateway Control Function
MGW	Media Gateway
MPLS	Multi-Protocol Label Switching
MRF	Media Resource Function
MRFC	Multimedia Resource Function Controller
MRFP	Media Resource Function Processor
MTP	Message Transfer Part

MSC	Mobile Switched Centre
NAT	Network Address Translation
NDS	Network Domain Security
NDS-IP	Network Domain Security/Internet Protocol
NE	Network Entity
NGN	Next generation Network
NIST	National Institute of Standards and Technology
OMA	Open Mobile Alliance
OSA-SCS	Open Service Access-Service Capability Server
OSI	Open System Interconnection
OTT	Over The Top
PaaS	Platform as a Service
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy-Call Session Control Function
PDA	Personal Digital Assistant (Handheld computer)
PDF	Policy Decision Function
PLMN	Public Land Line Mobile Network
PoC	Push to Talk over Cellular
PS	Packet Switched Domain
PSTN	Public Switched Telephone Network
PTT	Push to talk
QoS	Quality of Services
SA	Security Association
SaaS	Software as a Service
SAD	Security Association Database
S-CSCF	Serving-Call Session Control Function
SCTP	Stream Control Transmission Protocol
SDES	Security Description
SEG	Security Gateway
SGW	Signaling Gateway
SHA	Secure Hash Algorithm 74
SIP	Session Initiation protocol
SIP-AS	Session Initiation Protocol-Application Server
SLF	Subscriber Location Function
SPD	Security Policy Database
SPI	Security Parameter Index
SPQM	SIP based Proxy Quality of Service Modules
SRVCC	Single Radio Voice Call Continuity
SS7	Signalling System No. 7
SSO	Single Sign On
TISPAN	Technical Committee within ETSI that works with standards for Next Generation Networks
TCAP	Transaction Capability Application Part
TDM	Time Division Multiplexing
THIG	Topology Hiding Inter-Network Gateway
TLS	Transport layer Security
UE	UE User Equipment
UMTS	Universal Mobile Telecommunication Systems
VoBB	Voice over Broadband
VoIP	Voice over Internet Protocol
VoLTE	Voice over LTE
VPN	Virtual Private Network
WCDMA	Wideband Code Division Multiple Access
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

1 INTRODUCCIÓN

La evolución de las comunicaciones en Internet, por diferentes servicios propietarios como:

- WhatsApp, Mensajería Instantánea (ej. Skype, Facebook)
- Correo Electrónico (ej. Gmail, Yahoo, Hotmail)
- Telefonía sobre Internet (ej. Skype)
- Video bajo demanda por Internet (Netflix, etc.)

Hace que los operadores clásicos de telefonía básica tengan que replantear su modelo de negocios, frente a estos nuevos servicios OTT (**O**ver **T**he **T**op). Que explotan al máximo el ancho de banda de las redes.

Una alternativa sería la de enfocarse en una estrategia de basada en servicios de conectividad, por ejemplo vendiendo transporte IP y proveer accesos a Internet. Lo que les implicaría la imposibilidad de brindar servicios de valor agregado. Dada la evolución actual, el transporte de la red se está convirtiendo un "comoditie". Esto impactará muy negativamente en el mantenimiento del nivel de ingresos.

Otra opción podría ser reconvertir la actividad alrededor de aplicaciones IP, y evolucionar hacia un modelo de servicios globalizado.

La mayor motivación para abordar este problema es que aún no está dicha la última palabra, y el estándar IMS, fue ideado para un entorno de servicios convergente. Un actor Cuádruple Play podría desarrollar su modelo de negocio en base a esta arquitectura.

Creo que esta problemática no tiene una única solución, pero me gustaría poder hacer una aproximación bien precisa de las alternativas y soluciones posibles a la problemática planteada.

El éxito o fracaso de la solución planteada estará muy condicionada por la situación actual de cada empresa que se decida o no a adoptar esta solución. Por eso creo muy conveniente que en la solución presentada esté muy bien explicado para qué tipo de empresas de servicios está apuntando esta arquitectura y modelo de negocios.

Actualmente IMS, es un estándar internacional, reconocido; el cual especifica la interoperabilidad de las redes y roaming, proveyendo mecanismos de control, seguridad y tarifación. Está muy bien integrado con las redes existentes de voz y datos. Al mismo tiempo adopta las características de los dominios del mundo IT. Esto hace que IMS sea la clave para facilitar la convergencia fijo móvil y a los nuevos servicios de valor agregado.

El estándar IMS define una arquitectura genérica para ofrecer voz sobre IP (VoIP) y servicios multimedia. Primeramente fue especificado por 3GPP/ 3GPP2 (Third Generation Partnership Project), ver más adelante Historia de la arquitectura IMS. Este estándar soporta múltiples tipos de tecnologías de acceso, como ser: GSM, WCDMA, CDMA2000, UMTS, LTE, banda ancha fija y móvil.

IMS posibilita al mundo de los operadores, utilizar el concepto de una estructura de capas y potenciarlo más allá, definiendo una arquitectura horizontal, donde servicios disponibles y funciones comunes pueden ser reutilizados por múltiples aplicaciones. Estos servicios disponibles a proveer están muy bien estandarizados y la forma en que están estructurados permite la optimización de este tipo de estructura horizontal. Al mismo tiempo simplifica y acelera los procesos de creación de nuevos servicios y aprovisionamiento (Ver Caso con un ejemplo de un nuevo servicio de aprovisionamiento para Telefónica). De esta forma permitirá a los operadores pasar de un modelo vertical, donde la implementación de nuevos servicios es costosa y compleja, dada la estructura de las redes donde se solapan las funcionalidades de facturación, presencia, manejo de listas y grupos, como así también enrutamiento y aprovisionamiento; a un modelo horizontal, donde no hay solapamiento de funcionalidades o servicios.

Por ultimo cabe mencionar que IMS posibilita un camino de migración segura hacia una red basada en IP, que satisfacerá las demandas de los potenciales usuarios de los nuevos servicios a ofrecer.

Referencias: 1,2 y 3.

1.1 Antecedentes

IMS es una arquitectura que ya lleva 16 años en el mercado y está basada en un cambio de paradigma, como así en distintos tipos de tecnologías, generando un ecosistema diferente. Esta arquitectura fue desarrollada sobre una red totalmente IP, y soporta tanto aplicaciones en tiempo real (voz, video, conferencia), como no en tiempo real (mms, sms, push to talk, etc).

Adicionalmente IMS permite integrar la convergencia de servicios en redes de distinta naturaleza, como ser la convergencia fijo-móvil.

Por lo tanto adoptar una arquitectura IMS, se convierte en una estrategia que puede elegir un operador tradicional para reposicionarse en el mercado de servicios sobre IP; como también por un posible operador virtual que no posea redes de acceso o transporte, para desarrollar una red de servicios de valor agregado sobre IP.

La arquitectura IMS provee una red para poder brindar múltiples servicios y con múltiples accesos, con un gran nivel de seguridad.

Referencias: 1,2 y 3.

1.2 Tendencias del Mercado de Telecomunicaciones

Las necesidades de los usuarios y empresas conducirán a la evolución de los servicios multimedia, tanto para los operadores fijos como para los móviles. Los usuarios esperan hacer más cosas con sus servicios de comunicaciones, por menos dinero, y queda muy claro que los servicios están yendo, más allá de la voz. Cada vez están siendo atraídos por una amplia gama de servicios de entretenimiento y de información fáciles de usar y a un precio razonable. El usuario cada vez más, quiere estar siempre conectado, no importando donde este, en que momento, ni como sea la forma en que se conecta.

Existen tecnologías facilitadoras como los accesos de banda ancha, voz sobre IP (VoIP), y las redes LAN inalámbricas, que reducen las barreras de entrada a estos nuevos servicios, tanto en el mundo fijo como en el móvil. Los operadores necesitan crear paquetes de servicios que sean fáciles de usar y atractivos para los usuarios. El usuario hoy se ha vuelto más individualista, más independiente, más informado y sus necesidades practicas con-llevan a ser más demandantes de todos estos nuevos servicios. Por eso estos nuevos servicios tienen un rol clave en hacer de las telecomunicaciones una experiencia mucho más cara a cara. La forma de acceder a este tipo de nuevos servicios de información, entretenimiento y otros con alto contenido, es a través de diferentes formas o canales. Es aquí donde los operadores tienen una gran oportunidad de integrar y extender esta experiencia multimedia a través de servicios personalizados persona a persona, persona a contenido o grupos de servicios. El amplio uso de celulares y mensajes instantáneos, muestra como los usuarios están adoptando nuevos servicios que satisfacen sus emociones y sus necesidades de comunicación de diversas maneras. Los operadores pueden ayudar a los usuarios a extender dicho comportamiento con servicios enriquecidos que les permitan comunicarse en tiempo real por medio de la voz, video, fotos y mensajes o cualquier combinación de estas.

El uso de cualquier servicio nuevo deberá ser intuitivo y natural, para que se convierta en un suceso masivo de marketing. Así como la telefonía móvil y fija se utiliza en todas partes para llamar a cualquiera en cualquier parte del mundo. Se espera que estos nuevos servicios ofrezcan una nueva experiencia a través de múltiples tecnologías de acceso, dispositivos y ubicaciones.

La clave está en la interoperabilidad entre terminales y operadores. Al usuario final no le concierne que operador usan sus amigos, simplemente quiere que el servicio funcione.

Los mensajes de voz, los e-mails, los teléfonos celulares y las redes LAN inalámbricas, han revolucionado como los usuarios se interconectan. Pero lo que el usuario está buscando es una forma de controlar o manejar estos accesos, de forma tal que pueda administrar su presencia, de una mejor forma. Tal que pueda controlar como, donde, cuándo y por quien puede ser localizado.

Referencias: 1,2 y 3.

2 ESTADO DEL ARTE

2.1 Desarrollo e Historia

La arquitectura IMS fue desarrollada por la industria celular para acompañar la necesidad de crecimiento de las redes móviles, fijas y de datos.

Fue desarrollada en base a una necesidad de la industria de las telecomunicaciones, en particular la industria de telefonía celular. Para permitir un acceso a servicios multimedia desde cualquier ubicación y cualquier terminal.

IMS creció fuera del panorama político del momento. Esto moldeo muchos elementos de su diseño y arquitectura, y como resultado, es necesario analizarlo con esto en mente.

El estándar IMS fue desarrollado por un grupo llamado 3G.IP, el cual se formó en el año 1999. Este grupo se convirtió pronto en 3GPP, donde su trabajo se puso en sintonía con el trabajo requerido por la industria celular, quien aparentaba ser el principal usuario.

Originalmente IMS pretendía ser la evolución de las redes UMTS para poder brindar a usuarios móviles servicios multimedia sobre IP.

IMS como se ve en la tabla que sigue, arranca con una versión 5, como la evolución del Core de las redes de una tecnología de "circuit-switching" a "packet-switching".

Desde la teoría, IMS es una arquitectura, que nació hace ya 16 años, y está basada en un nuevo paradigma, generando un nuevo ecosistema. Esta arquitectura se desarrolla sobre una red IP. Soporta tanto aplicaciones en tiempo real (voz, video-conferencia), como no tiempo real (mms, sms, push to talk, etc).

IMS permite integrar la convergencia de servicios en redes de distinta naturaleza, como ser la convergencia fijo-móvil. Hoy VoLTE es un potenciador de la arquitectura IMS.

La arquitectura IMS provee una red para poder brindar múltiples servicios y con múltiples accesos, con un gran nivel de seguridad.

En la práctica, ha pasado por diferentes versiones, nació para redes móviles y luego fue adaptado al mundo fijo, teniendo un grado de adopción muy inferior al esperado en sus comienzos, debido a los altos costos de implementación de las redes, siendo el caso práctico más sobresaliente y representativo el de Telefónica Global.

Inicialmente IMS era un sistema basado íntegramente en IP, para asistir a los operadores móviles a brindar servicios interactivos de próxima generación, a un costo razonable, sobre una arquitectura que aprovechaba la flexibilidad de Internet.

De acuerdo a esto IMS se definió dentro de los estándares del 3GPP y sus desarrollos se pueden ver de acuerdo a las diferentes versiones.

2.2 IMS a través del tiempo

A continuación una figura que muestra la evolución de IMS en el tiempo hasta el Release 12:

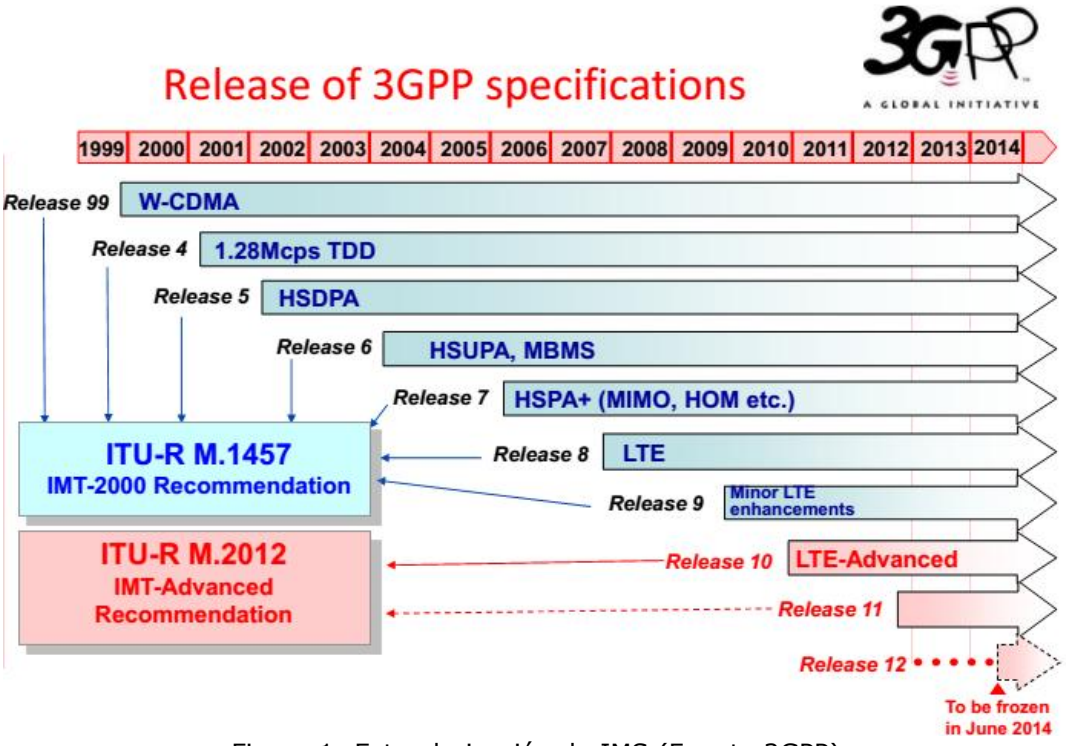

Figura 1: Estandarización de IMS (Fuente 3GPP)

A continuación una tabla con las versiones más relevantes de IMS a lo largo del tiempo hasta el último Release en curso, que aún sigue abierto:

Versión 3GPP	Año	Detalles
Rel-5	2001	Primera Introducción a IMS
Rel-6	2003	IMS servicios de Emergencia Servicios combinacionales Continuidad en las llamadas de Voz
Rel-7	2005	Continuidad en las llamadas de Voz por radio (SR-VCC) Teléfonos multimedia
Rel-8	2007	IMS servicios centralizados IMS servicios continuos Interoperabilidad Multimedia entre redes IMS y CS IMS telefonía multimedia y servicios suplementarios

Rel-9	2009	IMS llamadas de emergencia sobre GPRS y sistema de mejoramiento de paquetes (EPS). Mejoramiento del IMS servicio de alertas de tonos IMS servicios de restauración
Rel-10	2010	IMS servicios de continuidad y mejora de transferencia inter-dispositivo.
Rel-11	2013	Mejora en el canal de control para tráfico de bajada. Mejora en la coordinación de interferencia inter celda celular.
Rel-12	2015	La prioridad fue el uso de la tecnología LTE para servicios de emergencia y seguridad. Conteniendo especificaciones técnicas para aplicaciones de misión crítica.
Rel-13	2016	Completa las especificaciones de misión crítica. También hace hincapié en la seguridad, como DoS.
Rel-14	Abierto	Esta versión no está cerrada y sigue evolucionando y agregando más especificaciones. El foco sigue siendo la seguridad en las aplicaciones de misión crítica. También mejora en la eficiencia de LTE.
Rel-15	Abierto	Se estudia una nueva tecnología de acceso por radio. Flexibilidad del ancho de banda de LTE. Mejora de las radio bases con sistema de antenas activas.

Un gran empuje para IMS, fue que en el Congreso Mundial Móviles 2010, se anunció que GSMA estaba soportado. Lanzando el término de "Único Mundo". La iniciativa para trasporte de voz: VoLTE o voz sobre LTE.
Como los sistemas estaban basados en el uso de IMS, muchos operadores luego decidieron que era necesario incorporar capacidades de IMS a sus redes.

La figura siguiente muestra a IMS como el Core de una red para un dominio multimedia para CDMA, tanto para redes cableadas como de banda ancha.

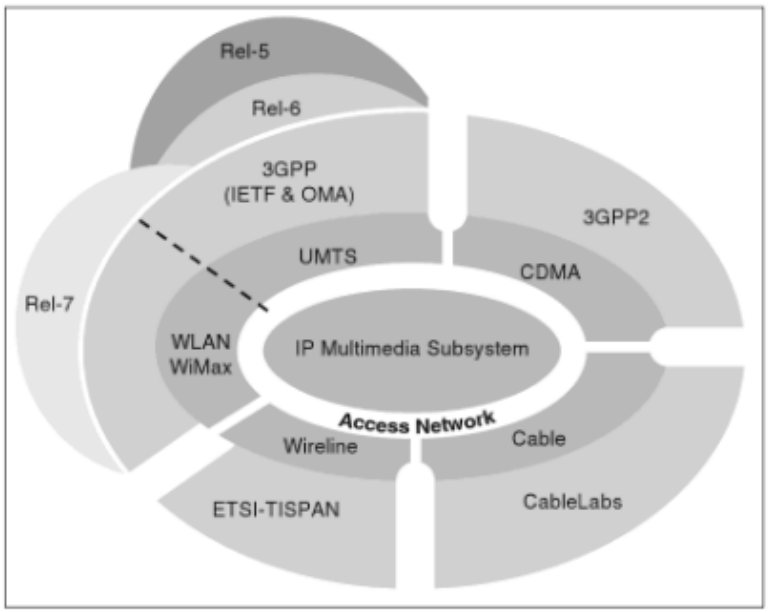

Figura 2: Evolución de IMS

Los principales impulsores de IMS son 3GPP2, ETSI (European Telecommunication Standards Institute), TISPAN (Telecommunications & Internet Converged Services & Protocols for Advanced Networks), y CableLabs. Ellos han aceptado a IMS como el siguiente paso obligado para la evolución a una red toda IP. El OMA (Open Mobile Alliance), quien define los habilitadores de servicios para la interoperabilidad de dispositivos móviles, ha contribuido en gran medida en la especificación de estos servicios para las redes IMS. IMS es el inicio de una perspectiva de armonía en la mezcla de múltiples estándares.

Es importante entender que IMS no es una tecnología, se define como una arquitectura de referencia. Los principios que se usaron para su definición han sido recolectados de lo mejor de cada solución. Ver figura siguiente:

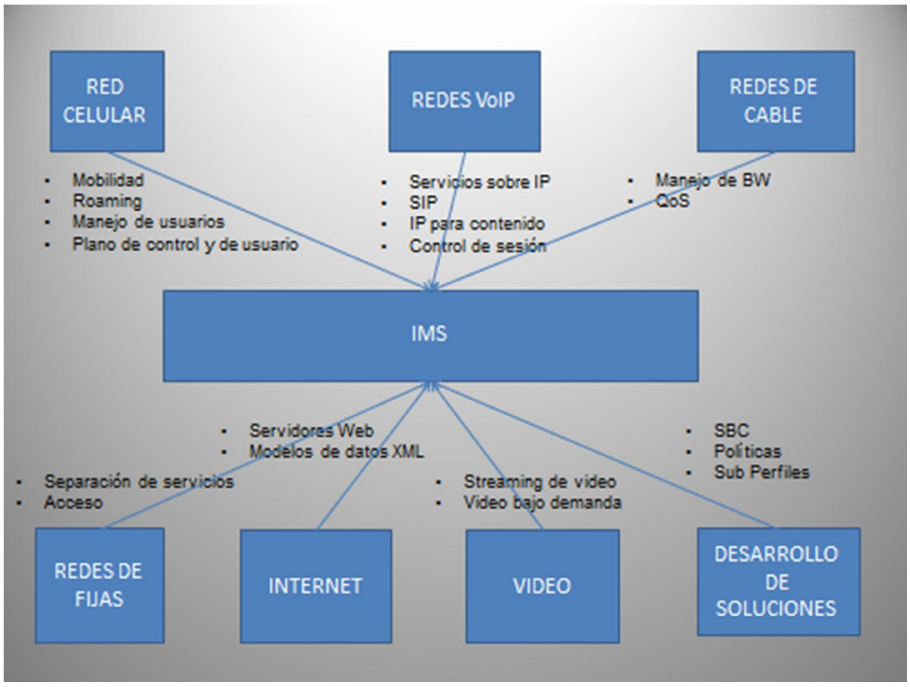

Figura 3: Principios Inherentes de las redes existentes

Las mejores prácticas tomadas de implementaciones basadas en estándares y nuevas innovaciones, terminaron en la definición de una arquitectura que parece tener un look perfecto. Desde que IMS ha sido definido como parte integral de una red celular, adopta en forma inherente los conceptos de movilidad, roaming y gerenciamiento de usuarios.

2.3 Arquitectura IMS

2.3.1 Modelo de capas OSI en IMS.

Cuando nos tenemos que referir a la comunicación entre sistemas, generalmente utilizamos un modelo de capas. Por eso el modelo OSI de capas es ampliamente usado.

El modelo OSI de 7 capas es lo más básico para muchos sistemas, lo mismo ocurre para IMS. Si bien el modelo OSI es muy general, es fácil adoptarlo para usarlo en IMS.

El modelo OSI de referencia fue desarrollado por ISO (International Organisation for Standardisation). Es un modelo usado en sistemas de comunicaciones para dividir los canales de comunicación en varios niveles o capas.

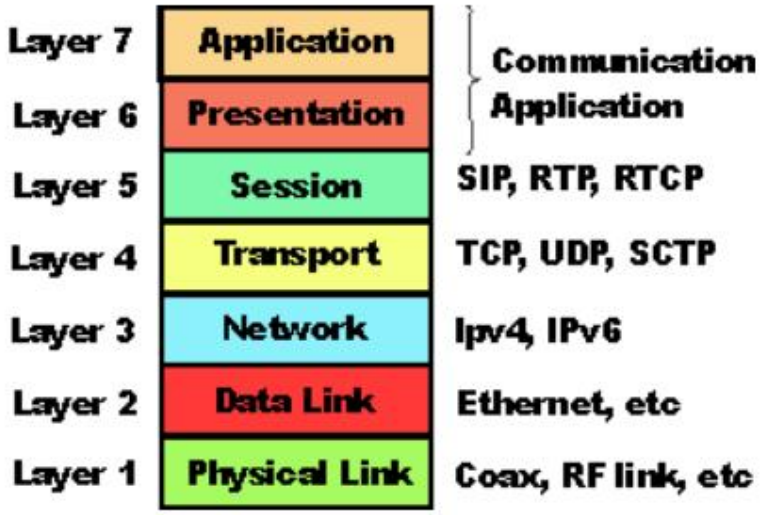

Figura 4 Modelo OSI de Referencia

Los protocolos mencionados arriba en el modelo OSI, son todos correspondientes al mundo IP, ninguno es específico de IMS. Sin embargo veremos más adelante como IMS se nutre de estos protocolos estándares para utilizarlos en su arquitectura.
Cada capa provee un servicio distintivo y bien definido hacia la capa adyacente superior en la pila. Sin embargo arriba de la capa 5 (y a veces la 4), la distinción se puede volver un poco indefinida, ciertos servicios se superponen. Es muy común que arriba de la capa 5 se vuelve muy específico cada servicio y depende del entorno en que nos encontremos. En IMS estas capas tienen su propia terminología y definiciones particulares.
Introduzco esta representación, ya que nos va a **resultar de suma utilidad cuando vayamos a comparar la arquitectura IMS, con otras opciones que han tomado fuerza en los últimos años**, impulsadas desde el lado de "nuevos players" OTT, que comienzan a competir en los mismos mercados que los Operadores Tradicionales.

Hay 3 capas principales en IMS que están adaptadas para su función. Se corresponden con la capa 5-6 y 7.Esto quiere decir que las 3 capas de abajo son siempre las mismas que se heredan del mundo IP. IMS solo define las 5, 6 y 7. Por eso decimos que IMS es agnóstico al acceso. En la capa 4 IMS, usa los protocolos TCP para la señalización y UDP para el transporte de la media, heredados de VoIP.
A continuación una comparación entre el modelo OSI y la suite de protocolos de IMS.

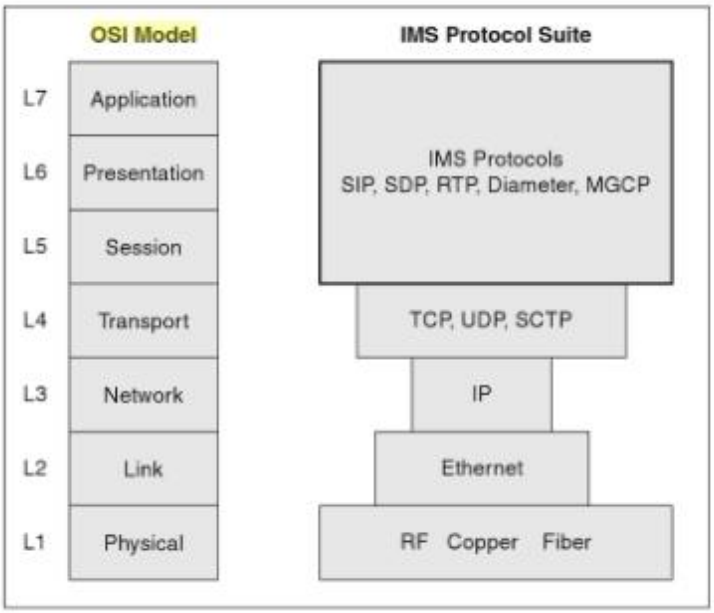

Figura 5: Suite de Protocolos IMS

Estas 3 capas de IMS son:

- Capa de transporte y punto de terminación. (OSI capa 4/5)
- Capa de control de sesión. (OSI capa 5)
- Capa de aplicación. (OSI capa 6/7)

2.3.2 Capa de Transporte:

Esta capa inicia y termina la señalización SIP(de capa 5), levanta los parámetros de una sesión y provee los servicios de por ejemplo la conversión formatos analógicos a digitales. Pero el transporte en si lo realiza TCP (de capa 4), sólo de la señalización.

Esta capa también provee todo el procesamiento de la media o contenido, incluyendo los media gateways. Estos se utilizan para un stream VoIP a un formato TDM de la PSTN. También provee los servicios de conferencia, ejecución de mensajes, reconocimiento de voz y sintetizado de la voz.

Los elementos en el plano de transporte que interactúan entre el Core de IMS y la PSTN son:

- SGW (Signalling Gateway): Usado para interconectar diferentes redes de señalización como SCTP/IP y SS7. Realiza la conversión de señalización nivel de transporte entre SS7 e IP.

- MRFP (Media Resource Function Processor): Provee recursos del plano de usuario que solicita y recibe del MRFC.
- MGW (Media Gateway): Es una puerta de enlace entre la arquitectura SIP de la red y el mundo TDM tradicional que no utilizan esta tecnología.

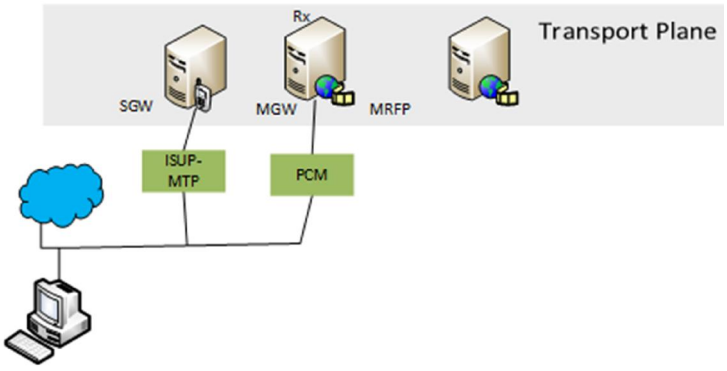

Figura 6 Plano de Transporte

2.3.3 Capa de control de sesión:

Esta capa contiene lo que se llama CSCF (Call Session Control Function), la cual provee al terminal la registración y el ruteo de los mensajes SIP (de capa 5). Así el terminal se lo rutea al servidor de aplicación correcto. CSCF también provee calidad de servicio (QoS). Esto lo garantiza dialogando con la capa de transporte.
Esta capa también incluye otros elementos como el HSS (Home Subscriber Server) quien mantiene el perfil del usuario, incluidos los detalles de registración y preferencias. Incluye también un servidor de presencia.
La principal función es la del control del media Gateway.
Los elementos clave del núcleo de la red IMS son las funciones de control de sesión de llamada (CSCF) y el Home Subscriber Server (HSS o servidor del suscriptor de la red origen). El CSCF ha tomado la mayoría de la funcionalidad del MSC en la arquitectura del IMS.

HSS (Home Subscriber Subsystem): Es la principal base de datos en IMS con la información de los usuarios. Cuenta con un subconjunto de la funcionalidad HLR/AUC la cual es requerida en redes de conmutación de circuitos y de paquetes.

- SLF (Subscription Locator Function) Mecanismo de resolución que facilita al I-CSCF, S-CSCF y al AS (Application Server) la ubicación de la dirección del HSS que contiene la información de un subscriptor en específico en caso de existir más de uno en la red desplegada por el operador de red. Pese a que

actualmente solo se maneja un solo HSS en un futuro cuando aumente la cantidad de HSS en la red IMS si se requerirá de uno o varios SLF.

CSCF (Call Session Control Function): Se encarga de las funciones de Control de Sesión. Constituido internamente por 3 grupos dependiendo de la funcionalidad:

- **P-CSCF (Proxy - Call Session Control Function):** Es el principal punto de contacto entre un UE y la red IMS, cuenta con un servidor proxy SIP.
- **I-CSCF (Interrogating - Call Session Control Function):** En el proceso de establecer una comunicación entre el UE y la red IMS esta entidad se encarga en el proceso de registro por primera vez de un usuario (UE) de preguntar en principio al S-CSCF quien luego se comunica con el HSS si existe información del subscriptor en su base de datos.
- **S-CSCF (Serving – Call Session Control Function):** Es el cerebro de IMS, realiza las tareas de control de sesión y servicios de registro para UEs. Descarga información del subscriptor desde el HSS. Suele estar ubicado en la home network.

El bloque de CSCF a su vez se comunica con:

- **BGCF (Breakout Gateway Control Function):** Es un servidor SIP que realiza funciones de enrutamiento cuando la llamada se dirige a una red de conmutación de circuitos, tales como PSTN. Se localiza la puerta de entrada adecuada en el circuito de conmutación de red de destino para el encaminamiento de la llamada saliente.
- **MRFC (Media Resource Function Controller):** Interpreta la señalización SIP recibida a través del S-CSCF y usa instrucciones de MEGACO para controlar el MRFP.

MGCF (Media Gateway Control Function) Facilita la comunicación entre los usuarios IMS y CS. Asimismo controla los canales multimedia para una entidad asociada de plano de usuario.

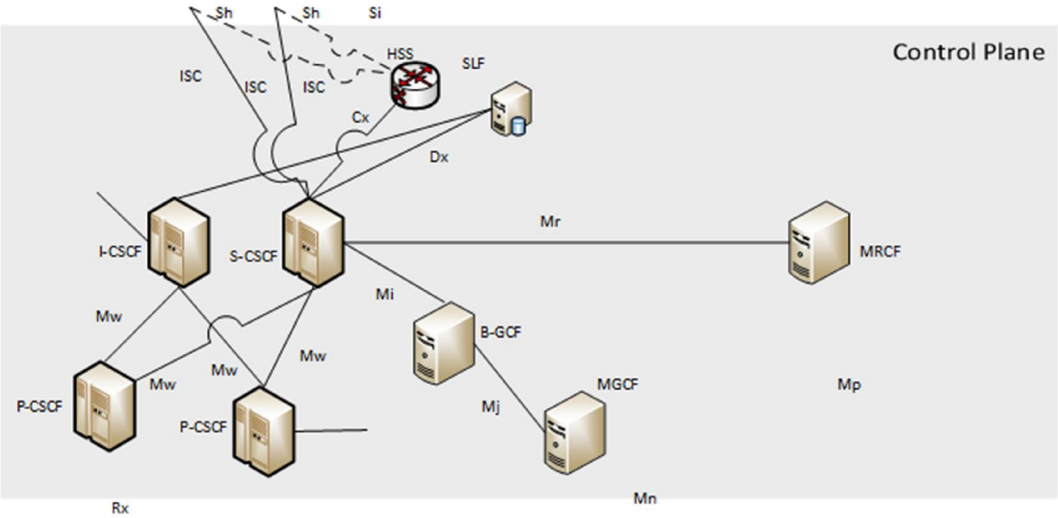

Figura 7 Plano de Control

2.3.4 Capa de aplicación o servicios:

Se ocupa del control de los servicios del usuario (de capa 6 y 7). La arquitectura IMS y el protocolo SIP, se diseñaron para ser bastante flexibles en algún modo, por eso es posible soportar servidores de telefonía y otro tipo de servidores en forma concurrente.

Entre los elementos primordiales de la arquitectura IMS se encuentran los servidores de aplicaciones, quienes se encargan de ejecutar la lógica de los servicios multimedia, es decir, como se invocan los servicios, que señalización es requerida y como los servicios interactúan ente sí.

AS (Application Server): Son entidades que brindan funciones en IMS pues ofrecen servicios de valor agregado en la infraestructura de IMS. Los servicios ofrecidos en IMS no se ofrecen solamente sobre SIP, pues el operador puede acceder a ciertos servicios brindados por otras plataformas como CAMEL (Customized Applications for Mobile Network Enhanced Logic) CSE (Service Environment) y OSA (Open Service Arquicteture).

OSA (Open Service Arquitecture) Utiliza características de capacidad de servicio como control, la interacción del usuario, status del usuario, control de datos de la sesión, las capacidades del terminal, administración de cuentas, la carga y administración de políticas para el desarrollo de servicios. OSA ofrece un mecanismo que le brinda un acceso seguro a terceros a la arquitectura de IMS, debido a que contiene características de acceso inicial, autenticación, autorización, registro y descubrimiento (EL S-CSCF no provee funcionalidades de autenticación y

seguridad para establecer acceso seguro y directo a terceros a IMS). OSA-SCS es utilizado para terminar la señalización desde el S-CSCF. Emplea una API (Application Program Interface) para establecer comunicación con el actual Application Server OSA.

SIP-AS es un servidor SIP que ofrece una gran variedad de servicios de valor agregado como presencia, mensajería y conferencia.

IM-SSF es una función que fue agregada a la arquitectura IMS para soportar la cantidad de servicios que son desarrollados en CAMEL Service Environment (trigger detection points, CAMEL Service Switching Finite State Machine, etc.) e interactúan con la interfaz CAP (CAMEL Application Part).

