UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

TECNOLOGÍAS OPEN SOURCE EN TELEFONÍA IP

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO ELÉCTRICO ELECTRÓNICO

P R E S E N T A:

NOPAL PASCUAL GIOVANNI ANDRÉS

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A:

ZÁRRAGA ESTRADA JUAN CARLOS

Director de Tesis:

Dr. Miguel Moctezuma Flores

México, D.F. **2008**

Agradecimientos

Agradezco primeramente a Dios, por permitirme llevar acabo este pasó decisivo en mi vida y por haber puesto en mi camino a aquellas personas que han sido mi soporte y mi compañía en momentos de angustia y desesperación.

A mis padres, Juan Manuel y Juliana, a quienes les agradezco su apoyo incondicional, comprensión, así como su confianza en mi realización profesional. Gracias por mostrarme que la educación esta ligada con el deporte, pues de este último he adquirido la disciplina.

A mis hermanos, Guillermo y Sergio, por su amistad y por todo lo que hemos compartido juntos.

A mis compañeros, a mis profesores y a todas aquellas personas que han dejado huella en mi vida, que compartieron o compartimos experiencias, conocimientos, develadas y triunfos.

Y a ti, por que "Sabes que te quiero como nadie debe saberlo".

Juan Carlos Zárraga Estrada

"El que no sabe poner su voluntad en las cosas, intenta darles algún sentido, lo cual le hace creer que hay una voluntad en ellas."(Principio de la fe)

A esa extraordinaria mujer, cuyo cariño, apoyo y comprensión incondicionales han motivado mis afanes diarios por ser mejor persona. Para ti madre, este modesto fruto de mi andar.

A mi familia, amigos, mentores y a todos aquellos con quienes he tenido la dicha de crecer y compartir momentos inolvidables. Deseo compartir con ustedes uno mas de ellos.

Giovanni Andrés Nopal Pascual

A los protagonistas de este proyecto, Beatriz, Nayeli, Ricardo, Marcote, Marquito, Memo y al Ing. Israel Ortega, por su participación activa, pero en especial por los momentos compartidos durante nuestra estancia en el Laboratorio de Tecnologías Emergentes de Redes de la UNAM en el grupo de trabajo de VoIP. A ustedes que colaboraron en la realización de esta investigación, hacemos extensivo nuestro más sincero agradecimiento.

Así también, a la Facultad de Ingeniería, a la cual debemos nuestra formación académica y a la Dirección General de Servicios de Computo Académico de la UNAM (DGSCA) a la cual agradecemos el apoyo brindado y las facilidades necesarias para llevar acabo este trabajo.

Gracias

Índice general

Introducción

La Universidad se ha caracterizado siempre por ser *líder en el desarrollo e incorporación de nuevas tecnologías*. La infraestructura de comunicaciones de la UNAM es una de las más complejas que existen a nivel nacional, no sólo por sus dimensiones, sino por la variedad de tecnologías que en ella conviven. Es precisamente esa riqueza y variedad de instalaciones lo que convierte a la Universidad en un laboratorio de pruebas inigualable.

> *"La Dirección General de Servicios de Cómputo Académico* de la UNAM es la entidad universitaria *encargada de la operación de los sistemas centrales de cómputo académico y de las telecomunicaciones de la institución*; su esfuerzo más amplio es la capacitación en tecnologías de la información, de prospección e innovación y de asimilación de estas tecnologías en beneficio de la Universidad y de la sociedad en general."

Actualmente, la UNAM vive un proceso de transición y convergencia tecnológica en su infraestructura de comunicaciones. Tradicionalmente, la UNAM había mantenido separadas las infraestructuras de Voz y Datos. Hoy por hoy, se ha optado por un modelo híbrido en el cual conviven la telefonía Digital y la telefonía IP (RUV)[1] , junto con la Red de Datos (RedUNAM).

Existen dependencias universitarias cuyas necesidades de comunicación exigen el planteamiento de propuestas innovadoras en el campo de las comunicaciones. Tales dependencias son candidatas idóneas para la realización de proyectos que integren tecnologías emergentes como lo es la telefonía IP.

En la actualidad, la telefonía sobre redes IP está pasando por un periodo de enorme crecimiento, acelerado por el acceso a características y aplicaciones de valor añadido que sólo la telefonía por IP puede proporcionar al usuario final. El unificar en una sola red los servicios de datos, de voz y video ha propiciado que está tecnología sea aceptada rápidamente.

Por otro lado, el movimiento de "Software Libre" ha permeado cada vez más en todos los ámbitos tecnológicos y la telefonía IP no podía ser la excepción. El sistema operativo Linux es el ejemplo más contundente de que la filosofía "Open Source" es capaz de ofrecer grandes beneficios a la comunidad en general. En este trabajo se presentan dos de las propuestas "Open Source" más populares en el mundo VoIP.

[1] Red Universitaria de Voz

La inclusión de la telefonía IP en los esquemas de telecomunicaciones de la Universidad favorece la simplificación de los sistemas de comunicación, aprovechando la infraestructura existente, se brindan facilidades y servicios de comunicación novedosos, tales como, mensajería unificada, video-llamadas, mensajería instantánea, etc. Además, el uso y desarrollo de plataformas basadas en "Software Libre" permite la reducción de costos de operación y mantenimiento, pues no son necesarios los contratos de servicios, ni la adquisición de licencias de software u otros, al tiempo en que la institución mantiene vigente el compromiso de formación de recursos humanos y tecnológicos en el área.

La intensión de esta tesis es abordar las bases fundamentales de la tecnología de Voz sobre el Protocolo de Internet (VoIP), así como brindar una perspectiva de las posibles alternativas de solución basadas en Software Libre. Se presentan las plataformas Asterisk y OpenSER como la base para el desarrollo de un sistema de telefonía IP viable para la Universidad.

Finalmente, se exponen los resultados del protocolo de pruebas aplicado tanto a Asterisk como a OpenSER, efectuado en el laboratorio de tecnologías emergentes de redes (NETLab) de la UNAM. Estas pruebas constituyeron un antecedente importante en la búsqueda de una solución más robusta que integre ambas tecnologías.

Capítulo 1

Evolución de las Redes de Voz y Datos

Vivimos en un mundo donde las telecomunicaciones han sufrido una revolución tecnológica notable en el último siglo. Nadie es ajeno a sucesos tales como la telefonía celular o la Internet, por citar los ejemplos más dramáticos. Las implicaciones de estos cambios no se restringen únicamente al ámbito tecnológico, sino que estan provocando una revolución social que ha dado lugar a la así llamada *"Brecha Digital"*. Es por ello que consideramos importante el conocer y comprender el proceso de transformación que las telecomunicaciones han recorrido hasta nuestros días.

En este primer capítulo revisaremos *brevemente* la evolución que ha vivido este sector, su impacto en la vida moderna y las tendencias futuras. En primer término, hablaremos de la evolución de las Redes de Voz y, en segundo término, el desarrollo de las Redes de Datos, finalmente revisaremos el proceso de convergencia que se vive actualmente.

1.1. Redes de Voz

El teléfono es probablemente el medio de comuncación con el que las personas se encuentran más familiarizadas. Sin duda alguna, las generaciones modernas no conciben un mundo sin teléfono; sin embargo, detrás del "infalible" servicio telefónico al que tan acostumbrados nos encontramos, existe un complejo universo desconocido por el usuario común. Es nuestra intención el hacer modesta mención de algunos de los personajes y hechos históricos que han contribuido al desarrollo del mundo de las telecomunicaciones tal y como hoy lo conocemos.

1.1.1. Antecedentes

Antonio Meucci y Alexader Graham Bell

Antonio Meucci, fue quien originalmente desarrolló el principio de la telefonía. En 1855, Meucci construyó un dispositivo, al cual llamó "Telégrafo Parlante", trató de comercializarlo con la compañía Telegráfica *Western Union*, lo cual nunca ocurrió. Meucci fue incapaz de mantener los costos de la patente definitiva y la perdió poco después.

El 14 de febrero de 1876, Alexander Graham Bell documentó una patente[1] que realmente no describe al teléfono, pero se refiere a él como tal. A este dispositivo le llamó "Teléfono electromagnético". La patente fue aceptada el 7 de marzo del mismo año. Aquel mismo día, Elisha Gray presentó un aparato similar, pero el aparato de Bell demostró ser el mejor y se convirtió en un éxito.

Los Estados Unidos comenzaron el seguimiento por fraude contra la patente de Bell, el juicio se pospuso de año en año hasta la muerte de Meucci en 1896, cuando el caso fue dejado. Reciéntemente, en el año 2001, se le atribuyó legalmente la invención del teléfono a Antonio Meucci.

Inicios y estructura de la Red Telefónica

En un principio eran pocos los privilegiados con el servicio de telefonía. No todos los usuarios, a pesar de que eran pocos, podían hablar al mismo tiempo y no existía el timbrado en los aparatos telefónicos. Con el paso del tiempo la red creció y con ello el sistema resultó insuficiente.

En los primeros días del servicio telefónico era necesario tender cableado entre todos y cada uno de los *abonados* (Ver figura 1.1). Conforme la red crecía el número de líneas requeridas resultaba exagerado y prohibitivo en términos económicos. Fue entonces que se recurrió al uso de *operadoras telefónicas*, personas encargadas de realizar las conexiones, en un punto central de la red donde concurrían todas las líneas telefónicas (Ver figura 1.2).

[1] Patente No. 174,465 titulada "Improvements in Telegraphy" (*Mejoras en Telegrafía*).

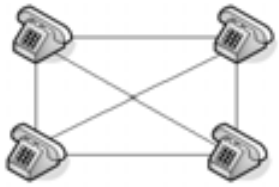

Figura 1.1: Modelo inicial de conexión del sistema telefónico

Figura 1.2: Operadoras telefónicas en un conmutador pequeño

El uso de *operadoras telefónicas* resolvió el problema del cableado excesivo(Ver figura 1.3); no obstante, la capacidad de este sistema se vió superada prontamente a causa de la creciente demanda por el servicio.

Figura 1.3: Modelo de la red telefónica empleando *operadoras telefónicas*

En sustitución de las operadoras se desarrollaron los conmutadores automáticos. Este sistema desempeñaba la misma tarea que las operadoras en un punto central del sistema desde donde salían las líneas hacia los abonados. La conmutación automática

permitió que cada vez más gente tuviera acceso al servicio telefónico. Los primeros modelos de conmutadores automáticos eran de tipo electromecánico (Ver figuras 1.4 y 1.5).

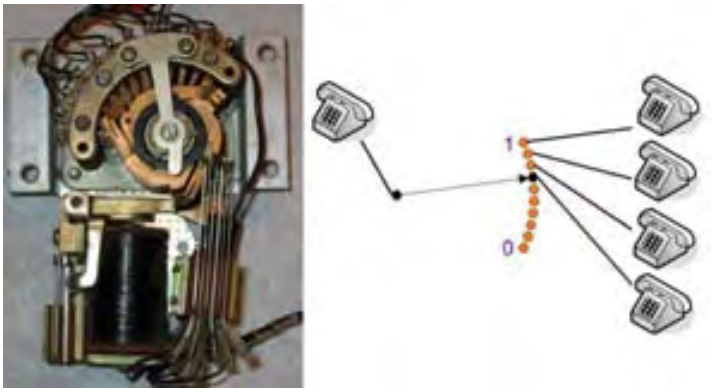

Figura 1.4: Selector de línea

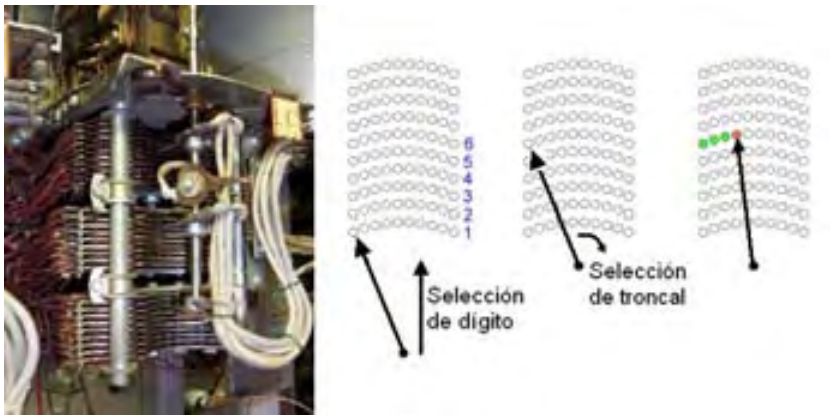

Figura 1.5: Conmutador Strowger de dos ejes

Conforme los avances técnicos lo fueron permitiendo aparecieron los de tipo electrónico en sus modalidades analógica y digital, tal y como los que hoy en día se utilizan(Ver figura 1.6).

En el apéndice A se incluye una cronologia histórica con los hechos más sobresalientes en la evolución de la telefonía.