Figura 8 Plano de Servicios

A continuación el esquema de 3 capas de IMS:

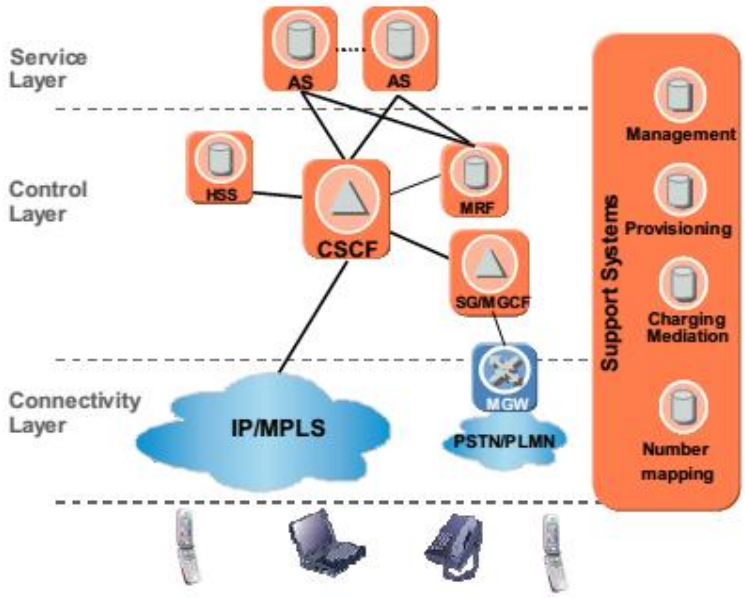

Figura 9 Modelo de 3 capas de IMS (Fuente 4)

2.3.5 Atributos del CORE de una Red IMS

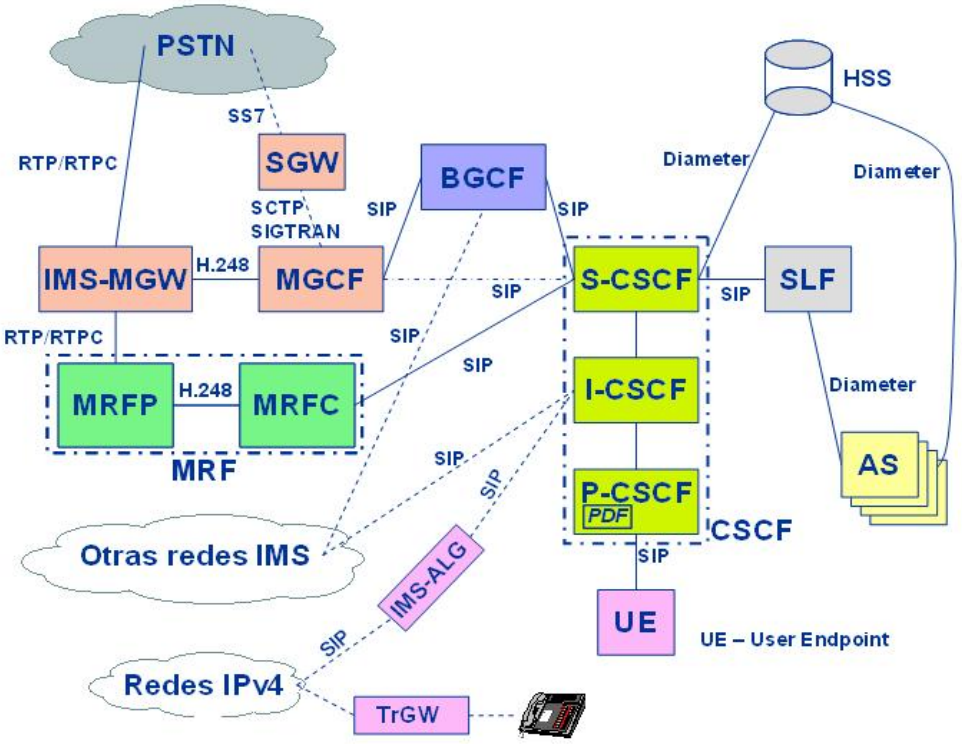

Figura 10 Esquema de red - Core IMS

El IMS provee una arquitectura multimedia, basada toda en IP. Soportando los atributos del Core de una Red, que permitirán brindar los servicios de valor agregado que se pretende.

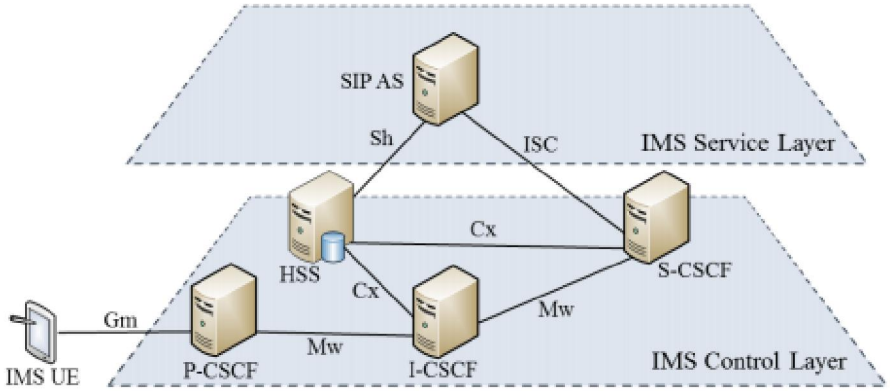

Figura 11 Arquitectura de IMS Simplificada (Fuente 4)

Dentro de estos atributos podemos mencionar:

- **Calidad de servicio (QoS):** Sin la cual los servicios multimedia en tiempo real no podrán ser proveídos a los usuarios que pagan por los mismos.
- **Disponibilidad de servicios:** La posibilidad de garantizar el acceso a un determinado servicio, de forma de asegurar los recursos de red necesarios y proveerlos durante el tiempo que dure el servicio requerido. Entendiendo que la necesidad de ese servicio puede ser vital, como un servicio de 911.
- **Billing:** La habilidad del operador de facturar apropiadamente por ese servicio. Por ejemplo, supongamos que un usuario inicia una comunicación de voz, y luego en el medio de la misma decide incluir el servicio de video conferencia. La arquitectura IMS asegura que se capturen los eventos necesarios que permitan facturas los cargos adecuados.
- **Flexibilidad de nuevos servicios:** La habilidad del operador de agregar nuevos servicios de valor agregado, para aumentar el ARPU o promedio de ingreso por usuario, (**A**verage **R**evenue **P**er **U**ser).
- **Inter operabilidad con diferentes proveedores de aplicaciones:** La habilidad de mezclar servicios de diferentes proveedores. Por ejemplo, proveer un servicio de juegos de un proveedor, mientras que permitir el servicio PTT de voz de otro proveedor.

A continuación veremos una serie de protocolos, que utiliza la arquitectura IMS, para poder comprender el marco teórico de esta arquitectura.

Referencias: 1

2.3.6 SIP: Session Initiation Protocol

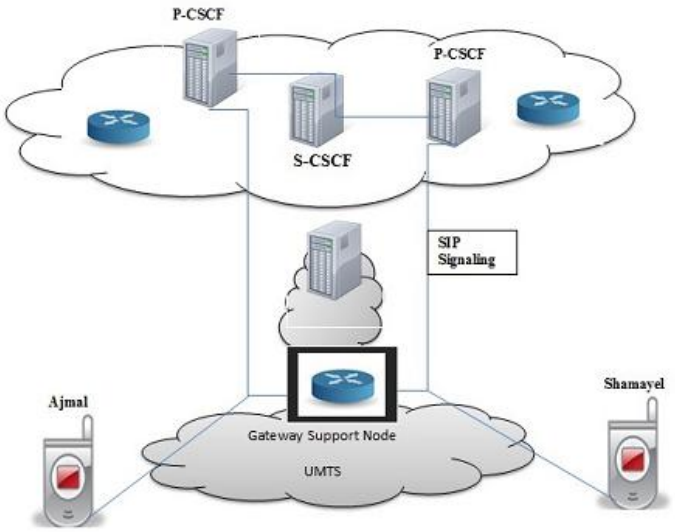

Figura 12 Señalización SIP (Fuente 37)

"**S**ession **I**nitiation **P**rotocol" o SIP (Protocolo de Iniciación de Sesión), es un protocolo de señalización definido por el IETF ("**I**nternet **E**ngineering **T**ask **F**orce") que permite el establecimiento, la liberación y la modificación de sesiones multimedia (RFC3261). Este protocolo hereda ciertas funcionalidades de los protocolos "http" ("**H**yper **T**ext **T**ransport **P**rotocol"), utilizados para navegar sobre la WEB y "SMTP" ("**S**imple **M**ail **T**ransport **P**rotocol"), utilizados para transmitir e-mails. SIP se basa en un modelo cliente / servidor como http. El direccionamiento utiliza el concepto "URL SIP" ("**U**niform **R**esource **L**ocator"), parecido a una dirección E-mail. Cada participante en una red SIP es entonces alcanzable vía una dirección, por medio de una URL SIP. Por otra parte, las respuestas a los requerimientos SIP son contestados por respuestas identificadas por un código. La mayor parte de los códigos de respuesta SIP han sido tomados del protocolo http. Por ejemplo, cuando no se ubica al destinatario, se devuelve un código de respuesta «404 Not Found». Un requerimiento SIP está constituido de "headers" o encabezamientos, al igual que en SMTP.

SIP ha sido ampliando con el fin de soportar numerosos servicios tales como la presencia, la mensajería instantánea (similar al servicio SMS en las redes móviles), la transferencia de llamada, la conferencia, los servicios complementarios de telefonía, etc.

SIP ha sido elegido por el 3GPP para la arquitectura: "**I**P **M**ultimedia **S**ubsystem" o "IMS" como protocolo para el control de sesión y el control de servicio. Reemplazando en un futuro, los protocolos "ISUP", utilizado para el control de llamada en la Red Telefónica Conmutada, e "INAP", utilizado para el control de servicio en la arquitectura de Red Inteligente.

El protocolo SIP es solo un protocolo de señalización. Una vez establecida la sesión, los participantes de la sesión intercambian directamente su tráfico de audio o video a través del protocolo RTP ("**R**eal-Time **T**ransport **P**rotocol"). Por otra parte, SIP no es un protocolo que permita reservar recursos, y en consecuencia, no puede asegurar la calidad de servicio. Se trata de un protocolo de control de llamada y no de control del medio.

SIP tampoco es un protocolo de transferencia de archivos tal como "http", usado con el fin de transportar grandes volúmenes de datos. Ha sido concebido para transmitir mensajes de señalización cortos con el fin de establecer, mantener y liberar sesiones multimedia. Mensajes cortos, no relativos a una llamada pueden sin embargo ser transportados por SIP al estilo de SMS.

Referencias: 4 y 5.

Entidades SIP

SIP define dos tipos de entidades: clientes y servidores. De manera más precisa, las entidades definidas por SIP son:

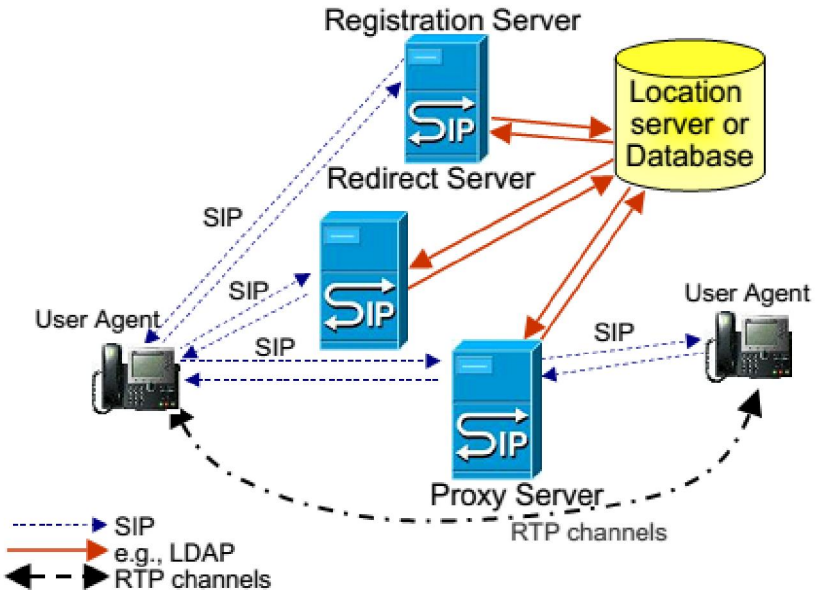

Figura 13 Entidades SIP (Fuente 4)

El Proxy Server: recibe solicitudes de clientes que el mismo trata o encamina hacia otros servidores después de haber eventualmente, realizado ciertas modificaciones sobre estas solicitudes.

El Redirect Server: se trata de un servidor quien acepta solicitudes SIP, traduce la dirección SIP de destino en una o varias direcciones de red y las devuelve al cliente. De manera contraria al Proxy Server, el Redirect Server no encamina las solicitudes SIP. En el caso de la devolución de una llamada, el Proxy Server tiene la capacidad de traducir el número del destinatario en el mensaje SIP recibido, en un número de reenvío de llamada y encaminar la llamada a este nuevo destino, y eso de manera transparente para el cliente de origen; para el mismo servicio, el Redirect Server devuelve el nuevo número (número de reenvío) al cliente de origen quien se encarga de establecer una llamada hacia este nuevo destino.

El User Agent o "UA": se trata de una aplicación sobre un equipo de usuario que emite y recibe solicitudes SIP. Se materializa por un software instalado sobre un "User Equipment" o UE: una PC, un teléfono IP o una estación móvil UMTS.

El Register: se trata de un servidor quien acepta las solicitudes SIP REGISTER. SIP dispone de la función de registro de los usuarios. El usuario indica por un mensaje REGISTER emitido al Register, la dirección donde es localizable (dirección IP). El "Register" actualiza entonces una base de datos de localización. El REGISTER es una función asociada a un Proxy Server o a un Redirect Server. Un mismo usuario puede registrarse sobre distintas UAs SIP, en este caso, la llamada le será entregada sobre el conjunto de estas UAs.

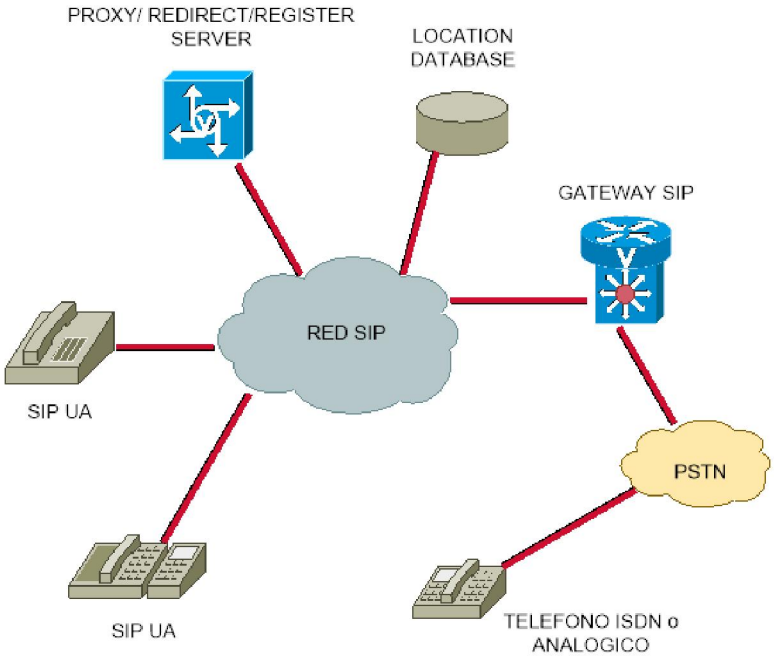

Figura 14: Entidades de una red SIP

Referencias: 4 y 5.

Métodos y Respuestas SIP

El RFC 3261 define seis solicitudes / requerimientos o métodos SIP.
El método "INVITE" es usado con el fin de establecer una sesión entre UAs. INVITE corresponde al mensaje ISUP IAM o al mensaje Q.931 SET UP y contiene las informaciones sobre el que genera la llamada y el destinatario así como sobre el tipo de flujos que serán intercambiados (voz, video,...).
Cuando un UA que emitió el método SIP INVITE recibe una respuesta final a la invitación (ejemplo: 200 OK), el confirma la recepción de esta respuesta por medio de un método "ACK".
Una respuesta del tipo "busy" o "answer" es considerada como final mientras una respuesta tipo "ringing" significando que el destinatario ha sido avisado es una respuesta provisoria.
El método "BYE" permite la liberación de una sesión anteriormente establecida. Corresponde al mensaje RELEASE de los protocolos ISUP y Q.931. Un mensaje BYE puede ser emitido por el que genera la llamada o el que la recibe.
El método "REGISTER" es usado por una UA con el fin de indicar al Registrar la correspondencia entre su Dirección SIP y su dirección de contacto (ejemplo: dirección IP).
El método "CANCEL" es utilizado para pedir el abandono de la llamada en curso pero no tiene ningún efecto sobre una llamada ya aceptada. De hecho, solo el método "BYE" puede terminar una llamada establecida.
El método "OPTIONS" es utilizado para interrogar las capacidades y el estado de un User Agent o de un servidor. La respuesta contiene sus capacidades (ejemplo: tipo de media soportada, idioma soportado) o el hecho de que el UA este indisponible.

Después de haber recibido e interpretado un requerimiento SIP, el destinatario de este requerimiento devuelve una respuesta SIP. Existen seis clases de respuestas:
Clase 1xx: Información, el requerimiento ha sido recibido y está en curso de tratamiento.
Clase 2xx: Éxito, el requerimiento ha sido recibido, entendido y aceptado.
Clase 3xx: Re-enrutamiento, la llamada requiere otros procesamientos antes de poder determinar si puede ser realizada.

Clase 4xx: Error requerimiento cliente, el requerimiento no puede ser interpretado o atendido por el servidor. El requerimiento tiene que ser modificado antes de ser reenviado.
Clase 5xx: Error servidor, el servidor fracasa en el procesamiento de un requerimiento aparentemente valido.
Clase 6xx: Fracaso global, el requerimiento no puede ser procesado por ningún servidor.

Referencias: 4 y 5.

Inscripción a la red SIP

El método "REGISTER" es utilizado por un "USER AGENT" con el fin de indicar a la función Register (físicamente implantada en un Proxy Server o un Redirect Server) la correspondencia entre su dirección SIP (por ejemplo:sip:juan.perez@banco.com) y su dirección IP (ejemplo: sip:juan.perez@192.190.132.20). La dirección IP puede ser estática u obtenida de modo dinámico por DHCP. La función Register actualiza entonces una base de datos de localización.

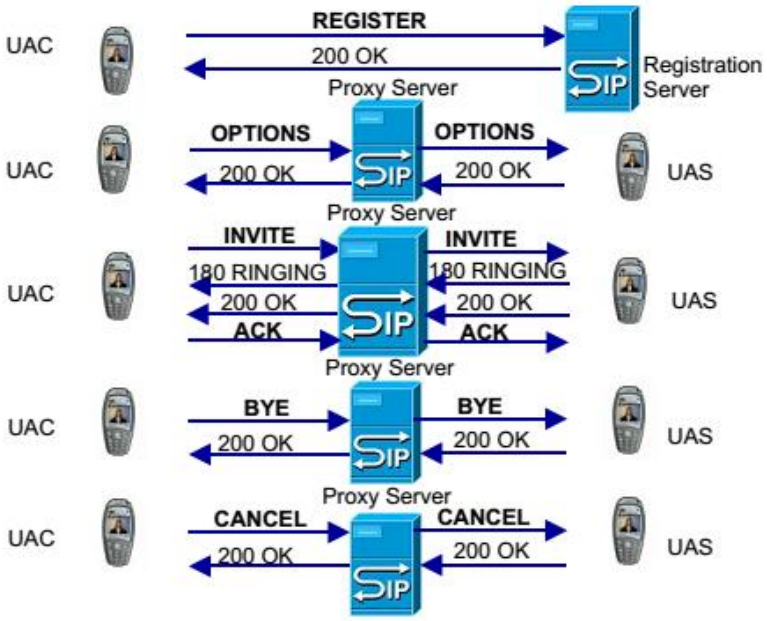

Figura 15 Solicitudes SIP (Fuente 3)

Desde este momento, el User Agent puede recibir llamadas ya que se encuentra ubicado. Si un usuario SIP desea reenviar sus llamadas de su dominio corriente hacia otro dominio, (ejemplo: del dominio banco.com al dominio

francetelecom.com), solo tendrá que indicar a la función Register de banco.com su dirección SIP en el dominio petrolera.com. Cuando un mensaje INVITE debe ser entregado por el Proxy Server del dominio banco.com a sip: juan.perez@banco.com, la base de datos actualizada por la función Register indica al Proxy Server que el mensaje tiene que ser relevado a sip:juan.perez@petrolera.com. Entonces, el Proxy Server efectúa una búsqueda por el DNS de la dirección IP del Proxy Server del dominio petrolera.com con el fin de relevar el mensaje SIP a encaminar al destino apropiado (sip:juan.perez@petrolera.com).

En una red IP Multimedia Subsystem o IMS, el Proxy Server corresponde a una entidad CSCF (**C**all **S**tate **C**ontrol **F**unction), mientras la base de datos de localización es representada por la entidad **H**ome **S**ubscriber **S**erver o HSS. El HSS en el IMS por los móviles es un HLR conteniendo por otra parte el perfil del usuario para los servicios IMS suscritos.

Referencias: 4, 5, 8, 10, 11, 12.

Establecimiento y liberación de sesión SIP

En el ejemplo siguiente, el que llama tiene como URL SIP sip:juan.perez@petrolera.com, mientras la URL SIP del destinatario de la llamada es sip: carlos.garcia@petrolera.com.

Un mensaje de establecimiento de llamada SIP INVITE esta emitido por parte de la UA SIP del que llama al Proxy Server. Este último interroga la base de datos de localización para identificar la localización del que está siendo llamado (dirección IP) y encamina la llamada a su destino. El mensaje INVITE contiene distintos "headers" o encabezamientos obligatorios, entre los cuales la dirección SIP de la persona que llama "From", la dirección SIP de la persona que recibe la llamada "To", una identificación de la llamada "Call-ID", un número de secuencia "Cseq", un número máximo de saltos "max-forwards". El encabezamiento "Vía" esta actualizado por todas las entidades que participaron del enrutamiento requerido INVITE. Eso asegura que la respuesta seguirá el mismo camino que el requerimiento.

Por otra parte, el requerimiento SIP INVITE contiene una sintaxis "**S**ession **D**escription **P**rotocol" o SDP. Esta estructura consiste en varias líneas que describen las características dela media del que llama, en este caso "Juan", que se necesita para la llamada. Juan Pérez indica que la descripción SDP utiliza la versión 0 del protocolo, que se trata de una sesión telefónica (m = audio), que la voz constituida en paquetes le debe ser entregada a la dirección de transporte (puerto UDP = 45450, dirección IP =192.23.34.45) con el protocolo RTP y utilizando un formato de

codificación definido en el RFC "**A**udio **V**ideo **P**rofile" o AVP y pudiendo ser G. 711 o G.728.

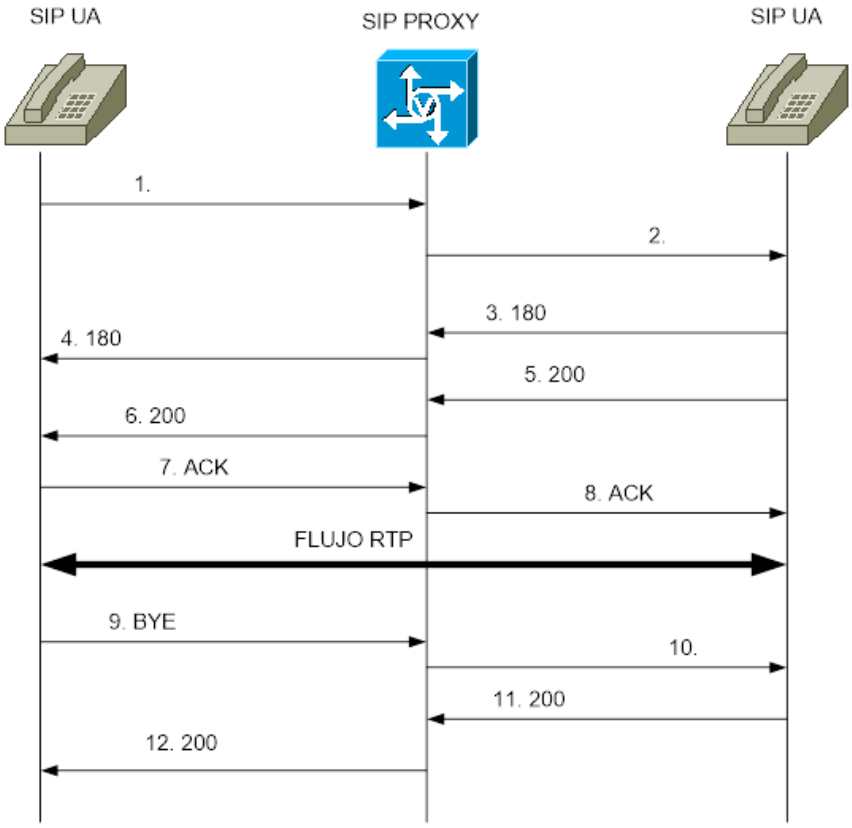

Figura 16: Establecimiento y liberación de sesión SIP UA

La respuesta 180 RINGING esta devuelta por el destinatario a la UA del que genera la llamada.

Cuando el destinatario acepta la sesión, la respuesta 200 OK esta emitida por su UA y encaminada hacia la UA del que genera la llamada.

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

La entidad Proxy Server participa al encaminamiento de la señalización entre UAs mientras que las UAs establecen directamente canales RTP para el transporte de la voz o del video en forma de paquetes sin implicación del Proxy Server en este transporte.

Cuando Juan cuelga, su UA envía un requerimiento BYE para terminar la sesión. Este requerimiento esta entregado al Proxy Server quien lo encamina a la UA de Carlos. Este último, devuelve la respuesta 200 OK.

Referencias: 4, 5, 8, 10, 11, 12.

Extensiones del protocolo SIP

Una entidad SIP puede suscribir a un evento con el fin de ser notificada de su ocurrencia. El requerimiento SUBSCRIBE permite la suscripción mientras el requerimiento NOTIFY es utilizado con el fin de notificar (RFC 3265). El método PUBLISH permite publicar su estado.

El método REFER (RFC3515) reenvía el receptor hacia un recurso identificado en el método. REFER permite emular distintos servicios o aplicaciones incluyendo la transferencia de llamada. Contemplamos T1, la entidad que origino la transferencia, T2 la entidad transferida y T3, el destinatario de la transferencia. La transferencia de llamada permite a T1 transformar una llamada en curso entre T1 y T2 en una nueva llamada entre T2 y T3, elegida por T1. Si la transferencia de llamada se lleva a cabo, T2 y T3 podrán comunicar mientras que T1 no podrá seguir dialogando con T2 o T3.

El método MESSAGE (RFC 3428) ha sido propuesto como extensión al protocolo SIP con el fin de permitir la transferencia de mensajes instantáneos. La mensajería instantánea o "Instant Messaging" o "IM" consiste en el intercambio de mensajes entre usuarios en pseudo tiempo real.

Este nuevo método hereda de todas las funciones ofrecidas por el protocolo SIP tales que el enrutamiento y la seguridad. El requerimiento MESSAGE puede transportar varios tipos de contenidos basándose sobre la codificación MIME.

El método INFO (RFC2976) permite transferir informaciones de señalización durante la llamada.

Entre los ejemplos de información se encuentran los dígitos DTMF, la información relativa a la tasación de una llamada, la imagen, etc...

Las respuestas finales 2xx, 3xx, 4xx, 5xx y 6xx a un requerimiento INVITE son satisfechas por el requerimiento ACK mientras las respuestas provisorias de tipo 1XX no son satisfechas.

Ciertas respuestas temporarias tales como el 180 Ringing son críticas y su recepción es esencial para la determinación del estado de la llamada, entre otros durante el proceso de interconexión con la RTCP. El método PRACK (RFC3262) ha sido definido con el fin de satisfacer la recepción de respuestas temporarias de tipo 1XX.

El método UPDATE (RFC3311) permite a un terminal SIP actualizar los parámetros de una sesión multimedia (por ejemplo: flujo media y sus codecs). El método UPDATE puede ser enviado antes de que la sesión sea establecida. UPDATE es entonces particularmente útil cuando se trata de poner al día los parámetros de

sesión antes de su establecimiento, por ejemplo en puesta en espera del destinatario.

Referencias: 4, 5, 8, 10, 11, 12.

Interfuncionamiento entre SIP y PSTN

Para el inter-funcionamiento entre la Red Telefónica Conmutada PSTN y SIP, es necesario introducir un Gateway PSTN/SIP como una interfaz entre la PSTN y una red SIP. Este Gateway cumple con dos funciones:

- Traducción de la señalización ISDN User Part o ISUP en señalización SIP y recíprocamente, conversión de señales audio en paquetes RTP y recíprocamente.

Este Gateway establece canales lógicos RTP con la terminal SIP y establece circuitos de palabras con un switch Class 4 o Class 5. El Class 5 representa un switch telefónico de acceso mientras el Class 4 es un switch telefónico de tránsito.

En el ejemplo contemplado en la figura siguiente, un terminal conectado a la PSTN llama un UA SIP. El Switch Class 5, al cual está conectado es el que genera la llamada y emite un mensaje ISUP IAM al Gateway PSTN/SIP. Este mensaje contiene el número del destinatario, el identificador del circuito elegido por el Switch Class 5 para la llamada (**C**ircuit **I**dentification **C**ode o CIC) así como información donde indica la naturaleza de la llamada (palabras, fax, datos, etc.).
El Gateway PSTN/SIP traduce este mensaje en un requerimiento SIP INVITE que contiene una dirección de destino SIP de la cual el campo "user" es un número telefónico. Pasa el mensaje al SIP Proxy Server que obtiene la dirección IP del destinatario con la dirección SIP por medio de la interrogación de una base de datos o de un servidor de localización. El mensaje INVITE esta relevado a la UA SIP. En paralelo, el Proxy Server notifica al Gateway la recepción del requerimiento INVITE por medio de la respuesta 100 Trying. El terminal SIP devuelve al Proxy Server una respuesta 180 Ringing para informar el que llama de la alerta del mensaje relevado por el Proxy Server al Gateway. El Gateway traduce esta respuesta en un mensaje ISUP "**A**ddress **C**omplete **M**essage" o ISUP ACM enviado al SwitchClass 5. Este mensaje esta traducido por el SwitchClass 5 en un mensaje "Alerting" si el terminal que origina la llamada es una terminal RDSI o en una señal "Ringing Tone" en el caso de una Terminal analógica.

Cuando el destinatario descuelga, una respuesta 200 OK es devuelta al Proxy Server quien la releva al Gateway. El Gateway pone el recibí de esta respuesta por un requerimiento ACK encaminado por el Proxy Server al destinatario. En paralelo, el Gateway genera un mensaje ISUP Answer Message o ISUP ANM emitido al Class 5 Switch.

Este intercambio de señalización ha permitido el establecimiento de canales RTP entre el terminal SIP y el Gateway así como la colocación de un circuito de voz entre el Gateway y el Class 5 Switch.

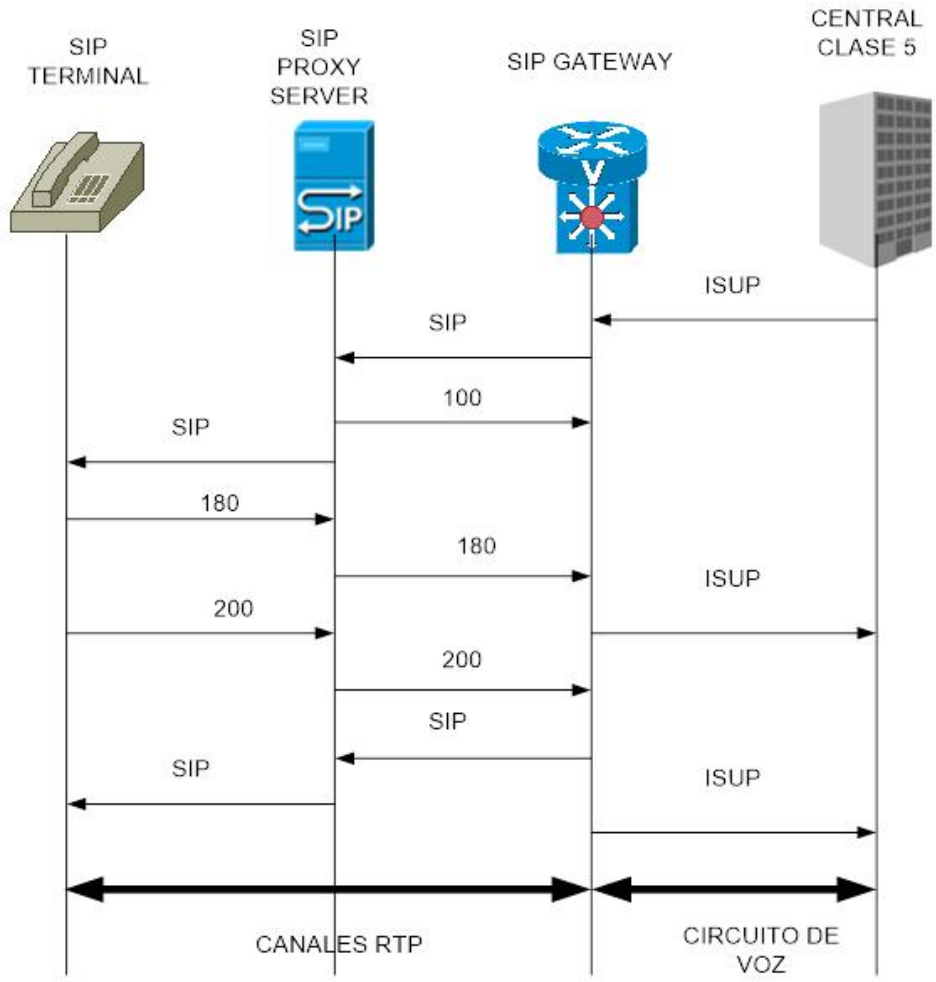

Figura 17: Interfuncionamiento PSTN/SIP

Durante la fase de transferencia de información, el Gateway convierte las señales de audio recibidas sobre el circuito de voz en paquetes RTP enviados sobre los canales RTP y vice versa.

Referencias: 4, 5, 8, 10, 11, 12.

Arquitectura de servicios SIP

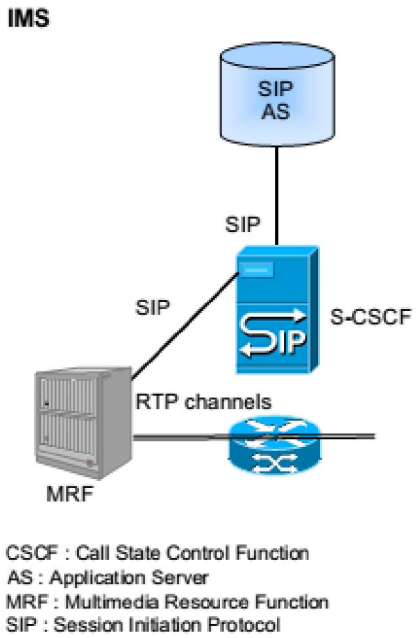

Figura 18 Arquitectura de servicios IMS (Fuente 3)

La arquitectura de servicios SIP de base está constituida por servidores de aplicación, por servidores de media y de S-CSCF.

El servidor de aplicación SIP ejecuta servicios (ejemplo: Push To Talk, Presence, Prepaid, Instant messaging etc.) y pueden influenciar el desempeño de la sesión a pedido del servicio.

El SIP **M**ultimedia **R**esource **F**unction o MRF establece conferencias multimedia, ejecuta anuncios vocales o multimedia y recoge información de los usuarios. Se trata de la evolución de la entidad **S**pecialized **R**esource **P**oint o SRP en el mundo multimedia.

El SIP Proxy Server tiene el papel de punto desde el cual un servicio puede ser requerido. El dispone del perfil de servicio del abonado que le indica los servicios suscritos por el abonado y bajo cuales condiciones invocar estos servicios. Corresponde al SSP de la arquitectura Red Inteligente.

Referencias: 4, 5, 8, 10, 11, 12.

Servidor de aplicación

Un servidor de aplicación SIP provee un ámbito donde se ejecutarán las aplicaciones, llamado "**S**ervice **L**ogic **E**xecution **E**nvironment" o SLEE. El provee un conjunto de servicios que permite simplificar las tareas de los desarrolladores de aplicaciones así como de los administradores. El objetivo es de disponer de una plataforma que pone en obra todas las funcionalidades permitiendo así al desarrollador enfocarse únicamente en la lógica "profesional" de la aplicación.

Las funciones de un servidor de aplicación son las siguientes:

- La gestión de recursos: el servidor de aplicaciones controla la creación y la utilización de recursos tales como la conexión de transporte, los componentes aplicativos (ejemplo: scripts CPL, servlets SIP) así como las sesiones de aplicaciones.
- La gestión de aplicaciones: la aplicación puede ser asociada a un perfil de configuración durante su despliegue. Este perfil puede contener parámetros que pueden ser modificados a través de la interface administrativo durante el despliegue de la aplicación o durante su ejecución.
- La composición de aplicación: el servidor de aplicación debe permitir la ejecución de varias aplicaciones por un mismo requerimiento SIP. Eso provee una capacidad de modularización. De hecho, elementos de servicio pueden ser desarrollados independientemente y pueden ser combinados según las necesidades de aplicación. Eso permite por otra parte un mejor control de las interacciones de servicio.
- La integración WEB: con el fin de proveer un GUI Web para la administración y el inter-funcionamiento con servidores WEB previendo servicios.
- La programación: el servidor de aplicación provee un soporte para el desarrollo de aplicación, i.e. APIs (JAIN API, SIP Servlet API, etc.) así como lenguajes de script. Los scripts pueden ser creados con el apoyo de ámbitos de creación de servicio.
- El inter-funcionamiento: el servidor de aplicación comunica usando el protocolo SIP con el servidor de media (IP media server) para las interacciones con el usuario y con el servidor de llamada (CSCF) para el encaminamiento y la señalización.

- La seguridad: el servidor de aplicación debe proveer mecanismos de encriptación, de autentificación y de autorización con el fin de asegurar un acceso segurizado a los servicios.
- Las capacidades no funcionales: alta disponibilidad, reparto de carga, tolerancia a los errores. Estas características son similares a las características exigidas por un SCP en la arquitectura de Red Inteligente.

Referencias: 4, 5, 8, 10, 11, 12.

El servidor de media SIP

El servidor media SIP es una plataforma poderosa y evolutiva para el desarrollo de servicios de portales vocales y servicios vocales / video interactivos capaces de soportar centenares y hasta millares de sesiones simultaneas en un amplio rango de configuraciones.

El servidor de media SIP es un equipo físico y pone en obra la entidad funcional "**M**ultimedia **R**esource **F**unction" o "MRF" definido por el "IMS". El servidor de media SIP provee las funciones permitiendo interacciones entre usuarios y aplicaciones a través de recursos vocales / video. Por ejemplo, él puede responder a una llamada y difundir un anuncio, o leer un mensaje electrónico usando funciones de síntesis vocales o colectar una información del usuario (ejemplo: clave, voto, número) y devolverla a la aplicación.

El servidor de media SIP pone en obra dos tipos de funciones:

Las funciones de recursos media tales como las funciones de detección de tonalidad, de síntesis vocal, de reconocimiento vocal, de traducción de la media, etc. Es la función "**M**ultimedia **R**esource **F**unction **P**rocessor" o "MRFP".

Las funciones de control del servidor de media que proveen a las aplicaciones los medios de controlar los recursos del servidor de media tales como, tocar un mensaje, colectar un voto, gravar un mensaje etc. Y eso, a través del protocolo SIP. Es la función "**M**ultimedia **R**esource **F**unction **C**ontroller" o "MRFC".

La arquitectura distribuida del servidor de media SIP / servidor de aplicación separa las aplicaciones voz / video del control de medias, lo que permite a los operadores reducir los costos de los recursos de red y albergar con costos menores las aplicaciones clientes. El servidor de media IP soporta el protocolo de control SIP. Además del servidor de media IP y del servidor de aplicación, las entidades siguientes pueden ser contempladas:

Browser Voice XML: este componente integrado en el servidor de media IP provee un ejemplo de ámbito de ejecución de aplicaciones vocales. Las aplicaciones

desarrolladas según las especificaciones Voice XML pueden ser interpretadas y ejecutadas por el Browser Voice XML.
Este Browser solo interpreta y determina las etapas atómicas del call flow. Es el servidor de media IP que interactúa con el usuario.

Servidor ASR: este componente provee el servicio "**A**utomatic **S**peech **R**ecognition" o ASR. El flujo de audio del usuario es transportado sobre RTP del Media Gateway o del teléfono IP del usuario al servidor ASR. El Browser Voice XML contacta el servidor ASR cuando un reconocimiento de palabra es necesario.

Servidor TTS: este componente provee el servicio "**T**ext-**T**o-**S**peech" o TTS. Una cadena de caracteres esta emitida hacia este componente y está convertida en un aviso vocal que puede ser emitido al usuario bajo la forma de flujo RTP. El browser Voice XML contacta el servidor TTS cuando un texto debe ser traducido en un mensaje vocal y entregado al usuario.

Servidor WEB: este componente es un servidor estándar http. Esta utilizado con el fin de albergar el contenido vocal. Este contenido consiste en un escrito Voice XML, anuncios vocales / video, mensajes de recepción y gramáticas de reconocimiento de la palabra. Los escritos Voice XML definen la lógica de aplicación. Mensajes de recepción apoyan el usuario en su navegación dentro de una aplicación. Las gramáticas contienen las palabras autorizadas o las frases que un usuario puede pronunciar cuando la aplicación le pide ingresar sus informaciones.

Referencias: 4, 5, 8, 10, 11, 12.

Funcionalidades del servidor de media

Las funcionalidades del servidor de media SIP incluyen las funciones de control de la media y de recursos dela media:

Anuncios: la mayor parte de los servicios evolucionados utiliza formas de anuncios, ya sea un mensaje de bienvenida durante el acceso al buzón de la mensajería unificada, o de un mensaje de introducción a un portal local. La utilización de un servidor de media SIP para realizar servicios de anuncios permite no tener que desplegar un nuevo servidor de anuncios; reduciendo así el número de elementos de red y simplificando la gestión de la red. Un equipo de almacenamiento externo puede ser utilizado para almacenar anuncios creando así una solución confiable y escalable. El protocolo RTP se utiliza para entregar el anuncio al usuario.

Automated **S**peech **R**ecognition (ASR): el reconocimiento de la voz es un componente de la mayor parte de los servicios al usuario tales como mensajería vocal (voicemail), la mensajería unificada, juegos interactivos y portales vocales.

Generación de la información de tasación: una tasación precisa y justa es una exigencia de los operadores de servicio con el fin de ofrecer servicios de voz y datos con fuerte valor agregado. El servidor de media SIP genera la información de tasación.

Interactive **V**oice **R**esponse (IVR): el servidor de media SIP debe soportar la detección de tonalidades DTMF enviadas en la banda, así como los dígitos recibidos vía SIP INFO.

Grabación: el servidor de media SIP tiene capacidades de grabación y de restitución (playback).
Numerosas aplicaciones tales como la mensajería vocal, la mensajería unificada, el push-to-talk y la conferencia utilizan esta función por ejemplo, grabación de la llamada para que sea restituida posteriormente. El servidor de media SIP utiliza servidores de almacenamiento que existen donde se encuentra el operador de servicios.

Text-**T**o-**S**peech: la tecnología "text-to-speech" está estrechamente asociada a la funcionalidad IVR. El "text-to-speech" es utilizado en aplicaciones tales como la mensajería unificada a fin de leer E-mail o fax a través del teléfono. La traducción puede ser realizada en varios idiomas.

Gestión del multipartes: el servidor de media SIP debe ser capaz de proveer todos los mecanismos de control de las llamadas con varios participantes. Esta funcionalidad es utilizada dentro de numerosas aplicaciones tales como conferencias o el Push-To-Talk.

Transcodificación: la transcodificación permite convertir un esquema de codificación digital en otro. En el caso de una conferencia donde los participantes no disponen de un mismo codificador común, el servidor de media SIP asegurara entonces las traducciones de media necesarias.

Interfaces estándares abiertas: el servidor de media SIP debe poder ser controlado a través el protocolo SIP y debe poder ejecutar escritos Voice XML.

Referencias: 4, 5, 8, 10, 11, 12.

Puesta en obra de servicios

El método de introducción del servicio depende del tipo de servicio y de su complejidad. Así mismo, un servicio puede ser puesto en obra sobre el terminal SIP, el servidor de media SIP, el servidor de aplicación o el Proxy Server.
Ciertos servicios requieren de una interacción compleja con el usuario (mensajería unificada, IVR). Para estos servicios vocales, un acercamiento centralizado es necesario con las entidades:

- **AS SIP** conteniendo la lógica de aplicación y
- Servidores de media SIP conteniendo el escrito vocal.

Algunos servicios requieren una base de datos centralizada. Para estos servicios de traducción de número (servicios de numero abreviado, servicio prepago, servicio VPN), es necesario un **AS SIP** que contiene la lógica de aplicación.
Algunos servicios de enrutamiento flexible necesitan una configuración personalizada por abonado. El lenguaje "Call Processing Language" o CPL puede ser usado para eso. Es posible ejecutar este escrito por un AS SIP o par el proxy server.
Algunos servicios no se prestan bien a un tratamiento centralizado. La aparición de terminales SIP basados sobre una maquina Java, ha ofrecido la posibilidad de desarrollar servicios sobre los terminales:

- El servicio timbre diferenciado permite modificar el timbre del puesto llamado según la identidad del que llama. Este servicio básico es típicamente un servicio que conviene desplegar sobre el aparato.
- El servicio de filtro de llamada es una evolución del servicio anterior en la cual la identidad del llamado sirve para determinar si la llamada debe ser aceptada, reenviada o bien rechazada.
- El servicio de guía telefónica subraya el interés de una conexión directa del terminal con una guía de empresa: permite al usuario consultar una base de datos vía LDAP desde el teléfono, seleccionar un número entre los resultados de la consulta y generar una llamada hacia dicho número.

Referencias: 4, 5, 8, 10, 11, 12.

2.3.7 Protocolo Diameter.

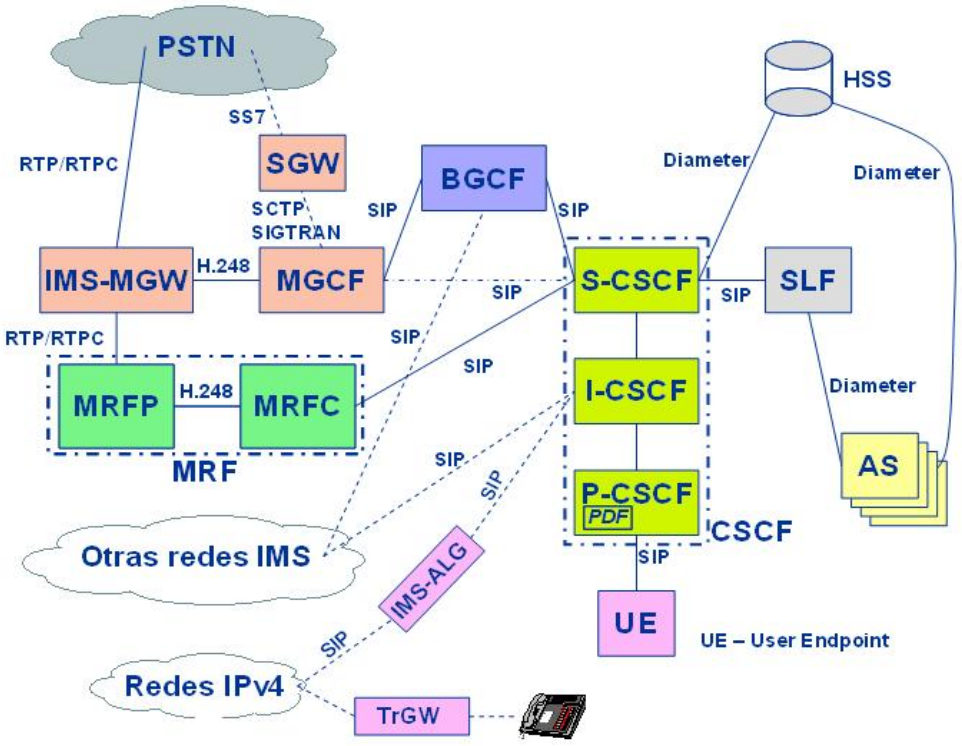

Figura 19 Esquema de red IMS - Diameter

Este protocolo es ampliamente utilizado en la arquitectura IMS para que las entidades intercambien información relacionada con AAA (**A**utenticación, **A**utorización y **A**ccounting). El protocolo Diameter constituye la próxima generación en AAA. Surge del protocolo Radius, con una gran cantidad de mejoras en varios aspectos, y se espera que sea el protocolo de la próxima generación en AAA.

Dado que la arquitectura IMS es el objeto de esta investigación, por lo que representa en la industria de las telecomunicaciones, creo que es necesario entender claramente este protocolo para poder entender la esencia de la arquitectura IMS. Por eso en esta parte de la investigación tratare de mostrar una introducción al protocolo Diameter y ver cómo trabaja.

Con las nuevas tecnologías emergentes y aplicaciones tales como redes inalámbricas y móviles basadas en IP; los requerimientos para la autenticación y autorización se han incrementado. Junto con los mecanismos de control de acceso que son cada vez más complejos. El protocolo RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice), resulta insuficiente para satisfacer estos nuevos

requerimientos. Se necesita un nuevo protocolo que sea capaz de soportar estas nuevas características de control de acceso, permitiendo cierta flexibilidad. Esto justamente es lo que se logra con el protocolo DIAMETER, que tratare de describir a continuación.

Referencias: 14, 15, 16, 17, 18.

AAA y Diameter

Antes de entrar en los detalles del protocolo, veamos que condujo a requerir un protocolo de AAA. Hace unos años cuando la gente se conectaba a su ISP, por medio de una conexión de Dial Up, proveía su ID y password a un Access Server, el cual autenticaba el usuario antes de proveer el acceso a Internet. En la mayoría de los casos, las credenciales de los usuarios no se guardan directamente en el Access Server, sino en un servidor LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol) detrás de un Firewall. Por ende un protocolo estandarizado se requiere entre el Access Server y la información del usuario en el servidor LDAP, para intercambiar información de autenticación, autorización y accounting. El protocolo RADIUS sirve para tal efecto, de una manera simple, pero eficiente, proveer esta capacidad de AAA.

Con la evolución de las aplicaciones de red y protocolos, surgieron nuevos requerimientos para la autenticación de los usuarios. Para más detalles se puede consultar la RFC2989. Entre estos se puede considerar la posibilidad de recupero ante fallas (failover), mecanismos de seguridad y auditoria. Aunque existen protocolos para extender la capacidad de RADIUS, el protocolo DIAMETER es más genérico, y surgió basado en un modelo de capas para soportar aplicaciones AAA.

Su nombre implica una versión mejorada de RADIUS. Incluye numerosas mejoras en varios aspectos, tales como manejo de errores y capacidad de envío de mensajes en forma segura. Extrae la esencia del protocolo RADIUS, en cuanto a todo lo que se refiere a AAA. Y además define un conjunto de mensajes que constituyen el CORE o núcleo de la base del protocolo DIAMETER. Las aplicaciones que requieren funciones de AAA, pueden definir sus propias extensiones en la base misma del protocolo. Pudiéndose beneficiar con las características generales del protocolo. La siguiente figura muestra la relación entre el protocolo de base DIAMETER y varias aplicaciones DIAMETER.

Figura 20: Relación entre el protocolo base y las aplicaciones Diameter

Referencias: 14, 15, 16, 17, 18.

Nodos y Agentes Diameter

La arquitectura del protocolo DIAMETER, está diseñado como peer to peer, y por ende cualquier host que invoca este protocolo puede actuar tanto como Cliente o como Server, dependiendo del diseño de la red. Por eso el término Nodo Diameter, se usa para referirse a un Cliente Diameter, un Server Diameter o un Agente Diameter. El nodo Diameter que recibe el pedido de conexión de un usuario, actuara como Cliente Diameter. En la mayoría de los casos, el Cliente Diameter es uno de los Server de acceso de la red. Luego de recibir las credenciales del usuario, como usuario y password, genera un mensaje a un Nodo DIAMETER pidiendo ser atendido. Podemos, por simplicidad asumir que es el Servidor DIAMETER. Este Server autentica al usuario basado en la información que se le provee. Si el proceso de autenticación es exitoso, los privilegios del usuario son devueltos en el mensaje de respuesta, que se envía al Cliente DIAMETER. Si por el contrario la autenticación falla, se devuelve un mensaje rechazando el requerimiento.
Aunque esta arquitectura que se describe parece una arquitectura tradicional client-server. El nodo que actúa como DIAMETER Server para ciertos pedidos puede actuar como un Cliente DIAMETER en algunas situaciones. El protocolo DIAMETER es una arquitectura peer to peer, en el sentido más genérico. Además, un nodo especial llamado DIAMETER Agent está claramente definido en el protocolo.

Típicamente existen tres clases de Agentes DIAMETER:

- Relay Agent: se usa para reenviar mensajes al destino apropiado, dependiendo de la información que contenga dicho mensaje. Posee la ventaja que puede agregar pedidos de diferentes regiones, para una región en particular, lo que elimina las configuraciones de los servidores de las redes de acceso por cada modificación en el servidor de DIAMETER.

- Proxy Agent: también puede usarse para reenviar mensajes, pero a diferencia del Relay Agent, puede modificar el contenido del mensaje, y por ende proveer servicios de valor agregado, hacer cumplir reglas para diferentes mensajes o realizar alguna tarea administrativa para una región especifica. La figura siguiente muestra cómo se usa el Proxy Agent para reenviar un mensaje a otro dominio. Si el Proxy Agent no modificara el contenido del pedido original, un Relay Agent sería suficiente para este caso.

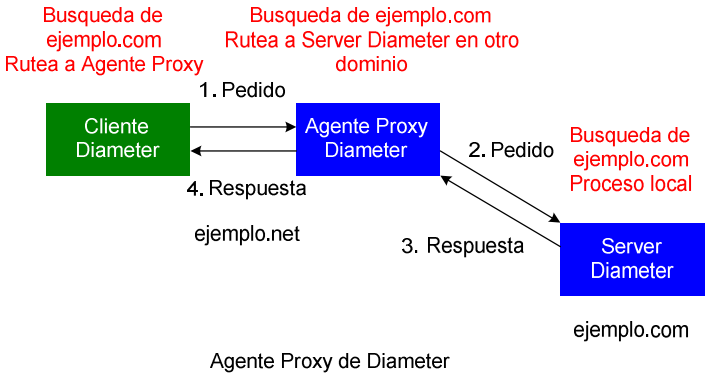

Figura 21: Agente Proxy de Diameter

- Redirect Agent: actúa como una base centralizada de la configuración para otros nodos DIAMETER. Cuando recibe un mensaje, chequea su tabla de ruteo, y devuelve una respuesta con la información re-direccionada al que la envió originalmente. Esto puede ser muy útil para otros nodos DIAMETER, ya que no necesitan mantener una lista de las posibles rutas localmente, solo buscar un Redirect Agent cuando lo necesiten. La siguiente figura muestra cómo trabaja un Redirect Agent. En este esquema es básicamente igual a la figura anterior, salvo que en este caso el Proxy Agent no conoce la dirección del nodo DIAMETER con la que tiene que comunicarse para localizar el domino ejemplo.com. Por ende busca al Redirect Agent para conseguir la dirección.

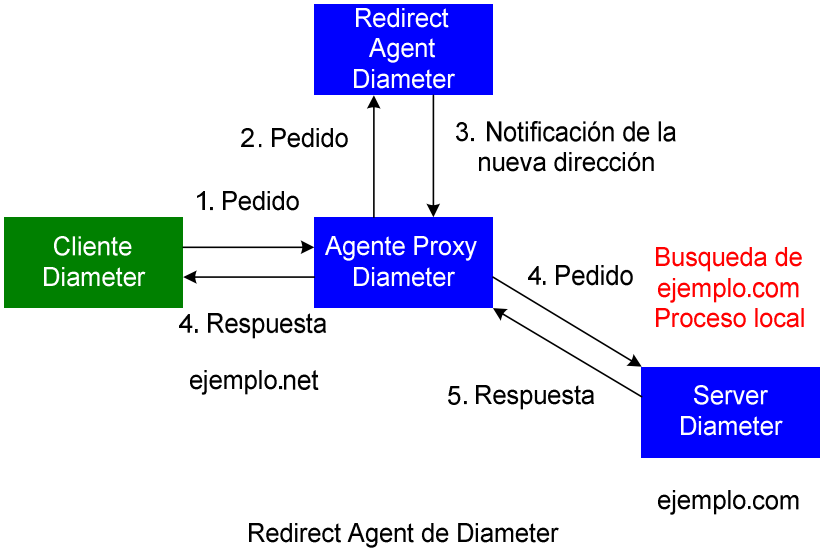

Figura 22: Redirect Agent de Diameter

- Translation Agent: este es un Agente especial. Su tarea es, es convertir un mensaje de un protocolo AAA en otro. Este Agent es de gran ayuda para un proveedor de servicios o un acompaña que necesita integrar la base de datos de usuarios de dos dominios de aplicaciones, manteniendo los protocolos originales AAA. Otra situación, es alguien que necesite migrar al protocolo DIAMETER, pero dado que la migración puede requerir varias etapas, El Translation Agent podría proveer la capacidad de volver atrás (Roll Back), para una migración segura, sin sobresaltos. La figura siguiente muestra como un Agent traduce el protocolo Radius en el protocolo DIAMETER, pero también es posible otro tipo de traducciones, como ser, Diameter a Radius, Diameter a TACACS+.

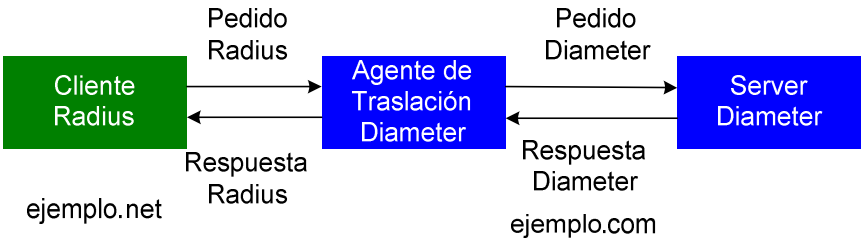

Figura 23: Agente de Translación Diameter

Referencias: 14, 15, 16, 17, 18.

Mensajes Diameter

Un mensaje Diameter, es una unidad básica que sirve para enviar un comando o una notificación a otros nodos DIAMETER. El protocolo DIAMETER define varios mensajes para diferentes propósitos, los cuales son identificados por un código de comando. Por ejemplo, un pedido de Accounting, reconoce que trae información relacionada con la cuenta. Mientras que un mensaje de pedido de intercambio de capacidades, reconoce que el mensaje trae información de capacidades del nodo DIAMETER que envió el mensaje.

Dado el modo en que DIAMETER intercambia los mensajes es sincrónico, cada mensaje tiene su correspondiente contrapartida que comparte el mismo código de comandos. En los ejemplos anteriores, el que recibe el pedido de Account, prepara una respuesta Account y la devuelve al que envió el mensaje originalmente.

El código de comando se usa para identificar la intención de un mensaje, pero los datos realmente se llevan en un conjunto denominado: AVPs (**A**ttribute **V**alue **P**airs). El protocolo DIAMETER tiene predefinido un conjunto común de atributos e impone cada atributo con la correspondiente semántica. Estos AVPs llevan el detalle de AAA, así como también la información de ruteo, seguridad y capacidad entre los dos nodos DIAMETER. Además, cada AVP se asocia con un tipo de formato AVP, el cual es definido dentro del protocolo DIAMETER, (por ejemplo OctetString, Integer32), por eso el valor de cada atributo debe seguir el formato de los datos.

La figura siguiente ilustra la relación entre menajes Diameter y su correspondiente AVPs.

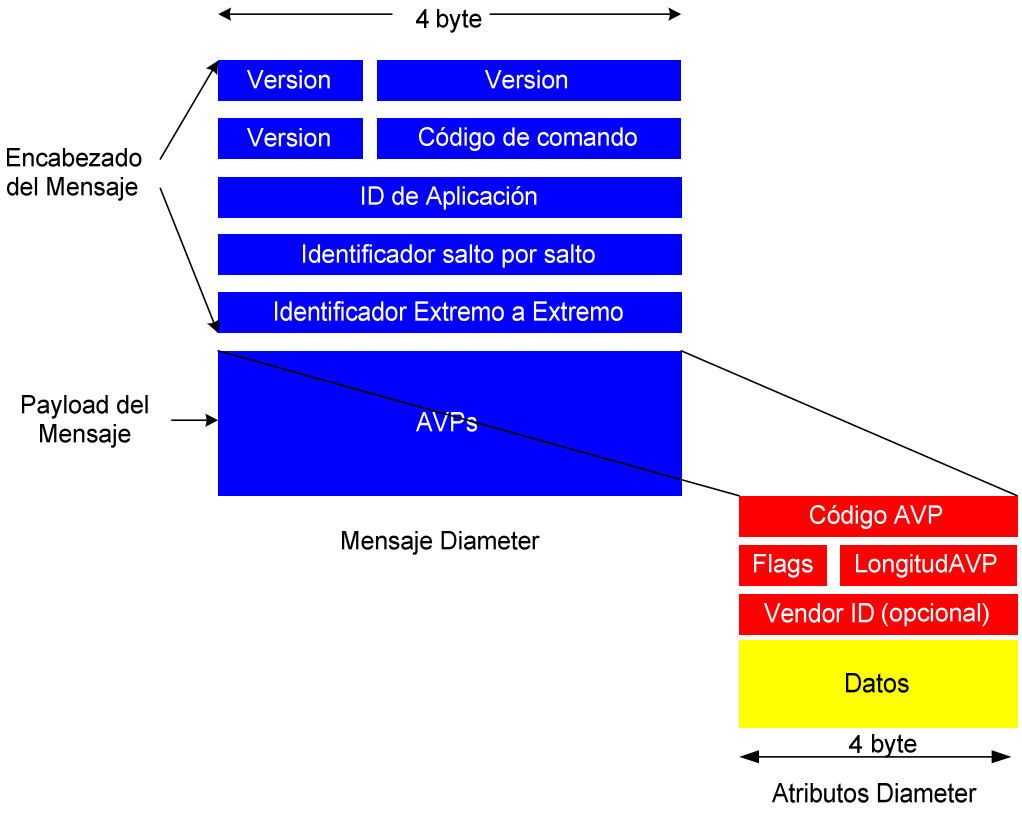

Figura 24: Formato del paquete Diameter

Tabla 1: Lista de todos los mensajes definidos en el protocolo Diameter

Nombre del Mensaje	Abreviatura	Código de Comando
Abort-Session-Request	ASR	274
Abort-Session-Answer	ASA	274
Accounting-Request	ACR	271
Accounting-Answer	ACA	271
Capabilities-Exchanging-Request	CER	257
Capabilities-Exchanging-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

Referencias: 14, 15, 16, 17, 18.

Descubrimiento del Par (Peer Discovery)

Anterior a la configuración de DIAMETER, el administrador del sistema debe manualmente configurar el servidor de acceso de la red, con la ubicación del servidor AAA. Por eso cuando un usuario se conecta, el dispositivo o NE (**N**etwork **E**lement), puede enviar el pedido a la dirección correcta. Esa configuración, puede ser tediosa para redes complejas. Una notable mejora en DIAMETER es la capacidad de descubrimiento de Pares. Además de la configuración manual, lo que debe ser soportado por todos los nodos DIAMETER, existen dos opciones: SRVLOC y DNS, que pueden usarse para descubrimiento de pares. El concepto es que se requiere que un servidor DIAMETER o un Agente Diameter, envíe en forma de broadcast, que aplicaciones lo soportan, junto con el nivel de seguridad proveída.
Los clientes DIAMETER, dependen de lo que desee la aplicación DIAMETER, nivel de seguridad e información de la región, para buscar el primer nodo DIAMETER, por medio del cual podrán reenviar mensajes DIAMETER. Para un nodo DIAMETER, el descubrimiento de ubicaron de pares, como así la información de ruteo, se guardara localmente, usando dos tablas:

- ✓ Tabla de Pares: es principalmente usada para almacenar la dirección de los nodos conocidos de DIAMETER. Además de la siguiente información: si el nodo DIAMETER fue ubicado dinámicamente o el status del mismo o información relacionada con la seguridad del nodo.

- ✓ Tabla de ruteo de pares: existen cuatro columnas importantes de esta tabla que requieren atención, para el ruteo de mensajes. Las dos primeras son el nombre de la región y de la aplicación, las cuales aplican el criterio de ruteo del mensaje. La tercera es la acción a tomar para el mensaje, que puede ser: Proxy, Relay, Redirect o Local. Local implica que el mensaje se procesara localmente, en lugar de ser reenviado a otros nodos. La última es una referencia a una entrada en la tabla de pares, usada para determinar la dirección actual del host de destino. Notar que la Tabla de pares, siempre contendrá un criterio por defecto para los mensajes que no encuentren un criterio de ruteo.

Referencias: 14, 15, 16, 17, 18.

Conexión y Sesión

Después que un Par apropiado fue descubierto, el próximo paso es establecer una conexión con ese Par. Llamando conexión al link físico entre dos nodos DIAMETER. Es mandatario para el protocolo DIAMETER, correr sobre TCP o SCTP. Comparado con UDP, que usa Radius, estos dos protocolos proveen un método de transporte más confiable, lo cual es crítico para intercambio de aplicaciones relacionadas con información relacionada con accounting.

Dado que DIAMETER es una arquitectura básicamente peer to peer, podría haber más de una conexión establecida para un nodo en particular. El protocolo DIAMETER explícitamente define que un nodo DIAMETER debe establecer una conexión con dos pares por región como mínimo, actuando como contacto primario y contacto secundario. Por supuesto, conexiones adicionales se pueden establecer cuando sea necesario.

Comparado con una conexión, una sesión es una conexión lógica entre dos nodos DIAMETER, y puede atravesar múltiples conexiones. El concepto de una sesión es el de una secuencia de actividades dentro de una trama de tiempo, y se refiere a la interacción entre un Cliente y un Servidor DIAMETER, en un periodo dado. Cada sesión en DIAMETER se asocia con un sesión ID de cliente que es único. Este ID se usa para identificar una sesión en particular durante la comunicación.

La figura siguiente muestra el concepto de una conexión y el de una sesión.

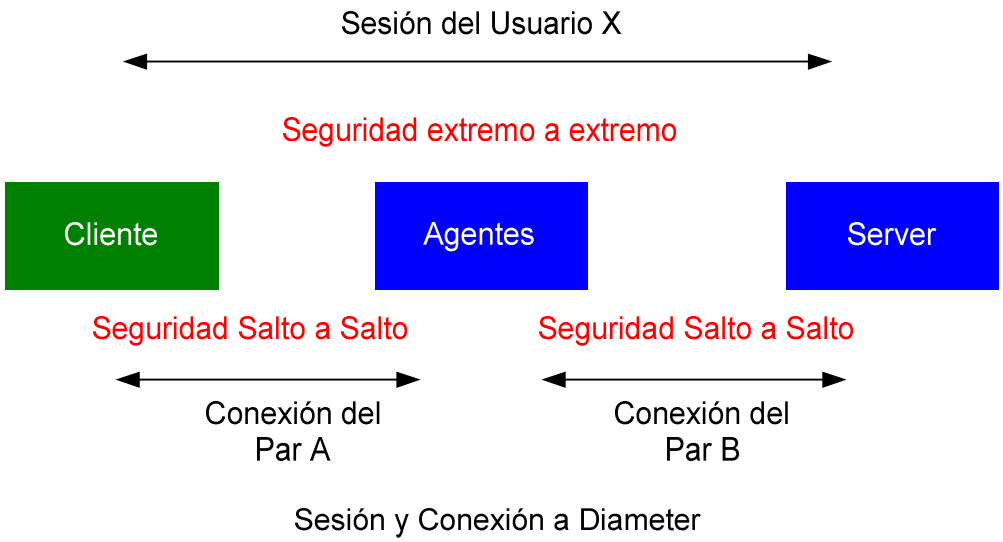

Figura 25: Sesión y conexión en Diameter

Referencias: 14, 15, 16, 17, 18.

Inicio de Sesión

Como la mayoría de los modelos de comunicaciones cliente-servidor, una sesión Diameter, comienza con un mensaje de requerimiento de un cliente al servidor. En el contexto de Diameter, un cliente Diameter enviara un pedido de autenticación conteniendo un Id de sesión único al servidor de Diameter (o al Proxy de Diameter si se requiere reenviar el mensaje). Luego de aceptado el mensaje con el pedido de autenticación, el servidor de Diameter puede incluir una autorización con determinado tiempo de vida, en su respuesta (AVP). Este tiempo indica la cantidad de segundos dentro de los cuales el cliente Diameter necesita ser re autorizado. Luego de un tiempo de gracia prefijado, el servidor Diameter remueve la sesión y libera todos los recursos utilizados por la misma.

Referencias: 14, 15, 16, 17, 18.

La sesión

Durante una sesión, el servidor Diameter puede iniciar una re autenticación o pedido de re autorización. Con los servicios pre pagos, este tipo de servicios, se usa para chequear si el usuario está todavía con crédito, y si no, el servidor remueve la sesión para evitar cargos adicionales.
También, el Id de origen y estado AVP, se usa para inferir un cierre excepcional de sesión. El que envía el pedido incluirá este AVP, y como se requiere un valor para este AVP que sea incrementado en forma monolítica, el que recibe el pedido puede fácilmente inferir que la sesión previa fue cerrada, ya sea porque el dispositivo de acceso fue cerrado en forma anormal o por alguna otra situación excepcional.
El que recibe el pedido puede luego remover la sesión de su lista, liberar los recursos.

Referencias: 14, 15, 16, 17, 18.

Terminación de Sesión

Los mensajes de terminación de sesión, son solamente usados en el contexto de autenticación y autorización, y cuando el estado de la sesión es mantenido. Para servicios de accounting, se envía un mensaje de parar.
Un mensaje de terminación puede ser iniciado tanto por el cliente como por el servidor Diameter. Cuando una sesión está por cerrarse, el cliente envía un pedido de terminación de sesión al Server. La cláusula de terminación se incluye en el AVP,

diciendo al Diameter server los motivos por los cuales la sesión se debe cerrar. Otra alternativa es que el servidor Diameter detecte que la sesión se debe cerrar, ya sea porque el usuario está quedándose sin crédito o por motivos administrativos, el servidor Diameter envía un mensaje de pedido de suspender la misma (**S**ession-**T**ermination-**R**equest) al cliente. Sin embargo dependiendo de las políticas o escenarios el cliente Diameter puede decidir no cerrar la sesión aun cuando reciba un mensaje de terminación del servidor, y dejar al usuario usar su servicio.

Referencias: 14, 15, 16, 17, 18.

Autenticación y Autorización

Como mencione más arriba, el protocolo Diameter se basa en un intercambio general de mensajes. Dado que la mayoría de los procesos de autenticación y autorización varían dependiendo de las aplicaciones. Por eso el protocolo Diameter no define los códigos o comandos y AVPS específicos para AAA. Esto es responsabilidad de la aplicación Diameter definir sus propios mensajes y los correspondientes atributos basados en las características de la aplicación.
Por ejemplo, el mensaje AA-Request, se usa para llevar información de autenticación y autorización en una aplicación de NAS (**N**etwork **A**ccess **S**erver), mientras que en una aplicación SIP, el mensaje se llama UAS (**U**ser-**A**uthorization-**R**equest).

Referencias: 14, 15, 16, 17, 18.

Cuentas (Accounting)

A diferencia de autenticación y autorización, el comportamiento y el mensaje a intercambiar para facturación están claramente definidos. La facturación en Diameter esencialmente sigue un modelo de server directamente. Lo que implica que el dispositivo que genera el proceso de facturación sigue la dirección de un servidor de autorización. Basado en el perfil del usuario, o en cualquier condición de negocios, el servidor Diameter informa al correspondiente cliente, cual es el comportamiento que se requiere. Como cuan seguido los registros de las cuentas deben ser enviados del cliente al server, o si los registros de las cuentas deben ser generados continuamente dentro de una sesión. Generalmente, dependiendo del servicio que se proveerá, existen dos clases de registros de cuentas: para un servicio de invocación de única vez, se usa EVENT_RECORD. Sin embargo, si el servicio será provisto durante un cierto periodo a medir, los tipos de registros de

cuentas son START_RECORD, INTERIM_RECORD, y STOP_RECORD, para marcar el comienzo, la actualización y el fin de la sesión.
Para prevenir la duplicación de los registros de las cuentas, cada mensaje de las cuentas se le asocia un Id de sesión AVP, junto con un número de registro de cuenta AVP. Como esta combinación puede unívocamente identificar un registro de cuenta, el nodo Diameter actúa como un agente Diameter que puede usar esta información para detectar mensajes duplicados de cuentas, enviados al servidor Diameter. Así evitando un proceso innecesario para el servidor Diameter. Esta situación se puede originar por problemas temporales en la red o clientes que se apagan. También se requiere, que el cliente Diameter, mantenga una copia en memoria (cache local), los mensajes hasta que se reciba el correspondiente acuse (ACK) de recibo de los mensajes.

Referencias: 14, 15, 16, 17, 18.

Manejo de Errores.

Los errores en Diameter están categorizados de dos maneras: errores del protocolo y errores de la aplicación. Los errores del protocolo se refieren a algo que está mal relacionado con el protocolo utilizado para transportar los mensajes Diameter, tal vez información incorrecta de las rutas o fallas temporales en la red.
Los errores de aplicación resultan de una falla en el protocolo Diameter en sí mismo, y existen múltiples fuentes de error de aplicación. Por ejemplo, cuando un AVP mandatario se pierde en un comando Diameter, se devuelve un código de error DIAMETER_MISSING_AVP. Cada mensaje de respuesta en Diameter, puede chequear este AVP, para ver si el mensaje previo fue procesado con éxito.
Para detectar las fallas de conexión, el protocolo Diameter define un mensaje DEVICE-WATCHDOG-REQUEST. Cuando dos nodos Diameter conectados no intercambian mensajes o un determinado periodo de tiempo, se envía este mensaje desde cualquiera de estos nodos para detectar posibles problemas en la red.
El protocolo Diameter comparte la misma semántica de definición de códigos de error que el protocolo http. El estado del mensaje enviado puede fácilmente identificarse chequeando el primer digito del código devuelto:

1xxx: Significa que el pedido no puede ser satisfecho y se requiere información adicional para el servicio al que se trata de acceder.

2xxx: Significa que el pedido fue procesado satisfactoriamente.

3xxx: Significa que hubo un error en el protocolo, cuando se transmitía el mensaje Diameter. Generalmente un proxy Diameter trata de arreglar este problema re enlutando el mensaje a otro servidor Diameter. O guardando el mensaje localmente y enviándolo más tarde nuevamente.

4xxx: Significa que el pedido no puede ser cumplido en ese momento, pero puede funcionar en un futuro. Un ejemplo es un servidor que no tiene más espacio físico de almacenamiento, para manejar cualquier pedido entrante.

5xxx: Significa que hubo un error en la aplicación cuando el servidor trataba de procesar el pedido. El que envió el mensaje no debería tratar de enviar el mensaje de nuevo, y debería determinar las causas del error de aplicación, chequeando el código de error, y corregir el problema.

Además del código AVP devuelto, el que envía el mensaje puede también chequear información adicional para el manejo de errores. El mensaje de error AVP lleva información de mensajes de error que se puede leer y usar para determinar la causa. El reporte de error del host, contiene la identidad del host que generó el código de error. Este AVP es muy útil, para detectar el origen del problema. El AVP fallado contiene el grupo de AVPs que causaron la excepción. Luego de haber sido detectado un error, el nodo envía todos los mensajes pendientes a otro nodo Diameter. Este proceso se llama Failover. Un mensaje pendiente es un mensaje que ha sido enviado, pero no se ha recibido su correspondiente respuesta. Se requiere que cada nodo Diameter mantenga una copia local de los mensajes enviados. La identificación de salto a salto, dentro de cada mensaje se usa para referenciar los mensajes salientes para cada par de destino.
Sin embargo, este proceso puede causar que un nodo Diameter reciba más de una vez el mismo mensaje. Como resultado, el nodo Diameter, debe utilizar, la combinación de la identificación de extremo a extremo del mensaje host originante del AVP, para unívocamente determinar el mensaje de un nodo Diameter especifico.