1.1.2. Elementos de la telefonía tradicional

Existen diversos elementos que hacen posible hablar con otra persona a distancia por medio de la Red telefónica convencional (PSTN)[2] . Al levantar el auricular se

[2] Public Switched Telephone Network - Red Telefónica Pública Conmutada.

Figura 1.6: Conmutador Digital Nortel DMS100

desencadenan numerosos procesos y diversos elementos interactúan con el único objetivo de transportar nuestra Voz hacia donde así lo deseemos.

La Red Telefónica Pública Conmutada *PSTN*

La PSTN (*Public Switched Telephone Network*) es una Red telefónica conmutada de circuitos diseñada y optimada para la transmisión en *tiempo real* de Voz "exclusivamente". Es la interconexión de varias centrales telefónicas alrededor del mundo con el fin de brindar servicios de Voz de forma ininterrumpida y hacia casi cualquier lugar del mundo.

Cuando se establece una llamada a través de la PSTN (ahora también conocida como POTS[3]), se cierra un circuito dedicado entre emisor y receptor. Esto garantiza la Calidad de Servicio (QoS), pues el circuito permanece activo en tanto dure la conversación independientemente de si los participantes se encuentran hablando o en silencio y hasta que alguno de los dos extremos cuelgue (termine la conversación).

La red telefónica es un red jerárquica, lo que significa que las centrales se encuentran las centrales interconectadas en niveles (Ver figura 1.7). Las distintas categorías son las siguientes: Centrales de Acceso a las cuales se conectan los abonados, Centrales Tandem (o de paso) que no atienden abonados, sino que redirigen el flujo de llamadas de una central a otra, Centrales Regionales y Centrales Internacionales que se encargan de administrar los enlaces troncales entre áreas alejadas o entre países respectivamente.

Un teléfono se conecta a una central por medio de un par de alambres de cobre llamado *Loop Local* o circuito local (Ver figura 1.8). La ruta completa desde el dispositivo donde es conectado el teléfono hasta la central se denomina *Línea telefónica*. Una trayectoria de comunicación entre conmutadores de distintas centrales se conoce como *Trunk* o Troncal.

[3] Plain Old Telephone Service - Viejo Servicio Telefónico o Servicio Telefónico Tradicional

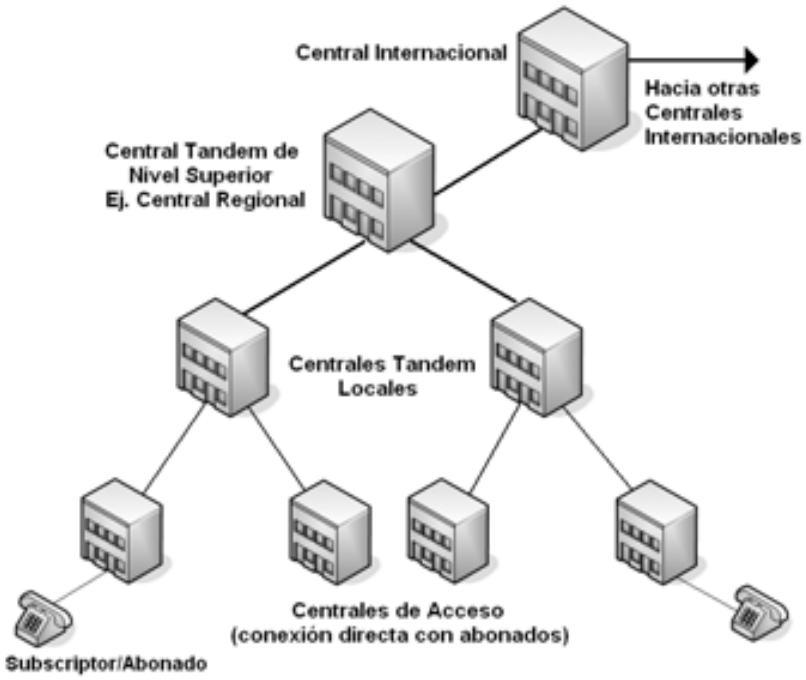

Figura 1.7: Topología jerárquica de conmutadores en la PSTN

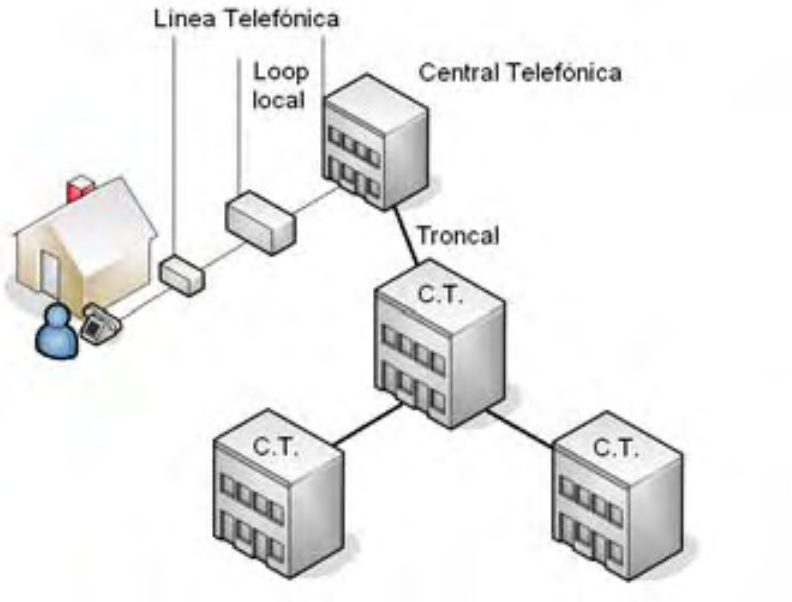

Figura 1.8: Esquema de conexión del abonado hacia la central

El PBX

PBX son las siglas en inglés de *Private Branch eXchange* y se refiere a la Central Telefónica Privada. En muchas ocasiones es referido también como una "centralita"

telefónica por el hecho de que da servicio a una considerable menor cantidad de abonados[4] . Físicamente un PBX se aloja en un sitio, (edificio, local o contenedor), dentro de una empresa o institución, llamado "*Site de comunicaciones*" en donde se alberga el equipo de conmutación y demás dispositivos necesarios para el establecimiento de conexiones telefónicas. En este lugar terminan las líneas de abonado y los enlaces con otras centrales.

El núcleo de un PBX no es otra cosa que una computadora de propósito específico. Su tarea es administrar el tráfico de llamadas internas y el de aquellas que provengan o se dirijan hacia la Red Pública. Las llamadas entre la PSTN y la Central Telefónica se enrutan mediante enlaces digitales (troncales) E1[5] o T1 con capacidad para 30 y 24 canales de Voz respectivamente. Debido a esto las empresas logran un mayor control del tráfico que se dirije hacia la PSTN. Esto es importante para efectos de tarificación de servicios y restricción de llamadas, pues se pueden manejar códigos de acceso a troncales.

Los PBX representan una ventaja para las empresas medianas a grandes que requieren cubrir sus necesidades de comunicaciones internas sin tener que pagar a la compañía telefónica por el servicio. En oficinas pequeñas en donde no es justificable el uso de PBX se utilizan teléfonos con líneas directas o dispositivos multilíneas (microconmutadores con teclas especiales para marcar a las extensiones o hacer uso de troncales).

Un PBX permite una mejor administración de los recursos y servicios de Voz, al igual que la automatización de procesos mediante servicios avanzados tales como: Contestadora Automática Interactiva de Voz mejor conocida como *IVR*, Buzón de Voz, Salas de Conferencia Telefónica, Directorio Institucional, Música en Espera, Desvío y transferencia de llamadas, etc. Un PBX requiere de poco mantenimiento y su vida útil es de alrededor de diez años y aunque la inversión inicial es importante, se amortiza rápidamente por las ventajas que esta solución representa.

Interfases FXS y FXO

La denominación **FXS** (*Foreign eXchange Subscriber*) y FXO (*Foreign eXchange Office*) corresponde a dos de las interfases más comunmente utilizadas en el entorno de la telefonía tradicional.

FXS es la interfase que provee el servicio de la PSTN en la ubicación del usuario final, en este puerto debe conectarse un equipo de subscriptor; por ejemplo: teléfonos, modems y/o una máquina de fax. Está provee los siguientes servicios primarios al suscriptor: ***Tono de marcado, Tensión de alimentación y Tensión de timbrado.***

[4] Aunque existen redes privadas de Voz con una enorme cantidad de extensiones, por ejemplo la Red Universitaria de Voz (RUV) de la UNAM.

[5] El estándar E1 corresponde con la norma Europea y es empleado en la mayoría de los países como México, Sudamérica, Australia, etc; mientras que el estándar T1 se emplea en Norteamérica y Japón.

Por otro lado la interfase **FXO** corresponde al puerto en el teléfono que recibe el servicio de la PSTN. Está interfase es la encargada de proveer las siguientes señales: ***Indicación de On-Hook (Colgado) e Indicación de Off-Hook (Descolgado)***.

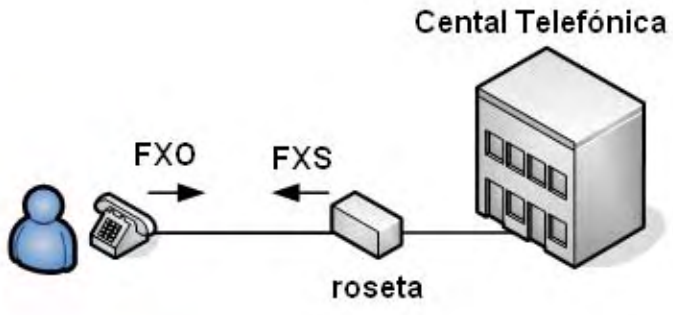

Figura 1.9: Interfases FXS y FXO

Resumiendo, una interfase FXS se ubica en un PBX o dispositivo de la central telefónica y es la interfase para conectar un equipo terminal de usuario. En contraparte, una interfase FXO se ubica en el dispositivo terminal del usuario, como un teléfono, modem o fax y es la interfase para conectar este dispositivo a la oficina central. No se pueden conectar dos interfases FXO entre si, por ejemplo dos aparatos telefónicos, ni tampoco dos interfases FXS. Estos dos puertos siempre se complementan.

Cuando se introducen elementos adicionales entre el abonado y la central telefónica, tales como un *PBX* se debe mantener la correspondencia entre puertos, es decir, los puertos FXO se conectarán a los puertos FXS del conmutador privado (PBX) y del mismo modo los puertos FXO del PBX se conectarán a los puertos FXS provistos por la compañía telefónica. En este caso los puertos FXS del PBX serán los encargados de proveer tensión de alimentación, de timbrado y tono de marcación a los dispositivos telefónicos, mientras que los puertos FXO del mismo deberán retransmitir las señales de On-Hook y Off-Hook hacia la red pública (Ver figura 1.10).

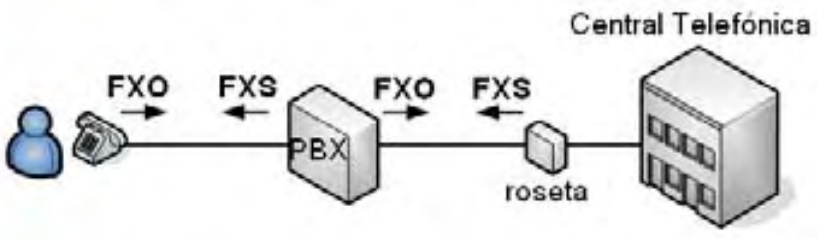

Figura 1.10: Interconexión hacia la central telefónica a través de PBX

Planes de numeración y marcación

El plan de numeración es la organización y asignación razonada y concensada de rangos de números telefónicos. Existen planes de numeración privados, nacionales e internacionales. En el caso de un plan de numeración privado se debe definir la cantidad de dígitos para realizar la marcación (comúnmente 5) y determinar los códigos de acceso a troncales, líneas especiales y/o de servicios, verificando su congruencia y garantizando que cada suscriptor cuente con un único identificador. En cuanto a planes internacionales se refiere, existe la recomendación de la ITU-T (E.164) en la que se establece que un plan de numeración internacional para los sistemas de telefonía pública se compondrá de hasta 15 dígitos, cada número asignado contiene un Código de País (CC), un Código de Área o Región (AC) y el número Local. El plan de numeración vigente en México se encuentra definido en el *Plan Técnico Fundamental de Numeración* elaborado por la *COFETEL* y actualizado al 16 de agosto de 2007.

La Red Digital de Servicios Integrados RDSI (ISDN)

La Red Digital de Servicios Integrados (ISDN), por sus siglas en inglés, es una evolución de las redes de Voz analógicas. Presenta conexiones digitales extremo a extremo ofreciendo una gran variedad de servicios. La capacidad básica de comunicación de un canal RDSI es de 64 kbps (véase la sección 2.2.1). Este modelo de Red se desarrolló con el objeto de integrar distintos servicios digitales (como voz, datos y video) aprovechando la infraestructura existente.