Tabla 2: Diferencias significativas entre los protocolos Diameter y Radius

	Diameter	**RADIUS**
Protocolo de Transporte	Protocolos orientados a conexión (TCP and SCTP)	Protocolo NO orientado a conexión (UDP)
Seguridad	Salto a Salto, Extremo a Extremo	Salto a Salto
Soporte de Agentes	Relay, Proxy, Redirect, Translation	Soporte implícito, lo que implica que el comportamiento del agente debe implementarse en un Server Radius
Capacidad de Negociación	Soporta Negociación de aplicaciones y niveles de seguridad	No soporta

Descubrimiento de Par	Configuración estática y búsqueda dinámica	Configuración estática
Mensaje iniciado por el server	Soporta. Por ejemplo, mensajes de re-autenticación, terminación de Sesión	No soporta
Máximo Tamaño de los datos de Atributos	16,777,215 octetos	255 octetos
Soporte específico de un Vendor	Soporta ambos mensajes específico de un Vendor y atributos	Soporta sólo mensajes específicos de un Vendor

Junto con el protocolo SIP, Diameter es uno de los protocolos de CORE utilizados en la arquitectura IMS, ambos en el plano de servicios y de control. IMS define un conjunto de referencias entre entidades IMS y algunas de uso de Diameter como el protocolo de intercambio subscripciones, tales como presencia, mensajes relacionados al billing. Por ejemplo, el punto de referencia Sh en IMS se define como un mensaje Diameter para suscripción y propósitos de notificación. Como IMS sigue evolucionando se espera que haya cada vez más aplicaciones Diameter, así como implementaciones relacionadas con Diameter.

Referencias: 14, 15, 16, 17, 18.

2.3.8 Virtualización de IMS

2.3.8.1 Sistemas en la NUBE y NFV (Network Function Virtulization)

Los sistemas en la nube se han convertido en un modelo fiable para los recursos de IT. Se aprovecha la tecnología de virtualización, para permitir un acceso bajo demanda a los recursos compartidos de red, (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) con auto gestión del aprovisionamiento y administración. Esto tiene tres principales modelos de servicio: Infraestructura como Servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS).

IaaS ofrece a los usuarios finales de sistemas, los recursos de procesamiento, almacenamiento, y la red como un servicio a través de una red. El usuario final puede aprovisionarse en forma dinámica y des-aprovisionarse de los recursos de acuerdo a su necesidad. Los proveedores de servicios utilizan PaaS para la provisión de las aplicaciones y servicios que ofrecen como SaaS, sobre una base de pago por uso para los usuarios finales u otras aplicaciones. PaaS facilita el proceso de aprovisionamiento mediante la adición de niveles de abstracción a la infraestructura ofrecida como IaaS. Las soluciones PaaS varían ampliamente en las

capacidades que ofrecen. Sin embargo, todas tienen la capacidad básica para desplegar aplicaciones en IaaS.

La tecnología NFV ofrece una nueva manera de diseñar, desplegar y gestionar los servicios de red. Desacopla las funciones de red que se implementan en software desde el hardware propietario subyacente y ejecuta el software como aplicación, es decir, funciones de red virtuales (VNFs). El cambio hacia el software basado en funciones red conduce a una mayor flexibilidad como el caso de los VNFs, que pueden ser fácilmente desplegados en varios lugares, actualizados, y ampliados; sin la necesidad de un cambio en el hardware.

NFV fue desarrollado para beneficiar a las redes con la tecnología de virtualización, para consolidar y ejecutar en VNFs el hardware comercial, tales como servidores y switches. Promete muchos beneficios para la industria de telecomunicaciones tales como la flexibilidad, estándares abiertos, mayor agilidad en los servicios de red y la reducción de los gastos de capital(CAPEX) y los gastos operativos (OPEX).

Aunque están relacionados, los sistemas en la NUBE y NFV son diferentes conceptos. Los sistemas en la NUBE se refieren al concepto de entrega del recurso de IT como un servicio, mientras que NFV se centra en la migración de las funciones de la red para funcionar en hardware comercial. Sin embargo, aprovechando los sistemas en la NUBE, NFV puede tomar ventaja de sus beneficios y trasladarlos a la industria de telecomunicaciones. Los beneficios incluyen la eficiencia de los recursos, y aún más reducción en CAPEX y OPEX.

La arquitectura de NFV, está siendo estandarizada por las normas europeas de telecomunicaciones Institute (ETSI), se representa en la figura siguiente:

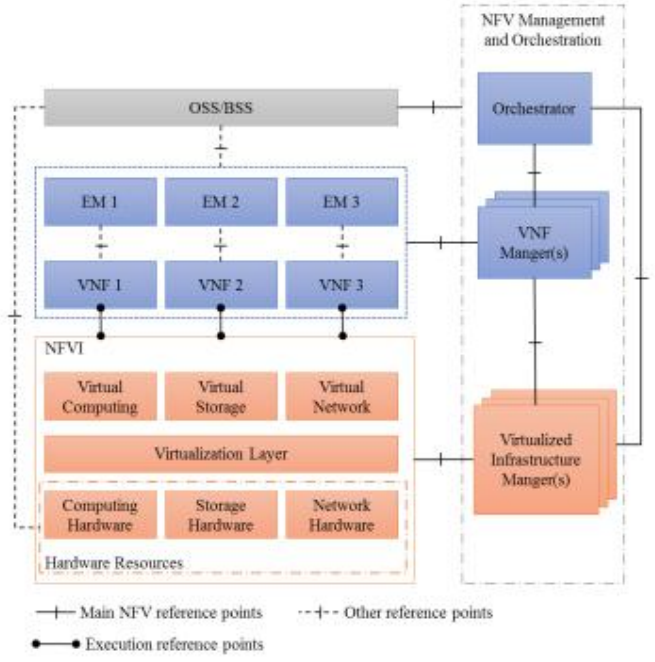

Figura 26 Arquitectura de NFV (Fuente 37)

Comprende la infraestructura NFV (NFVI), VNFs, la gestión NFV y capas de orquestación. NFVI proporciona el entorno en el que VNFs se puede ejecutar. Proporciona las capacidades de cómputo comparable a un IaaS, aunque por lo general con mucho más requisitos de rendimiento. También es compatible con la conectividad de red dinámica entre VNFs, que puede ser logrado mediante el aprovechamiento de las tecnologías emergentes, tales como la creación de redes definidas por software (SDN). El gerenciador de la infraestructura virtualizada lleva a cabo la gestión y asignación de recursos. El administrador de VNF maneja el ciclo de vida VNF de la gestión (por ejemplo, creación de instancias, escalamiento y la terminación). El orquestador de VNF, es el principal responsable del ciclo de vida de la gestión de los servicios de red, que por lo general incluyen varias instancias de VNF.

2.3.8.2 Requerimientos para Virtualizar IMS

El IMS ha sido diseñado para 3G con aplicaciones centradas en humanos, sin embargo, la idea de virtualizar es atender tanto para aplicaciones humanas y centradas en aplicaciones M2M, (ej. Smart grid). Esto requiere un rediseño del IMS, y los sistemas en la NUBE, que es la base ideal ya que permite funciones tales como la escalabilidad y la eficiencia en el uso de recursos. Consideramos que los siguientes requisitos son los más importantes para virtualizar IMS:

- Escalabilidad elástica: IMS hoy se basa únicamente en el uso de entidades funcionales pre-asignados con un exceso de aprovisionamiento para cumplir con el pico de la demanda. La nueva capacidad requiere esfuerzos significativos para añadir manualmente nuevos equipos para el sistema. Por otra parte, un IMS en la NUBE debe aprovechar la elasticidad de la nube para adaptarse dinámicamente a la creciente o a la reducción de los requisitos de carga mediante el ajuste de la asignación de recursos de una forma granular. Además, debe ser capaz de manejar sin problemas un número masivo de IMS UE. En efecto, se espera 10-100 veces más dispositivos para ser conectados a 5G, en comparación con la actualidad.
- Latencia: las tecnologías 4G/ 5G, soportarán una amplia variedad de aplicaciones para humanos y otras M2M que toleran diferentes valores de latencia. Algunas de estas aplicaciones pueden tolerar latencias del orden de

unos pocos segundos, mientras que otros tienen más estrictos requisitos de latencia que lo que existe hoy. Por ejemplo, tele-protección es una aplicación de misión crítica para empresas de servicios públicos. Incluye monitoreo en tiempo real y alertas, funcionalidades que requieren la transferencia de los mensajes con alrededor 8 milisegundos en la capa de aplicación. El IMS en la NUBE o IMS virtualizado, debería ser capaz de soportar las aplicaciones que requieren diferentes niveles de latencia. Esto incluye las aplicaciones que tienen requisitos de latencia muy estrictas en comparación con la actualidad. También debe ser capaz de mantener la latencia necesaria bajo un alto grado de carga.

- Eficiencia de los recursos: Hoy en día, el IMS se instala con exceso de aprovisionamiento de recursos para dar cabida a la demanda pico. Sin embargo, el cambio hacia capacidad bajo demanda, hace que la eficiencia de los recursos sea más crítica, ya que una ineficiencia de recursos se traduciría directamente en un mayor costo de funcionamiento (es decir, OPEX) con el modelo de precios de pago por uso.
- Sígueme: La idea básica detrás de la "follow-me", es el concepto de que los servicios en la NUBE siguen los usuarios finales durante su movimiento. Los operadores móviles utilizarán múltiples IaaSs, que son geográficamente distribuidos e interconectados. Servicios IMS podrían ser desplegados en diferentes lugares para ofrecer una mejor experiencia al usuario. Por lo tanto, tan pronto como el usuario final se mueve, el servidor de aplicación podrá proporcionar al IMS el cambio de servicio. En el futuro, el servicio debe seguir al usuario final y siempre debe ser accesible desde la aplicación del servidor y a través de las entidades funcionales de IMS que aseguran la mejor experiencia al usuario. Hoy en día, las entidades P-CSCF y S-CSCF se asignan al IMS UE y no cambian durante la registración. A través de este período, los usuarios pueden acceder a sus servicios IMS a través de estas entidades asignadas. Por lo tanto, para tener movilidad de los servicios en este modelo, el IMS UE debe cancelar el registro de las entidades IMS asignados y luego registrarse de nuevo, lo que provocará la interrupción del servicio.

Estos requisitos mencionados a menudo entran en conflicto. Se deberán hacer algunas compensaciones cuando se diseñen las nuevas arquitecturas. Veamos el conflicto entre la escalabilidad elástica, la latencia y la eficiencia de los recursos. Está claro que el nivel de granularidad de hoy, (es decir, entidades funcionales 3GPP) es un impedimento para la escalabilidad elástica. Sin embargo, el perfeccionamiento de ese nivel de granularidad a través de la división de las

entidades funcionales por lo general conduce a un costo adicional (por ejemplo, la complejidad de gestión, entre las comunicaciones de entidades sub-funcionales). Estos costos pueden (o no) compensar las ganancias esperadas de la refinación de la granularidad. Además, esta puede impedir que los requisitos de latencia de se alcancen. Por lo tanto, se convierte en la clave.

2.3.8.3 Primera Opción de Virtualización de IMS

Esta sección revisa un enfoque que se centran en toda la arquitectura IMS según los requisitos establecidos en el apartado anterior. Con esta idea algunos recursos son dinámicamente asignados a entidades funcionales de IMS.

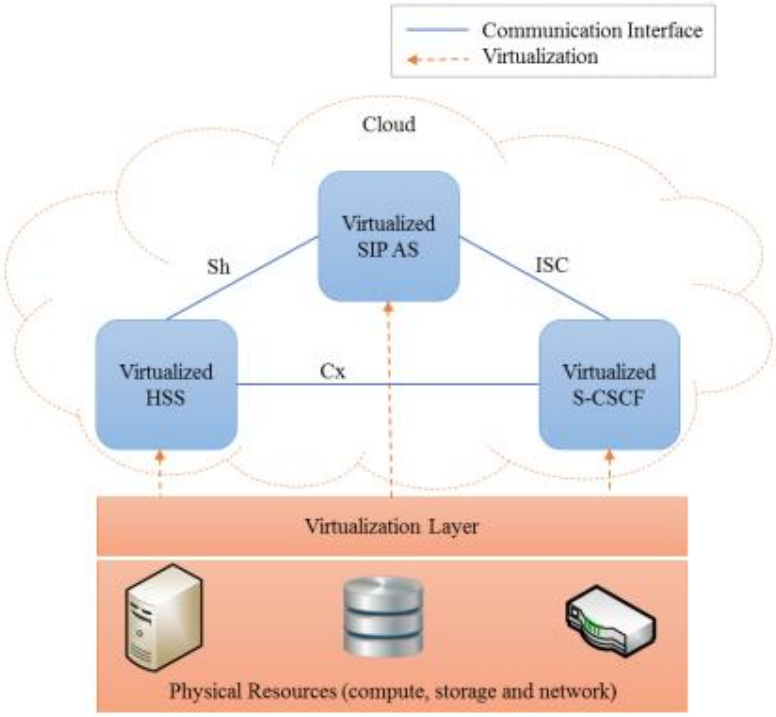

Figura 27 IMS Virtualizado

Los recursos computacionales de cálculo, el almacenamiento, y los recursos de red están virtualizados. Esto permite un IMS con un conjunto de entidades funcionales virtuales que interactúan entre sí, (es decir, entidades funcionales que dependen de los recursos virtualizados).

Se propone una plataforma en la nube para el Core IMS, que ejecuta las entidades IMS en máquinas virtuales en la NUBE (VM). La plataforma propuesta es compatible con la asignación dinámica de recursos y protección de desastres. El algoritmo propuesto de asignación de recursos, puede asignar de forma dinámica y desasignarla virtual CPU (CPU virtual) y los recursos de memoria para las máquinas

virtuales de acuerdo con la carga de trabajo actual. Los objetivos del algoritmo son permitir que a la plataforma satisfacer el tiempo de respuesta con nivel de operador, para lograr una alta utilización de los recursos y reducir costes.

Además, el algoritmo supone que cada VM arranca con una CPU virtual y memoria asignada. Cada máquina virtual también tiene una cantidad máxima predefinida de CPU virtual y memoria que se pueden asignar. Cuando la utilización de los recursos supera un umbral predefinido, el sistema añade una CPU virtual o más memoria si el VM no ha alcanzado el máximo permitido de recursos. Si la máquina física (PM), que alberga la máquina virtual, no tiene suficientes recursos para ampliar los recursos de la VM, el algoritmo lleva a cabo la migración en caliente de la máquina virtual para otra PM (Physical Machine) con suficientes recursos. El algoritmo también puede elásticamente escalar el número de las PMs activos en la infraestructura de la NUBE de forma automática, de acuerdo con la carga de trabajo. Esto permite alcanzar una alta utilización de los recursos y reducir los costos de consumo.

El algoritmo de asignación de recursos propuesta puede elásticamente escalar verticalmente para adaptarse a la carga de trabajo. Sin embargo, escalabilidad horizontal, no se está considerando. La arquitectura de IMS, para muchas de las entidades funcionales (por ejemplo, S-CSCF) dificulta la aplicación de la escalabilidad horizontal. Por ejemplo, sería difícil de poner fin a un S-CSCF, cuando se maneja una llamada en curso, porque esto haría requerir la transferencia del estado de almacenado a otra instancia de S-CSCF.

No se evalúan la latencia a lograr por la arquitectura. Ni se abordan el requisito de "followme". Sigue siendo un problema en la propuesta de diseño debido a la asignación estática de entidades funcionales de IMS para un determinado IMS UE en el proceso de registro.

2.3.8.4 Segunda Opción IMS como Servicio

Otra opción sería tener tres arquitecturas para IMS virtualizado, con NFV virtualizados y basados en IMS, Split-IMS y Merge-IMS. En la arquitectura IMS-virtualizado, cada IMS se implementa como una entidad funcional, como software que se ejecuta en una VM sola. Las interfaces con componentes externos no se cambian. El Split-IMS mueve el estado de los abonados, que se mantiene en muchas entidades IMS (por ejemplo, P-CSCF y SCSCF), a una entidad funcional externa llamada de memoria compartida. Esto hace que las entidades IMS sean independientes del estado. Un balanceador de carga es posicionado como un punto de entrada para las nuevas entidades sin estado para distribuir la carga.

Además, el Merge-IMS, agrupa cuatro entidades principales de la arquitectura de IMS (es decir, P-CSCF, S-CSCF, I-CSCF y HSS) y los despliega en una máquina virtual llamada IMS-VM. Se introduce la entidad IMS-Locator, que asigna los abonados a una instancia en particular de IMS-VM durante el proceso de registro. Todas las entidades de HSS en casos IMS-VM comparten la misma base de datos para almacenar información de abonado.

La arquitectura IMS virtualizada puede escalar mediante los procedimientos ya estandarizados por 3GPP en cierta medida. Sin embargo, la escalabilidad es limitada debido a la arquitectura statefull. La arquitectura Split-IMS separa la lógica funcional y el estado de las entidades por lo que la lógica puede escalar fácilmente Creando nuevas entidades sin estado y añadirlos al balanceador de carga.

Por otra parte, la arquitectura Merge-IMS mediante la creación de un nuevo IMS-VM que tiene todos los componentes. Por lo tanto, la escalabilidad elástica está limitada, ya que es difícil de escalar debido al nivel de granularidad (es decir, IMS-VM) y la arquitectura statefull.

2.3.8.5 Tercera Opción IMS virtualizado por entidad

Esta sección revisa los enfoques que se centran en concreto en entidades IMS. Las principales entidades IMS que han atraído la atención son el HSS y el servicio de presencia. Esto es mucho menos complejo que otros nodos tales como la CSCF.

HSS: esta arquitectura propone un HSS virtualizado y basados en la nube. La distribución del HSS en una capa de recursos y una capa de gestión. La capa de recursos se implementa en la. La solución propuesta permite una ampliación independiente de los recursos y las capas de gestión.

Servicio de Presencia: se propone una arquitectura para virtualizar el servicio de presencia. Una aplicación basada en la nube de servicio de presencia. El servidor de presencia se implementa en una máquina virtual.

2.3.9 IPv6.

IPv6 es un protocolo que ya está ampliamente adoptado, más allá de la arquitectura IMS. Igualmente IMS se nutre de todas las nuevas ventajas de IPv6. La migración de IPV4 a IPv6ya es un hecho. Pero como forma parte del cambio de paradigma y esa necesidad del usuario de estar siempre conectado, es que vamos a escribir unas líneas sobre el mismo, y los requerimientos para una transición segura y confiable.

Existe alguna problemática de la introducción del IPv6 en la arquitectura IMS en origen IPv4

La arquitectura IMS, solo se ve beneficiada con la adopción de IPv6, dado que IMS es agnóstico al acceso y tanto IPv4/6 son protocolos de capa 3. Por ende son transparentes a la arquitectura IMS. Como vimos la suite de protocolos IMS arranca en la capa 5.

Dada la convergencia y desarrollos en cuanto a conectividad, cada vez más dispositivos se están conectando a Internet. Esta tendencia ha generado una escasez de direcciones IP. **I**nternet **P**rotocol **v**ersión **6**, (IPv6) promete remediar esta situación.

Desde su desarrollo inicial, **I**nternet **P**rotocol **v**ersión **4**, (IPv4), se ha convertido en un estándar de protocolo de la capa de red, usado en Internet, y en la mayoría de las redes de computadores de todo el mundo. Esta versión ha venido siendo usada por la comunidad de Internet por varios años. Sin embargo, con el aumento global en las comunicaciones y servicios, junto con los nuevos desarrollos de aplicaciones para Internet, IPv4 empieza a presentar limitaciones. La nueva generación de este protocolo, IPv6, se diseñó para reemplazar a IPv4, por las limitaciones existentes en las direcciones disponibles de IPv4, y para proveer un amplio rango de beneficios operativos y un mejor soporte para las nuevas aplicaciones.

Un cambio en las expectativas sobre IPv6

El RFC original del IETF, (**I**nternet **E**ngineering **T**ask **F**orce), sobre IPv6, fue escrito haya por el año 1990. Esta actividad estaba relacionada con el crecimiento de redes de computadoras y con los servidores (hosts) asociados a Internet. Varias tecnologías intermedias, como CIDR, (**C**lassless **I**nter-**D**omain **R**outing), NAT, (**N**etwork **A**ddress **T**ranslation), IPSec, (**I**P **S**ecurity), han ayudado a solucionar la limitaciones en el direccionamiento, pero también están llegando al límite de su efectividad.

¿Qué es lo que no cambio?

La necesidad primaria de más direcciones que originó el diseño de IPv6, continúa hoy siendo una prioridad. La gran expansión de los métodos de comunicación está alimentando una tendencia global al intercambio de información en el backbone de Internet. Un fenómeno que comenzó con la adopción de la Web, revolucionó el mercado de consumo de productos de electrónica, telecomunicaciones y computadoras. Con la potencialidad de billones de dispositivos comunicándose a través de millones de redes, habrá un incremento en la demanda de las

comunicaciones globales de toda la ciudadanía. Con un marcado aumento de las redes y dispositivos de comunicaciones en las regiones de Asia del Pacifico, donde se ha notado un gran incremento en la demanda de direcciones IP. Mientras que en mercados más maduros e innovadores como Japón, Taiwán y Australia, ha habido una mayor velocidad en la adopción de los usuarios de todas estas nuevas demandas, más que en regiones como China, Korea e India. Este rápido crecimiento está creando un desafío único para la región de Asia del pacifico, debido al limitado número de direcciones IP asignado durante la distribución de direcciones en los comienzos.

Pensando en lo que vendrá, los que estamos relacionados con el sector de IT, estamos analizando a la tecnología IPv6 para poder realizar integraciones transparentes y coexistir con la infraestructura existente dadas las nuevas capacidades de direccionamiento, tunelamiento (VPN) y translación de direcciones (NAT). IPv6 resuelve estos desafíos posibilitando el aumento en las redes y las aplicaciones de seguridad, lo cual ayuda a proteger el manejo y transmisión de la información.

Un nuevo driver de IPv6 incluye el uso de dispositivos móviles 3G, IMS para redes convergentes y juegos en línea. Todo esto está generando la incorporación de más dispositivos conectados a Internet, por ende consumiendo más direcciones IP.

¿Qué es lo que está cambiando?

Si el motivo original para migrar a IPv6, sigue siendo válido hoy, ¿por qué se está tardando tanto para migrar a IPv6?. Una posible respuesta, puede deberse a la necesidad de testear más el protocolo en laboratorios y mediante varias redes de prueba que posibiliten que esta versión esté disponible para entornos de producción. Otra posible respuesta podría ser, cuan exitosas fueron las tecnologías intermedias como NAT y CIDR, resolviendo el problema concerniente al direccionamiento.

Lo que realmente ha cambiado las nuevas expectativas generadas por los proveedores de servicios y empresas en general por la tecnología IPv6 de nueva generación.IPv6 provee una nueva tecnología que permite generar una plataforma estratégica, flexible para aplicaciones de redes centralizadas. Para poder desarrollar este nuevo sistema y continuar proveyendo comunicaciones y servicios de misión crítica. IPv6 permitirá a las redes globales satisfacer todas las nuevas demandas para las aplicaciones basadas en IP. Esto requiere un aumento de las performance, mayor disponibilidad y una considerable mejora en la calidad de servicio (QoS).

¿Por qué?

IPv6 no es solamente cuestión de todos los aspectos vistos más arriba, sino sobre la convergencia en las comunicaciones. El desarrollo de IPv6 trata de proveer una infraestructura robusta y flexible que pueda soportar las aplicaciones de nueva generación. Las aplicaciones de IPv6 posibilitan el trabajo colaborativo, acortando las distancias alrededor del mundo.

Nuevas Aplicaciones y Servicios sin Límites.

El pasado de las redes con IPv4, soportando aplicaciones que eran primariamente intercambio de información basada en simples textos ha quedado atrás. Con los avances tecnológicos, usuarios sofisticados más demandantes de tecnología, organizaciones que están expandiendo sus redes cada día más. Están surgiendo un nuevo tipo aplicaciones. Estas nuevas aplicaciones son catalizadores del estándar IMS.

Aplicaciones Clásicas y Limitaciones en los Servicios

La mayoría de las aplicaciones basadas en IPv4, basadas en intercambio de texto, y que normalmente se accedían desde ubicaciones fijas, como ser correo electrónico, grupos de noticias, usan NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol), y navegadores de Internet. El cambio tecnológico que permitió pasar de una tecnología de banda angosta a una de banda ancha, junto con el aumento en la disponibilidad y reducción de costos de los accesos de banda ancha, permitió la adopción de navegadores gráficos. Esta disponibilidad de accesos de banda ancha combinado con las tecnologías de accesos remotos tales como SSL (**S**ecure **S**ocket **L**ayer), VPNs (**V**irtual **P**rivate **N**etworks), y el enorme crecimiento de WLANs (**W**ireless **L**ocal **A**rea **N**etwork), permitiran cada vez mas, conecciones de Internet mobiles; junto con el uso de aplicaciones tales como VoIP (Voice over IP), y productos colaborativos basados en IP. La adopción y maduración de IPv4, posibilitó el desarrollo de aplicaciones que permitieron metodos de comunicación instantánea. Dentro de tales tecnologias podemos mencionar: la estandarizacion de IP sobre todo tipo de medios de trasmision, y el uso de MPLS (**M**ulti**P**rotocol **L**abel **S**witching).

Sin embargo, algunas propiedades inherentes de IPv4, presentan limitaciones para algunos servicios, por ejemplo, la limitacion del espacio de direccionamiento en los encabezados de las tramas de IPv4. Dedido a esta restriccion, se han creado

esquemas de direccionamiento de IPs que utilizan direcciones privadas. Usando NAT en el borde de las redes, para conectar direcciones de las redes privadas con las publicas. El uso de NAT permitió transitoriamente lidiar con el problema de la limitacion de direcciones de IPv4, pero a su vez genero una complejidad adicional a los administradores de redes. La otra gran limitacion de IPv4, es carecer de un mecanismo de seguridad integrado para la trasnmision de datos.

Soporte para Nuevas Aplicaciones y Servicios

Una importante característica de IPv6, es la auto-configuración de direcciones o posibilidad plug&play, que hace innecesario a los administradores de red o usuarios configurar los dispositivos cuando se conectan a una red. Esto es un gran avance para el aumento de redes móviles. Con la instauración de IPv6, y el uso de IPSec integrado, los usuarios de redes móviles, tendrán la posibilidad contar con una comunicación entre dispositivos tales como PCs, Tablets y teléfonos celulares inteligentes (Smartphone). Este modelo de red peer to peer, pondrá a disposición un modelo para nuevos tipos de comunicación y trabajo colaborativo, asegurando autenticación segura, e integridad de datos durante las comunicaciones. Además, las comunicaciones peer to peer de redes ad hoc, serán más fáciles de establecer. La incorporación de mecanismos como Tipo de Servicio: ToS (**T**ype **o**f **S**ervice) en IPv6, proveerán mejor calidad de servicio para las nuevas aplicaciones, debido a la menor latencia y jitter a estas aplicaciones por un mejor transporte en la red. La identificación del tipo de tráfico por medio de una etiqueta en el encabezado de IPv6, los routers podrán identificar y proveer un manejo especial para los paquetes que pertenecen a un tráfico de determinado tipo. Por ejemplo para una mejora en la calidad de aplicaciones de distribución de video o IPTV y aplicaciones colaborativas de voz. El soporte mejorado de seguridad en IPv6, por la integración de IPSec, aseguran un estándar confiable y seguro en la capa IP, para un modelo de capas. IPSec, también asegura la autenticación de comunicaciones, asegurando la integridad de la conexión punto a punto, sin la necesidad de tunelizar o encriptar tráfico. Esta capacidad impide el manejo de tráfico o ataques de tipo spoofing.
Estas características integradas de IPv6, permitirán expandir las redes más allá de las limitaciones generadas por IPv4 y generando un conjunto de métodos de comunicaciones enriquecidos.

Aplicaciones demandantes de IPv6

Dentro de los factores que alimentan el crecimiento de IPv6, podemos mencionar:

- El incremento de usuarios de PCs dentro de todo tipo de organizaciones.
- La explosión de dispositivos electrónicos, que no son PCs.
- EL aumento de tiempo que los usuarios pasan on line para poder realizar sus trabajos con mayor eficacia y no estar desinformados.

De particular interés es el crecimiento de aplicaciones colaborativas, que están permitiendo nuevas experiencias de comunicaciones y computacionales, para este tipo de usuario que quiere vivir on line, y también para las empresas de equipos electrónicos que producirá dispositivos para estas nuevas necesidades.

Componentes de una Implementación exitosa de IPv6

IPv6 fue concebido para superar la escalabilidad de las direcciones y los desafíos de configuración de IPv4. Y ayudar a reenfocar la capacidad de comunicación que originalmente tuvo TCP/IP en la instauración de las redes. No hay duda que Internet seguirá creciendo exponencialmente, y los usuarios cada vez más sofisticados adoptaran dispositivos que estén listos para este mundo IP, que soporten aplicaciones que los ayuden en sus actividades diarias, cada vez más demandantes.

Algunos administradores de red, están en el proceso de implementación de IPv6 en el backbone de su red. Mientras que otros recién están terminando el plan de transición. Y sea que la implementaron de IPv6 este en proceso de planificación, entre los administradores de red hay una consciencia clara de los nuevos componentes para una implementación de IPv6 y cómo deben estar relacionados unos con otros.

Aplicaciones de IPv6

Posiblemente lo más relevante de una implementación de IPv6, serán las aplicaciones propias de este nuevo protocolo. El desarrollo e implementación productos basados en IPv6 está ocurriendo en varias organizaciones. Muchas de estas nuevas capacidades de IPv6 discutidas anteriormente, conducirán a la adopción rápida de este nuevo protocolo.

Además la posibilidad de utilización del espacio de direcciones ampliado de IPv6, permitirá que nuevas aplicaciones tomen ventaja de esto y provean comunicaciones punto a punto controladas en una infraestructura de red transparente. Para poder asegurar una óptima performance, las aplicaciones necesitarán implementar una arquitectura dual, con un doble stack o pila, con lo cual ambos protocolos IPv4 e

IPv6 compartan el modelo de capas. Las aplicaciones podrán ser independientes de esto utilizando APIs, (**A**pplication **P**rogramming **I**nterface) que automáticamente utilizaran IPv6 o IPv4. Las aplicaciones podrán tomar ventaja de algunas capacidades tales como IPSec para intercambio de claves: IKE (**I**nternet **K**ey **E**xchange) y encripción de datos. Además de la capacidad de ToS, para dar un conjunto de niveles de servicios para dar consistencia a comunicaciones punto a punto.

Infraestructura de IPv6

La transición de IPv4 a IPv6 es importante porque IPv6 proveerá una infraestructura de Red que es mucho más segura y con una mayor escalabilidad que IPv4. Por ende el segundo componente más importante de una implementación de IPv6, será una infraestructura robusta que proveerá un amplio rango de características que cubrirán las funcionalidades tanto de red como de seguridad, para los nuevos desarrollos que requerirá la convergencia.

Optimización de la performance de IPv6

IPv6 tiene varios posibles escenarios de implementación, su desarrollo en las redes de proveedores de servicios, de empresas, de investigación y gubernamentales, refuerza este hecho. Como en IPv4, el paradigma de la implementación puede variar entre las diferentes aplicaciones. Por ejemplo un proveedor de servicios tomara un aproche diferente en la implementación que una empresa.

Para poder acomodar el amplio rango de escenarios posibles, una solución de IPv6 debería incorporar un amplio conjunto de equipamiento de redes y seguridad que sean compatibles con este nuevo protocolo, de manera de asegurar una buena performance y confiabilidad. Así mismo ofrecer una configuración y operación simple de la red por medio de una amplia gama de herramientas integradas, (CLI, APIs, NMS).

Para ayudar a realizar exitosamente una implementación de IPv6 en una organización, los equipos de redes y de seguridad deben soportar todas las funcionalidades de IPv6 y simplicidad en las múltiples plataformas que deberán ínter operar entre sí y con productos de otras marcas. Debido a que IPv6 ha pasado del laboratorio a escenarios de misión crítica, cualquier solución debe proveer los niveles de calidad, y una alta disponibilidad, junto con las herramientas necesarias para permitir integración y coexistencia con las redes anteriores.

IPv4 e IPv6 coexistirán en las redes por algún tiempo, la implementación de un stack dual (pila dual), que permita soporte simultaneo de IPv4 e IPv6, generara una transición sin sobresaltos entre una tecnología y otra.
Finalmente, para asegurar una optimización en el entorno de las aplicaciones, los equipos de redes y seguridad de IPv6, deben ser capaces de proveer una óptima performance por medio de hardware (ASIC-Based) de enrutamiento y un mecanismo en capas que separe en una capa el control y en otra el enrutamiento.

Mecanismo de Transición Flexible de IPv6

IPv6 posee herramientas de integración y transición que simplifican las operaciones y minimizan los costos de la implementación. La infraestructura de IPv6 provee varios mecanismos para la transición como NAT/NAPT, como así también un amplio rango de opciones para MPLS, de tunelamiento de tráfico, que harán más sencilla la conversión de IPv4 a IPv6.
Los productos de seguridad deben, así mismo permitir pasar de túneles de IPv4 a IPv6 y de IPv6 a IPv4. Estas translaciones dinámicas permitirán integrar IPv6 sin tener que reemplazar las redes con IPv4. Las plataformas deberán asegurar la coexistencia de IPv4 e IPv6, sin generar ningún tipo de problema en la performance de las redes.
Finalmente, las nuevas plataformas necesitarán mecanismos capaces de transportar TDM (**T**ime **D**ivisión **M**ultiplexing), o tráfico basado en circuitos, sobre la plataforma IP. Sobre todo en las redes de los operadores. Ya que la base instalada se seguirá migrando a IP, durante la transición de Pv4 a IPv6.

Comprendiendo la Seguridad de IPv6

Como IPv6 se está desarrollando en las redes existentes, el aseguramiento tanto de la información y de los sistemas que se transportan es crucial. Esto es particularmente importante, dado los aumentos de delitos y ataques a la seguridad, que se están generando y sobre todo en las redes del gobierno. Por ende otro componente importante de una implementación exitosa de IPv6 es la compresión de los mecanismos de seguridad que se pueden crear con IPv6, generando una red segura. Desde las aplicaciones mismas a través de los requerimientos de los clientes, de las redes y de las soluciones punto a punto.

Capa de Aplicación

Utilizando IPv6, las aplicaciones pueden tomar ventajas de las nuevas características de seguridad, que resolverán algunos de los problemas discutidos más arriba. Algunas de las mejoras en la seguridad de IPv6 incluyen una mejor protección contra ataques de escaneo de direcciones y puertos, y un requerimiento para todas las implementaciones de IPv6 de soportar IPSec para autenticación y y/o protección de encripción del trafico IPv6. IPSec se controla en forma centralizada, con una política de administración. La configuración de estas políticas se aplica directamente al sistema operativo. Esto elimina la necesidad de utilizar aplicaciones para monitorear los niveles de seguridad, con las nuevas características que configuran y controlan IPSec. También permite un desarrollo uniforme y consistente de IPSec en las diferentes redes.

Premisas del usuario

Ya sea para una oficina remota, oficinas regionales u oficinas centrales, el uso de aplicaciones y sistemas de seguridad es primordial. Estas aplicaciones de seguridad se requieren para implementar políticas de seguridad, incluyendo firewalls, encripción VPN y manejo del tráfico en todas las sucursales o puntos de nuestra red. Los firewalls actúan como la primera capa de seguridad, controlando quien y que tiene acceso a la red, empleando un control de acceso y autenticación para los usuarios. Proveyendo así una segmentación de la red, conteniendo a los usuarios en segmentos virtuales, y protegiéndolos contra ataques de denegación de servicio, (**D**o**S**) por medio de la capacidad de inspección completa del estado del paquete (statefull firewall). La siguiente capa de protección usa una solución de VPN para encriptar las comunicaciones que atraviesan un medio no confiable que puede ser Internet o un segmento de red interno. Finalmente esta aplicación de seguridad necesitara proveer una protección adicional para una variedad de ataques, incluyendo virus, troyanos, Web-filtering y métodos de anti spam.

En una transición de IPv4 a IPv6, se necesita implementar aplicaciones de seguridad que puedan proveer capacidades de Firewall de estado completas (statefull firewall) junto con IPSec VPN, tanto para tráfico IPv4 e IPv6. Estas aplicaciones necesitaran además proveer un soporte completo de IPv6, dado que varios de los mecanismos de transición tendrán que lidiar con los mecanismos de ruteo y esquemas de direccionamiento tradicionales para poder desarrollar IPv6 en ambientes de producción o en redes con ambientes híbridos. Estas aplicaciones de seguridad deben además proveer una óptima performance para todas las

aplicaciones por medio del uso de hardware integrado de aceleración de aplicaciones.

Infraestructura de las Organizaciones

El equipamiento de red que se utiliza en la infraestructura de las organizaciones provee un transporte crítico para todas las aplicaciones punto a punto. Estos productos de infraestructura incluyen una variedad de plataformas de ruteo tanto para sitios pequeños como para grandes redes corporativas. Todas estas redes están corriendo sistemas operativos estándar lo que mantiene cierta unificación en las mismas para todas las plataformas. Para una transición a IPv6, los productos de infraestructura necesitarán soportar plena capacidad de ruteo, además de MPLS y proveer un conjunto de servicios IP, entre los cuales debemos mencionar seguridad, políticas y control de tráfico, tanto para IPv4 como para IPv6. Estos componentes de seguridad para los productos de infraestructura de IPv6, deben incluir esquemas sofisticados que protejan los dispositivos en tiempo real de los accesos no autorizados y de los ataques no deseados, tanto de paquetes generados como de paquetes falsamente originados por manipuleo de tráfico. Utilizando hardware para filtrado de paquetes junto con IPSec, los equipos podrán proteger el sistema y sus interfaces. Al mismo tiempo que proteger el plano de control y el plano de datos durante la comunicación entre dispositivos. El uso de un flujo sofisticado de monitoreo y técnicas de limitación de la velocidad en este tipo de infraestructura ayudaran a detectar y detener ataques al mismo tiempo que proveer una operación estable de ruteo y manejo de aplicaciones de tráfico.

Herramientas de Gerenciamiento de IPv6

Las herramientas de gerenciamiento de IPv6 son un componente muy importante en la implementación exitosa de IPv6. El desarrollo de IPv6 en las nuevas redes, permitirá un nuevo conjunto de aplicaciones y servicios colaborativos. La configuración, operación y gerenciamiento de esta nueva plataforma será más simple y sencillo de implementar. Por medio de todos los componentes discutidos, desde aplicaciones hasta dispositivos de infraestructura, será muy importante complementar la capacidad de gerenciamiento de IPv4 mediante el protocolo SNMP (**S**imple **N**etwork **M**anagement **P**rotocol), con las herramientas de IPv6, que incluyen una interfaz de comandos intuitiva CLI, APIs flexibles y mecanismos de transición simplificados.

También debe soportar ambas versiones de ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol), tanto para IPv4 como para IPv6, y las aplicaciones tales como Telnet, Ping, Traceroute, FTP, entre otras. Además de soporte para diagnósticos en tiempo real y un buen sistema de logs y trace de eventos. Todo esto facilitará el gerenciamiento de las redes durante la transición.

Consideraciones de Desarrollo con IPv6

Es necesaria una significativa planificación previa a una transición exitosa a IPv6. Con una gran base instalada de IPv4, una clave a considerar es entender como migrar a todas las nuevas aplicaciones, al mismo tiempo que soportar las anteriores. Claramente, no habrá una forma inmediata de convertir todos los sistemas de comunicaciones a un mundo 100% IPv6. Deberán existir tecnologías de transición que permitirán coexistir ambas versiones de protocolos.
La inevitable migración a IPv6, hace que sea imprescindible planear una estrategia de transición que incluya tecnologías de tunelamiento y la compra de equipamiento y software que soporten IPv6 e IPv4 simultáneamente. Los dispositivos de próxima generación deberán tener una muy buena performance y una alta confiabilidad para operar en las redes de próxima generación.

Funcionalidad de la Transición

No es suficiente proveer soporte para el Core de las redes en lo que se refiere a ruteo y seguridad. Para una transición exitosa se requerirá una funcionalidad muy robusta. Como es de esperarse una transición en un determinado período de tiempo, deberá tener un proceso de múltiples etapas. Los equipos encargados de la transición deberán considerar coexistencia e interoperación. Esto incluye soporte simultáneo tanto para IPv4 como IPv6, o capa IP dual, llamado "Longhorn" o stack dual, además de las características de tunelamiento. Dentro de estas funcionalidades se incluyen:

- ✓ Firewalls que puedan asegurar la red durante la transición.
- ✓ Pleno soporte del stack de IPv6 en todos los dispositivos de la red.
- ✓ Routers y servidores de alta performance que permitan simultáneamente correr aplicaciones en IPv4 e IPv6.
- ✓ Aprovisionamiento para la transición de IPv6 a IPv4.

Como generalmente un recambio de todo el equipamiento no es posible, la forma recomendada de realizar esta transición es primero asegurarse que el firewall

soporte todas las funcionalidades de IPv6. Una vez que esto fue implementado, se recomienda deshabilitar IPv6 en el perímetro de la red e inspeccionar el protocolo 41 de IPv4. El protocolo IP 41 se usa para marcar los paquetes encapsulados de IPv6. El tráfico de paquetes que entra y sale de la red, a través de túneles (Protocolo IP 41), debe tener la inspección de paquetes habilitada, similar a la inspección de tráfico que es nativo de IPv4 e IPv6.

Mecanismos de tunelamiento de IPv6 a IPv4 incluyen:

- ✓ Configuración manual de túneles IPv6 sobre IPv4 provee conectividad entre dos puntos de la red IPv4. Sin embargo, es difícil de escalar y administrar ya que esta configuración es estática.
- ✓ Tunelamiento automático de 6 a 4, basado en la RFC 3056, provee un método para transmitir paquetes IPv6 a través de una red IPv4. El equipamiento debe tener una única dirección global IPv4 para poder implementar este protocolo.
- ✓ ISATAP se define en la RFC 4214, y describe un mecanismo de tunelamiento que automáticamente conecta routers o PCs con IPv6 sobre redes con infraestructura IPv4.
- ✓ IPv6 usando circuitos de cros-conexión MPLS (CCC) permite comunicación con IPv6 sobre una red IPv4 MPLS con productos de infraestructura.
- ✓ Túneles IPSec VPN ya sea IPv4 sobre IPv6 e IPv6 sobre IPv4en productos de seguridad permiten una fácil transición segura de las VPNs de IPv4 a IPv6, además de permitir el trafico IPv4 atravesar el backbone de la red de IPv6.

Escenarios de Desarrollo Transitorios

Las siguientes figuras proveen algunos pasos básicos para la implementación transitoria, así como aspectos claves de la funcionalidad requeridos para una solución IPv6.

La figura siguiente muestra el primer paso en la transición, en el cual la organización de IT primero habilita el perímetro del firewall para bloquear el trafico IPv6, tanto nativo como tunelizado. Segundo, los servidores DNS y DHCP se implementan en la red como máquinas de snack dual.

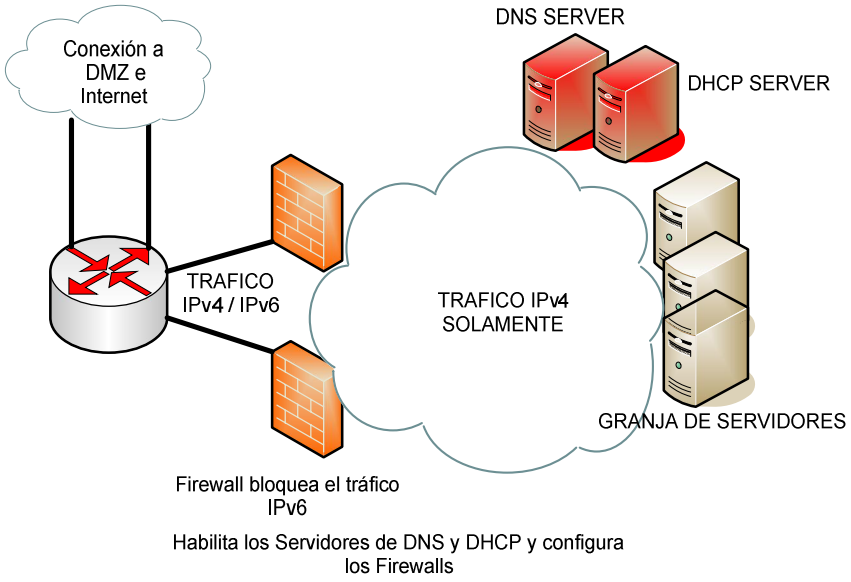

Figura 28: Habilita los Servidores DNS y DHCP y configure los Firewalls

El segundo paso, muestra un típico método para una fácil integración en organismos gubernamentales. El desarrollo de un servidor ISATAP que provee conectividad transitoria a los servidores. Se configuran túneles estáticos de IPv6 entre los firewalls para proveer conectividad en IPv6 controlada a los sitios remotos. Una alternativa viable a ISATAP es 6 a 4. Pero la conectividad 6 a 4 es una alternativa viable que requiere de la organización, que ya esté usando una arquitectura de direccionamiento de IPv4 global.

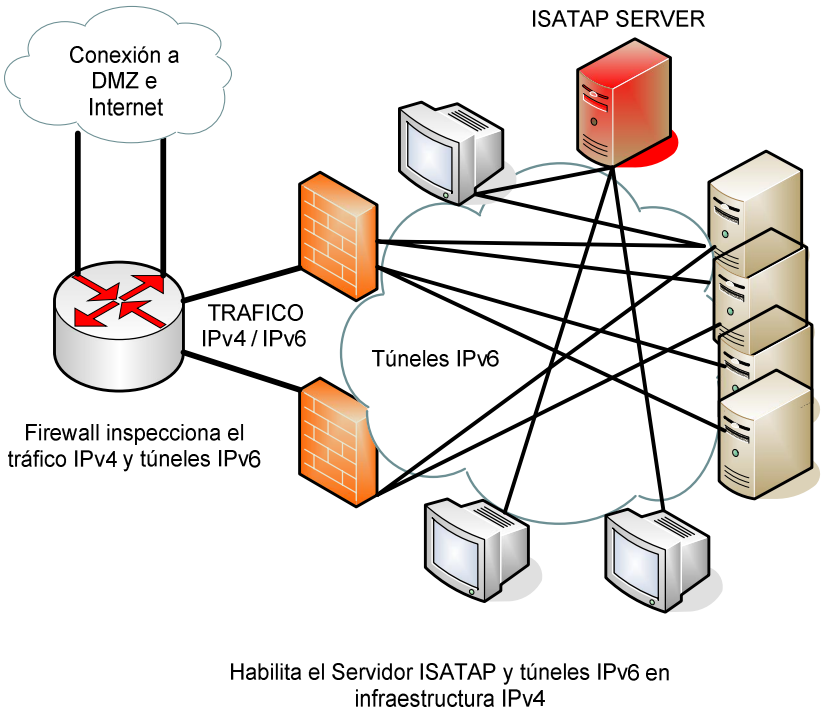

Figura 29: Habilita el Server ISATAP y túneles IPv6 en la Infraestructura IPv4

El escenario final, se muestra en la siguiente figura (30). Routers de stack dual se habilitan en el backbone para proveer servidores nativos IPv6 e IPv4 en la red. Los gateways de seguridad en cada lugar tienen capacidad de inspección de paquetes completa (stateful firewall) en cada sitio. Routers MPLS de borde se habilitan para proveer conectividad IPv4 e IPv6 entre los sitios, reemplazando los túneles estáticos. Se implementan nuevos roles en los servidores, tales como Web, email, y servicios de archivos.

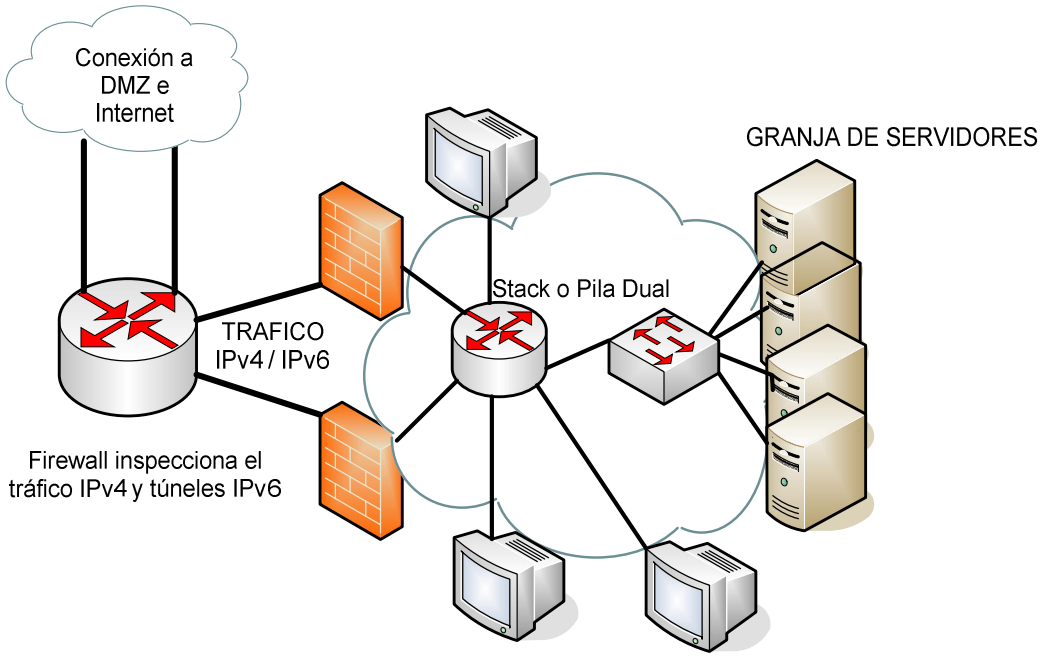

Figura 30: Infraestructura de stack dual con IPv6 nativo e IPv4

El stack de próxima generación dual representa una evolución en las funcionalidades de los sistemas operativos, que permite soportar tanto IPv4, como IPv6, para brindar conectividad con muy buena performance en las nuevas redes. Este stack TCP/IP dual permite una doble arquitectura de capas en las que las implementaciones de IPv4 e IPv6 comparten un transporte común y capas de enlace, como se muestra en la siguiente figura 31.

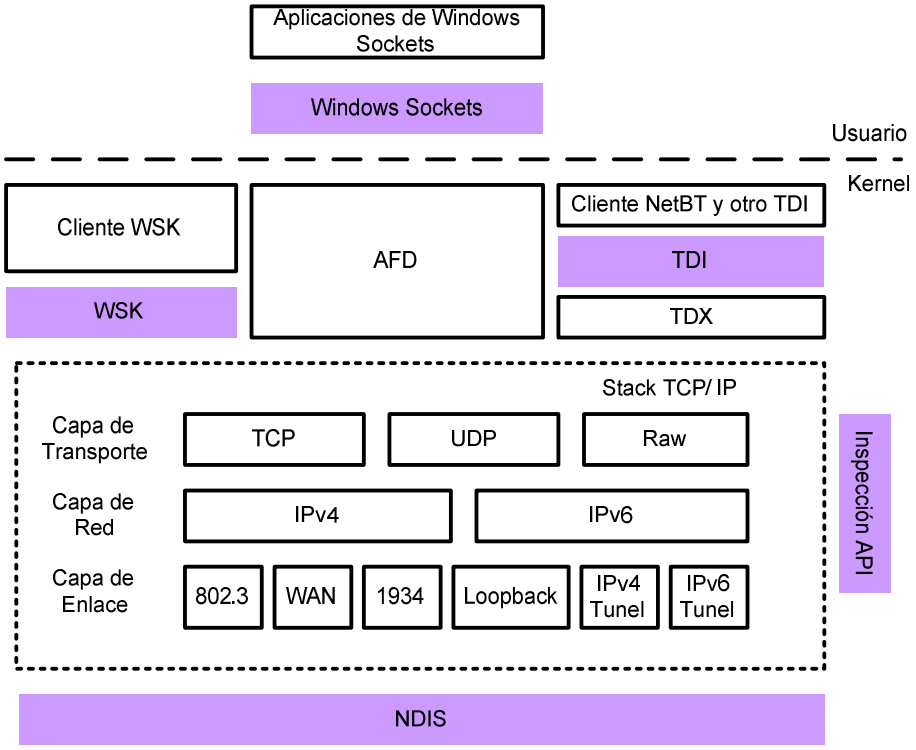

Figura 31: The Dual IP Layer Architecture of the Next Generation TCP/IP Stack

IPv6 permitirá que las nuevas aplicaciones que estén disponibles tengan una mayor performance, mejoren la disponibilidad de las redes, y tengan una mejor calidad de servicio.

Referencias: 13.

3 IDENTIFICACIÓN DEL PROBLEMA

La identificación del Problema podría sintetizarse en 2 preguntas claves: ¿Por qué IMS?, ¿IMS hoy es la única alternativa para enfrentar el cambio de paradigma y de modelo?

La esencia de la pregunta planteada refleja un cambio de paradigma con respecto a los servicios a brindar en un marco de convergencia fijo-móvil y de cuádruple play. Hoy supongamos que se establece una comunicación celular sobre la red LTE (red de 4ta generación 4G), si existieran problemas de cobertura se necesita pasar a la red 3G del Operador en cuestión (siempre y cuando la tuviera). Si este Operador dispusiera de la arquitectura IMS esta complejidad no existe y se resuelve de manera casi transparente. Para este ejemplo particular, sin adoptar esta arquitectura, la solución técnica es bastante más complicada.

3.1 Definición del problema

Se pretende resolver la problemática que plantea este cambio de paradigma con los servicios a brindar en un marco de convergencia fijo-móvil y de "cuádruple play".

Este problema es altamente actual e involucra tecnologías de punta.

Además es de gran importancia dado que involucra a empresas como los operadores clásicos de telefonía y posibles operadores virtuales, para empresas que hoy no forman parte del negocio de las telecomunicaciones.

Hoy nos encontramos en medio de una convergencia de Internet y banda ancha sobre celular, WiFi, WiMax, cable, fibra, líneas de potencia y con un incremento en las expectativas de los usuarios demandantes de mayores servicios y aplicaciones. Los usuarios están forzando a los proveedores de servicios de proveer combos de servicios, con calidad de servicio y a un determinado precio. Con características relacionadas con la movilidad y multimedia. Estas expectativas son los conductores principales para la implementación de una arquitectura de servicios IMS.

Cabe mencionar existe un foro de IMS, enfocado en testear y certificar por procesos muy rigurosos en todas la empresas proveedoras de servicios, proveedores de equipamiento, así como todo tipo de industria para poder informar, educar y promover interoperabilidad de servicios en la arquitectura IMS.

Hoy el proyecto de 3GPP, es el cuerpo del estándar para la arquitectura de servicios IMS, asegurando la distribución confiable de servicios móviles sobre IP, con cualquier red de acceso, tal como WiFi, WiMax, Femtocell, celular, etc. La arquitectura IMS, está concebida para poder brindar todo tipo de aplicaciones a suscriptores en cualquier red de acceso, a través de una red común con arquitectura IMS. La red IMS es agnóstica respecto al acceso, servicios y ubicación.

Permitiendo a los operadores de red realizar una convergencia completa y que además reutiliza parte del equipamiento. Hoy los operadores tienen numerosos incentivos para desarrollar una red IMS, incluyendo convergencia fijo-móvil (FMC). Creación de servicios, incremento del revenue por usuario, y reduciendo Capex (gastos de capital) OpEx (gastos de operación).

En última instancia el éxito o no de IMS, va a depender de los servicios disponibles en la red, y no del equipamiento de red. Como se mostró anteriormente, los servicios dentro de la arquitectura residen en la Capa de Servicios, la cual permite combinar servicios para rápidamente poder desplegarlos a los usuarios en la red. Esto cambia el paradigma de los operadores tradicionales, que ya no son Carriers de tuberías de bits, sino proveerán servicios innovadores de valor agregado y personalizados para cada usuario. Como también se planteó en este trabajo, esto permite brindar servicios que incrementen la medida de ARPU (o utilidad por usuario). Al mismo tiempo, los operadores tradicionales podrán competir mejor con la figura de operador móvil virtual (MVNO). Por otro lado, IMS provee un acceso seguro con QoS, dando a los operadores de la red, una ventaja competitiva para la provisión de servicios sobre las redes de los MVNO, que no tienen control de los recursos de la red. El resultado es una red capitalizada en términos de facturación y no una red comoditizada, como una tubería de bits.

Por último, como parte de la definición del problema de si adoptar o no esta arquitectura, los operadores tradicionales tienen muy en claro los beneficios de IMS, pero también reconocen y hay que mencionarlo, que es la complejidad de la arquitectura IMS. Muchos operadores en tren de buscar una solución que provea todos los beneficios de IMS, pero sin la complejidad de su arquitectura, han adoptado arquitecturas menos complejas, para lo cual IMS, provee cierta capa de trabajo, se están denominando "Pre-IMS", "IMS-Lite" o "IMS-Like". Colapsando con muchos de los componentes e interfaces externas. Reduciendo también CapEx, OpEx y acelerando el despliegue de servicios IP.

Esta problemática es actual e involucra tecnologías de punta.

Además es de gran importancia dado que involucra a empresas como los operadores clásicos de telefonía y posibles operadores virtuales. Empresas que hoy no forman parte del negocio de las telecomunicaciones móviles.

En este trabajo no nos basaremos en el marco regulatorio de nuestro país o de algún país en particular, a efectos de realizar un análisis asociado a la potencialidad de la tecnología sin considerar en esta instancia restricciones que al fin y al cabo son ajenas a la tecnología y nos impondrían restricciones a nuestras conclusiones (por ejemplo excluir el caso del cuádruple play). Un abordaje posterior requiere

personalizar las conclusiones a las condiciones Legales y regulatorias del país en cuestión.

3.2 Problemas a Resolver

3.2.1 **Hipótesis 1:** *Podemos afirmar que IMS es el único estándar desarrollado para poder integrar un modelo de servicios sobre redes IP: con independencia del acceso, seguridad y múltiples servicios para el usuario, por eso sigue estando vigente.*

Pasaron 16 años desde su aparición, y en ese período aparecieron nuevas tecnologías, algunas de las cuales incrementaron su confiabilidad en la oferta de servicios.

- ✓ IMS está vigente?
- ✓ Que cosas prometía IMS (a nivel de servicios)? Y Cuales de estas promesas se cumplieron?
- ✓ Que otras tecnologías prometen o hacen efectivamente las mismas cosas?
- ✓ Atributos tecnológicos seleccionados:
    1. Independencia del acceso
    2. Seguridad
    3. Multiplicidad de servicios
    4. Flexibilidad para soportar nuevos modelos de negocios.

3.2.2 **Hipótesis 2:** *La arquitectura IMS es la única solución actual que permite inter-operabilidad con redes existentes. Respecto de las tecnologías existentes, esta arquitectura permite soportar e inter-operar con las redes existentes.*

5. Interoperabilidad con otras redes, que otras tecnologías aparecieron en los 16 años y prometen lo mismo, a pesar de eso IMS sigue siendo la mejor opción.

3.2.3 **Hipótesis 3:** *La arquitectura IMS se puede implementar por etapas, lo que permite una introducción progresiva de servicios, lo que facilita la justificación del plan de negocios.*

Es factible una implementación progresiva, con incorporación progresiva de prestaciones y servicios, lo que facilita la justificación económica del plan de negocios.

4 Solución al problema planteado en las Hipótesis

4.1 Solución al problema planteado en la Hipótesis 1– Estudio de Casos

En este punto, estudiaremos dos casos, relacionados a dos nuevos servicios que el operador necesita brindar.
Por este método de casos trataremos de demostrar las dos primeras preguntas de la hipótesis 1, a saber:

- ✓ IMS está vigente?
- ✓ Que cosas prometía IMS (a nivel de servicios)? Y Cuales de estas promesas se cumplieron?

En el primer caso un operador se ve necesitado de incorporar un nuevo servicio en la NUBE. Brindar servicios de conferencias de audio, video y web. Para eso veremos que necesita en su red IMS para incorporar dicho servicio.

En el segundo caso el operador ya cuenta con un Core IMS, y necesita introducir el servicio de VoLTE. Para eso veremos que necesita agregar en su red IMS para incorporar dicho servicio.

4.1.1 Primer Caso: Incorporar en una red IMS "Servicio de Conferencias de Audio, Video y Web."

El objetivo de este proyecto es presentar un escenario utilizando la arquitectura de red IMS para brindar un "**Servicio de Conferencias de Audio, Video y Web".**

Arquitectura:

La arquitectura de red para la implementación del Servicio de Conferencias de Audio, Video y Web, sigue la definición de capas del Modelo IMS que se viene tratando en el presente trabajo.

- Capa de acceso
- Capa de control
- Capa de aplicación

A continuación, se muestra un esquema de esta arquitectura de red.

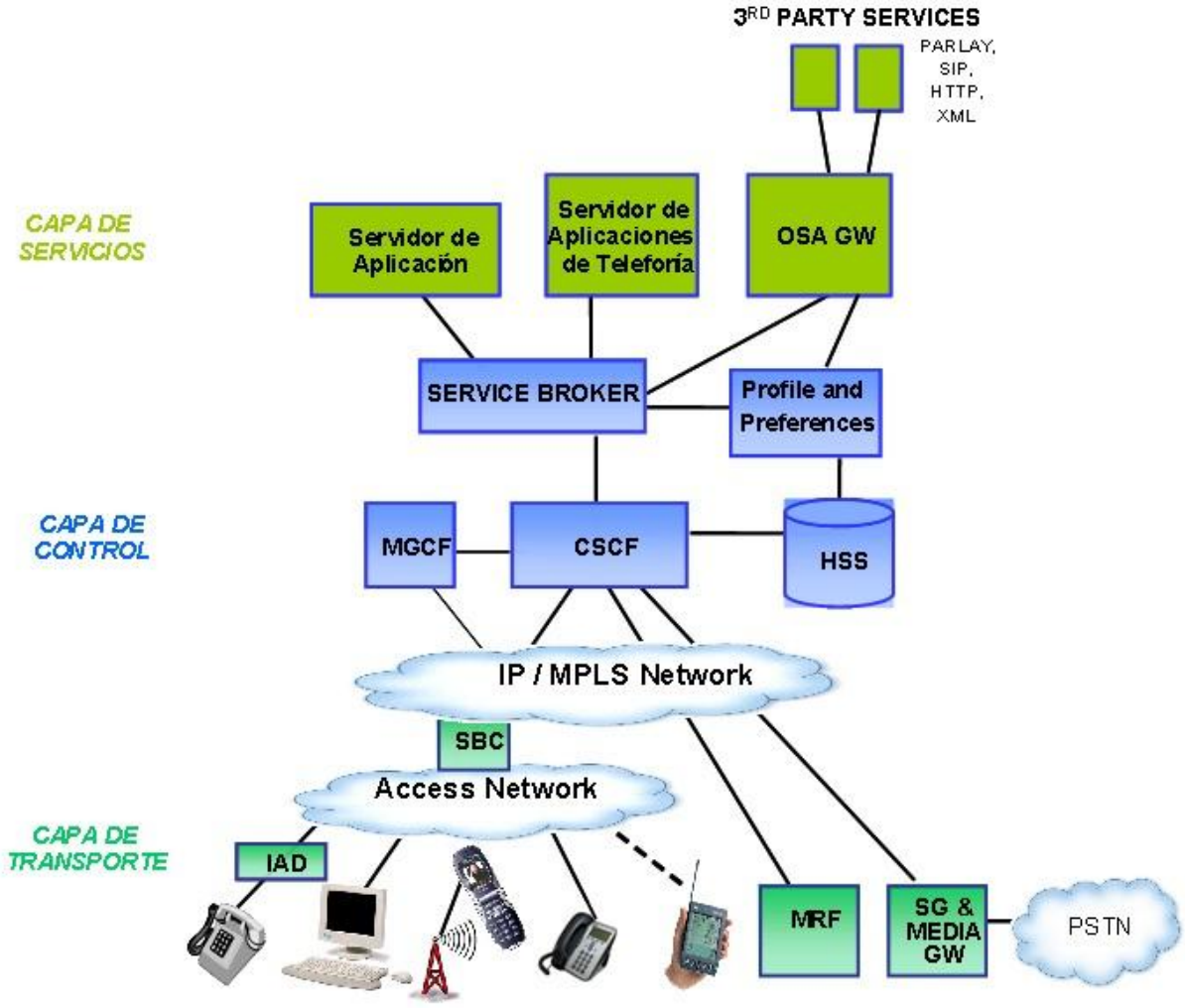

Figura 32: Arquitectura de Red

Capa de Aplicación (Application Layer): contiene los servidores para la ejecución de los servicios de valor agregado para el usuario. En esta capa se encuentra el Application Server que soportará el Servicio de Conferencias de Audio, Video y Web.
Capa de Control (Control Layer): contiene todas las aplicaciones y equipamientos de control, siendo el elemento más importante de esta capa el **CSCF** que cumple la función de Call Session y Control Function. Esta capa también contiene las aplicaciones de aprovisionamiento.
Capa de Conectividad o Transporte: contiene los routers y switches, ambos elementos necesarios para el backbone y acceso a la red IP

Esta arquitectura IMS, para la prestación del Servicio de Conferencias de Audio, Video y Web, se implementará en forma distribuida en los operadores de telefonía fija (OTFs).

El **CSCF** atenderá las necesidades de cada oficina técnica; de esta manera, los usuarios SIP serán autenticados y controlados por su CSCF, que buscará la información de esos usuarios en el HSS, que será un servidor externo al CSCF con funciones de base de datos de los usuarios y servicios.

La facturación de los servicios será responsabilidad de un elemento de Mediación, que tendrá la funcionalidad de generar los CDR y facturar las llamadas (billing). En las OTFs que poseen el mediador BMP podrán utilizar el mismo equipamiento. El cual, a través del protocolo FTP o Radius, dependiendo de su configuración, recibirá los archivos (logs) de llamadas realizados por el CSCF y por el Application Server. De esta manera, cada una de las oficinas técnicas será responsable por la facturación de sus clientes.
De la misma forma ocurre con el SBC y el Media Server, los cuales, también deberán estar distribuidos en cada OTF.
La aplicación de Aprovisionamiento podrá ser accedida por diversos niveles de las OTFs, para lo cual, se contará con los siguientes 5 niveles de acceso:

- Proveedor del Sistema
- Proveedor de Servicios
- Administrador de Grupo
- Administrador de Departamento
- Usuario final

El equipo Service Broker y la Capa de Aplicación forman parte de la solución para el soporte del servicio detallado en la Especificación del Servicio Conferencias de Audio, Video y Web.

La plataforma de Conferencia Audio se comunicará con la plataforma de Conferencia Video mediante protocolo SIP, o sea un usuario de VoIP controlado por el Application Server, en este caso de Broadsoft, al discar el código de acceso a una sesión de conferencia, será direccionado hacia la plataforma de conferencia video por protocolo SIP.

Modelo Distribuido

Este modelo distribuido permite que no todas las OTFs requieran de todos los servicios en una primera etapa.

Todos los equipos utilizados en la solución quedaran con la nomenclatura funcional estandarizada en la arquitectura IMS, presentada en el esquema de Arquitectura de red de este documento.

Este esquema permite una gran escalabilidad de los equipos en función de los servicios y cantidades de usuarios.

Alcance de la Solución

Plataforma – consiste en las funcionalidades de lógica de aplicación, variando en función del número de usuarios y servicios de conferencias (contempla hardware y software.

MRF – elemento necesario para soportar el servicio de conferencia que está distribuido en las OTFs para la recepción del tráfico de media.

Licencias – se consideran todas las licencias de software sobre los servicios/aplicaciones a ser prestados por la plataforma de servicios

Media Server – contempla hardware + software + licencias VXML o de otros protocolos o codecs necesarios.

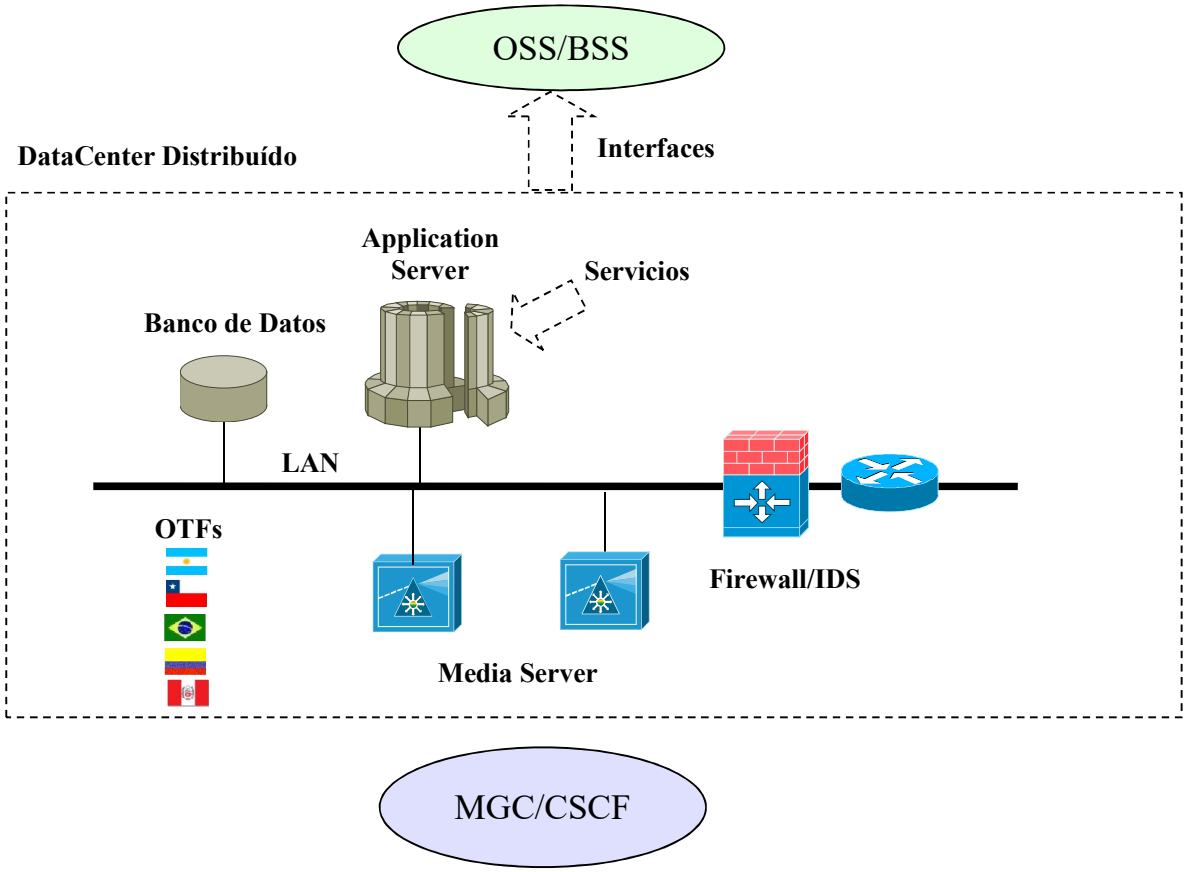

Figura 33: Data Center Distribuido

Servicios a proveer para el desarrollo de interfaces

Desarrollo de interface Conector JAVA como EAI.

Desarrollo de interface como el WebServer externo, a ser utilizado por el operador a futuro.

Desarrollo de interface con sistemas legados

Criterios Generales

Se prevé utilizar estructuras redundantes en todos los módulos/funciones que están presentes en la Plataforma.

La gestión de la plataforma se integrará con el sistema del operador.

Criterios de Ingeniería

La solución para cada modelo contempla todas las unidades, software, piezas y partes (bastidores y sub-bastidores) de los equipos, materiales, servicios, gestión,

proyecto, necesarios para el perfecto funcionamiento del mismo y para cumplimiento de las cantidades de interfaces de las Tablas de este documento.
Los dispositivos son equipos Carrier Class, es decir, aptos para brindar servicio continuo en una Red Pública. Por lo cual, cuentan con dispositivos redundantes en los bloques críticos para el manejo de tráfico, manteniendo el servicio sin interrupciones ante eventuales fallas de hardware y/o software.
Cada equipo se vinculará al BB IP mediante un switch 10/100/1000 BaseT. Asimismo tiene la capacidad de detectar la pérdida de conectividad con el BB IP.
La distancia para cables/Cordones de fibra óptica, desde cada dispositivo a la patchera/DIO de acceso al switch de acceso a Red IP será de veinte (20) metros.
Los equipos serán conectados a un mismo par de Switches redundantes para conectarse al Backbone IP.
Los dispositivos cuentan con redundancia en las interfaces que los vinculan al Backbone IP y de Gestión (EER), manteniendo el servicio sin interrupciones ante eventuales fallas de hardware.
Al conectarse al Backbone EER a través de un Switch, los equipos tendrán herramientas de supervisión de caída de las interfaces / vínculos Switch – Edge Router.

Referencias: 20, 21, 22 y 23.

4.1.2 Segundo Caso: Incorporar en una red IMS VoLTE

Hay una necesidad que es indiscutible, y es la necesidad de poder brindar VoLTE, en las redes de los operadores actuales. Por ende, ya no se trata de un servicio de conferencias sino de algo un poco más crítico para los operadores móviles. Veremos a continuación cuan simple o no es brindar voz sobre LTE (VoLTE), en una red actual IMS.

Arquitectura IMS para soportar VoLTE

Considerando un futuro crecimiento y después de la evolución de TDM a IP y la inminente evolución de la red GSM / CDMA / UMTS a LTE en el lado de la red de radio y la evolución de la CS a IMS en el lado de la red central, a continuación se analizan múltiples puntos de vista, las tecnologías y caminos de evolución para los servicios de voz LTE, para tomar la decisión de invertir en un Core IMS que soporte VoLTE.