Los elementos (grupos funcionales) que componen este modelo, son los siguientes: TE1 (Terminal Equipment 1), TE2, NT1 (Network Terminator 1), NT2, LT (Line Terminator) y CT (Central Terminator); así mismo, se definen los puntos de referencia R, S, T, U y V que definen las interfases lógicas entre grupos funcionales (Ver figura 1.11).

- **CT:** El Terminador de Central se encarga de conmutar la información a su destino específico, soporta la señalización del usuario y el envío de información en modo paquete.
- **LT:** El Terminador de Línea tiene por función, adaptar la señal al medio de transmisión.
- **NT1:** El Terminador de Red 1, también conocido como NTU (Network Terminal Unit) tiene la misma función que el terminador de línea excepto que éste se ubica en el hogar del usuario y marca el fin de la red que esta bajo la responsabilidad del proveedor (Punto de demarcación).
- **NT2:** El Terminador de Red 2, es responsabilidad del usuario y realiza las funciones de conmutación local. A él se conectan los dispositivos que el usuario usa tales como teléfonos o computadoras; por ejemplo: el PBX.
- **TE1:** Los Equipos Terminales 1 son dispositivos, tales como teléfonos digitales, tarjetas de PC, equipos de video conferencia, etc., compatibles con RDSI.

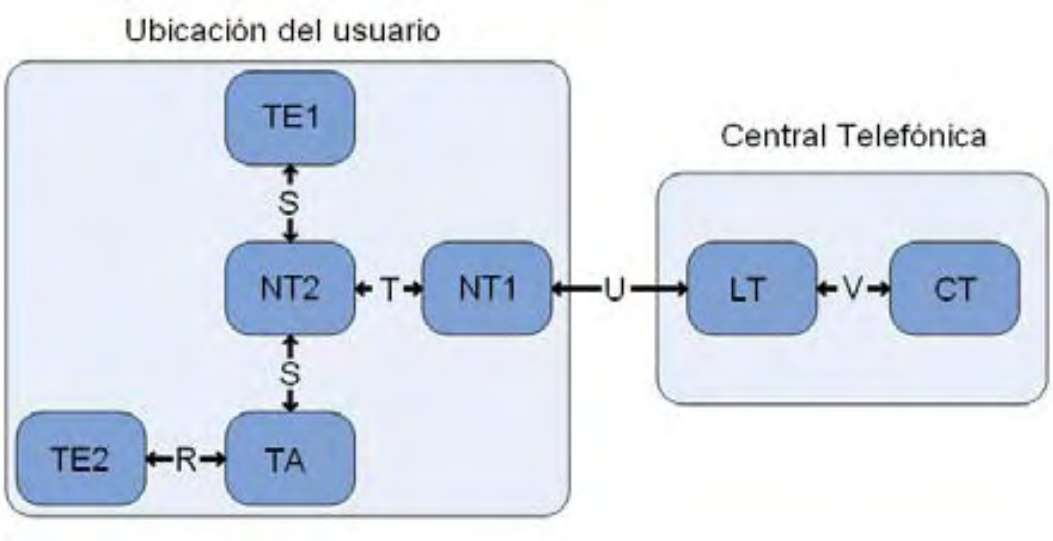

Figura 1.11: Modelo RDSI. Relación entre interfases y grupos funcionales

- **TA:** Los Adaptadores de Terminal son elementos que permiten adaptar a la RDSI dispositivos que no son compatibles por si sólos. La mayoría de los adaptadores de terminal se ubican en los TE1 o se acoplan como módulos a éste mismo.
- **TE2:** Los Equipos Terminales 2 son dispositivos que no son compatibles por si sólos con la RDSI, ejemplos de éstos son los teléfonos analógicos y los modems.

Interfases o puntos de referencia

Las interfases pueden ser reales o virtuales. Los puntos de referencia virtuales no son accesibles o en algunos casos coinciden con otras interfases.

- **Interfase V:** Marca la separación entre las funciones de la conmutación y transmisión en la central. Es una interfase virtual, ya que se encuentra en la misma placa junto con el CT.
- **Interfase U:** Es una interfase física que consiste de alambres de cobre tendidos desde la ubicación del usuario hasta la central.
- **Interfase T:** Es la separación entre la transmisión de línea y la transmisión en el hogar del usuario. Es un punto de transmisión que en algunos casos puede coincidir con el punto de referencia S.
- **Interfase S:** Es una interfase física a través de la que se conectan los dispositivos terminales ISDN.
- **Interfase R:** Es también una interfase física que conecta dispositivos no compatibles con la ISDN con el Adaptador de Terminal.

Muchas veces las interfases S y R concurren en el mismo NT2 que en su interior incluye el TA.

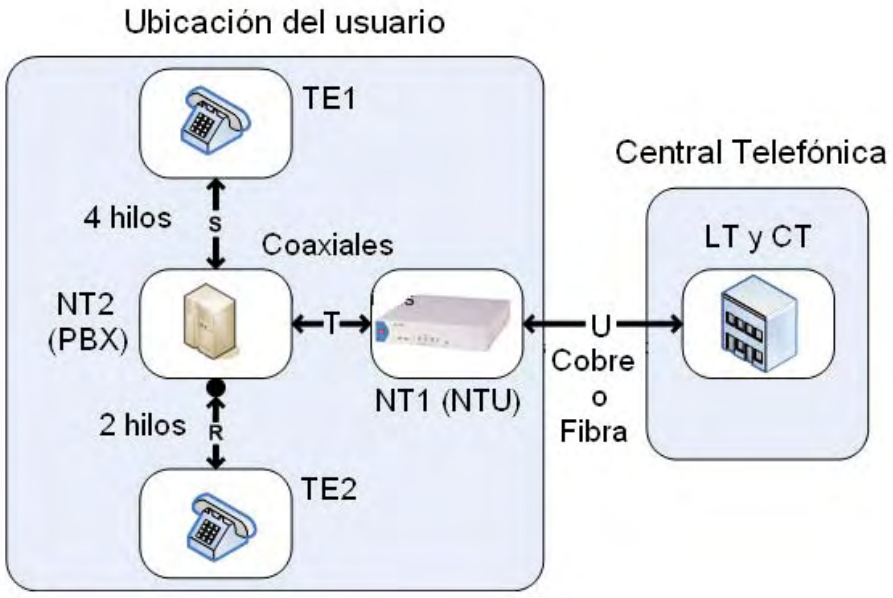

Figura 1.12: Ejemplo real de elementos e interfases en una RDSI

Servicio RDSI BRI *Basic Rate Interface*

El canall básico de la RDSI tiene un ancho de banda (BW) de 64 kbps (comúnmente llamado DS0). El servicio básico, denominado BRI ofrece 2 canales para transmisión de datos denominados canales B y un canal de 16 kbps llamado canal D usado para transmitir la información de señalización. En ocasiones, el canal D también puede ser empleado para la transmisión de información del usuario. Es por ello que comúnmente se encuentra que el servicio BRI tiene un ancho de banda de 192 kbps.

Este servicio es poco común, generalmente se puede usar para tener una conexión a la Internet a la vez que se tiene disponible un canal más para la línea telefónica.

Servicio RDSI PRI *Primary Rate Interface*

El servicio PRI ofrece 23 canales B en el caso de Estados Unidos y Japón, mientras que para México y Europa se emplean 30 canales B y 1 canal D de 64 kbps. En ambos casos se incluye un canal extra para efectos de sincronización. De esta forma la tasa de transmisión en México es de 2048 kbps; sin embargo, al sólo emplearse 30 canales efectivos de los 32 disponibles, la tasa efectiva es de 1920 kbps $\approx$ 2 Mbps. En este servicio es posible agrupar varios canales para transferencia de Video y Datos. Por ejemplo:

- **Canal H0:** 6 canales B de 64 kbps, bitrate total de 384 kbps (Video).
- **Canal H10:** 23 canales B de 64 kbps, bitrate total de 1472 kbps.
- **Canal H11:** 24 canales B de 64 kbps, bitrate total de 1536 kbps.
- **Canal H12:** 30 canales B de 64 kbps, bitrate total de 1920 kbps.

1.1.3. Protocolos de señalización para redes de Voz TDM

La necesidad de contar con métodos de control del flujo de llamadas y así mismo de información sobre el estado de la Red de Voz, dió como resultado los métodos de señalización. El objetivo primario de estos es permitir a los sistemas de conmutación intercambiar información necesaria para el tratamiento de tráfico telefónico.

Existen dos tipos de señalización: *Señalización Usuario - Red* y *Señalización Red - Red*. La primera se emplea para que el usuario final se comunique con la Red Telefónica (PSTN o PBX). Por su parte la *Señalización Red - Red* es utilizada entre switches de las redes telefónicas.

Señalización Usuario - Red

El método más comúnmente utilizado para este tipo de señalización es el sistema DTMF, también conocido como señalización en banda. El sistema DTMF (Dual-Tone Multi-Frequency: Multi-Frecuencia de Doble Tono) es un método de señalización[6], que hace uso de dieciséis combinaciones de frecuencias de audio, cada una consta de dos señales senoidales. Se utilizan tonos en la banda de frecuencias de la voz humana (300 Hz a 3400 Hz)[6] y las características requeridas para los equipos que operen con DTMF se encuentran establecidas en la Norma Oficial Mexicana *NOM-151-SCT1-1999*.

En la tabla 1.1, se muestran los pares de frecuencias que componen los códigos usados en la Señalización Multifrecuencial, así como los niveles de potencia mínimos en [dBm] establecidos en la Norma, ya antes mencionada.

La señalización DTMF tiene varias ventajas sobre la de pulsos, incluyendo una mayor rapidez de marcado y la posibilidad de enviar señales de control a través de la línea telefónica. La marcación de tonos se distingue fácilmente por los sonidos característicos que genera al digitar cada entrada.

Cuando el usuario presiona uno de los botones del teléfono, ver tabla 1.1, se genera un tono conformado por un par de frecuencias de acuerdo al número presionado. El tono viaja hasta el switch en la central telefónica y allí se identifica el dígito presionado.

Por otro lado, cuando hablamos de *métodos de señalización fuera de banda* nos referimos a aquellos que emplean un canal por separado exclusivamente para la señalización. Tal es el caso del método de señalización empleado en los sistemas RDSI. En un sistema RDSI la voz es transportada en canales tipo B de 64 kbps, mientras que la señalización se transporta por un canal tipo D que puede ser de 16 kbps ó 64 kbps.

[6] Ésta es la razón por la que se denomina señalización en banda.

Dígito	Frec. inferior [Hz]	Nivel [dBm]	Frec. superior [Hz]	Nivel [dBm]
1	697	- 8,0 $\pm 2,0$	1209	- 6,0 $\pm 2,0$
2	697	- 8,0 $\pm 2,0$	1336	- 6,0 $\pm 2,0$
3	697	- 8,0 $\pm 2,0$	1477	- 6,0 $\pm 2,0$
4	770	- 8,0 $\pm 2,0$	1209	- 6,0 $\pm 2,0$
5	770	- 8,0 $\pm 2,0$	1336	- 6,0 $\pm 2,0$
6	770	- 8,0 $\pm 2,0$	1477	- 6,0 $\pm 2,0$
7	852	- 8,0 $\pm 2,0$	1209	- 6,0 $\pm 2,0$
8	852	- 8,0 $\pm 2,0$	1336	- 6,0 $\pm 2,0$
9	852	- 8,0 $\pm 2,0$	1477	- 6,0 $\pm 2,0$
*	941	- 8,0 $\pm 2,0$	1209	- 6,0 $\pm 2,0$
0	941	- 8,0 $\pm 2,0$	1336	- 6,0 $\pm 2,0$
#	941	- 8,0 $\pm 2,0$	1477	- 6,0 $\pm 2,0$

Tabla 1.1: Señalización multifrecuencial DTMF

Algunas de las ventajas que trae consigo el uso de métodos de señalización fuera de banda *"Out of band"* son:

- Mayor uso del ancho de banda disponible para la transmisión de Voz.
- Mayor posibilidad de establecimiento satisfactorio de la llamada.
- Menor retraso en el procesamiento de la llamada, (no se reenvían los tonos en cada switch).
- Se evita la pérdida de tonos.

En la PSTN el método de señalización Usuario - Red más comúnmente utilizado es el DTMF, mientras que en las redes RDSI se emplea el método de señalización fuera de banda.

Señalización Red - Red

Existen, al igual que en el caso de señalización Usuario - Red, esquemas de señalización Red - Red "in band" y "out band".