Se tomaron 4 enfoques fundamentales de la tecnología que pueda brindar este servicio. Entre ellas:

El repliegue de conmutación de circuitos (CSFB):

LTE sólo proporciona servicios de datos, y cuando una llamada de voz debe ser iniciada o recibida, caerá de nuevo al dominio CS.

Ventaja: Cuando se utiliza esta solución, los operadores sólo tienen que actualizar el MSC en lugar de desplegar el IMS, y por lo tanto, pueden proporcionar servicios de forma rápida. Desventaja: demora en el de establecimiento de llamada.

En la mayoría de los casos, la solución CSFB es adecuada como una solución provisional antes del despliegue de IMS. Además, se puede utilizar para manejar las llamadas de voz en el escenario de LTE itinerancia. Por ejemplo, cuando la red visitada no tiene IMS o cuando el protocolo de itinerancia IMS aún no se ha desplegado, CSFB puede proporcionar servicio de voz de guardia para usuarios de roaming LTE entrantes.

Voz Simultánea y LTE (SVLTE):

SVLTE es un doble enfoque microteléfono radio, el teléfono funciona simultáneamente en los modos de LTE y CS, con el modo de LTE proporciona el servicio de datos y en el modo CS proporciona el servicio de voz.

Ventajas: Esta es una solución basada exclusivamente en el teléfono celular, que no tiene requisitos especiales en la red y no requiere el despliegue de IMS tampoco.

Desventaja: el teléfono puede llegar a ser caro con alto consumo de energía. Terminales de radio, actualmente duales que ofrecen 1x CDMA y LTE ya están disponibles y utilizados por algunos operadores CDMA como solución provisional antes del despliegue de IMS, mientras que los terminales de radio dual protagonizados GSM / UMTS y LTE aún no están disponibles.

Uso de los servicios over-the top (OTT):

El uso de aplicaciones como Skype, WhatsApp y Google Talk para proporcionar servicio de voz LTE.

Ventaja: LTE cuenta con características como el amplio ancho de banda, baja latencia, siendo siempre en línea, y All-IP, la creación de conveniencia natural para el desarrollo de la OTT y hacer llamadas de voz OTT casi sin barreras.

Desventaja: el servicio de llamadas de voz es, y seguirá siendo, la principal fuente de ingresos para los operadores móviles. Así que la entrega del servicio de voz sobre LTE completamente a los actores OTT es, pues, algo que se espera no recibir demasiado apoyo en la industria de las telecomunicaciones.

En el futuro, el porcentaje de llamadas OTT puede aumentar drásticamente, sobre todo para la llamada de larga distancia. Sin embargo, el servicio de llamada proporcionado por los operadores de telecomunicaciones seguirá siendo la corriente principal durante un largo tiempo.

VoLTE basado en IMS.

Finalmente, IMS se ha convertido en la arquitectura estándar de la red central en la era All-IP, ya que soporta múltiples modos de acceso y una amplia gama de servicios multimedia. Después de desarrollarse y madurar en los últimos años, IMS hoy ha cruzado la sima para convertirse en la corriente principal para la elección VoBB y migración de la red PSTN en el campo de guardia fijo, y también se ha identificado como la arquitectura estándar para el servicio de voz móvil y por el 3GPP GSMA.

De los enfoques anteriores, tanto CSFB y SVLTE confían en el dominio de CS para proporcionar servicio de voz y ambos tienen algunas limitaciones. Pueden ser utilizados como la elección y aplicación provisional no convencionales, lo que llamamos pre-VoLTE. Sólo IMS puede proporcionar una solución de voz con la garantía de QoS basado en LTE. En otras palabras, VoLTE basada en IMS es el camino inevitable para el desarrollo de las tecnologías de red inalámbrica y de Core.

VoLTE está basado principalmente en la Centralización y Continuidad, dos mecanismos que son implementados por medio de una serie de servicios de IMS muy específicos identificados como ICS (IMS centralized Services) y SRVCC (Single Radio Voice Call Continuity). Para esto, no solo es necesario Core IMS y su correspondiente servidor de aplicación VoIP estándar (MMTel), sino un nuevo servidor de aplicación cuya principal función es establecer una conexión entre el

mundo IP (PS) y el mundo de circuitos (CS), cuando el usuario pierde cobertura LTE.

Luego de observar la notable ventaja de IMS sobre el resto de las tecnologías, se propone desplegar la infraestructura necesaria para brindar el servicio VoLTE (Voice Over LTE). Al igual que la disponibilidad masiva de terminales compatibles con VoLTE

Los principales cambios a realizar sobre el Core son los siguientes:

Plano de servicios:

Realizar una actualización en SIP-AS (servidor SIP), para incluir dos servidores adicionales que están cercanamente relacionados, encargados de las rutas de señalización para las llamadas entrantes y salientes

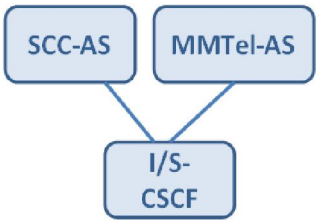

Figura 34: Actualización del Plano de servicios

MMTel –AS (MTAS):

Es un servidor de aplicación de VoIP estándar el cual forma parte del Core IMS. Este servidor ofrece servicios de voz y video sobre accesos LTE. Los servicios de voz pueden enriquecerse con videos y combinarse con otros servicios mejorados basados en IP como voz HD, presencia, localización, mensajería instantánea, videos compartidos y agendas telefónicas mejoradas.

SCC- AS:

Es un servidor de aplicación de continuidad y centralización que complementa al servidor de VoIP MMTel, facilitando la conexión a diferentes accesos en el dominio natural LTE de conmutación de paquetes IP y en la red de conmutación de circuitos para cuando se pierda la cobertura LTE.

El servidor se encarga del Handover de VoIP hacia CS cuando el usuario pierde cobertura de LTE bajo mecanismo SRVCC (Continuidad de llamada de Voz de Radio Única):

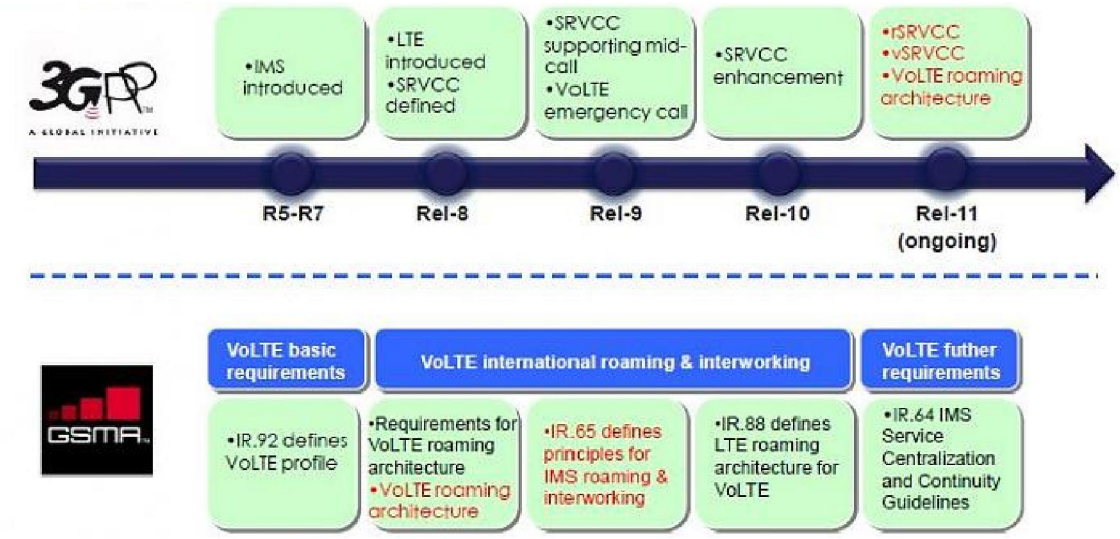

Figura 35: Estado de estandarización de VoLTE

Se deduce de esto último, la íntima relación de EPC con IMS constituyéndose éste último una pieza indispensable (no opcional), para desarrollar VoLTE.

La segunda funcionalidad, conocida como ICS, permite disponer de un punto central, único en el dominio IMS tanto para los accesos LTE y 2G/3G. De esta manera el usuario no percibe diferencias y todos los servicios son brindados de igual manera con independencia de la tecnología de acceso

SRVCC e ICS:

A medida que la cobertura de LTE crece, la probabilidad de que una llamada tenga que ser accedida vía 2G/3G disminuye. Es entonces cuando se despliega VoLTE. Sin embargo como esa probabilidad no es nula, para brindar los servicios de voz dentro del área de cobertura LTE y al mismo tiempo disponer de un handover de las llamadas hacia 2G/3G, la red necesita ofrecer dos facilidades:

- ***Continuidad***: Una sesión establecida es continuada sin interrupción (o con una interrupción menor a un umbral preestablecido del orden de 100-

200 milisegundos) cuando el usuario pierde cobertura LTE y entra en una red 2G/3G RAN

- ***Consistencia de Servicios:*** El punto de partida es un servicio VoIP alineado con la normativa 3GPP definida en MMTel, lo cual supone conectividad IP. Sin embargo, en un escenario de handover, esa conectividad se pierde y el acceso se debe re-establecer a través de la red de Circuitos. Los servicios de voz ofrecidos al usuario deben ser consistentes, idealmente idénticos sin importar si se accede al mismo vía LTE o la red 2G/3G.

Plano de Control y Plano de transporte:

Es necesaria la actualización de SBC para incluir dos servidores:
El Access Transfer Gateway (ATGW) es controlado por el Access Transfer Control Function (ATCF) y juntos proveen el anclaje del media para las llamadas VoLTE durante el handover SRVCC entre LTE y las redes conmutadas de circuitos móviles 2G/3G. Debido al anclaje del ATGW, no se necesita realizar renegociación end-to-end durante la transferencia de acceso, sino que solo el acceso es el que cambia.

- ***ATCF (Access Transfer Control Function):*** Actúa como punto de anclaje de señalización SIP y está localizado en el camino de la señalización entre el P-SCSF y el S-CSCF e informa al SCC AS que la sesión de transferencia se ha realizado. Este elemento puede ser implementado como parte del P-CSCF o IBCF.
Según las políticas del operador, el ATCF debería incluirse a sí mismo para las sesiones SIP e instruir al ATGW para anclar los caminos de media para iniciar y terminar las sesiones, hacer seguimiento de las sesiones para ser capaz de realizar transferencias de acceso, actualizar al ATGW con los nuevos caminos CS al realizar transferencia de acceso y manejar las fallas ocurridas durante la transferencia de acceso.

- ***ATGW (Access Transfer Gateway):*** Actúa como punto de anclaje de media y es controlado por el ATCF. Si se utiliza el SRVCC mejorado y ATCF, el ATGW permanece en el camino de sesión de media por la duración de la llamada y luego de una transferencia de acceso, basado en las políticas locales de la red.
El ATGW soporta transcodificación luego de SRVCC handover en el caso de que el contenido media utilizado antes del handover no sea soportado por el servidor MSC. Dependiendo de la localización del ATCF, diferentes nodos físicos pueden ser considerados para el ATGW como por ejemplo el IMS-AGW o el TrGW. El ATCG y

ATGW son entidades vitales y tenerlos en la red reduce la duración del tiempo de interrupción durante el SRVCC handover.

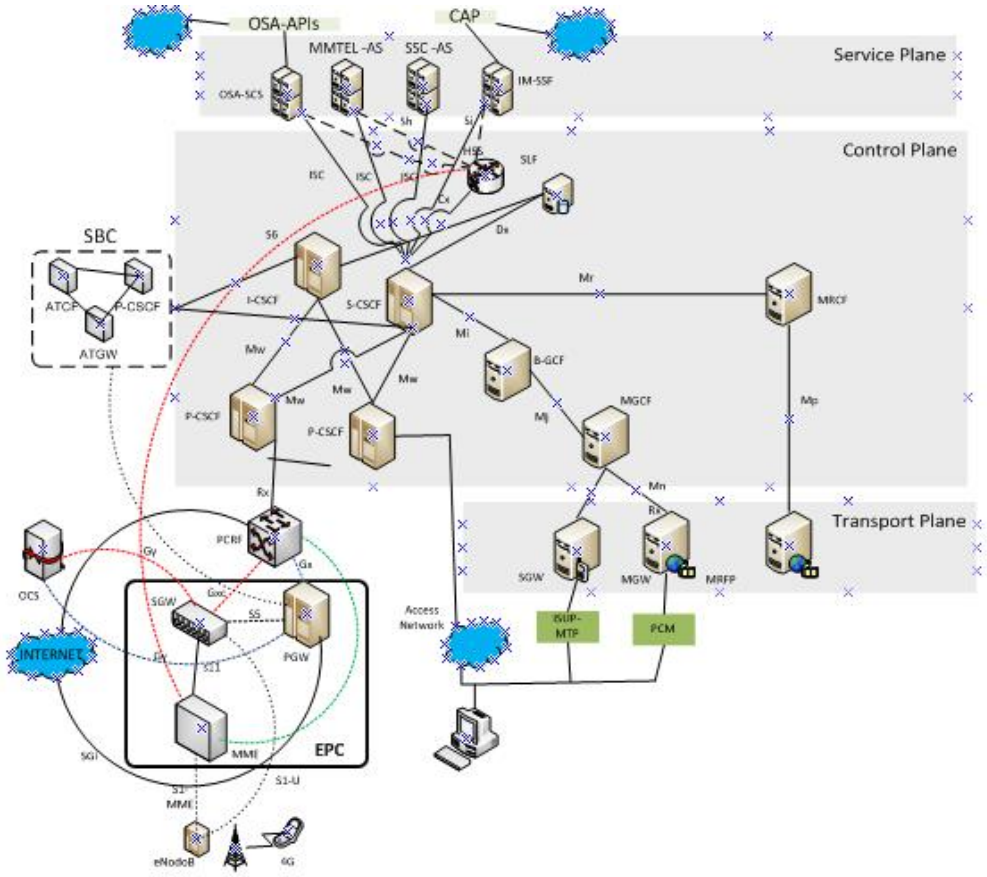

Figura 36: Arquitectura Core IMS como base para soportar 4G

Interworking Function VOLTE

Interworking Function (IWF) es una solución de superposición que ayuda a los operadores de telefonía móvil 4G / LTE implementar SR-VCC de forma rápida y rentable. Este tipo de solución elimina la necesidad de mejorar o actualizar la red de conmutación de circuitos con nuevas interfaces IP, reduciendo así el costo y la complejidad de implementar esta función crítica (servicio de voz) del negocio en la red LTE y acelerar el tiempo de lanzamiento al mercado del servicio de Voice Over LTE (VoLTE).

VoLTE IWF es compatible con CSFB y permite la rápida inserción de dispositivos compatibles con 4G-CSFB sin tener que actualizar el Core de la red CS para soportar las interfaces SG's. CSFB-IWF realiza todas las funciones de inter-funcionamiento necesarios para habilitar el servicio de SMS a dispositivos CSFB, así

como de ejecutar los "trigger" de retorno para habilitar los servicios de voz desde el Core de la red CS. Esta aplicación es ideal como una solución provisional ya que se puede desplegar CSFB-IWF primero, y más tarde realizar una actualización de software para habilitar la funcionalidad SRVCC IWF, evitando así, la necesidad de actualizar el MSC para soportar el CSFB o SRVCC.
La IWF mitiga la necesidad de inversión continua en redes CS por el bien de la implementación de dispositivos y servicios 4G. Esta es una solución basada en software que está totalmente desplegada sobre la infraestructura de la nube del operador.

4.1.3 Algunas consideraciones respecto a los casos anteriores:

A continuación resumo una serie de consideraciones respecto a los 2 casos desarrollados y como contribuyen a responder la cuestión de la vigencia de IMS.

Caso 1: Incorporar en una red IMS "Servicio de Conferencias de Audio, Video y Web."

El Caso planteado muestra la vigencia de IMS, ya que permite:

- Tener un escenario distribuido, con billing por regiones
- Contar con un Core pre-existente de IMS
- La estandarización de parámetros
- La no duplicidad de funciones para los servicios ofrecidos, ej. El usuario ya está autenticado en la plataforma. Solo necesito levantar su perfil para ver qué servicios tiene contratados
- La seguridad extremo a extremo de la comunicación

Algunas salvedades. Si bien no podemos extraer una conclusión general a partir de un caso, y en particular, no podemos basarnos solo en ese caso para justificar la implementación de una red IMS en un operador actual, esta implementación está comercialmente disponible a pesar que con otras tecnologías (por ej. tecnologías web RTC), y cualquier PABx nativa IP de mercado puedo dar los servicios que necesito para poder satisfacer los requerimientos del mencionado caso.

Caso 2: "Incorporar en una red IMS VoLTE"

Una llamada que se inicia sobre una red 4G y por un tema de cobertura de red, se necesita cambiar a 3G, esto lo pudimos ver en el caso, que se resuelve fácilmente con una red IMS.

El Caso planteado muestra la vigencia de IMS, ya que:

- Hoy no existe una solución VoLTE con QoS, que no utilice un Core IMS
- Permite ir adoptando la solución final en etapas
- Garantiza el handover a 2G y 3G
- Provee seguridad extremo a extremo

Algunas salvedades. Si bien la solución de VoLTE IMS, podría ser realizada por la combinación de otras tecnologías, tal el caso de Skype, podemos afirmar que su calidad de servicios es "best effort". También la opción de WhatsApp para llamadas.
Pero estas alternativas no dan una respuesta aceptable a Operadores como Telefónica o a AT&T, deben brindar una calidad de servicio para sus servicios muy diferente (calidad "carrier grade").

Por ende podemos decir que hay dos visiones del mismo problema: Best effort vs Carrier Grade, y dependiendo del prestador del servicio y sus obligaciones tendremos dos opciones o modelos de negocios y diferentes opciones de arquitectura.

4.2 Independencia del Acceso

Definición de independencia de acceso: significa que no importa desde que punto de conexión estoy accediendo a la red. Es decir puedo acceder desde un wifi público, desde mi hogar con una conexión ADSL, o a través de una red celular.
Se pretende que este tipo de arquitectura, le permitan al usuario acceder a una amplia variedad de comunicaciones, información y/o servicios de entretenimiento con consistente calidad de servicio, independientemente del dispositivo usado, la red sobre la que esas aplicaciones corren y la locación del usuario.

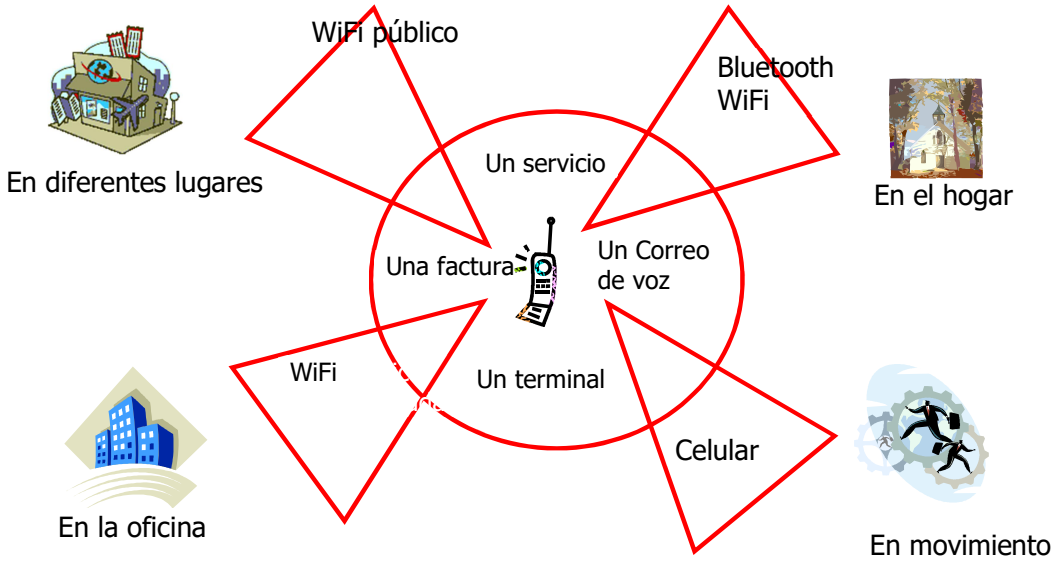

Figura 37: Acceso a la red sin importar donde este el usuario

Los servicios de comunicaciones (voz, video, chat, etc.) estarán disponibles con cualquiera de los siguientes **medios de acceso**: cableado, ya sea cable modem o xDSL e inalámbrico, como WLAN, UMTS, HSPA y LTE.

Dada esta variedad de sistemas de acceso, los **terminales móviles** deberán soportar dos, o más tecnologías de acceso para permitirles operar en los diferentes entornos. Un ejemplo de hoy sería los teléfonos inteligentes (smartphones), que soportan 3G o LTE y WLAN. Este último utiliza SIP y RTP para acceder a una red IMS.

La **red IMS multi-acceso (IMA),** es una solución estandarizada en una solución IMS con servicios centralizados (IMC). Esta última facilita la conexión a una red IMS a los diferentes terminales y redes de acceso.

La clave para poder generar una IMA, es que IMS separa estrictamente la capa de control y la capa de usuario. Esta separación hace posible, el transporte del canal de audio o media, entre los llamantes, por la mejor ruta y con una determinada QoS. A diferencia de las redes basadas en conmutación de circuitos (circuit-switches), IMS no establece el circuito de voz, cuando se establece una llamada o sesión. La capacidad de transporte de voz o media, no se reserva hasta tanto no se establece la sesión de transporte. Así se pueden optimizar acciones como derivación o transferencia de llamadas.

IMA (IMS Multi Acceso), permite acoplar a dispositivos no-IMS (ejemplo GSM) a una red IMS y a sus servicios. Permitiendo el control de las sesiones y llamadas desde el SIP-AS con cualquiera de los terminales que estén conectados a la red.
Con IMA, los usuarios de la red IMS, pueden establecer llamadas y recibir llamadas en teléfonos GSM, UMTS o ISDN. Por ejemplo, un usuario registrado con un teléfono GSM, es ruteado por la red IMS, donde el usuario recibe todos los servicios. Esto se conoce como overlay. Dentro de la red IMS estas llamadas disparan los servicios IMS. Esto permite que usuarios que tengan un teléfono SIP, y teléfono móvil GSM, las llamadas sean enrutadas a ambos aparatos o en secuencia.

En base a todo este tipo de beneficios que tendrá el usuario, el objetivo es brindar en base los casos analizados, las herramientas necesarias, para que un operador pueda analizar si le conviene o no integrar una arquitectura IMS. O por lo menos poder hacer un análisis de donde se encuentra y como está su red, frente a los posibles cambios que ya están entre nosotros y como eso le impactará en su captación de nuevos clientes, y poder aumentar o no su nivel de facturación.

Referencia 35

4.3 Seguridad

Definición de Seguridad: Significa poder establecer una comunicación extremo a extremo sin que pueda ser intervenida, ni monitoreada. Hay dos partes en este tema, la seguridad en el acceso y la seguridad de las redes.
IMS soporta un acceso seguro a los servicios. Aplicando un método de autenticación, como se vio anteriormente, tanto para la autenticación del usuario, como para el operador. Las funciones de autenticación las controla CSCF. Una vez que el usuario se identificó puede acceder a todos los servicios que tiene disponible en la red IMS.

El servidor de HSS (Home Subscriber Server), se utiliza para administrar los servicios contratados por los usuarios. HSS provee la autenticación y la autorización para brindar acceso a los servicios de la red. Las especificaciones del HSS están definidas por 3GPP. Hay varios servicios que provee el HSS:

- Autorización de un servicio
- Autorización del acceso
- Manejo de la Identidad del usuario
- Seguridad del usuario

- Perfil del servicio
- Gerenciamiento de la movilidad

En esta arquitectura, ya vimos que los usuarios, deben pasar múltiples procesos de autenticación y de homologación de claves, para tener acceso a los servicios de la red IMS. La seguridad es hoy una de las principales preocupaciones para el diseño de nuevas implementaciones y sistemas. En un sistema de comunicaciones basado en IMS toda la seguridad se basa detectar las amenazas sobre una red IP.
La seguridad dentro de una red IMS, se basa en dos puntos fundamentales. El primero es la seguridad en el acceso a la red, y la segunda, la seguridad de la red en sí misma. En el primero caso, se basa en la autenticación del usuario y los mecanismos de autorización, independientemente del tipo de red o acceso que el usuario utilice para conectarse. Que sea independiente del tipo de acceso o nodo desde el cual el usuario está accediendo, no significa que las credenciales y acceso que se le brinden al usuario, sean siempre las mismas. Por el contrario, el usuario puede tener los servicios reducidos por el tipo de dispositivo que usa para conectarse. En el segundo caso, la seguridad de la red (Dominio), involucra proteger el tráfico de datos la terminal del usuario y el Core de la red IMS, que puede ser inter-domain, o intra-domain.

4.3.1 Seguridad en el Acceso

El proceso de autenticación y autorización de usuarios para acceder a los servicios de una red IMS, es lo primero que se hace. EL siguiente paso del proceso, es establecer la señalización. Para asegurar el protocolo SIP. Para esto se ejecuta IP-Sec en ambos lados, es decir lado usuario y lado del servidor P-CSCF. En el servidor S-CSCF es donde se lleva a cabo el proceso de autenticación y autorización, en conjunto con el HSS, para determinados perfiles de usuario específicos.

4.3.2 Seguridad en la RED

El proceso de seguridad en la red es responsable por el resto de la comunicación en términos de asegurar el tráfico de datos en la red IMS. Las políticas y reglas de seguridad las establece el operador de la red.

4.3.3 Seguridad en el Dominio de la Red

Este proceso con lleva a implementar un Gateway de Seguridad (SEG) entre dos Dominios de red, con criptografía, encripción, integridad de datos y autenticación; junto con Internet Key Exchange o IKE.
Las redes IMS se basan en el concepto de arquitectura de red local o visitante. Por ende existen dos casos en los que un usuario se conecta a un Core IMS. En el primer caso se conecta a una red local y en el segundo a una red que no le pertenece. La ubicación del usuario la especifica el P-CSCF.

4.3.4 Base de datos de las políticas de Seguridad (SPD)

Esta base de datos mantiene las políticas de seguridad que diferencian el tráfico dentro de la red o fuera de la misma. La decisión de reenviar un paquete está basada en las políticas de esta base de datos (SPD). Las políticas pueden ser las siguientes:

- Asignar los servicios de IPSec a un paquete
- Descartar el paquete
- Permitir al paquete saltear los servicios de IPSec

4.3.5 Seguridad en IMS

Como se vio más arriba, la seguridad en IMS se basa en la seguridad en el acceso y la seguridad de la red. Los datos son protegidos entre terminal y nodos. Significa que el usuario y la red son seguros por medio de la seguridad del protocolo SIP. El principal objetivo de una red IMS es proveer seguridad e integridad de los datos en todo el acceso a la red con seguridad punto a punto.

4.3.5.1 Tipos de ataques

La convergencia de redes IP con redes móviles y de telecomunicaciones tendrán los problemas de seguridad de las redes IP. Esto tendrá un impacto negativo en las redes basadas en SIP.

Espionaje (Eavesdropping): el atacante escucha o roba los mensajes SIP. Para prevenir esto se usa la encripción.

Laguna de registro (Registration loop hole): el atacante envía un mensaje de registración con un ID robado de un usuario.

Ataque al servidor proxy (Proxy server attack): cuando un servidor falso toma el control del tráfico de un usuario.

Manipulación del mensaje (Message tampering): SIP envía mensajes en texto plano. Estos mensajes no son seguros y pueden ser accedidos.
Denegación del servicio (Denial of Service): se envía un pedido falso a la red el cual puede causar que los servicios no estén más disponibles.

Intensificación (Intensification): similar a DoS pero con mayor cobertura de red.

4.3.5.2 Arquitectura de Seguridad:

En una red IMS la seguridad se implementa para proteger las señales SIP, con mecanismos de autorización y autenticación.

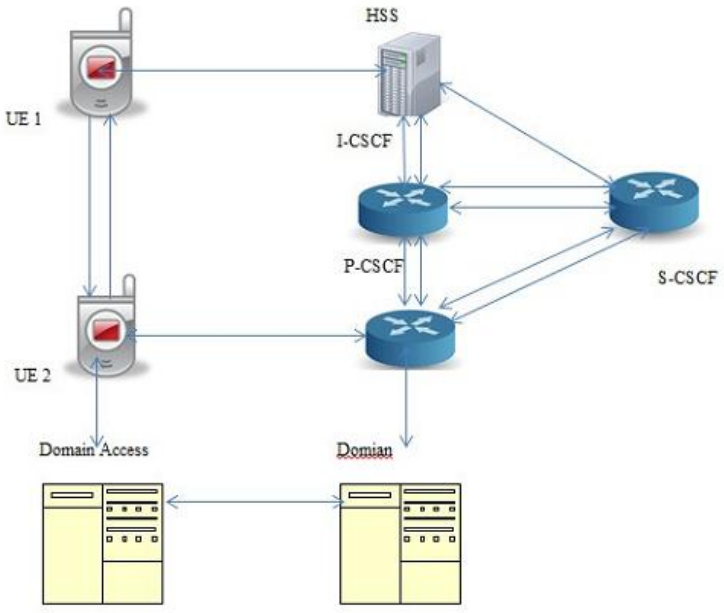

Figura 38: Arquitectura de Seguridad en IMS

De acuerdo a la figura:

- El equipo del usuario (UE) y la red IMS se autentican mutuamente. El server S-CSCF ejecuta una función de control que enviará una alerta al HSS para obtener las claves.
- El UE se conecta vía el P-CSCF, ambos van a requerir asegurar el link.
- El HSS y las funciones de control del S-CSCF también se conectan con links seguros.
- En modo roaming, el UE crea un link seguro en la red visitada.
- Se implementa la seguridad entre P-CSCF y UE si ambos están en la red local.

4.3.5.3 UMTS autenticación y aceptación de claves (AKA)

Este protocolo de seguridad de autenticación e intercambio de claves, se implementa para autenticar al UE en la red IMS.

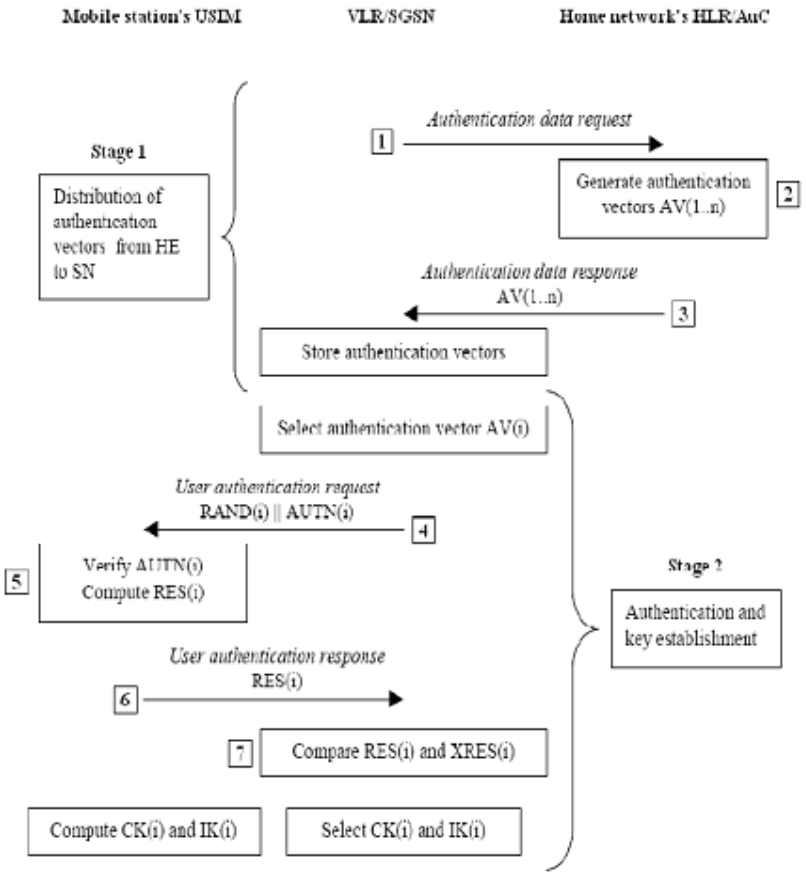

Figura 39: Sistema de Seguridad de Autenticación UMTS (Fuente 36)

En este procedimiento, la red visitada envía a la red local los datos para ser autenticados. La red local envía un vector de autenticación (AV) a la red visitada. La red local luego evalúa el AV usando una clave secreta. La clave secreta se ubica en la red local y el UE. La red local responde y envía el AV a la red visitada. Cuando el vector AV llega a la red visitada selecciona y envía una respuesta, con los mensajes RAND y AUTN. El UE evalúa el AUTN, usando la clave secreta. Por último el UE genera una respuesta RES y la envía a la red visitada y la compara con XRES.
En este escenario, el atacante no puede robar la clave secreta mientras escucha la trasmisión, ya que la clave no se trasmite.

4.3.5.4 Protocolo de Seguridad (SDES)

El protocolo SDP (Session Description Protocol), es un protocolo de seguridad con funciones de criptografía para el tráfico de datos. SDP se implementa en el establecimiento de SIP y garantiza la seguridad al transporte SIP.
En la solución de seguridad SDES las claves están establecidas en el mensaje SIP. Se establece una sesión SIP y el protocolo SRTP comparte las claves encriptadas. Un usuario envía la clave encriptada en el mensaje SIP para asegurar los datos. El otro usuario también envía la clave en el mensaje. Asegurando ambos extremos.

4.3.5.5 Solución Mikey-Ibake

Es una solución de seguridad propuesta por el 3GPP. La implementación de seguridad se basa en claves e identidad encriptadas. El mecanismo se basa en un intercambio de claves de 3 vías para todo el proceso de autenticación.

4.3.5.6 DTLS- SRTP

Este protocolo configura los parámetros y algoritmos para implementar el protocolo SRTP. Este protocolo provee seguridad punto a punto. Provee una comunicación segura entre UE que se desconocen con el uso de un certificado. Esto incluye un certificado en el mensaje SIP para evitar el ataque hombre en el medio (man in the middle).

En una red IMS existe como se vio una solución robusta para la seguridad de autenticación y acceso. Hay 5 requerimientos que debemos tener en cuenta para asegurar una red IMS:

- Asegurar el link entre UE y P-CSCF (quien posee las funciones de control)
- Autenticación mutua (en ambos extremos)
- Asegurar la seguridad del HSS
- Asegurar el P-CSCF con la red visitada
- Asegurar el S-CSCF

4.4 Múltiples Servicios y Flexibilidad para adoptar nuevos modelos de negocios

Definición de Multiplicidad de servicios: Significa que puedo tener diferentes servidores de aplicación, propios o de terceros, con varios servicios que quiero brindar en mi red, a saber: llamada en espera, conferencias, video bajo demanda, video llamadas, push to talk, etc.

Definición de Flexibilidad para adoptar nuevos modelos de negocios: Significa que con el agregado de servidores de aplicaciones puedo rápidamente desarrollar un modelo de negocios, con gran parte de los problemas resueltos de antemano.

4.4.1 Ecosistema

A continuación mostramos un breve cuadro, mostrando un Ecosistema, donde aparecen los tipos de operadores, las aplicaciones y las tecnologías involucradas. Donde IMS dejaría de ser una simple tecnología y ser un Ecosistema que involucra a todos los componentes del cuadro de abajo.

Operadores	Aplicaciones	Tecnologías
	Empresas: voz, Internet, email, mensajería, presencia, FFA, CRM Entretenimiento: voz, música, deportes y TV Consumidores: voz, juegos, mensajería, presencia	
	Infraestructura empresaria: seguridad de HW, gestión del middleware	

	Infraestructura hogareña: servicios de medios	
Fijo Móvil ISP Cable Integrado Etc.	Accesos, dispositivos y terminales Sistemas operativos: Android, IOS, RIM, Symbian, Windows, etc. Dispositivos: teléfonos inteligentes, PDA's, PC's HiFi, TV, etc. Puntos de Acceso: set-top-box, WiFi, adaptadores de medios.	IMS SIP IP UMA Etc.
	Infraestructura de Red Accesos celulares: GSM, CDMA, iDEN, WCDMA, LTE, etc. Accesos inalámbricos: Bluetooth, 802.11,16,21, malla, etc. Accesos fijos: DSL, cable, FO. Servicios: OSS, Gestión de red, etc.	

4.4.2 Drivers del Mercado Masivo

El mercado masivo puede impulsar este cambio basado en la necesidad de una mejora de la cobertura Indoor, permitir tener menores precios y simplicidad en precios fijos. Ofreciendo para clientes sofisticados, servicios y terminales innovadores. Dando servicios autoinstalables, plug and play y de uso intuitivo. Con una gran flexibilidad, fácil uso, servicio de roaming con un número, una casilla de mensajes y un dispositivo.

4.4.3 Drivers del Mercado Corporativo

El mercado corporativo en cambio puede impulsar también basado en mejora de la cobertura Indoor, con menores precios de roaming, simplicidad tanto en comunicaciones internas y externas y con acceso a los distintos servicios de empleados sobre un solo terminal.

4.4.4 Drivers de los Operadores

El mercado de los operadores en cambio se puede dividir en tres: operadores fijos, móviles e integradores. Para los primeros las claves del cambio se basan en la oferta de servicios de valor agregado, el aumento del ARPU y la retención de clientes, pudiendo ofrecer una ventaja de combos a través de acuerdos con operadores móviles.

Por otro lado para los operadores móviles, los más importante es el aumento del market share, la diferenciación de servicios, la retención de clientes, el aumento del

ARPU, una mejora de la calidad y movilidad y por último el aumento del tráfico de banda ancha móvil.
Para los integradores lo puntos más relevantes que impulsarán el cambio son: la retención de clientes, el aumento del ARPU por nuevos servicios y combos, la mejora de calidad y movilidad, la baja del OPEX y la ventaja sobre las inversiones en redes celulares

4.4.5 Inhibidores en los diferentes Segmentos de Mercado

En los diferentes segmentos de mercado vemos que se presentan ciertos inhibidores, contrario al punto anterior.
En el sector de la industria, vemos que la disponibilidad limitada de terminales atractivos, junto con que el negocio fijo y móvil está separado para la mayoría de los operadores, y que los operadores móviles deben estar convencidos de la conveniencia de este modelo de negocios. Por último la necesidad de integración de back office por los operadores.
En el sector de las empresas, dentro de estos inhibidores podemos mencionar, la complejidad en la solución a la vista de los departamentos de IT/telecomunicaciones y de los empleados, la incertidumbre de seguridad en la solución, la limitación en la elección de terminales y que no hay una baja de costo como en la solución IP.
En el sector de los consumidores, la dependencia a un único operador, la ausencia de percepción de valor del servicio, la pérdida de terminales atractivos comparados con los el servicio móvil exclusivo, la complejidad de ofertas y la complejidad de implementación técnica que complica el soporte a cliente, son los inhibidores más significativos.

4.5 Solución al problema planteado en la Hipótesis 2

Respecto de las tecnologías existentes, esta arquitectura permite soportar e inter-operar con las redes existentes, sin ningún tipo de problemas.
Poder inter-operar con los actuales operadores incumbentes, que no cuenten con redes sobre IP, IMS resulta ser fundamental.

4.5.1 Interoperabilidad con redes existentes

Definición de interoperabilidad con otras redes: Significa que puedo establecer comunicaciones con operadores de otras redes, teniendo perfectamente definido el billing y la conexión en sí misma. Por eso es tan importante el concepto de red local y red visitada en IMS.

Del análisis realizado sobre los casos planteados anteriormente sobre el Proyecto "Servicio de Video Conferencias de Audio, Video, Web; junto con el Modelo de VoLTE. Se puede ver que cuando se trata de un operador de la talla de Telefónica, que tiene presencia en varios países, la arquitectura IMS es realmente un facilitador y sobre la misma arquitectura se van haciendo nuevos requerimientos de servicios, como es el servicio de Video Conferencias, en base a lo que cada región vaya demandando. Quedando luego todo disponible para poder ofrecer el mismo servicio en una ubicación diferente. Pudiendo amortizar una operación en forma regional, y no en un único país. Además por la región que nos ocupa que en términos regulatorios no está avanzando en los diferentes lugares de la misma forma. Entonces, ya tener listo un servicio, por demanda de una región, hace que cuando ese mismo servicio pueda ser desplegado en otro lugar el tiempo de mercado (time to market), sea realmente mínimo.

Por otro lado y no es una ventaja menor, cuando se requiere integrar cualquier equipo a la red IMS, y el operador debe salir a comprarlo, el esquema donde debe conectarse el equipo es muy fácil de visualizar en esta arquitectura. Los requerimientos son los mismos en cuanto a la integración del equipo en la red. Ya sea se necesite conectar teléfonos IP o el complejo sistema de Video Conferencia, como los parámetros de la arquitectura están perfectamente definidos, lo único que cambia en cada requerimiento es el conector o equipamiento y sus funcionalidades. O el servicio y lo que se pretende del mismo.

Siguiendo con esta misma idea, pero si ahora nos ponemos en el lugar de una pequeña cooperativa del interior de nuestro país, la posición, o el análisis es un poco diferente, ya que no tienen la posibilidad de estar en varias regiones y poder absorber costos entre varios países. Por ende tal vez habría que hacer un análisis puntual de su red, que equipamiento se podrá reutilizar, y como se podrá ir integrando capas de la nueva arquitectura. Al principio ofrecer menor cantidad se servicios e ir creciendo paulatinamente en términos de lo que mande cada mercado regional. Tampoco en este tipo de pequeños operadores se realizan compras tan

masivas que demanden mucha tarea a los ingenieros que deban preparar las especificaciones de los equipos o elementos de red que se requieran.

4.5.2 ¿Interoperabilidad o Dependencia del Vendor?

Si bien hemos visto hasta acá, que la arquitectura IMS inter-opera perfectamente con redes existentes, es agnóstica del acceso y demás. Aquí trataremos de analizar de qué forma no quedar esclavo del Vendor elegido a la hora de adoptar una solución IMS. O peor aún, no poder llevar a buen puerto la implementación de esta arquitectura.

Para ello se formuló un breve cuestionario que cada ingeniero a la hora de realizar un análisis, le pueda facilitar o servir de guía frente a que Vendor elegir.

Por eso ya habiendo analizado la arquitectura, en términos de estándar, la variedad de vendors que hoy brindan productos para las redes IMS es bastante amplia. Dado que hoy en día todos los fabricantes ofrecen la posibilidad de hacer pruebas y consultas, lo que debe estar muy acotado es el tiempo, por ende con este pequeño decálogo de preguntas se pretende hacer una pequeña depuración de los players que están hoy en el mercado y básicamente ahorra tiempo de laboratorio y eficiencia en las pruebas y cronogramas de implementación comercial.

Comencemos:

P1: ¿Qué protocolos y estándares de la industria soporta la solución ofrecida?

Primero que nada, cuidado con el término "LITE", que hemos mencionado, pero desde el punto de vista de la especificación. Dado que en general esto desde el punto de vista del fabricante se traduce en una solución inmadura.

Usualmente los fabricantes usan el término IMS, para referirse a los servicios de una arquitectura definida por GSM/UMTS, lo cual gano rápida aceptación entre diferentes tipos de proveedores de servicios, como ser operadores de cable, ISP y operadores tradicionales de telefonía.

IMS como pudo analizarse en este trabajo es mucho más que la convergencia de servicios en las redes existentes. Significa que la colaboración entre los métodos de acceso y los proveedores de servicios debe ser a un nivel muy estrecho.

Por ende se necesita una solución IMS que funcione en múltiples dominios, por 3 grandes razones:

- Usuarios experimentados: los usuarios irán de un dominio a otro en su vida real. Se debe poder brindar un servicio de máxima calidad en donde se encuentre, en un mismo dispositivo o diferentes.
- Velocidad en las ganancias: cuando los servicios puedan disponibilizarse a través de los diferentes métodos de acceso, se tendrá una rápida aceptación.
- Preparado para el futuro: se necesita tener cierta flexibilidad en el equipamiento que me permita direccionar y desarrollar nuevos modelos de negocios para 2 o 3 años vista.

El equipamiento no debería tener inconvenientes en trabajar todos los dominios de servicios. Con interfaces abiertas que soporten un amplio rango de clientes y aplicaciones, aumentando la oportunidad de diferenciación frente a la competencia.

Por eso es muy importante saber con exactitud que estándares de la industria soporta el equipamiento. Pero más importante aún es si estos estándares son soportados en forma simultánea y dinámica en el mismo Core de red. Por ejemplo: IMS o 3GPP, 3GPP2 (MMD o dominio multimedia), TISPAN, ITU-T FG NGN, ATIS NGN-FG, IETF, Packet Cable 2.0.
También es importante conocer si el fabricante está asociado a algún foro, participando en el desarrollo de determinado estándar.

P2: ¿La solución de IMS adhiere a la arquitectura IMS de CSFC, HSS y servidores de aplicación?

No es recomendable aceptar soluciones, que estén diseñadas en una sola caja. O que un solo appliance resuelva toda mi arquitectura.
El diseño modular de la arquitectura IMS ha sido considerado cuidadosamente en el estándar con funciones muy específicas a cada componente. La separación por lo menos de los módulos CSCF, HSS y Servidores de Aplicación, permite un rápido crecimiento en la red, como así también le aporta gran flexibilidad.

Además debemos considerar que todo en una misma caja, que traerá problemas a la hora de crecer en la cantidad de servidores de aplicación. Para uno o dos servicios no habrá problema, pero esa no es la idea de esta arquitectura.

Analicemos un caso en particular, el módulo HSS, debería estar accesible por todos los controladores de políticas, de sesión y servidores de aplicación. Por ende los datos de los usuarios deben estar disponibles para todas las aplicaciones (o múltiples instancias de una misma aplicación) en tiempo real. Los usuarios deberán conectarse con un único login, con autenticación centralizada y único lugar donde se realice la facturación de sus consumos en base a los servicios que requiera. Para esto un servicio de aprovisionamiento de la información de los suscriptores, a través de un servicio integrado de creación de entornos de usuarios. Esto puede ser tan sencillo como agregar capacidad a un servicio existente, es decir agregando otro procesador blade en el rack respectivo.

Para el HSS sólo verá las aplicaciones que se corresponden con el estándar de ISC (IMS Service Control).
Otra cuestión a considerar es si el proveedor del equipamiento posee interfaces propietarios o fuera del estándar. Asegurarse si la relación que uno necesita es de uno a muchos entre los elementos que si utilizan el estándar abierto.

P3: ¿Cómo funciona la integración de los sistemas?

Si nos están ofreciendo que requiere de una integración mínima, dado que el equipamiento cumple con el estándar. Tampoco es un argumento muy válido, de acuerdo con la arquitectura IMS.

Siempre hay algún tipo de integración que realizar. Se debe estar capacitado para poder combinar el equipamiento que sea necesario de diferentes marcas, para poder crear la mejor solución, y que dicha solución pueda evolucionar en el tiempo en base a las necesidades y capacidades requeridas. Un desarrollo que sea multivendor requiere soporte de una amplia base de protocolos. En general desde el punto de vista del vendor, es deseable tener siempre la última versión del protocolo disponible corriendo en sus productos. Y eso no es bueno desde el punto de vista de la interoperabilidad, desarrollo, testeo y certificación de componentes de los diferentes vendors que se tienen que integrar en la solución. En un escenario

así, lo deseable es tener las herramientas y recursos para ejecutar pruebas en escala real.

P4: ¿Qué experiencia tiene en SIP?

Es crucial poder determinar el grado de experiencia que pueda tener el vendor elegido en este protocolo, y no basta con que haya participado en algún comité del IETF. Una red IMS depende de la eficiencia e interoperabilidad de sus mensajes SIP.
Es importante conocer en detalle los desarrollos SIP, la experiencia en integración y compararla con la siguiente lista:

- Interconectar redes de voz: por medio de trunks SIPs. Esta es una buena forma de medir la experiencia del fabricante en SIP, dado que este tipo de implementación requiere tanto el rigor de alto volumen, delays de la voz, en una red multi carrier, y seguramente también multi vendor.
- Desarrollo de servicios SIP: o qué nuevos servicios multimediales SIP tiene pensado desarrollar.
- Interoperabilidad de dispositivos SIP: en IMS siempre se requiere distribuir nuevos servicios a través de nuevos tipos de accesos. Por eso es importante conocer con que endpoints SIP está familiarizado.

P5: ¿Qué tan bien escala la solución?

Una arquitectura como IMS, soportará muchos cambios, desde su inicio hasta su operación a pleno. Deberá expandirse tanto en tamaño, como alcance geográfico.

Además deberá ir incorporando nuevas tecnologías y oportunidades de negocios que aún no se encuentran disponibles. Por eso es tan importante la escalabilidad de la red. Podríamos decir que la escalabilidad de una red, es la habilidad de la red de soportar este crecimiento mencionado, sin comprometer la performance de la red.

Podemos resumir algunos conceptos a tener en cuenta, para el análisis de la escalabilidad de una red. A saber:

- Escalabilidad del servicio: Agregando nuevos usuarios a los servicios, o cambiando el conjunto de servicios, no debería impactar la performance de los servicios existentes.

- Costo de escalabilidad: Debería haber una relación aceptable entre el costo total de la red y el tamaño de la red. No se querrá una red que cueste lo mismo cuando sirve a 100 abonados que cuando sirve a 100000. Aun cuando la red ofrezca costos competitivos en su límite superior, se deberá considerar los costos durante las fases iniciales.
- Escalabilidad Geográfica: El crecimiento de una red en cuanto a cobertura geográfica se refiere, incluirá varios factores. Tales como, eficiencia en los costos y performance cuando se extienden los servicios a áreas de la red con diferentes densidades de población, o la limitante que la distancia impondrá en la distribución del servicio a todas las áreas geográficas.
- Escalabilidad de la tecnología: Cuando hoy se planea este tipo de redes, se deberá considerar como las nuevas tecnologías serán introducidas en la red. Aun cuando estas nuevas tecnologías ofrezcan grandes ventajas, nuevos servicios, mayor movilidad, capacidad de expansión o mejora de costos. No se querrá que esa migración cause un mayor impacto a los servicios actuales, junto con la performance de la red. Una solución bien diseñada incorporará nuevas tecnologías con un impacto muy pequeño o despreciable en los servicios actuales.

P6: ¿Cómo la solución soporta o realiza la tarifación?

Una de las mayores ventajas de los servicios con esta convergencia que está sucediendo, es que la arquitectura debe ser capaz de testear un potencial nuevo servicio, al mismo tiempo suscribir nuevos usuarios, y retener a los antiguos. Una estrategia en IMS debe incluir un plan sólido de soporte a la base de usuarios, la base de utilización, y tarifación bajo demanda. La flexibilidad de tarifación es necesaria para poder soportar toda la variedad de servicios definidos.

Como proveedor de servicios, se ha invertido seguramente bastante en los sistemas de tarifación, y en otras áreas como OSS (operaciones y soporte del sistema).
Para tomar ventaja de la implementación IMS, tanto el OSS como el IMS requerirán cambios en el sistema de tarifación y procesos. Hoy el modelo tiende a un sistema de tarifación basado en transacciones en el uso de aplicaciones y subscripción de perfiles. Y se complica aún más cuando se piensa en una tarifación basada en contextos y tarifación diferenciada de acuerdo a la QoS. Además considerar que en muchos casos el servicio de IMS lo podrá brindar una tercera parte. En este caso se

necesitará una integración de los procesos del OSS para poder habilitar los servicios del tercero que brinda IMS.

P7: ¿Cuan confiable es su solución de red?

Las redes de tipo "carrier class", son muy confiables. No tienen sorpresas y proveen una muy sólida performance. Si alguna parte de los componentes de esta red tiene los famosos cinco nueves de disponibilidad, eso no significa necesariamente que el sistema completo tendrá ese nivel de confiabilidad. Cuando ese componente de la red forma parte de un todo que es la red del operador debe comportarse para ser administrado, mantenido y conformar las expectativas de los requerimientos del entorno.

La realidad es que la única forma de medir la confiabilidad de una red es por su performance a lo largo del tiempo. Esto no es una situación que ayude a tomar una decisión acerca de la arquitectura IMS.
Como un sustituto de estos datos, las redes pueden ser evaluadas por su confiabilidad entendiendo como se comportan en los siguientes atributos:

- Mantenimiento en servicio.
- Supervivencia de la red
- Tolerancia a fallos
- Rápido recupero de desastres

Una excelencia en estos atributos está muy relacionado con, como el producto ha sido desarrollado y validado, y también tiene que ver con la tecnología utilizada.

Significa que se puede ver la confiabilidad, sabiendo que la solución refleja una experiencia sólida en los procesos.
Por ende hay que preguntar bien al proveedor del equipamiento los procesos que utiliza para el testeo, integración de la red y de sistemas a gran escala. El rigor de estos procesos nos dirá suficiente para ver cómo es la performance en tiempo real.

P8) ¿Qué Aplicaciones están disponibles con la plataforma?

La gran promesa de IMS, trata sobre la personalización de servicios, movilidad y seguridad. Se deberá trabajar con el vendor de la arquitectura para que nos

transfiera la experiencia en el desarrollo de servicios, y que pueda disponibilizar los servicios que se hayan identificado como para la estrategia de la empresa.

Seguramente para una estrategia de largo plazo necesitemos una multiplicidad de servicios, no solo los de nuestro vendor. Por ende deberíamos poder conectar en nuestra red servidores de aplicación rápidamente, manteniendo la red de Core establecida.

Esto es muy importante ya que no vamos a querer que las alternativas de largo plazo estén supeditadas a un único vendor. Lo deseable es poder utilizar cualquiera de las miles de aplicaciones que se espera que empiecen a aparecer en el mercado. Es importante conocer que aplicaciones el fabricante ya tiene disponibilizadas con la aplicación. Además de, con qué terminales y clientes es compatible. También deberemos conocer que planes de interoperabilidad tiene con otros fabricantes de servidores de aplicación. ¿Podrá inter-operar con otro servidor de aplicación cualquiera?

P9) ¿Cómo es la Arquitectura de Hardware?

El crecimiento exponencial en las demandas de performance en la red del operador, deben tener una contraparte en cuanto a innovación en la arquitectura de la red.

Este caso de negocios requiere usar componentes que estén disponibles comercialmente y que estén garantizados para poder ser desarrollados en redes de operadores.

En respuesta a este gran desafío para la industria de telecomunicaciones, PCIMG (PCI Industrial Computer Manufacturers Group) estableció un estándar abierto de especificaciones que definen una arquitectura modular para equipamiento de telecomunicaciones. El resultado fue el estándar ATCA (Advanced Telecommunications Computing Architecture), lanzado en el 2005. Los equipos construidos de acuerdo al estándar ATCA podrán trabajar en el Core de una red cableada, o wireless o de un cable operador.

Este estándar permitirá que surja un gran ecosistema de proveedores que podrán disponibilizar componentes para la arquitectura de las redes.

Los proveedores de servicios se beneficiarán con un mejor "time to market", bajo costo del equipamiento y pasos acelerados de innovación para introducir nuevos servicios y características.

Por ende es primordial si nuestro fabricante elegido nos dará estos beneficios de ser o no ATCA. Tener cuidado con algunas soluciones de primera generación de ATCA, que tuvieron problemas. Y sobre todo preguntar en cuanto a la evolución hacia una segunda generación de ATCA, lo siguiente:

- Además del hardware, el middleware es abierto y carrier class?
- Compartirán sus planes de mejoras con la industria, para mantener un ambiente multi plataforma.
- Como la configuración minimiza los errores en el mantenimiento tanto de unidades activas cómo no?
- Si un elemento falla, el técnico tiene un tiempo razonable para realizar la reparación.
- La plataforma soporta un upgrade de software sin interrupción del servicio?.
- Esta optimizada la performance pensando en el estándar ATCA?
- Como la solución realiza el almacenamiento de la configuración?
- Son redundantes las interfaces IP de la red?
- Está disponible esta segunda generación ATCA?

P10) ¿Con que otros fabricantes inter-opera la solución de IMS?

Una de las grandes promesas de la tecnología IMS es la posibilidad de proveer una gran experiencia de los usuarios, gracias a una red completamente convergente que integra múltiples dispositivos de acceso, dominios de red, ya sea cableada, wireless o de un cable-operador.

La otra gran promesa es que será posible elegir de un gran ecosistema de aplicaciones de muchos fabricantes y posibilitar una compleja interacción entre esas aplicaciones.

Para conseguir esto, se necesita combinar equipamiento de diferentes fabricantes. Dado que no se puede saber de antemano de quien surgirá la mejor de las soluciones.

Esto significa que el vendor de IMS, no solo debe inter-operar con el equipo que uno desee usar hoy, sino tener el compromiso de que tendrá lo necesario para inter-operar en el futuro.
La única forma de asegurar la interoperabilidad de los componentes IMS es testearlos en nuestro laboratorio, o ver alguna prueba certificada en alguna red abierta.

Igualmente debemos evaluar al fabricante en lo siguiente:

- ¿Cómo integrará los componentes periféricos de IMS?, como ser servidores de aplicación de terceros.
- ¿Qué experiencia real tiene en construir e integrar redes multi plataforma?
- ¿Qué políticas, presencia, firewall y servidores de aplicaciones ha testeado?
- ¿Posee experiencia en integración aplicaciones sobre redes cableadas, inalámbricas o de un cable-operador?
- ¿Tiene una lista de interoperabilidad certificada con otros vendors del mercado?
- ¿Tiene una comunidad de desarrolladores de aplicaciones?

Con esta serie de preguntas podemos hacer un perfil del vendor bastante profundo y analizar si está a la altura de nuestras necesidades.

4.6 Nuevas tecnologías sustitutas y los 5 atributos de IMS como lo resuelven las nuevas tecnologías

A Continuación proponemos un tablero para analizar los atributos tecnológicos que posee IMS (que se han desarrollado con profundidad en párrafos anteriores) y comparar el grado de presencia de los mismos en otros posibles sustitutos del IMS (RCS y WebRTC).

		Alternativas tecnológicas			
		IMS	RCS	Web RTC	Otras?
Atributos	Independencia de acceso	SI			
	Seguridad	SI			
	Multiplicidad de servicios	SI			
	Flexibilidad para adoptar nuevos modelos de negocios	SI			
	Interoperabilidad con otras redes	SI			

4.6.1 RCS (Rich Communications Services)

4.6.1.1 ¿Qué es RCS?

Es una plataforma que permite establecer comunicaciones más allá de la voz y SMS. Provee al usuario servicios de mensajería instantánea o chats, ya sea uno a uno o a grupos, también provee video en vivo y compartir archivos en cualquier red.

RCS marca una transición de la capacidad de las redes con tecnologías orientadas a circuitos, tanto de voz y mensajes a un mundo todo IP.

Hasta acá podemos decir las mismas capacidades que IMS.

¿Cuáles con algunas ventajas de RCS?:

- Está disponible para todos los usuarios sin necesidad de bajar una aplicación o loquearse a un servicio web.
- Inter-opera con todo tipo de redes.
- Ofrece al usuario soluciones competitivas con aplicaciones alternativas.
- Asegura a los operadores retener a los usuarios más relevantes.
- Entrega de mensajes de sólo lo que el usuario está buscando.
- Provee al usuario un servicio seguro.
- Construido sobre las únicas premisas de un operador: ubicuidad, inter-operabilidad global, servicios seguros, gerenciamiento de la privacidad y seguridad. Confiabilidad como operador de servicios.
- Ofrece la oportunidad de expandir los productos de Core y servicios.
- Es un camino para desarrollar propuestas más adecuadas y a la medida del cliente.

- Es una manera de obtener un retorno de la inversión en IMS desde el principio, permitiendo a los operadores ofrecer nuevos tipos de tráfico mediante la creación de aplicaciones y servicios B2B.
- Permite al operador desarrollar rápidamente RCS como un set de servicios stand alone a través de soluciones hosteadas. El operador se beneficia con un costo de sólo pagar mientras se va creciendo. Sin la necesidad de comprar e instalar equipamiento IMS.

A continuación plantearemos algunos interrogantes sobre esta plataforma de servicios:

P1) La interoperabilidad limita la diferenciación de un operador?.
Todo lo contario, ya lo planteamos para IMS, como una gran ventaja. Con RCS es también una ventaja parcial. Tanto SMS y MMS son buenos ejemplos de servicios exitosos que han prosperado con la inter-operabilidad, junto con la proliferación de servicios de valor agregado. RCS provee las funcionalidades del Core, posibilitando el desarrollo de aplicaciones, basándose en la inter-operabilidad y compatibilidad. La inter-operabilidad asegura que los servicios de Core de RCS funcionaran entre usuarios, sin importar a que operador pertenecen o que teléfono celular utilicen.

P2) Qué infraestructura necesita un operador para desarrollar y para tomar ventaja de RCS?
Los servicios de RCS se basan en IMS. Los operadores pueden implementar sus propias soluciones IMS o pueden acceder a los servicios hosteados para acceder a una implementación parcial de IMS.

P3) Puede un cliente RCS que está en una red fija como un teléfono IP registrado en un IMS, podrá conectarse con un cliente móvil RCS?
Un cliente RCS podrá estar en una red IMS con un teléfono IP y la interconexión será posible si las redes están interconectadas.

P4) Dado que ya existen aplicaciones como WhatsApp, Viber, Line; que están basadas en IP, cuál es el valor agregado de RCS?
El factor diferenciador de RCS es que se integra en forma nativa en los teléfonos móviles. No se necesita intervención del usuario. Además sólo los servicios relevantes son ofrecidos. Simplemente funciona.

Como vimos en este punto, RCS se basa en una arquitectura IMS, por ende, podemos concluir que como tal, no es independiente del acceso, como plataforma en sí misma. Si lo es a través de IMS. Con la seguridad, ocurre lo mismo. No fija pautas de seguridad. Si podemos decir que permite multiplicidad de servicios, pero en si a mi juicio es un servicio más para IMS. Si podemos decir también que es flexible para adoptar nuevos modelos de negocios. Por su rápido despliegue. Si bien lo dicho es que interopera con otras redes, la verdad es que esa interoperabiliadad se basa en una conexión pre-establecida, como se menciona más arriba.

4.6.2 Web RTC

4.6.2.1 ¿Qué es Web RTC?

Es un proyecto abierto, que provee a los navegadores (o browsers) y aplicaciones móviles con comunicaciones en tiempo real, mediante simples APIs.
Los componentes de Web RTC han sido optimizados para este propósito.
Web RTC es una iniciativa de Google, Mozilla y Opera.

Haciendo una breve reseña histórica de Web RTC: Uno de los mayores desafíos para la Web es poder brindar una comunicación de voz y video, es decir comunicaciones en tiempo real: RTC. RTC debería ser tan natural en una aplicación web como entrar texto en un cuadro de dialogo. Sin esto estamos limitando la manera de interactuar de las personas.
Integrar la tecnología RTC con los contenidos existentes de datos y servicios ha sido particularmente difícil en la web.
Gmail video chat se hizo popular en 2008 y en 2011 Google introdujo "hangouts", que usa el servicio de Google Talks. Google adquirió la empresa GIPS, una empresa que desarrollaba muchos componentes de RTC, como codecs y técnicas de cancelación de eco. Google hizo de esto estándares abiertos y los junto con estándares relevantes de IETF y W3C.
Web RTC está implementado en estándares abiertos para comunicaciones en tiempo real y plugins para video.

La necesidad real es que:

- Muchos web services usan RTC, pero necesitan bajas aplicaciones o plugins. Entre ellos podemos mencionar: Skype, Facebook (que usa Skype), Google Hangouts (que usa Google talks).
- Bajar, instalar y actualizar plugins puede ser complejo.
- Plugin puede ser difícil de desarrollar, buscar errores, testear y mantener.
- También es difícil convencer a los usuarios que instalen plugins.

El principio fundamental del proyecto Web RTC es que las APIs deben ser fuentes abiertas, gratis, estandarizadas y embebidas en los navegadores web y a su vez más eficiente que las tecnologías existentes.

4.6.2.2 Componentes de la Web RTC

Web RTC se basa en 3 APIs, a saber:

- MediaStream (o getUserMedia): accede al stream de datos, como por ejemplo de la cámara y micrófono del usuario.

- RTCPeerConnection: llamada de audio o video, con facilidad de encripción y manejo de ancho de banda.

- RTCDataChannel: comunicación peer a peer de datos genéricos.

Muchas veces se menciona que una plataforma soporta Web RTC y generalmente sólo soporta la primera de las 3 APIs.

Web RTC necesita realizar lo siguiente:

- Obtener los streaming de audio, video o datos
- Obtener información de la red, como dirección IP y puertos. Intercambiar estos con otros clientes Web RTC para establecer la conexión.
- Coordinar la señalización de la comunicación para reportar errores, e iniciar o cerrar la sesión.
- Intercambiar información de la media y del cliente, como resolución y codecs.
- Transportar los streaming de audio, video o datos.

Un tema no menor es la señalización, es decir, el control de sesión, información de la red y media.

Web RTC usa RTCPeerConnection para comunicar el streaming de datos entre navegadores o peers. Pero necesita un mecanismo para coordinar la comunicación y enviar mensajes de control, lo que llamamos señalización. Los métodos y protocolos de señalización no están especificados por la Web RTC. La señalización no es parte de la API RTCPeerConnection. Los desarrolladores de aplicaciones Web RTC pueden elegir cualquier protocolo de señalización como SIP o XMPP.

Al igual que para IMS, la señalización en Web RTC se usa para:

- Control de los mensajes de la sesión: inicia o cierra la comunicación y reporte de errores.
- Configuración de la red: en el mundo exterior cual es mi IP y puerto.
- Capacidad del medio: que codecs y resolución se pueden utilizar por mi navegador y por el que se intenta comunicar conmigo.

A continuación una figura que muestra el protocolo de Java para establecimiento de la sesión: JSEP (Java Script Session Establishment Protocol)

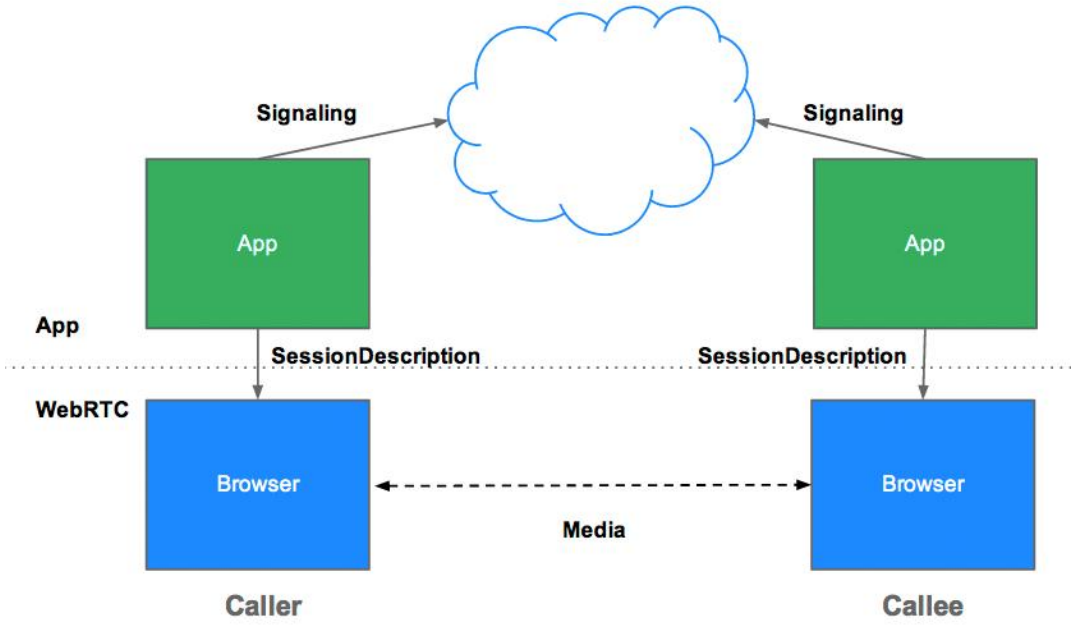

Figura 40: Arquitectura JSEP

El intercambio de información del proceso de señalización debe ser exitoso antes de que empiece el streaming peer a peer.

RTCPeerConnection, es el componente de Web RTC que establece una comunicación eficiente del streaming de datos entre los peers. A continuación una figura que muestra la arquitectura Web RTC, mostrando el rol de la API RTCPeerConnection.

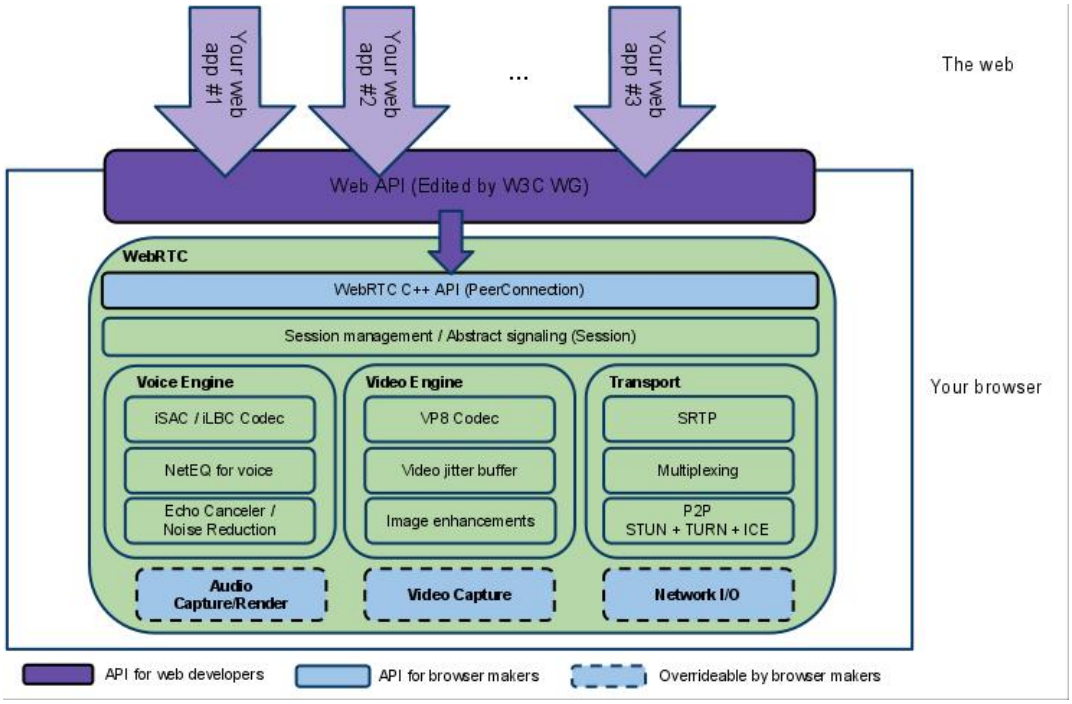

Figura 41: Arquitectura Web RTC

Topología de la red soportada por Web RTC. Web RTC está actualmente implementado para soportar comunicaciones uno a uno. Pero puede ser usado en escenarios más complejos con múltiples peers. Vía una unidad de control de multipunto (MCU). Que es un servidor que puede manejar un gran número de participantes y realiza un streaming selectivo y lo puede mezclar. Además de grabar audio y video. A continuación una figura con dicho escenario:

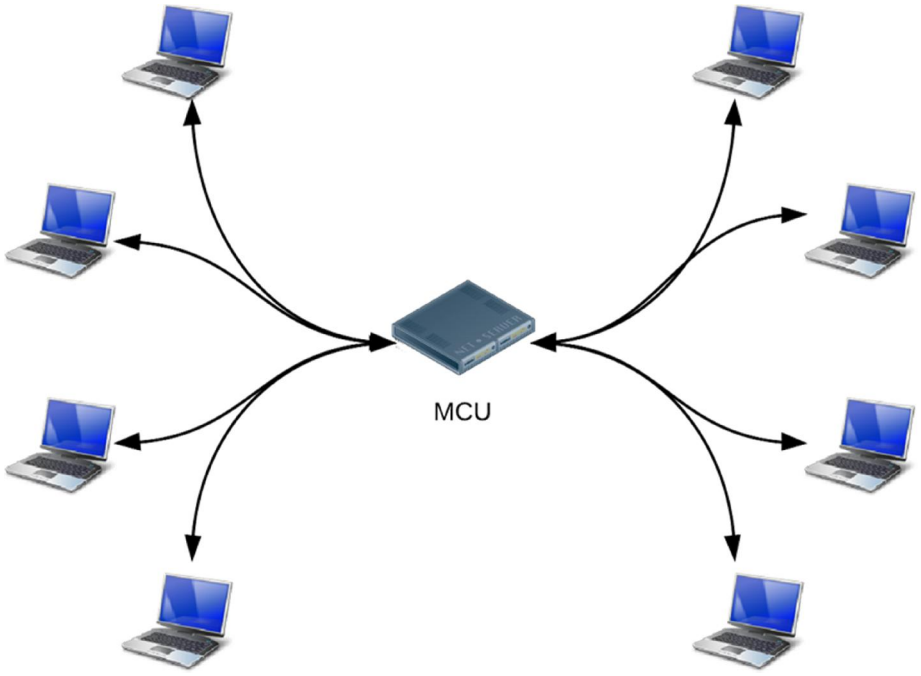

Figura 42: Topología de una unidad de control multipunto

Muchas de las aplicaciones WebRTC solamente pueden establecer una comunicación entre navegadores. Pero cabe mencionar que existen servidores que permiten interactuar con teléfonos de la PSTN o sistemas VoIP.

RTCDataChannel: esta es la última API, que permite intercambiar peer a peer cualquier tráfico en forma arbitraria. Con baja latencia y alta velocidad.

Hay muchos casos de uso de esta API:

- Juegos en red
- Aplicaciones de escritorio remoto
- Chats en tiempo real
- Transferencia de archivos
- Redes descentralizadas

Esta API posee ciertas funcionalidades:

- Aprovechamiento de la sesión establecida
- Múltiples canales simultáneos, con priorización de tráfico

- Utiliza protocolos de seguridad como DTLS
- Se puede utilizar con o sin sesión de audio o video

4.6.2.3 Seguridad en Web RTC

Existen varias formas en que una aplicación en tiempo real puede comprometer la seguridad, a saber:

- Los datos o la media sin encriptar pueden ser interceptados en la ruta entre los navegadores o entre navegador y servidor.
- Una aplicación puede grabar y distribuir un video o audio, sin que el usuario lo sepa.
- Un malaware o virus pueden ser instalados con plugins o aplicaciones.