Para el primer caso se utiliza la señalización MF (*Multi Frecuency*), cuyo modo de operación es similar al sistema DTMF, pero a diferencia de éste último, utiliza un rango distinto de frecuencias. El sistema MF se basa en señales analógicas, lo cual es poco común hoy en día, pues la mayoría de las redes telefónicas son digitales.

Respecto al esquema de señalización *Red - Red fuera de banda* las compañías telefónicas hacen uso de dos tipos de señalización. El primero corresponde a Europa y países como México que emplean el método SSCC7 (Sistema de Señalización por Canal Común

número 7), el segundo caso es el de Estados Unidos y Japón que emplean el denominado SS7 (System Signaling Number 7). El CCITT recomienda el SSCC7, aunque ambos sistemas operan en forma similar difiriendo sólo en detalles y es común referirse a ellos como el sistema de señalización SS7.

SSCC7 fue diseñado a finales de la década de los 70's por la CCITT y se basa en el intercambio de mensajes entre switches para el control de las llamadas. Lo anterior incluye, establecimiento de la llamada, ruteo de las mismas, operaciones de registro y facturación y otros servicios avanzados.

Sistema de Señalización por Canal Común No. 7

Este sistema consta de 3 elementos principales:

- SSP (Service Switching Point)
- STP (Signal Transfer Point)
- SCP (Signal Control Point)

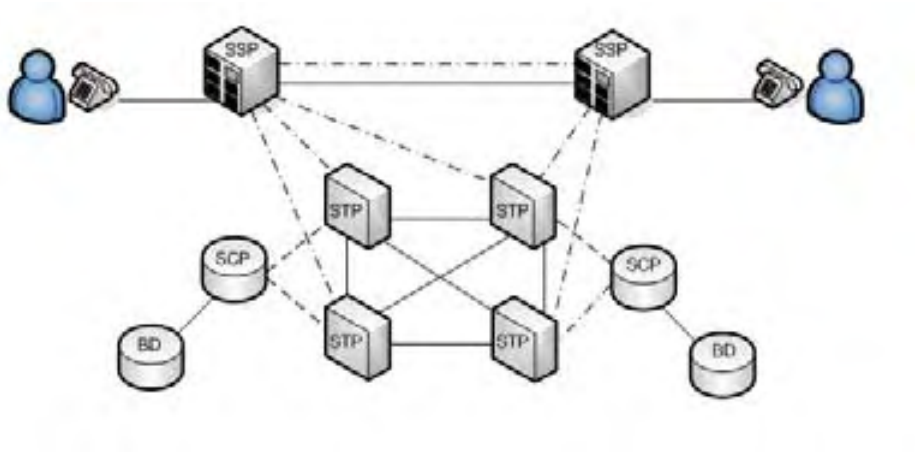

Figura 1.13: Elementos de Red SSCC7

Los SSP son conmutadores telefónicos ubicados en las centrales y conectados directamente a los usuarios. Su labor es originar y terminar las llamadas. Si se ubican en el núcleo del sistema, operan como switches tandem entre otros SSP's.

Los STP se encargan de enrutar (encaminar) los mensajes de señalización. Proveen conectividad lógica entre SSP's sin requerir de una trayectoria directa entre ellos. Poseen enlaces redundantes y se configuran generalmente en pares. Existen distintos tipos de STP's. De acuerdo a su nivel jerárquico, estos pueden ser: Local STP (LSTP), Regional STP (RSTP), National STP (NSTP), International STP (ISTP) y Gateway STP (GSTP).

Finalmente, los SCP son una interfase de conexión con *Bases de Datos* en donde se almacena información para el ruteo de servicios especiales, tales como 01 800 ó 01 900.

Los elementos de una Red SS7 se interconectan mediante enlaces de señalización full duplex de 56, 64 kbps, o múltiplos de estos.

Por otra parte, existen tres modos de señalización en los sistemas SS7: ***Asociado, No Asociado y Cuasi-Asociado***(Ver figura 1.14).

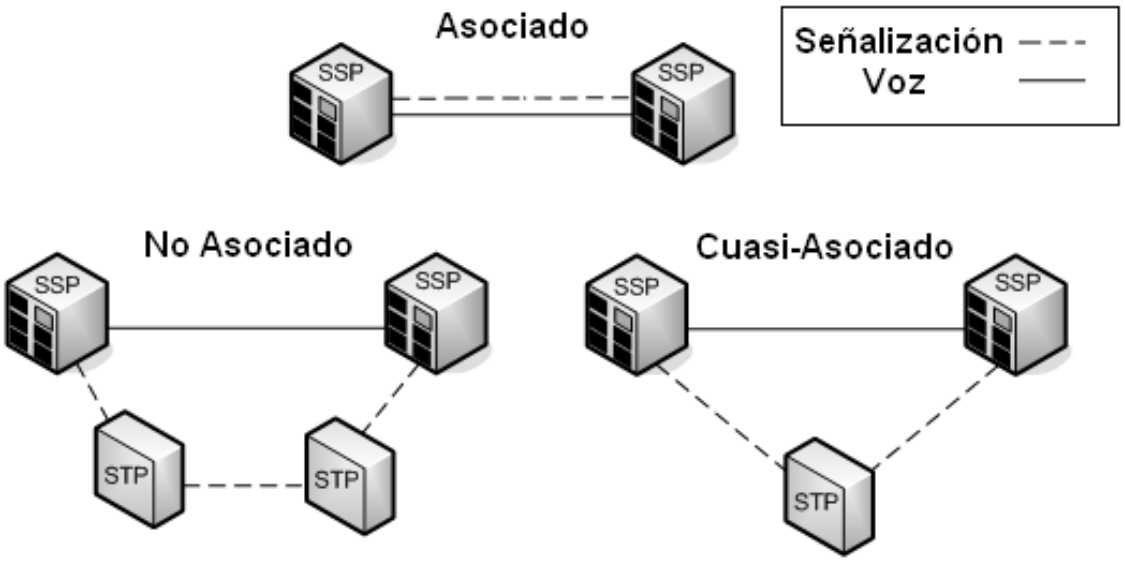

Figura 1.14: Modos de señalización SSCC7

Los enlaces entre elementos de redes SS7 se clasifican en los siguientes tipos:

- Enlace A - De un SSP o un SCP hacia un STP.
- Enlace B (Bridge) - Entre parejas de STP's que operan un mismo nivel jerárquico.
- Enlace C (Cross) - De un STP hacia un STP de respaldo.
- Enlace D (Diagonal) - Entre parejas de STP's de distintos niveles jerárquicos.
- Enlace E (Extended) - De STP a STP alternativo en distintos niveles de jerarquía. Son poco comunes.
- Enlace F - Entre SSP's que utilizan la misma trayectoria para Voz y señalización. Se usan cuando no existen STP's disponibles. Comunes en México y Europa.

Todos los puntos de señalización tienen rutas predefinidas, pero a la vez dentro de sus tablas cuentan con rutas alternas con el fin de garantizar la conetividad lógica entre todos los elementos.

Señalización por Canal Asociado (CAS) MFC/R2

El sistema de señalización por canal asociado más ampliamente usado en nuestro país y en diversos lugares es el MFC/R2[7]. Éste es un protocolo de señalización para telefonía cuya antigüedad es de unos 50 años. Fue originalmente diseñado para transmitir señalización entre registros (Switches), sobre pares de cobre analógicos a una velocidad aún mayor de la que era posible usando pulsos[7] . Su nombre completo es Multi-Frecuency Compelled Region 2 Signaling System y tiene distintas variantes dependiendo del país donde es usado; sin embargo, todas ellas se encuentran basadas en la serie de especificaciones ITU-T Q.400. En el caso de México es conveniente revisar la Norma Oficial Mexicana NOM-EM-012-SCT1-1994 referente a los métodos de transmisión entre centrales telefónicas privadas.

Históricamente las primeras versiones del protocolo fueron analógicas. Al surgir los circuitos digitales E1, el protocolo MFC/R2 sufrió adaptaciones para trabajar sobre estos. Hoy en día coexisten tanto la versión analógica como la digital; sin embargo, es ésta última la que sigue siendo usada ampliamente en muchos lugares del mundo, por ejemplo, México.

MFC/R2 es señalización "peer to peer", lo cual significa que ambos lados son iguales desde el punto de vista de la señalización, es decir, no existe un "cliente" y un "servidor", por lo que ambos lados del enlace operan de la misma forma.

Existen dos tipos de señalización dentro de MFC/R2, estas son: señalización de línea (Definida en ITU-T Q.421) y señalización entre registros (ITU-T Q.441). La señalización de línea se utiliza para representar el estado de la línea (ocupada, libre, congestión, bloqueo, etc.). Para lograr esto, se utilizan cuatro bits (ABCD) del canal 16 del E1(Ver figura 1.15). Cada bit tiene un significado; sin embargo, los bits C y D son rara vez empleados y generalmente se fijan a los valores 0 y 1 correspondientemente, siendo éste el caso de México.

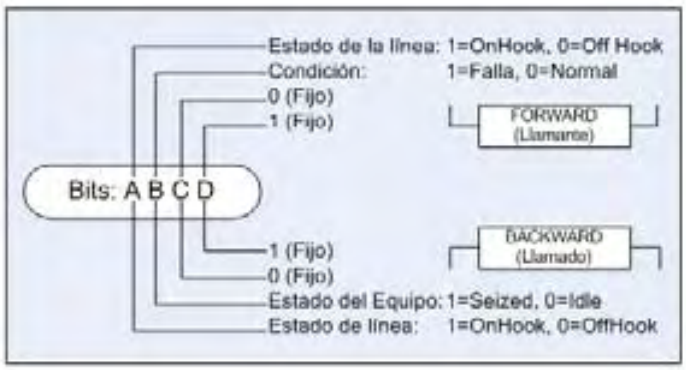

Figura 1.15: Significado de los bits ABCD

[7] `http://www.soft-switch.org/unicall/mfcr2/` - Steve Underwood - *The MFC/R2 protocol module for Unicall* - User manual - 2005

Es pertinente que revisemos antes dos conceptos importantes. Nos referimos a las señales hacia adelante y hacia atrás o de ida y de regreso de las llamadas, comúnmente Forward y Backward. Se definen como señales hacia adelante (Forward) aquellas que viajan desde el extremo que originó la llamada (llamante) hacia el extremo receptor (llamado). En contraparte, las señales hacia atrás (Backward) viajan en sentido opuesto.

En la tabla 1.2 se muestran los distintos códigos y estados relacionados para la señalización de línea según la recomendación ITU-T Q.421. Por otro lado, en la tabla 1.3 se muestra la codificación de línea aplicada en México[8] .

Estado del Circuito	FORWARD Bits Af Bf	BACKWARD Bits Ab Bb
Idle/Released	1 0	1 0
Seized	0 0	1 0
Seizure Acknowledge	0 0	1 1
Answered	0 0	0 1
Clear-back	0 0	1 1
Clear Forward	1 0	0 1
Clear Forward	1 0	1 1
Blocked	1 0	1 1

Tabla 1.2: Señalización de línea MFC/R2 ITU-T Q.421

Número	Estado del Circuito	FORWARD Bits Af Bf	BACKWARD Bits Ab Bb
1	Libre	1 0	1 0
2	Toma	0 0	1 0
3	Acuse de recibo/toma	0 0	1 1
4	Señal de registro MFC/DTMF	0 0	1 1
5	Contestación después de 4 ó 7	0 0	0 1
6	Conservación	0 0	0 1
7	Reposición	0 0	1 1
8	Desconexión después de 3, 4 y 7	1 0	1 1
8’	Desconexión después de 5 y 6	1 0	1 1
9	Liberación de Seguridad	1 0	1 0
10	Bloqueo después de 1 y 8	1 0	1 1
11	Desbloqueo	1 0	1 0

Tabla 1.3: Señalización de línea MFC/R2 México

En cuanto a la señalización entre registros se refiere, éstas son señales multitono compuestas por 2 frecuencias de un conjunto de 6 [9] . Por lo tanto, existen 15 combinaciones

[8] Manual NEC 7400 ICSa MFC Signallling

[9] Por esta razón también es denominada señalización 2 de 6

posibles y en consecuencia 15 códigos diferentes. Tales frecuencias se encuentran dentro del ancho de banda de la Voz humana, es por ello que esta señalización es conocida como señalización en banda. Las señales multifrecuencia usadas para la señalización entre registros viajan en el *slot* (ranura de tiempo), correspondiente al canal de señalización, es decir, junto con la propia voz.

De forma análoga a la señalización de línea, en la señalización entre registros encontramos señales hacia adelante y hacia atrás. En la tabla 1.4 se resumen los códigos utilizados para tal efecto. Nótese como existen diversos grupos que representan diferentes etapas en el proceso de direccionamiento y estableciemiento de una llamada. La tabla 1.4 esta basada en la recomendación de la ITU-T Q.441. En la tabla 1.5 se muestra la variante usada en México (vease la Norma Oficial Mexicana [5]).

Código	Grupo I FW	Grupo II FW	Grupo A BW	Grupo B BW
1	Dígito 1	Subscriptor s/prioridad	Sig. dígito (n+1)	*Reservado p/uso nacional
2	Dígito 2	Subscriptor c/prioridad	Dígito (n-1)	Envía tono de inf. especial
3	Dígito 3	Equipo en mantenimiento	Direccionamiento completo, cambiar a recepción de señales G-B	Línea ocupada
4	Dígito 4	*	Congestión en red nacional	Congestión luego de cambio de grupo A a B
5	Dígito 5	Operadora	Enviar categoría del llamante	Número no encontrado
6	Dígito 6	Transmisión de Datos	Direccionamiento completado, cargo, listo para conversar	línea libre (cargos)
7	Dígito 7	Subscriptor u operadora sin facilidad de transferencia	Dígito (n-2)	Línea libre (s/cargos)
8	Dígito 8	Tranmisión de datos	Dígito (n-3)	Línea fuera de servicio
9	Dígito 9	Subscriptor c/prioridad	*	*
10	Dígito 0	Operadora con facilidad de transferencia	*	*
11	Indicador de código país (CC), supresión de eco saliente	*	Envía indicador CC	*
12	Indicador CC, sin supresión de eco	*	Envía idioma o dígito discriminante	*
13	Indicador llamada de prueba	*	Envíe tipo de circuito	*
14	Indicador CC, supresión de eco saliente insertada	*	Petición de info sobre supresión de eco	*
15	No usada	*	Congestión en línea internacional	*

Tabla 1.4: Códigos para señalización interregistros MFC/R2 ITU-T Q.441

En México se distinguen tres grupos de señales hacia adelante, G-I, G-II y G-III. Los códigos utilizados por cada grupo son los mismos, sólo cambia su significado en función de la etapa en el proceso de establecimiento de la llamada. El Grupo I contendrá la información referente al destino, el Grupo II informa al otro extremo sobre la categoría del origen de la llamada, es decir, si es un subscriptor ordinario, un equipo en mantenimiento, una cabina telefónica de monedas, etc., el Grupo III de señales hacia adelante se utiliza para transmitir información sobre el origen de la llamada (número del llamante, comúnmente conocido como Caller-ID).

Por su parte, los grupos de señales hacia atrás denominados G-A, G-B y G-C transmitiran peticiones de información sobre el destino, información sobre el estado de la línea y peticiones de información sobre el origen de la llamada respectivamente. Son, digámoslo así, "señales de acuse de recibo" para los grupos de señales hacia adelante.

Código	Grupo I	Grupo II	Grupo III	Grupo A	Grupo B	Grupo C
1	Dígito 1	Operadora	Dígito 1	Envía señal G-I Dígito (n+1)	Línea libre con cargo	Envía señal G-III primer y siguiente Dígito
2	Dígito 2	Subcriptor ordinario	Dígito 2	Envía primer dígito	línea ocupada	Envía señal G-I primer dígito y cambia a recepción G-A
3	Dígito 3	*Reservado	Dígito 3	Envía señal G-II y cambia a recepción señales G-B	*	Envía señal G-II y cambia a recepción señales G-B
4	Dígito 4	*	Dígito 4	Congestión	Bloqueo	Congestión
5	Dígito 5	*	Dígito 5	*	*	Envía señal G-I prox. dígito y cambia a recepción G-A
6	Dígito 6	*	Dígito 6			Envía señal G-I mismo dígito y cambia a recepción G-A
7	Dígito 7	*	Dígito 7	*	*	*
8	Dígito 8	*	Dígito 8	*	*	*
9	Dígito 9	*	Dígito 9	*	*	*
10	Dígito 0 (LADA)	*	Dígito 0	*	*	*
15	*	Fin de numeración	*	*	*	*

Tabla 1.5: Códigos para señalización interregistros MFC/R2 México

En la figura 1.16 se ejemplifica un trazado en el tiempo, que muestra la operación del protocolo MFC/R2. Los trazados están hechos de acuerdo con los grupos de señales definidos por la ITU-T serie Q.400. En este escenario, el usuario conectado al switch "A" inicia la llamada al descolgar el auricular y marcar los dígitos DTMF (señalización usuario - red), posteriormente el conmutador "A" manda señal de toma de línea (*seize*)

al conmutador "B" y éste contesta con una señal de acuse de recibo (*ACK*) con lo cual el switch "A" es invitado a enviar los dígitos marcados (*señalización entre registros*). Una vez completado el número, el switch "A" envía otra señal que contiene información sobre la categoría del usuario llamante (si es un usuario normal, con privilegios, etc.) para que el extremo "B" sepa como procesar esta llamada. En este caso, al tratarse de un subscriptor normal, el switch "B" transmitirá la llamada al usuario destino enviándole un tono de timbrado (*RING*) y regresando hacia el switch "A" el mismo tono (*RINGBACK*). Cuando el usuario llamado descuelga el auricular (*Off-hook*), el conmutador "B" entiende que la llamada ha sido contestada y manda esa respuesta al conmutador "A", estableciendose así el circuito para la conversación. Finalmente, en nuestro ejemplo el usuario "B" termina la llamada (*On-hook*) y el switch "B" transmite una señal de liberación del canal (*CLEAR-BACK*) a la cual el switch "A" contesta con la señal correspondiente (*CLEAR-FORWARD*), de esta forma el canal es liberado y puede ser usado para una nueva conversación.

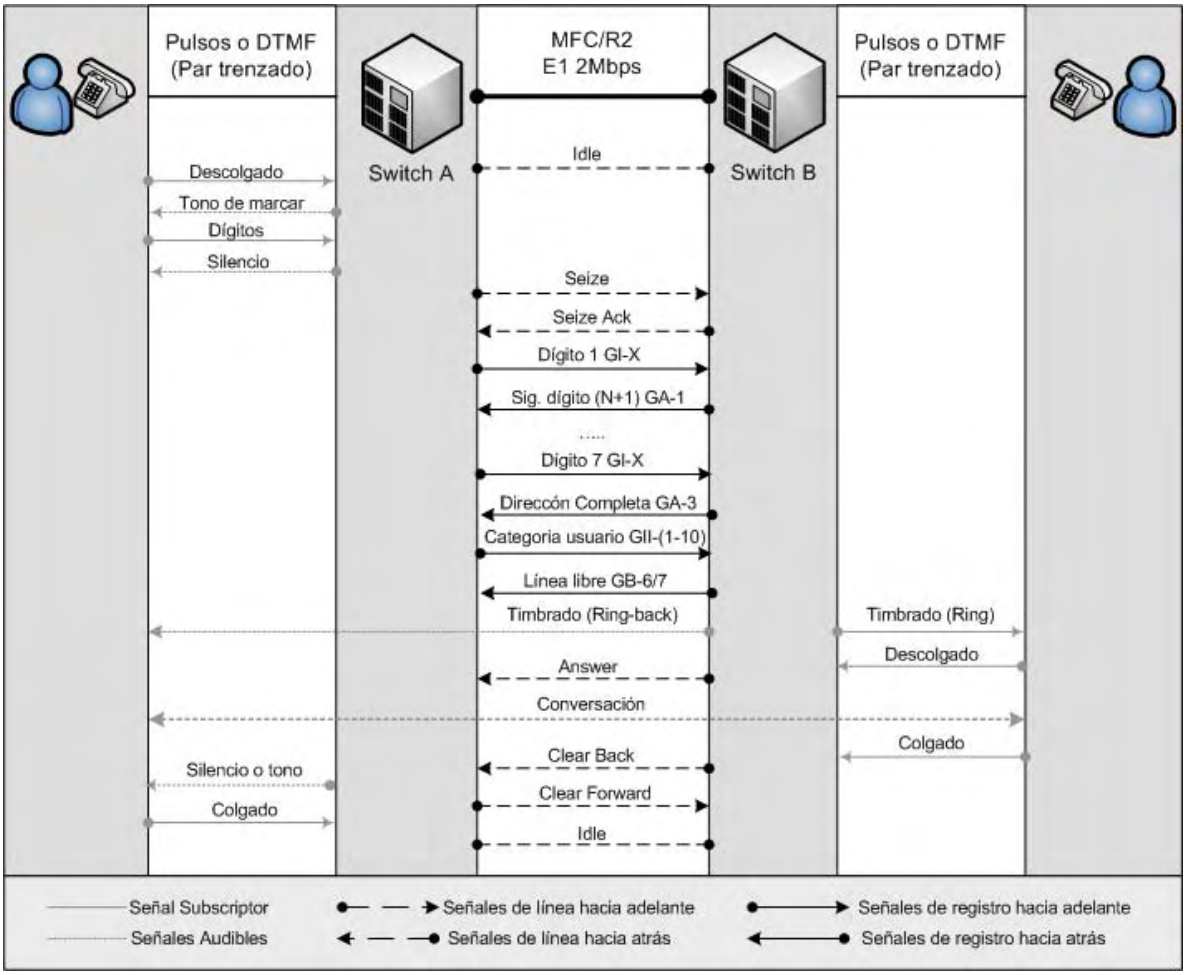

Figura 1.16: Trazado MFC/R2 (ITU-T Q.421 y Q.441)

Q.SIG

Es un sistema de señalización punto a punto para redes corporativas de Voz. Q.SIG es un protocolo basado en RDSI, ITU-T Q.931(Véase sección 1.1.2 referente a RDSI *ISDN*), desarrollado para interconectar sistemas de conmutación pertenecientes a distintas marcas y que soporten servicios suplementarios de manera transparente como: Caller ID, Transferencia de llamadas, etc.

Q.SIG esta basado en estándares, que permiten la interconexión de equipos de distintos fabricantes, así como la interconexión transparente entre PBX, interoperabilidad con la RDSI y No impone restricciones en planes de numeración privados.

Q.SIG tiene sus orígenes en los estándares definidos por la ECMA (European Computer Manufacturing Asociation) a mediados de los 80's. A principios de los 90's, estos estándares fueron remitidos a la ISO para su globalización y, luego de algunas adaptaciones de acuerdo con los requerimientos de otros países, fueron publicados como estándares globales en 1994.

Q.SIG es de gran utilidad en los sitios en donde se desea o se requieren extender los servicios de comunicaciones entre equipos de diferentes marcas sin tener que sacrificar la eficiencia del sistema al pasar por la red pública. Q.SIG nunca será rival de los protocolos propietarios (como NEC CCIS); sin embargo, es una opción para obtener un alto nivel de integración entre diversos fabricantes.

Los servicios que brinda la tecnología Q.SIG son los siguientes:

- Servicio Básico (QSIG-BC), para configurar y terminar llamadas.
- Servicio de Funciones Genéricas (QSIG-GF) que permiten la interoperabilidad entre fabricantes con sistemas no estandarizados.
- Servicios suplementarios tales como: transferencia de llamadas, reenvío, estacionamiento de llamadas, identificador de llamantes, etc.

1.1.4. Servicios y facilidades en la telefonía tradicional

Los principales servicios y facilidades que una Red de Voz (privadas por lo general) es capaz de brindar actualmente son los siguientes:

- Transferencia de llamadas con y sin supervisión (Call transfer).

  Permite trasferir una llamada hacia otra extensión. Cuando la transferencia es supervisada, la extensión que originó la llamada "A" queda en espera y la que transfiere la llamada "B" intenta conectarse con la extensión destino "C", si la llamada es contestada, entonces "B" puede colgar anunciando a "C" que tiene un llamada y la conversación se establecerá entre los extremo "A" y "C". Si la transferencia se realiza sin supervisión (Blind Transfer en inglés), entonces "B" se limita a marcar el código de transferencia y automáticamente el sistema

intentará establecer comunicación entre "A" y "C", pero "B" no supervisará si se completa o no la llamada.

- Reenvío de llamada incondicional, en estado ocupado, en estado de no contesta o no disponible y en estado de no molestar (Call Forwarding).

  Cuando se realiza un reenvío incondicional el sistema automáticamente reenvía la llamada hacia otra extensión previamente establecida por el usuario. Este tipo de reenvío también se conoce como *Sígueme* (Followme en inglés). Puede intuirse naturalmente la operación de las modalidades ocupado, no contesta/no disponible y DND.

- Buzón de Voz (Voicemail).

  Es un servicio que permite que los llamantes depositar un mensaje hablado dirigido al usuario en caso de que este no sea capaz de contestar su extensión. El mensaje es almacenado en un espacio de memoria del sistema y el usuario puede consultarlo, posteriormente mediante el uso de un código de servicio más un identificador de buzón y una clave de acceso. Algunos sistemas incorporan recordatorios automáticos para avisar al usuario que cuenta con X mensajes nuevos en su buzón.

- Llamada en espera (Call Waiting).