Web RTC posee algunas funciones para evitar estos problemas:

- Las implementaciones web RTC usan protocolos de seguridad, tales como DTLS y SRTP. Los mismos que IMS.
- La encripción es mandatoria para todos los componentes de Web RTC, incluidos los mecanismos de señalización.
- Web RTC no es un plugin, sus componentes están embebidos en un navegador, y no en procesos separados. No se requiere una instalación aparte y se debe actualizar cada vez que se actualiza el navegador.
- El acceso de la aplicación a la cámara y micrófono debe ser explícitamente permitido. Cuando la cámara o el micrófono están en uso, esto debe ser claramente mostrado al usuario.

Claramente Web RTC, es el desafío más difícil que plantea el cambio de paradigma. Dado que es una OTT. Pero convengamos que no es independiente del acceso, para que funcione necesito tener determinado navegador en determinada plataforma. Si bien habla de seguridad y encripción. Todo está basado en un navegador web, que de por sí, no son seguros. Solo en principio puedo brindar comunicaciones uno a uno, si con Web RTC, quisiera brindar el los servicios del caso 1 planteado. Creo sería un problema, o tendría que desarrollar unas cuantas hojas de código. Si considero que es flexible a nuevos modelos de negocios. Y por último no creo que inter opere bien con otro tipo de redes, sin poner infinidad de gateways en el medio y hojas de código.

4.6.3 Otras

Durante la investigación del presente trabajo, no he podido encontrar otras arquitecturas, tecnologías o plataformas que se puedan comparar con IMS.

A continuación volcamos el cuadro comparativo con las respuestas sobre IMS, RCS, Web RTC y otras arquitecturas

		Alternativas tecnológicas			
		IMS	RCS	Web RTC	Otras?
Atributos	Independencia de acceso	SI	NO	NO	NO
	Seguridad	SI	NO	NO	NO
	Multiplicidad de servicios	SI	SI	NO	NO
	Flexibilidad para adoptar nuevos modelos de negocios	SI	SI	SI	NO
	Interoperabilidad con otras redes	SI	NO	NO	NO

Abajo sigue un dibujo del modelo OSI, comparando las 3 tecnologías:

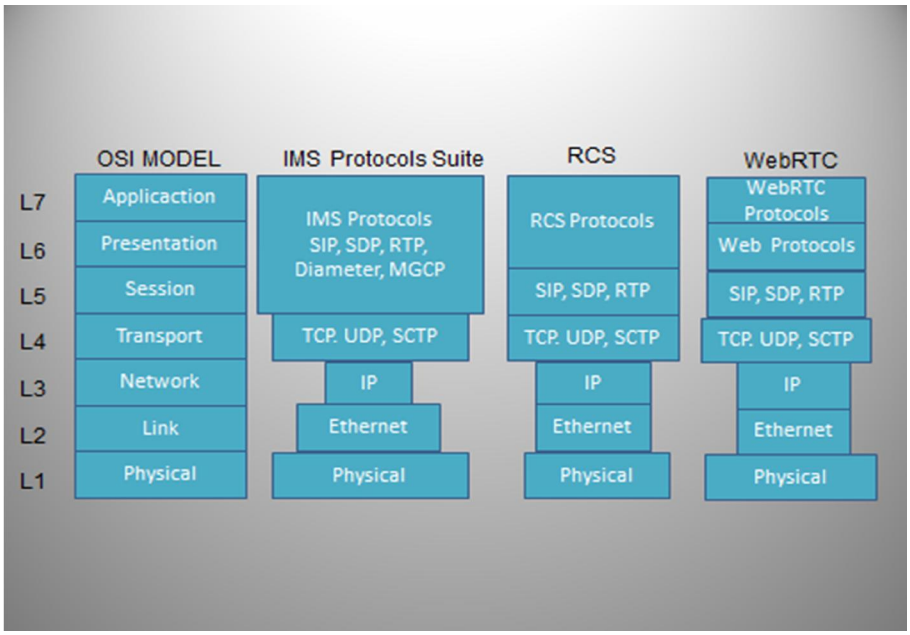

Figura 43 Modelo OSI vs Tecnologías

Veamos los resultados planteados en el cuadro de arriba.

Primero la columna acerca de RCS. Como RCS se basa en IMS, como infraestructura para poder desarrollar sus servicios. Por eso en sí mismo RCS no tiene una independencia del acceso, ni seguridad. Si resulta ser seguro, a través de la seguridad que le ofrece IMS. En cambio sí podemos decir que ofrece multiplicidad de servicios y se puede adaptar a varios modelos de negocios. Por ultimo no podemos decir que interopera con otras redes, solamente a través de IMS.

Segundo, en cuanto a WebRTC, tampoco podemos decir que es independiente del acceso, dado que para poder utilizar este servicio, necesito una conexión Web y un navegador de determinado tipo. La seguridad, tampoco me la brinda WebRTC en sí, sino la red y el dispositivo a través del cual me estoy conectando a la aplicación. Tampoco podemos brindar una multiplicidad de servicios, la solución WebRTC ofrece solamente comunicaciones en tiempo real de voz y video. En cambio sí podemos decir que soporta nuevos modelos de negocios. Tampoco podemos decir que interopera con otras redes. Hoy por ejemplo desde WhatsApp no puedo recibir llamadas de Skype. Y tampoco hacer roaming entre aplicaciones diferentes.

4.7 Solución al problema planteado en la Hipótesis 3

4.7.1 **Hipótesis 3:** *La arquitectura IMS se puede implementar por etapas, lo que permite una introducción progresiva de servicios, lo que facilita la justificación del plan de negocios.*

Es factible una implementación progresiva, con incorporación progresiva de prestaciones y servicios, lo que facilita la justificación económica del plan de negocios.

Muchos operadores con un Core IMS pequeño, manteniendo su red híbrida en un principio, por un tema de costos. Esto ya les permite tener la red separa en planos de control y servicios. Luego ir migrando toda su red de transporte a todo-IP. Al ya tener el Core IMS, no pierdo control, ni visibilidad de la red. Para luego ir adoptando los servicios que mejor se adapten a mis necesidades como operador, VoLTE, RCS, IPTV, etc.

4.7.2 Estudio de un caso: Ericsson con Telefónica de Alemania en 2014 para ofrecer un servicio de VoLTE.

Telefónica de Alemania es uno de los primeros operadores europeos que está preparado en un 100% para lanzar comercialmente VoLTE.
Los usuarios disfrutarán la voz en HD y un establecimiento de llamada instantáneo, mientras que utilizan servicios súper rápidos en un SmartPhone LTE.
Telefónica de Alemania puede ofrecer servicios sobre su red inalámbrica o cableada en forma indistinta en un Core IMS.
Telefónica de Alemania es el operador móvil más grande de Alemania, en términos de usuarios. Con esta contratación completó la actualización de su red para lanzar VoLTE comercialmente.
VoLTE fue desplegado en todas las áreas que Telefónica tiene cobertura LTE.
Ericsson le proveyó del siguiente equipamiento: SRVCC (Single Radio Voice Call Continuity), esta funcionalidad permite handover de una llamada de LTE a redes 3G y 2G.
La solución elegida de VoLTE está basada en el portfolio de productos de Ericsson, que le permitirá a Telefónica en un fututo proveer servicios multimedia de alta velocidad como video llamadas, video conferencia y servicios de colaboración. Independientemente si están en la red móvil o fija del operador.
El contrato provee el siguiente equipamiento: CSCF (Call Sesion Control Function), MTAS (Multimedia Telephony Application Server), MRS (Media Resource System) y servicios de integración para la red de Telefónica.
Nada mejor que citar a uno de los expertos de Telefónica de Alemania: Karsten Schroder: "Cuando se comenzó hace seis años con la inversión en IMS para brindar servicios de voz DSL, vimos la necesidad estratégica de modernización de nuestra arquitectura de Core. Con la llegada de VoLTE, cosechamos los frutos de utilizar el mismo Core IMS para nuestros clientes móviles, siendo el primer operador en demostrar que VoLTE no es sólo un estándar, y puede ser usado en la vida real, con un ambiente multi-vendor. Como resultado la arquitectura convergente, permite desplegar servicios siendo completamente agnósticos al acceso físico por el cual el usuario se conecta a nuestra red."

Con este caso, no sólo vemos que IMS es una arquitectura que me permite ir creciendo en el tiempo, y desarrollando nuevas aplicaciones en la medida que van apareciendo, sino que vemos que con el agregado del servidor de SRVCC, puedo

tener el handover tan temido a la hora de ofrecer VoLTE sobre plataformas anteriores como 3G y 2G.

En este caso, podemos decir que la evolución de IMS en el tiempo fue la siguiente:

Año de Incorporación	Tecnologías adoptadas
2008	Telefónica de Alemania adopta un Core IMS de Ericsson, para ofrecer servicios de voz sobre tecnologías de xDSL.
2014	Telefónica adopta tecnología IMS de Ericsson, para poder brindar VoLTE, reutilizando el mismo Core IMS que ya tenía, ampliando su gama de servicios sobre la misma red.

4.7.3 Estudio de un caso: China Mobile con ZTE.

A continuación describimos en una línea de tiempo, como fue creciendo la red de China Mobile a lo largo del tiempo, e incorporando nuevos y diferentes servicios sobre IMS.

Año de Incorporación	Tecnologías adoptadas
2009	China Mobile adquiere un sistema comercial IMS, para video conferencias en HD. Este sistema fue introducido en las oficias de China Mobile, a los efectos de reducir OpEx y Capex, a través de una red unificada y de simple operación.
2010	China Mobile adquiere un Core IMS, en las principales provincias de China. En 3 meses la red IMS tendrá 1,4 millones de abonados. Esto le permitirá ofrecer varios servicios de convergencia fijo/ móvil, como único número, conferencias, etc.
2011	Aplicaciones IMS para PC. ZTE le provee aplicaciones para IMS. Estas aplicaciones brindarán al usuario servicios de video conferencia, mensajería instantánea y poder utilizar teléfonos IP.
2015	Despliegue de servicios VoLTE. En esta etapa harán un upgrade de la red existente cubriendo 28 provincias. La solución IMS abarca el Core de la red, la plataforma de servicios, sistemas de acceso, terminales, y otros plataformas de soporte.
2016	ZTE se asocia con China Mobile para lanzar un laboratorio de pruebas 5G.

De acuerdo a estos dos casos planteados de dos empresas bien diferentes, Telefónica de Alemania y China Mobile, lo que podemos ver es que lo más difícil de justificar, tal vez haya sido migrar a un Core IMS, ambas por la misma fecha 2008

y 2010; pero una vez en esta senda, los nuevos servicios surgen en forma natural. Permitiendo hacer más sustentable la inversión inicial. Como dice Kan Yulun GM de ZTE: "China Mobile y el resto de los operadores están invirtiendo una increíble suma de dinero en redes IMS, existe un gran desafío para que las aplicaciones prometidas sean un éxito." Hablando del acuerdo de aplicaciones para PC, "Este acuerdo es importante dado que este set de aplicaciones serán la ventana para que usuario vea el revolucionario set de nuevas aplicaciones disponibles".

4.8 Justificación teórica

La justificación del uso de IMS, es básicamente hacer el gerenciamiento de las redes más sencillo. La red IMS es una arquitectura funcional que promete solucionar la creación y desarrollo de servicios multimedia. Así como soportar la interoperabilidad y convergencia de las redes. IMS le permitirá a los operadores jugar un rol central en la distribución de tráfico, en lugar como ya hemos mencionado, de ser tuberías de bits. Por estas razones IMS ha generado grandes esfuerzos de estandarización e investigación.

IMS es una arquitectura punto a punto que soporta diferentes tipos de equipamiento. Además de ser "agnóstico al acceso", lo que significa que la provisión del servicio es independiente de la tecnología de acceso.

Mientras que el ARPU por usuario para varios operadores de red está decreciendo, IMS está visto que es una solución. Le permitirá al operador jugar un rol importante en la provisión de los servicios. Dado que se generarán nuevas perspectivas de negocios para los operadores como para terceras partes. El rápido desarrollo de los servicios IMS, reducirá el "time to market" y estimulará la innovación. La combinación de varios servicios en una única sesión. El "single logon" y una tarifación unificada se supone incrementará el interés del usuario e incrementará las oportunidades de negocios.

IMS está diseñado para ahorrar en la infraestructura de las redes y en su gerenciamiento. Teniendo un sustancial ahorro en los costos. Debería también decrecer la inversión para el desarrollo de nuevos servicios, gracias a la plataforma unificada de servicios.

5 CONCLUSIONES

5.1 Conclusiones sobre la vigencia de IMS y atributos no superados por otras opciones

- Los siguientes proyectos de reconocimiento a nivel internacional:
  - Caso de plataforma Servicio de Conferencias de Audio, Video y Web.
  - Caso de VoLTE.
  - Caso de China Mobile

Dos de los cuales se han analizado con profundidad (caso 1 y caso 2), son realidades comerciales y evidencian que IMS sigue vigente.

- Está vigente IMS, ya que:

  - Re-valoriza la red existente, y evita que se convierta en un comodity, porque como hemos visto, cuando el Operador brinda aplicaciones o servicios de valor agregado, entonces evita ser una tubería de bits.

  - Permite la oferta de servicios que generan un mayor Revenue (Ventas), tal lo muestran los siguientes indicadores asociados a servicios IMS del operador China Mobile (ver referencia 39)

  - Posibilita incrementar el ARPU (ingresos por cliente) porque:

    - ❖ Se crean servicios multimedia, servicios combinados, basados en la ubicación: como ser servicio de localización que se utilizó, para una mejor experiencia de usuario, tal como muestra caso de Ericsson con SoftBank Mobile, (ver referencia 41). Esto se logró con una política basada en la ubicación de los usuarios para mejorar el espectro de frecuencias. Por la alta congestión de redes móviles.
    - ❖ "Time to market" acelerado para desplegar nuevos servicios, tal lo muestra el caso de Telefónica de Alemania (ver referencia 41)
    - ❖ Reduce el efecto Churn y aumentar la fidelización, ya que permite ofrecer servicios de valor agregado, lo que me permite diferenciarme de la competencia. Puede verse el caso de plataforma de servicios de conferencia audio, video y web.

- Posibilita la rápida creación de servicios y despliegue, como lo muestra el caso de Plataforma de Audio, video, Web. (Ver referencia 22).

- Tener un escenario distribuido, con billing por regiones
- La estandarización de parámetros
- La no duplicidad de funciones para los servicios ofrecidos, ej. El usuario ya está autenticado en la plataforma. Solo necesito levantar su perfil para ver qué servicios tiene contratados

- Posibilita las siguientes Interfaces abiertas: para la creación servicios de terceros asociados, como ser convertir cualquier dispositivo WebRTC en un dispositivo de mi red IMS, para poder inter-operar con cualquier otro elemento de la red IMS. (Ver referencia 44).

- Promueve la aparición de ofertas de MVNO, ya que IMS permite a los operadores virtuales, poder inter-operar con operadores reales para contratarles el transporte real de sus redes, y a su vez disponer de una plataforma de billing de sus clientes.

- Son soluciones Multi Vendor, ya que podría comprar a Ericsson, que tienen interoperabilidad basada en estándares. Ver caso de caso de Ericsson con Bouygues Telecom, donde se hizo una integración IMS en una plataforma multi-vendor. (Referencia 43).
- La velocidad de migración a IMS desde su arquitectura legacy tiene el ritmo que decida el operador. Dado que puedo ir agregando nuevos servicios, de acuerdo a las necesidades que demande el mercado.

- El Core de IMS es Agnóstico, ya que permite ser independiente de los servicios y aplicaciones, así como del acceso.
  - Acceso agnóstico (convergencia fijo-móvil)
  - Servicio agnóstico (red multiservicios)
  - Locación agnóstica

Todo esto es deseable ya que permite tengo el control total de mi red, independientemente desde donde se conectan los usuarios y también tengo un control total de las aplicaciones o servicios, aunque sean de un tercero.

- Posibilita la reducción CapEx, porque re-utilizo Core existente ante nuevos servicios y el OpEx porque administro un único Core.
    - Único Core de red, me permite desplegar todos los múltiples servicios que quiera ir incorporando.
    - Re-utilización de equipamiento del Core de red, con el agregado de nuevos servicios, ver caso de Telefónica de Alemania (Referencia 40).

- Permite Servicios diferenciados, dado que tengo disponible una plataforma de servicios, donde puedo ir agregando los servicios que el cliente vaya demandando de acuerdo a la necesidad de cada operador.
    - FMC. La convergencia fijo-móvil, ya es un hecho, y junto con IMS los operadores han podido integrar sus redes, con un sólo Core IMS.

    - QoS end to end. Como se vio en este trabajo podemos garantizar la calidad de servicio extremo a extremo, en este tipo de arquitectura.

    - Seguridad. Como vimos este es un diferencial importante, dado que esta arquitectura permite segurizar el acceso y las redes en sí.

    - Movilidad. Esta arquitectura permite movilidad y handover para todos su UA.

- Los servicios IMS tienen la suficiente flexibilidad como para satisfacer las necesidades crecientes de multimedialidad de los usuarios, que van tener las siguientes características: de voz, datos y llamadas de video. Como es el caso de Canadian Telus, con servicios RCS y VoLTE. (ver referencia 45).

- IMS soporta VoLTE que tiene hasta tres veces más capacidad de voz y de datos de 3G UMTS y hasta seis veces más que 2G GSM, hablando en términos de eficiencia espectral. Como consecuencia, se libera ancho de banda porque los paquetes cabeceras de VoLTE son más pequeños que los de VoIP / LTE sin optimizar. Ver caso Sofbank Mobile con Ericsson, por la mejora en el uso del espectro. (Referencia 42).
- Hoy no existe una solución VoLTE con QoS, que no utilice un Core IMS
- Permite ir adoptando la solución final en etapas
- Garantiza el handover a 2G y 3G
- Provee seguridad extremo a extremo

- La necesidad de una arquitectura IMS para VoLTE, principalmente radica en la continuidad de Servicios de voz entre redes de acceso LTE y 2G/3, que es proporcionada por la tecnología SRVCC (Single Radio Voice Call Continuity) en el núcleo de red (Core EPC y Core 2G/3G). Por medio de un nuevo servidor de aplicación IMS (SCC-AS), esto se traduce en la introducción de nuevas interfaces que vinculan el mundo de CS (circuito) con el de paquetes a nivel de Core. El handover está entre LTE y 2G/3G garantizado. Ver caso Telefónica de Alemania (Referencia 40).

- IMS posibilita la coexistencia de red legacy (circuitos) y nueva red de paquetes, es decir una red híbrida donde haya muchas aplicaciones o servicios dedicados a compatibilizar el funcionamiento de ambas redes.

- Vemos que se abre una posibilidad única, para los operadores móviles virtuales, para grandes empresas de otros segmentos, como retail. Esta figura todavía no está funcionando en nuestro país, pero está próxima a regularse. Es una forma de incrementar la competencia y por ende las opciones de elección para la gente. Este tipo de empresas no podría surgir sino es en una arquitectura como la descripta en este trabajo, dado que el MVNO, necesita inter-operar en un 100% con las redes de operadores reales, a los cuales les contrata el transporte y los vínculos. Por eso debe tener un control de su base de datos de clientes para el billing y a su vez controlar lo que le cobran los operadores reales por el uso de la red.

- Para virtualizar IMS como vimos, se requiere un rediseño de la arquitectura. Los requisitos más importantes son:

  - Escalabilidad elástica
  - Latencia
  - Eficiencia de los recursos
  - Sígueme ("Follow-me")

Estos requisitos a menudo entran en conflicto, se deberán hacer algunas compensaciones cuando se diseñen las nuevas arquitecturas.

De las opciones vistas:

- La primera opción de virtualización (ver figura 27), es compatible con la asignación dinámica de recursos y la protección de desastres (Disaster Recovery). Si bien el algoritmo de la asignación de recursos puede escalar verticalmente, para adaptarse a la carga de trabajo, sin embargo no escala

horizontalmente. Difícil de poner fin a S-CSCF cuando se maneja una llamada en curso. Sigue siendo un problema de diseño debido a la asignación estática de entidades funcionales de IMS.

- La segunda opción, IMS como servicio. En este caso la escalabilidad elástica es limitada, debido a la arquitectura statefull y el nivel de granularidad de IMS.
- La tercera opción, IMS por entidad. Es menos compleja solo propone un HSS virtualizado y un servicio de presencia. Permite una ampliación independiente de los recursos y las capas de gestión.
- De estas opciones podemos concluir que IMS virtualizado, no está del todo maduro. Como vimos tiene algunas limitaciones. A mi criterio el que este decidido a ir por este camino, lo debería encarar como en la tercera opción, es decir, ir virtualizando entidades de IMS.

5.2 Conclusiones respecto a otras tecnologías que aparecieron y se solapan con la promesa IMS y si pueden reemplazar a IMS dejándola obsoleta

- Hace más de 10 años era una promesa de arquitectura potencialmente disruptiva y un catalizador único para los operadores. La promesa de nuevos servicios innovadores y aplicaciones con la calidad y confiabilidad de las redes de los operadores sonaba como algo extremadamente bueno. Todo el mundo del ecosistema de las telecomunicaciones hablaba de cuan bueno sería esta arquitectura.
- Diferentes vendors, como ser Ericsson, Huawei, ZTE, Alcatel, coinciden, gracias a esta arquitectura, en los estándares que proponía la nueva red. Por su robustez técnica y soporte abrumador de todos los involucrados, IMS prometía ser un éxito, que nunca termino de despegar.
- Las cosas no sucedieron de la forma que prometían, parados al día de hoy, ya que los nuevos servicios y aplicaciones no están viniendo de la mano del IMS, sino de los OTTs, que poco entienden de IMS.
- La gente, en especial las nuevas generaciones, no usan la voz, e IMS busca nuevos caminos, que no eran los de 16 años atrás. El ARPU y MOU de la voz están declinando en un mercado maduro. La gente está encontrando otra forma de comunicarse.
- Los servicios y aplicaciones innovadoras, como: agendas con presencia, marcado con un click, compartir en forma instantánea imágenes y video,

video llamadas, contact centers inteligentes, servicios de localización, etc, vemos que están disponibles hoy pero como servicios OTT.

- VoLTE es el primer servicio, en donde IMS se vuelve realmente una necesidad con razones que la justifican y que van asociadas al mejor aprovechamiento de los recursos y espectro.
- OTT hoy no posee los estándares de IMS, y de hecho invocan otras tecnologías que parecen ganarle la carrera a IMS. OTT está replicando muchas aplicaciones y servicios, que cada vez funcionan mejor.
- A OTT no le interesa la ganancia por usuario o la interoperabilidad universal. OTT está haciendo todas las cosas que prometía IMS, pero con "best effort", que siempre fue sinónimo de poca calidad de servicio. Sin embargo a medida de esas aplicaciones se consolidan logran estándares de calidad muy aceptables. Parecen ser gratis, pero se financian con esquemas de negocio innovadores, y no es el usuario final el que paga.
- RCS y WebRTC son los competidores directos de IMS, pero no logran brindar todos los atributos IMS
- WebRTC:
  - Es el intento de los OTT de mejorar la calidad y experiencia de clientes, ya que brinda una nueva posibilidad de comunicarse cada que esté conectado a la web.
- IMS para redes fijas no representó nada nuevo, porque en esa época les redes no estaban maduras para ir a todo-IP.
- IMS para redes Móviles implicó la introducción de nuevas posibilidades asociadas a la convergencia de los servicios fijo-móvil.

Tal como lo resume el cuadro:

		Alternativas tecnológicas			
		IMS	RCS	Web RTC	Otras?
Atributos	Independencia de acceso	SI	NO	NO	NO
	Seguridad	SI	NO	NO	NO
	Multiplicidad de servicios	SI	SI	NO	NO
	Flexibilidad para adoptar nuevos modelos de negocios	SI	SI	SI	NO
	Interoperabilidad con otras redes	SI	NO	NO	NO

- **Falencias de RCS:**

- Independencia de acceso, falla, porque se basa en IMS como plataforma, y como puede verse en los cuadros donde se ven que capas se ven involucradas en cada plataforma.

- Seguridad, falla, porque como vimos utiliza protocolos de IMS en algunas capas, por ende delega su seguridad al sustrato de IMS que utiliza.

- Interoperabilidad entre redes, falla, porque no contempla servicios de handover. Además necesita que las redes estén interconectadas.

- **Falencias del WebRTC:**

- Independencia de acceso, falla, porque es un servicio que requiere un acceso web, de banda ancha. No me puedo conectar desde cualquier cliente, como por ejemplo GPRS.

- Seguridad, su seguridad, la basa en la seguridad que tenga mi conexión web, por ende delega la seguridad de acceso al proveedor de Internet.

- Interoperabilidad entre redes, falla porque, corre sobre una única red, que es Internet. Es imposible que sea interoperable cuando no sabemos qué hay del otro lado de la llamada, es decir, si no somos dos usuarios de Skype, perfectamente registrados y ubicados, es imposible interconectaros con esta tecnología. Si queremos tener interoperabilidad en WebRTC deberíamos hacer un poco de reingeniería y poner algunas restricciones, como ocurrió con Messenger y Skype. En IMS existen protocolos definidos, existe una importante capa de señalización o control. Todas cosas que WebRTC no posee o usa las mismas que IMS. WebRTC sólo puede funcionar donde tengo perfectamente controlado ambos extremos de cualquier sesión. Como vimos, dos usuarios de Skype. Si esto no ocurre se puede volver impredecible y volátil.

- Multiplicidad de servicios, falla porque solo pretende brindar un acotado tipo de servicios de comunicación. En su concepto, sólo pretende que cada usuario que tiene una conexión web pueda comunicarse con otro, en tiempo real.

- Entre IMS y las nuevas plataformas como WebRTC y RCS hay principalmente dos vistas de dos mundos diferentes. Por eso podemos decir que existen dos tipos bien diferentes de necesidades, a saber:

SUPUESTOS IMS FULL	SUPUESTOS COMUNICACIÓN IP
Garantizar la QoS es un requisito fundamental.	Internet funciona más o menos, nos adaptamos cuando la capacidad se estrecha y reconectamos cuando se cae la conexión.
La voz funciona independientemente del acceso a Internet.	Acceso a Internet está, y la voz es otro servicio IP.
Roaming es parte fundamental de la experiencia móvil.	La gente odia pagar por roaming, por eso bypasea el servicio si quiere.
Roaming requiere que la red visitada soporte QoS y cargos de roaming.	Solo conectar al servidor más próximo. Solo se incorpora el roaming de datos. O solo se accede por WiFi restringiendo también el roaming de datos, para no tener ningún tipo de cargo.
Estándares son esenciales para roaming, interoperabilidad de redes, y anchi de banda.	Usar los estándares para acceder a las redes.
Dispositivos que no sean smartphones son soportados.	Se asume que los smartphones están en todos lados, el cliente es sólo una aplicación más.
VoLTE y RCS, requieren de IMS. RCS necesita como plataforma IMS. (Ver punto 4.6.1)	Cliente puede tener VoLTE y RCS, y sólo se requiere un servidor que soporte esas aplicaciones.

- Hay regulaciones asimétricas: sanciones para unos por Calidad y falta de obligaciones para los OTT. El kid de la cuestión es si un operador se puede arriesgar a tener una plataforma sin QoS o variable. Si por ejemplo Telefónica de Alemania, estrena su nuevo sistema VoLTE y deja a los usuarios de Iphone 7, sin servicio. Sufre un reclamo y es sancionado. Además de un deterioro de imagen muy difícil de revertir. Pero deja claro que un operador no puede utilizar una solución WebRTC y brindar soluciones best effort, sin QoS.

  En cambio si un día Skype o Google Talk o WhatsApp, no funcionan, la gente estará disconforme, pero al no estar regulada, no sufrirá sanciones de los entes gubernamentales. Parecen ser gratis, pero el flujo de ingresos viene de otro lado, por ejemplo publicidad.

  Como también lo vimos el handover en redes 4G o LTE a redes 3G o 2G, no es fácil de realizar sobre WebRTC, con un simple servidor. En este

caso, IMS presta soluciones muy robustas, como vimos en este trabajo en Telefónica de Alemania y el caso de implementación de VoLTE basado en IMS.

- IMS, la única alternativa para enfrentar el cambio de paradigma y de modelo: el único estándar desarrollado para poder integrar un modelo de servicios sobre redes IP, con independencia del acceso, seguridad y múltiples servicios para el usuario, que se verá beneficiado con todas las ventajas y servicios que una arquitectura de este tipo podrá ofrecer.

5.3 Conclusiones sobre la factibilidad de su introducción progresiva y los servicios asociados que permiten monetizar la inversión IMS de manera gradual

- Es posible plantear una implementación por etapas, y de esta forma una inversión progresiva que le otorgue un mayor sentido económico, ya que puede ir creciendo en etapas y adoptando cada servicio de IMS en la medida de su plan de negocios y aprovechando la inversión inicial del Core IMS, como hizo Telefónica de Alemania y China Mobile, en los casos presentados.
- Un operador invierte en un Core IMS, primeramente para pasar de un modelo basado en CS a un modelo basado en todo IP. Esto le brinda las ventajas ya vistas de la arquitectura IMS, como por ejemplo, bajar los costos de mantenimiento de la plataforma vieja basada en CS. La inversión en el Core es la primera inversión a realizar, con tal vez el agregado de algún servicio, que se quiera brindar. Como ser voz sobre DSL, para el caso de Telefónica de Alemania. De manera de ir invirtiendo luego en nuevos servicios y aplicaciones. Este es el camino obligado que tiene que seguir un operador de determinada envergadura, con una estrategia final en IMS, para seguir agregando otros servicios. Este tipo de operador requiere tener un control de su infraestructura. La estrategia de invertir en su propio Core y no en una plataforma de terceros, para un operador existente, se basa en que la idea de empezar a brindar servicios de valor agregado y controlar su base de datos de clientes, y no

delegar las tareas del Core en un tercero. Convirtiendo al operador en una tubería de bits.

- De acuerdo a estos casos analizados un plan de despliegue que Yo recomiendo en el tiempo es:

Etapa 1, de duración: 6 meses, que consiste en implementar un Core IMS, servicios IMS introducidos: servicios de voz sobre DSL, o sobre la tecnología de acceso que el operador tenga desplegada.

Etapa 2, de duración: 3 meses, que consiste en implementar VoLTE y RCS, servicios IMS introducidos: voice over LTE y RCS.

Etapa 3, de duración: 3 meses, que consiste en plataforma IPTV, servicios IMS introducidos: IPTV bajo demanda.

- Respecto de las tecnologías existentes (como ser un Core basado en CS), esta arquitectura permite soportar la interoperabilidad entre diferentes operadores para poder inter-operar con los que hoy tienen su Core basado en CS. Todo esto es fundamental, dado que le permite al operador actual poder adoptar esta solución en etapas. Dado que puedo tener mi red híbrida (CS y CP), hasta que paso todo IP.

- IMS es una arquitectura de red de cuarta generación, orientada a la convergencia de los servicios. Al presentar una arquitectura distribuida en capas y elementos, ha logrado optimizar las prestaciones multimedia, disminuyendo procesos, facilitando las operaciones y brindando mejores servicios a los usuarios.
- Como se vio en el caso de China Mobile, la decisión más difícil tal vez haya sido migrar el Core a IMS. Esta justificación está basada fundamentalmente en la necesidad de bajar los costos de mantenimiento de plataformas viejas basadas en CS, o face out. Y que nos quedemos sin servicio por parte de los vendors, para dichas plataformas. Luego el paquete de aplicaciones o la posibilidad de migrar la red para soportar VoLTE, ya está justificado, dado que la gran inversión ya fue realizada, tal vez lo más difícil es justificar la primer gran inversión en el Core IMS. Adicionalmente están montando junto con ZTE un laboratorio para upgradear el presente Core, a una versión que soporte 5G. Las nuevas aplicaciones y nuevas tecnologías se van integrando a esta arquitectura. Básicamente impulsado por grandes vendors como ZTE, Ericsson y

empresas como Telefónica de Alemania, o China Mobile, que quieren mantener sus redes con la última tecnología, pero en forma segura, sin arriesgar a perder calidad de servicio.

6 Bibliografía

1. IP Multimedia Subsystem: Principios y arquitectura, Simon ZNATY, Jean-Louis DAUPHIN y Roland GELDWERTH, EFORT, http://www.efort.com
2. IMS – IP Multimedia Subsystem, The value of using the IMS architecture, White Paper, Ericcson, October 2004.
3. Introduction to IMS, Standards, protocols, architecture and functions of the IP Multimedia Subsystems, Dan Leich, Dave Halliday, Motorola, IMS White Paper Series: Part 1, Referencias SIP
4. SIP : Session Initiation Protocol, Simon ZNATY, Jean-Louis DAUPHIN y Roland GELDWERTH, EFFORT, http://www.efort.com
5. "SIP : Session Initiation Protocol ", J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, RFC 3261, June 2002.
6. "Specific Event Notification", B. Roach, RFC 3265, June 2002.
7. "Call Processing Language Framework and Requirements", J. Lennox, H. Schulzrinne, RFC 2824, May 2000.
8. "The SIP INFO Method ", S. Donovan , RFC 2976, October 2000
9. "Reliability of Provisional Responses in the Session Initiation Protocol, J. Rosenberg, H. Schulzrinne, (SIP)", RFC 3262, June 2002.
10. SIP UPDATE Method, J. Rosenberg, RFC 3311, September 2002.
11. SIP Extension for InstantMessaging, Campbell, J. Rosenberg, H. Schulzrinne, C. Huitema, D. Gurle, , RFC 3428 , December 2002.
12. SDP: Session Description Protocol, M. Handley, V. Jacobson, RFC 2327, April 1998.
13. IPV6, Enabling the Next Generation of Networkingwith End-to-End IPv6, White Paper, Part Number: 200212-001 April 2007
14. The Diameter Base Protocol, RFC3588.
15. Criteria for Evaluating AAA, Protocols for Network Access, RFC2989.
16. Diameter Network Access Server Application, RFC4005.
17. Authentication, Authorization and Accounting (AAA) Transport Profile, RFC3539.
18. Diameter Session Initiation Protocol (SIP) Application: The Diameter Session Initiation Protocol (SIP) Application specification.
19. Securing wireless communications with the WebSphere Everyplace Connection Manager" (developerWorks, March 2004): Focuses on the many

security options in the WebSphere® Everyplace Connection Manager components. DeveloperWorks Wireless technology zone: Specializing in Web-based solutions.

20. Plataforma de Servicios de Nueva Generación, GT.ER.1906.1001 (DX-DXE-BR) Edición 01 – Octubre 2006.
21. Media Server, GT. ER.0809.1001 (DX-DXE-BR), Edición 01 – Octubre 2006.
22. Servicio Conferencias de Audio, Video y Web, TL.ER.B.8.0008, Edición 2da. - Abril 2008.
23. SIP, GT.ER.3203.003, Edición 1, Diciembre 2004.
24. Requisitos Gerais de Integracao com o Sistema SIGRES, GT.ER.1703.1003 (DX-DXS-BR), Emisión 01, Dez.2007
25. TELEMANAGEMENT FORUM (TMF)
26. GB910 – "Telecom Operations Map 2.1"
27. GB921 – "Enhanced Telecom Operations Map (eTOM)"
28. GT.NA.0024.001(DT-DTR-BR).BR Em.01 JUN2005 – "Modelo Geral de Gerência de Serviços"
29. GT.NA.0024.002.BR EM.01 JAN2006 – "ARQUITETURA LÓGICA DO PLANO DE SISTEMAS COMUNS T-LATAM PARA O PROJETO CANDELARIA"
30. GT.PT.0024.1001(DX-DXT-BR) EM.01 NOV2007 - "Plano de Sistemas OSS para a Convergência Fixo-Móvel"
31. "Connector Development Guide for Java", IBM
32. http://www.radio-electronics.com/info/telecommunications_networks/ims-ip-multimedia-subsystem/tutorial-basics.php
33. http://networks.nokia.com/portfolio/solutions/voice-over-lte
34. http://www.mavenir.com/products/applications-and-services/voice-and-video/volte-iwf/default.aspx
35. Multi-access for the IMS network, Rogier Noldus, Ralf Keller and Bo Åström, Ericsson Review No. 2, 2012
36. https://www.ericsson.com/news/1864321
37. Investigation IMS architecture, According to Security and QoS context, Master of Science Thesis [Network and distributed system]. AJMAL MUHAMMAD-RAJA MUHAMMAD SHAMAYEL ULLAH
38. Cloudifying the 3GPP IP Multimedia Subsystem for 4G and Beyond: A Survey, Mohammad Abu-Lebdeh,Jagruti Sahoo, Roch Glitho, Constant Wette Tchouati, CIISE, Concordia University, Montreal, QC, Canada.Ericsson, Montreal, QC, Canada.
39. China Mobile to build IMS network with ZTE- Press Clipping.

40. Telefónica Germany selects Ericsson for Voice over LTE, PRESS RELEASE, OCTOBER 21, 2014.
41. Ericsson and SoftBank demonstrate mobility-based policy to improve performance, PRESS RELEASE, AUGUST 11, 2014.
42. Ericsson's complete voice over LTE solution selected by SoftBank mobile, PRESS RELEASE, OCTOBER 31, 2013.
43. Bouygues Telecom chooses Voice over LTE from Ericsson for its 4G network in France, PRESS RELEASE, MAY 21, 2014.
44. New Platform from Ericsson brings Communications simplicity to developers, PRESS RELEASE, January 8, 2013.

7 Índice de Figuras

8 Índice de Tablas