  Cuando se cuenta sólo con una línea y está ocupada, las llamadas entrantes se anunciarán mediante un timbre distintivo. La extensión destino podrá intercambiar entre una y otra mediante un botón especial o un código dejando en espera de forma alternada a sus llamantes, pero sin perder la comunicación con ninguno de ellos.

- Captura de llamada (Call Pickup).

  Cuando suena una extensión dentro de un grupo de extensiones, al cual llamamos grupo de captura, es posible que cualquiera de ellas "capture" la llamada mediante un código o tecla especial.

- No molestar (DND).

  Con esta función se bloquea el ingreso de llamadas hacia nuestra extensión. Generalmente éstas son redirigidas hacia el Buzón de Voz. El sistema además incorpora un anuncio recordando al usuario que tiene esta facilidad activada. Lo anterior evita que el usuario piense que existe alguna falla en su extensión al no recibir llamadas y haber olvidado que tiene el DND activo.

- Marcado rápido (Speed Dial).

  Algunos aparatos telefónicos incorporan una memoria para que el usuario almacene los números más frecuentemente marcados y los relacione con una tecla del mismo aparato con la finalidad de no tener que remarcarlo completamente. Cuando el aparato no posee estas características, también es posible realizar esta facilidad a través del sistema (Conmutador), siendo éste quien almacena en su memoria los números de marcado rápidos de cada extensión.

- Estacionamiento de llamadas (Call Parking).

  Esta facilidad permite a un usuario "estacionar" una llamada entrante dejándola en espera por un tiempo determinado, pero al mismo tiempo liberando la extensión desde donde fue estacionada, luego entonces, es posible recuperar la llamada

desde otra extensión haciendo uso de una clave. Las llamadas no quedan estacionadas indefinidamente, sino que son liberadas cuando se excede un tiempo máximo de espera.

- Directorio Institucional
  Algunas soluciones de telefonía tradicional incorporan esta funcionalidad en la cual el sistema busca la extensión de una persona por medio de las tres primeras letras de su apellido ingresadas desde el teclado telefónico, en caso de que desconozcamos el número.
- Remarcado del último número (Last Number Redial)

  Con este servicio el sistema marcará automáticamente por nosotros el último número marcado desde nuestra extensión. Ahora es muy común encontrar un botón especial en el aparato telefónico que nos permite realizar esta función.
- Acceso Directo al Sistema (DISA)

  Mediante este servicio es posible obtener tono interno de una Red privada a través de otra pública o privada. Esto es útil para reducir costos y acceder a servicios de nuestro propio sistema desde una extensión no perteneciente a él.
- Identificador de llamadas (Caller ID).

  Esta es quizás la facilidad más conocida por la mayoría de las personas y nos sirve para identificar al llamante antes de contestar.
- Música en espera (Music on Hold).

  Cuando se deja en espera a un llamante, la sensación de silencio es molesta y genera ansiedad; por ello se incorporan sistemas de música en espera que reproducen una melodía, mientras el usuario es atendido.
- Grupos de llamadas (Ring Groups).

  Esta facilidad es empleada sobre todo en los Centros de Atención Telefónica (Call Centers) en donde una llamada entrante hace que varias extensiones timbren, ya sea al mismo tiempo, en secuencia o de forma incremental dependiendo de la estrategia. Una vez que alguna de las extensiones conteste la llamada, las demás dejan de timbrar.
- Troncales Analógicas (Trunks).

  El uso de troncales es requerido cuando necesitamos realizar llamadas hacia otros sistemas no pertenecientes a nuestra Red de Voz, por ejemplo: llamadas locales hacia otras empresas o personas, llamadas de larga distancia, llamadas hacia Red de telefonía celular, etc.
- Conferencias Telefónicas (Conference Rooms)

  Se trata de un servicio poco conocido, que no poco común, pues nos permite establecer una conferencia de Voz entre diferentes personas que de otra forma no estarían en condiciones de asistir a una reunión personalmente. Existen al menos dos modalidades de salas de conferencia, con y sin administrador. La primera es libre, cualquiera puede crear una sala de conferencia e ingresar en ella, mientras que la segunda es más restrictiva, pues se requiere una clave para ingresar al cuarto y además incorpora un administrador, el cual decide cuando se abre y cierra el cuarto de conferencia.

- Colas de llamadas (Queues).

  Es similar a las llamadas en espera. En esta modalidad más de una llamada se pone en una cola en tanto exista una extensión libre, (*agente*), que la atienda. Su uso es esencial en Centros de Atención Telefónica. Quién de nosotros no ha eschuchado algo como: "Por el momento ninguno de nuestros agentes está disponible, le suplicamos esperar en la línea en tanto se libere uno de nuestros agentes para atenderle, gracias."

- Contestadora Automática por Guía Auditiva (IVR).

  Esta es una facilidad muy conocida. Con ella es posible atender de forma automática a miles de usuarios. El IVR es una contestadora compuesta de menús de voz en niveles y con la cual el usuario interactúa por medio de su teclado telefónico. El sistema interpreta la tecla o combinación de ellas para pasar al siguiente nivel o dar una respuesta a la consulta del usuario.

- Retrollamada (Callback)

  Cuando deseamos que el sistema reintente marcar por nosotros después de un tiempo dado en caso de que nuestro primer intento haya fallado recurrimos a la facilidad denominada Call Back.

- Voceo e Intercom (Paging & Intercom).

  Al activar el voceo en una terminal, se envía un mensaje a todas las terminales del grupo por medio del altavoz. No importa si las extensiones se encuentran ocupadas, el voceo activa el altavoz e interrumpe toda actividad.

1.2. Redes de Datos

Actualmente, las redes computacionales son muy grandes y complejas. Sin embargo, es importante tener en cuenta que el crecimiento de las redes de datos se encuentra estrechamente ligado a las redes de Voz, quienes fueron las primeras redes de caracter mundial. Es por ello que mucha de la experiencia adquirida en el desarrollo de las redes de Voz fue retomada para el diseño y operación de las actuales redes informáticas. A continuación exponemos algunos de los elementos que consideramos clave para el entendimiento de las redes de computadoras.

1.2.1. Antecedentes

El antecedente más notable de las redes de datos, es la Red creada a finales de la década de los 70's por la Agencia para Proyectos de Investigación Avanzada en Redes del Departamento de Defensa de los Estados Unidos llamada ARPANET (*Advanced Research Projects Agency NETwork*). Debido a la naturaleza de esta Red, de caracter militar, podemos comprender algunas de las directivas que tenía. En esta primera Red se establecen las bases fundamentales de lo que ahora es la Internet.

- No existe autoridad central.
- Todos los nodos en la red tienen el mismo estatus y la misma capacidad de enviar, recibir y transmitir información.
- El mensaje será dividido en paquetes.
- La ruta tomada por el paquete es irrelevante siempre y cuando llegue a su destino.
- El orden de llegada no importa, pues los paquetes son reordenados en el destino.

Estos principios siguen vigentes hasta nuestros días. En realidad la *Red de Redes* esta conformada por múltiples Redes autónomas interconectadas entre sí, a través de enlaces dedicados de alta velocidad, la mayoría de ellos rentados a proveedores de servicios de telefonía. La gestión de esta Red no es centralizada en tanto que nadie es dueño absoluto de la misma, sino más bien, es administrada de forma coordinada a través de instancias reguladoras como la Internet Society (ISOC), la Internet Engineering Task Force (IETF); por citar algunas (véase la referencia [12] donde se explica mas detalladamente el funcionamiento y orgacización de la Internet). Otras como la W3C (Worl Wide Web Consortium) aún no son reconocidas oficialmente; sin embargo, juegan un rol importante en la definición y desarrollo de nuevos protocolos para la Internet.

Citando textualmente a Steven Shepard [12], "Juntas, todas estas organizaciones aseguran que la Internet opere como un sólo organismo de forma coordinada. Esto es notable, ¿no lo creen así? La Red menos administrada del mundo y al mismo tiempo la más grande, es también, la que mejor funciona."

1.2.2. El modelo OSI

En cuanto comenzó la batalla por imponerse en el amplio mundo de los protocolos de Red, se hizó necesario establecer estándares que garantizarán la interconectividad entre sistemas de diversos fabricantes. El desarrollo inicial fue impulsado por las investigaciones en redes experimentales como ARPANET, esto propició que los fabricantes desarrollaran sus propias "Arquitecturas de Red". Es así como surge el *Modelo de referencia para la Interconexión de Sistemas Abiertos*[10] o modelo OSI por sus siglas en inglés Open Systems Interconection.

Este *modelo de referencia* consiste en siete capas acomodadas una encima de otra, es decir, apiladas (en stack). Cada capa desempeña un conjunto de funciones específicas que brindan servicio a una capa superior y reciben servicios de la capa inferior. En un sistema de comunicaciones basado en el modelo de referencia OSI, sólo las capas que tengan su equivalente en el extremo remoto podrán comunicarse entre sí. La información viaja en forma de paquetes a través de todas y cada una de las capas del modelo, cada una de ellas agrega información de control al paquete de información. A este proceso se le conoce como encapsulamiento.

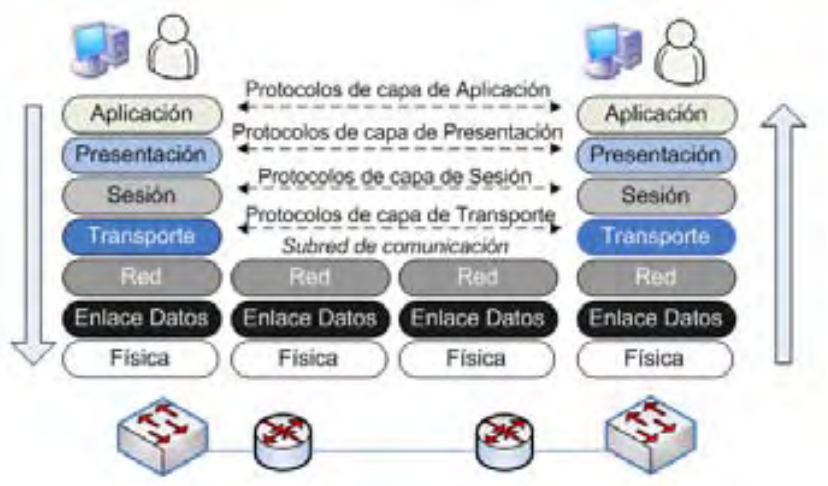

Figura 1.17: Modelo OSI

A cada una de las siete capas se le ha asignado un nombre de acuerdo con las actividades o funciones que realiza. Así tenemos, de arriba hacia abajo, las capas de Aplicación, Presentación, Sesión, Transporte, Red, Enlace y Física.

La capa de *aplicación* es la capa más alta en la arquitectura del modelo OSI. Todas las demás capas existen sólo para brindar soporte a ésta. Los protocolos de esta capa

[10] En 1977 la ISO creó el comite SC16 encargado de desarrollar un modelo de referencia, 18 meses después de la primera junta del comite sucedida en marzo de 1978 el modelo estaba terminado y pasó al comite técnico TC97 en donde a fines de 1979 fue adoptado para servir de base para la definición de estándares.

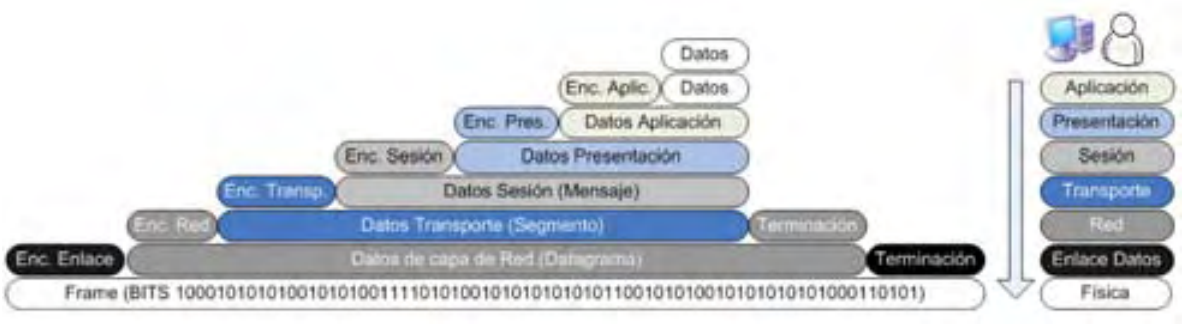

Figura 1.18: Encapsulamiento

sirven directamente al usuario final. Algunos ejemplos de protocolos que funcionan en la capa 7 son: SSH, FTP, Telnet, HTTP, SMTP, etc.

Por su parte, la capa de *presentación* tiene como propósito, el proporcionar un conjunto de servicios que pueden ser seleccionados por la capa de aplicación para poder interpretar el significado de los datos intercambiados. Se encarga, pues de la representación de la información. Esto es necesario debido a que distintos equipos representan los caracteres de forma diferente internamente. De esta manera, no importa la representación interna de los datos (ASCII, EBCDIC, Intel, Motorola, etc.), pues la capa de presentación se encarga de que lleguen de manera reconocible.

La capa de *Sesión* inicia, mantiene y finaliza las conexiones entre usuarios (procesos o aplicaciones) finales. Es la que se encarga de mantener el enlace entre dos computadoras para que estén trasmitiendo información. Esta capa realiza los siguientes servicios: *Administración de la sesión (vinculando y desvinculando a las entidades de presentación)* y *Diálogo de sesión.*

La capa de *transporte* existe para dar los servicios de transporte de datos en asociación con los servicios provistos por los niveles inferiores. Su función básica es aceptar la información enviada por las capas superiores, dividirla en pequeñas partes si es necesario, y pasarla a la capa de red. Acepta dos modalidades de envío de los datos, la primera es la que garantiza que los paquetes arriven a su destino en el mismo orden en que fueron creados y libre de errores, mientras que la segunda no garantiza la llegada de los paquetes en su secuencia original, pero si garantiza que todos lleguen al destino por medio de la retransmisión de aquellos paquetes perdidos en el proceso. Los dos principales protocolos que operan en este nivel son TCP y UDP. En el caso de UDP no se garantiza la completa transmisión de todos los datos, sin embargo es más rápido y útil para trasmisiones en tiempo real como Voz y Video. Por otro lado TCP puede garantizar que todos los paquetes lleguen en orden y sin errores, aunque es más lento que UDP.

La función de la capa de *red* es hacer que los datos lleguen desde el origen al destino, aún cuando ambos extremos no se encuentren conectados directamente. Los dispositivos que facilitan tal tarea se denominan “routers” en inglés o encaminadores en castellano,

aunque es más común encontrar el término inglés y, en ocasiones enrutadores.

Adicionalmente, la capa de red debe administrar el tráfico de la red y tratar de evitar los congestionamientos en la misma, (Cuello de botella). Un protocolo de capa tres es el conocido Protocolo de Internet IP.

La capa de *Enlace de Datos* se ocupa del direccionamiento físico, de la topología de la red, del acceso al medio, de la notificación de errores en la distribución ordenada de las tramas y del control de flujo. Todo ello para garantizar una trasmisión sin errores en el medio físico.

Por último, la *capa física* se encarga de definir las características mecánicas, eléctricas, funcionales y de procedimientos para establecer, mantener y liberar las conexiones físicas entre entidades de enlace de datos.

1.2.3. El conjunto de protocolos TCP/IP

Ya mencionamos antes que los inicios de la Internet están estrechamente ligados a la milicia de los Estados Unidos (La Red ARPANET). El protocolo original seleccionado para la Red ARPANET fue llamado NCP (Network Control Protocol), el antecesor de TCP (Transmition Control Protocol). No obstante, NCP no era capaz de direccionar redes ni hosts y no contaba con control de errores extremo a extremo, puesto que se pensaba que ARPANET sería la única Red y el protocolo no requeriría de un método de control de errores ni de direccionamiento hacia otras redes. Entonces, se decidió desarrollar un nuevo protocolo que cumpliera con los requerimientos de un ambiente de Redes de Arquitectura Abierta. La primera versión escrita de lo que a la postre sería el "stack" de protocolos TCP/IP se distribuyó en septiembre de 1973 en una reunión ocurrida en la Universidad Sussex en el Reino Unido.

La primera versión del protocolo TCP fue publicada en un artículo publicado por Robert E. Kahn y Vinton G. Cerf[11] . Ésta incluía un único protocolo, TCP. Fue hasta 1978 que la tarea de controlar las comunicaciones dentro de la Red se dividió entre TCP y el reciente Protocolo de Internet. Por lo que respecta a IP, éste se encarga de enrutar los paquetes de un dispositivo a otro, mientras que TCP tiene la tarea de asegurar la comunicación extremo a extremo. Estos dos protocolos son la columna vertebral de lo que hoy conocemos como el *Stack de Protocolos TCP/IP*. Juntos garantizan que el conjunto de Redes Autónomas conocidas como la Internet funcionen como una única Red Lógica.

TCP/IP está diseñado en una estructura en capas, fundamentada en el estándar de la organización ISO, modelo OSI. Cada una de las capas es responsable de llevar a cabo una tarea específica de la comunicación. A diferencia del modelo OSI, TCP/IP se compone unicamente de 4 capas.

La capa física (Physical Layer) asociada al medio de comunicación físico y de enlace, capa 1 y 2 de OSI, incluye los drivers que controlan las tarjetas de red, (Ethernet, Token Ring, FDDI, etc.), y toda la gestión de la conexión entre el hardware, los cables

[11] `http://www.isoc.org/internet/history/brief.shtml`

Figura 1.19: Modelo Jerárquico TCP/IP

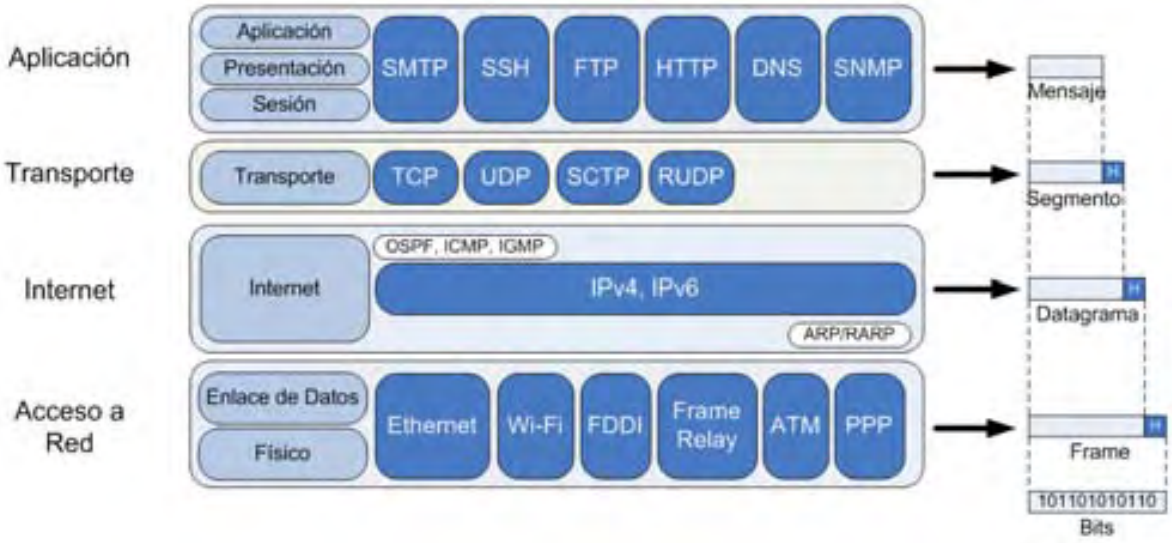

Figura 1.20: Stack de Protocolos TCP/IP

y dispositivos de red. Los protocolos asociados a este nivel no pertenecen propiamente a TCP/IP, pero son la base sobre la que éste se desarrolla.

La capa de red (Network Layer, o capa 3 de OSI) se encarga del envío y recepción de los paquetes a través de la red, así como de encaminarlos por las diferentes rutas que deben recorrer para llegar a su destino. Principalmente el protocolo IP, junto a ICMP.

La capa de transporte (Transport Layer, o capa 4 de OSI) se encarga de manejar los flujos de datos entre equipos. Existen dos protocolos principales a este nivel: TCP, un protocolo fiable y orientado a conexión, y UDP, un protocolo más simple que no garantiza la recepción de los datos y no orientado a conexión pero que es más rápido en comparación con TCP.

Por último la capa de aplicación (Application Layer, que en OSI corresponde a las capas 5, 6, 7) gestiona las características de las comunicaciones propias de la aplicación. En TCP/IP en este nivel se encuentran numerosos protocolos, como Telnet, FTP, HTTP, SNMP, NFS, NNTP, etc.

1.2.4. Capa de acceso a Red - La tecnología Ethernet

La tecnología Ethernet[12] es la más difundida y usada en la actualidad en las Redes de Datos de Área Local (LAN). Ethernet esta basada en la transmisión de tramas de datos. Ésta tecnología define las características del cableado y señalización a *nivel físico* y los formatos de trama a nivel de *enlace de datos* del modelo OSI. Aunque la historia de Ethernet se encuentra ligada a la empresa Xerox, donde la tecnología fue desarrollada, la versión actual esta definida en el estándar 802.3 de la IEEE.

Las tecnologías de redes de área local basan su funcionamiento en el hecho de que el medio de transmisión, ya sea fibra óptica, cobre o radiofrecuencias, es compartido y por ello es necesario optimizar al máximo su uso. Podemos decir, que la diferencia entre Ethernet y otras tecnologías LAN es el algoritmo de *control de acceso al medio* (MAC) que emplean. Mientras que otras tecnologías emplean métodos de acceso como el de estafeta con paso de testigo en topología anillo (p. ej. Token Ring o FDDI), Ethernet emplea el método conocido como CSMA/CD (Carrier Sense Multiple Access with Colision Detect) que podemos traducir al español como: Acceso Múltiple por Sensado de Portadora con Detección de Colisiones. Estos algoritmos se encuentran implementados en la tarjeta de Interfase de Red (NIC por sus siglas en inglés). A cada tarjeta controladora de Red se le asigna un identificador único formado por 12 dígitos hexadecimales (48 bits = 6 Bytes) conocido como dirección física[13] o "MAC address"(Ver figura 1.21).

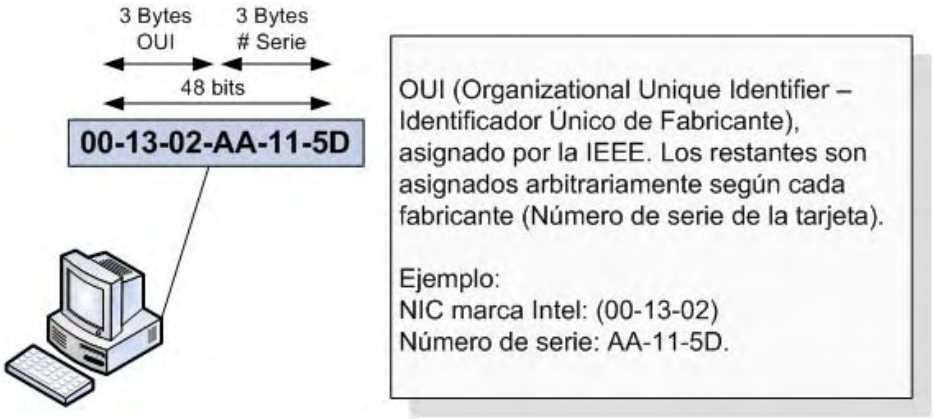

Figura 1.21: Composición de la dirección física (MAC Address)

La idea básica es simple, las estaciones deben detectar si el canal ya esta en uso antes de transmitir, es decir, si existe "portadora", en cuyo caso esperarán a que la estación activa termine para poder iniciar transmisiones. Cuando una estación se encuentre transmitiendo, estará continuamente vigilando el medio físico por si se produce alguna

[12] `http://en.wikipedia.org/wiki/Ethernet`
[13] Las direcciones físicas se encuentran grabadas de forma permanente en el Hardware

colisión, si está se produce dejaran de transmitir y retransmitirá más tarde, esperando un tiempo aleatorio para evitar una nueva colisión.

La trama Ethernet (Ver figura 1.22) se compone de:

- *Preámbulo*: Es una secuencia de bits empleada para sincronizar y estabilizar el medio físico antes de la transmisión de datos. Este patrón representa una forma de onda periódica.
- *Start Of Frame*: Patrón de 1 Byte de longitud que sirve para indicar el inicio de un frame (10101011).
- *MAC Destino*: Indica la dirección física (en formato EUI-48), hacia la cual se dirige el frame o trama.
- *MAC Origen*: Indica la dirección física origen del frame o trama.
- *Tipo*: Indica el protocolo de Red de alto nivel asociado con el paquete o en su defecto la longitud del campo de datos.
- *Datos*: Es la carga útil de la trama.
- *Frame Check Sequence - Secuencia de Verificación de Trama*: Contiene un valor de verificación CRC (Control de Redundancia Cíclica), que es calculado con los datos de la trama con el fin de verificar la integridad de la misma.

Preámbulo	SOF	MAC Destino	MAC Origen	Tipo	Datos	FCS
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 a 1500 Bytes	4 Bytes

Figura 1.22: Trama Ethernet

La tecnología Ethernet ha conseguido una notable aceptación. Aunque inicialmente Ethernet fue pensado para cubrir las necesidades de redes LAN, en la actualidad Ethernet ha alcanzado una tasa de transmisión de 10 Gbps, lo cual la convierte en seria candidata para extenderse a nivel WAN.

1.2.5. Capa de Internet - El sistema de direccionamiento IP

El protocolo de Internet (IP) se localiza en la capa 2 del Modelo TCP/IP (capa de Internet), correspondiente a la capa 3 (capa de Red), del modelo de referencia OSI. El protocolo IP tiene las funciones de: fragmentar los datagramas provenientes de la capa de acceso a Red y encaminarlos por la mejor ruta a través de diversas redes para que lleguen a su destino. El protocolo IP no es orientado a conexión, lo cual quiere decir, que no se preocupa por la correcta entrega de los paquetes, puesto que de eso se encarga la capa de transporte. El proceso de enrutamiento se lleva a cabo por medio del uso de direcciones lógicas, contrario a las direcciones físicas mencionadas en la sección

anterior. Estas direcciones lógicas reciben el nombre de direcciones de red o direcciones IP.

Una dirección IP es un identificador lógico asignado a una interfase de un dispositivo en una Red que utilice el protocolo IP. Las direcciones IPv4[14] se conforman por cuatro octetos, 32 bits en total, separados por un punto decimal. Cada dirección IP se conforma de dos partes, la primera parte corresponde al identificador de Red y la segunda al identificador de Host. Existen dos tipos de direccionamiento IP, el que esta basado en clases classfull (Ver figura 1.23) y el que omite el uso de clases de direcciones (classless)[2]. Existen cinco clases de direcciones IPv4 A, B, C, D y E. En la figura 1.23 se muestran sólo las tres primeras de ellas, que son las disponibles para uso privado. Las direcciones clase D son direcciones especiales empleadas en transmisiones Multicast, como Videoconferencia, mientras que las de clase E están reservadas para uso experimental.

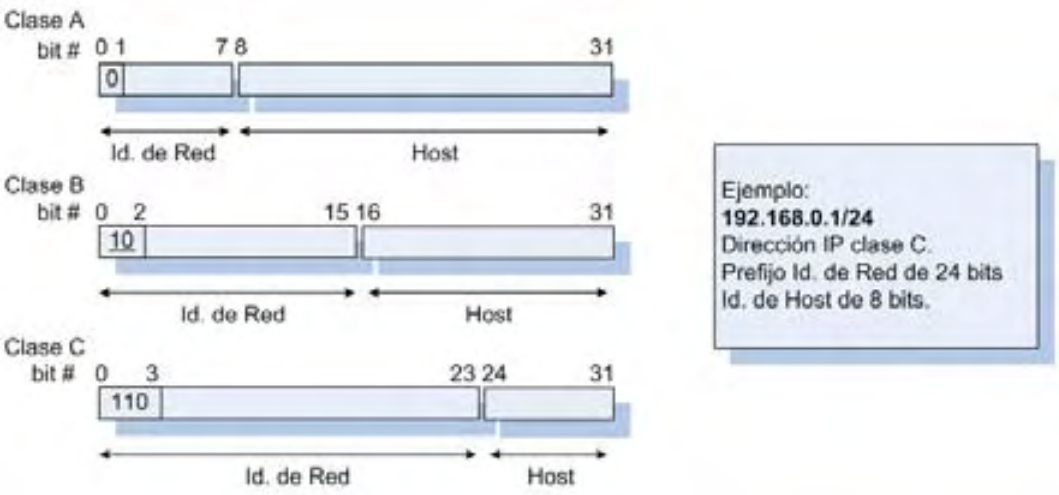

Figura 1.23: Direccionamiento IP por clases

La ventaja del direccionamiento "classfull" es que se incluye en la misma dirección la clave (bits más significativos del primer octeto) que indica la clase a la que tal dirección pertenece y por lo tanto el punto de separación entre el identificador de Red y el identificador de Host. Esto simplifica el trabajo de ruteo o al menos lo hacía en los primeros años de la Internet. La desventaja de este sistema es que existe un número reducido de redes que consumen un importante porcentaje del número de direcciones disponibles sin ser aprovechadas en su totalidad; por ejemplo, las redes de clase A son sólo 126 cada una con un número posible de hosts de 16,777,214. A medida que el

[14] Protocolo de Internet versión 4. Actualmente coexiste con la versión 6 del mismo. Se estan migrando de forma gradual los sistemas en IPv4 hacia IPv6. Éste surgió como solución a las carencias del actual IPv4. Mejora en aspectos como seguridad, mayor universo de direcciones, autoconfiguración de Red y Routers, Calidad de Servicio QoS, computación móvil, etc.
Para mayores detalles vea: `http://www.ipv6.org/` y `http://www.ipv6.unam.mx/`

espacio de direcciones se fue agotando[15] , el esquema de direccionamiento por clases redujó su efectividad y fue necesario incorporar un esquema en el cual se pudieran subdividir las enormes redes clase A y B, y así obtener mayor provecho de ellas. Es así como surgió el direccionamiento Classless.

En el direccionamiento classless utiliza el esquema classfull, pero además se recurre al uso de máscaras de Red de longitud variable para relizar un proceso conocido como "subneteo" que no es otra cosa, sino la subdivisión de redes grandes en redes de menor tamaño. La máscara de red esta conformada por unos y ceros. Al aplicar la máscara de Red, la dirección IP se divide ahora en tres partes: el Id. de Red, el Id. de Subred y el Id. de Host, tal y como aparece en la figura 1.24. Al unir el Id. de Red con el de Subred se obtiene lo que se denomina prefijo de Red extendido, que nos ayudará a identificar la subred.

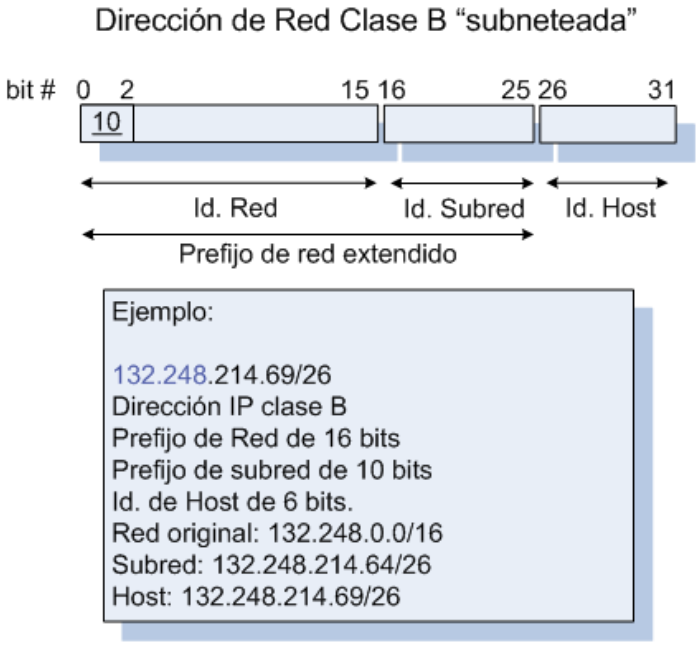

Figura 1.24: Dirección IP "Classless" luego del proceso de subneteo.

1.2.6. Capa de transporte - TCP y UDP

El Protocolo de Control de Transmisión (TCP) opera en el nivel de transporte de los modelos TCP/IP y OSI respectivamente. TCP es un protocolo de comunicación orientado a conexión[16] . Su función es garantizar que los datos sean entregados a su destino final sin errores y en el mismo orden en que fueron transmitidos. Para lograr lo

[15] Las causas han sido: el crecimiento de las redes, la masificación de la Internet y la inequitativa distribución de los segmentos de direcciones IP.

[16] TCP utiliza un proceso denominado *3-way handshaking* para establecer conexiones entre hosts.

anterior, TCP utiliza números de secuencia en cada segmento e incorpora el concepto de "acknowledge" para asegurarse de que el tráfico de usuario es transportado de forma confiable. La unidad de paquete de datos (PDU) fundamental en la capa de transporte se denomina segmento.

Por su parte, UDP (*User Datagram Protocol*) es un protocolo no orientado a conexión y no define métodos como el secuenciado de los paquetes, ni los "acknowlegements" de TCP. UDP es usado cuando no son necesarias todas las capacidades de TCP. Debido a su operación, TCP introduce retrasos de tiempo que van del orden de algunos segundos incluso. Eso es contraproducente para las aplicaciones que requieran de la transmisión de datos en tiempo real, tal y como ocurre en telefonía IP. Es por ello que se prefiere el uso de UDP como protocolo de transporte en lugar de TCP, ya que realiza la entrega de forma más rápida, aunque menos confiable.

Tanto TCP como UDP emplean el concepto de *socket* para la conexión entre extremos. Un socket es un identificador conformado por una dirección IP y un puerto lógico asociado a la aplicación que hace uso de los servicios de TCP o UDP. Debido a que cada dirección debe ser única en toda la Internet, cada socket es un identificador único para cada extremo de la conexión. A los sockets también les llama direcciones de transporte.

Figura 1.25: Estructura del segmento TCP

En la figura 1.25 se ilustra la estructura del segmento TCP. Podemos advertir la presencia de los campos: puerto de destino y origen en el encabezado, el número de secuencia del segmento que es importante por si queremos que los datos lleguen exactamente en el orden en que fuero emitidos o para que sean reordenados en el extremo final, el número de ACK, el offset de datos que especifica el tamaño del encabezado, un campo reservado y los campos de banderas que son bits de control, el tamaño de la ventana que determina la cantidad de bytes a ser recibidos sin pedir confirmación, para agilizar el proceso, la suma de verificación para detectar errores en el encabezado o en los datos, el campo de puntero urgente, el campo de opciones y finalmente la carga útil (Datos).

Por otro lado, en la figura 1.26 podemos advertir la enorme diferencia entre TCP y UDP. Para comenzar el segmento UDP no incorpora métodos de control de la transmisión como el número de secuencia o el ACK. Su estructura es mucho más sencilla y

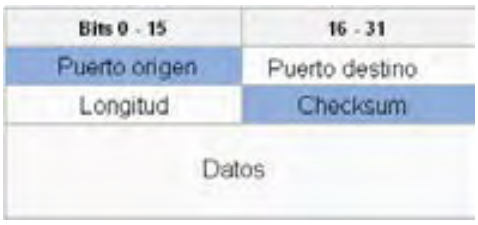

Figura 1.26: Estructura del segmento UDP

sólo incorpora un campo de suma de verificación, más los respectivos campos de puerto de origen y destino, así como el campo de longitud del datagrama entero y la carga útil. Del campo longitud podemos deducir que el tamaño teórico máximo de un datagrama UDP es de 65535 bytes; sin embargo, el límite práctico es de 65,507 bytes.

1.2.7. Capa de aplicación - Los servicios de la Internet

Actualmente, la Internet ofrece una gran cantidad de servicios de comunicación. Entre los más destacados y populares se encuentran: el correo electrónico, la mensajería instantánea, la publicación web de páginas personales (blogs), el *media-streaming* tanto de video como de audio (voz y música) en tiempo real, los servicios peer2peer como Ares o Bittorrent, etc. Ahora bien, estos servicios finales son soportados por otros menos conocidos, pero de suma importancia, que tienen la nada fácil tarea de hacer que los procesos resulten transparentes para el usuario final. Entre los servicios de soporte en la Red de redes tenemos, por ejemplo:

- **El sistema de resolución de nombres de dominio** - Mejor conocido como DNS, cuya misión es traducir nombres de páginas Web como: `www.voip.unam.mx` a su correspondiente dirección IP y viceversa.
- **Los servidores de descarga de archivos por FTP y TFTP** - Este sistema de descarga resulta útil para obtener programas desde el sitio oficial del fabricante.
- **Los servicios de conexión remota** - Telnet en antaño y ahora SSH son las herramientas más empleadas para establecer sesiones remotas en equipos cuyos recursos no son accesibles para cualquier usuario, servidores de aplicaciones por ejemplo.
- **ENUM** - Se perfila como uno de los servicios más interesantes y útiles para los próximos años. Con ENUM se busca que cualquier usuario pueda comunicarse por medio del servicio de su preferencia o el que tenga disponible mediante un único número, éste tendrá un formato de número telefónico convencional. En términos más sencillos, con el mismo número podré hacer una llamada VoIP, recibir un correo electrónico, ingresar a una sala de chat, observar mi página Web personal, etc. Este servicio se basa en el sistema de DNS y actualmente se encuentra en etapa de pruebas.

En las siguientes líneas enlistamos algunos de los principales servicios que la Internet brinda a los usuarios.

- **Correo electrónico** - El correo electrónico fue uno de los servicios iniciales de la era de la Internet y no ha habido quién reniegue de sus bondades. El correo electrónico se ha convertido en una herramienta de trabajo esencial para la operación de cualquier empresa o institución. En este rubro, los principales exponentes son *Hotmail*, *Yahoo* y *Gmail* a nivel público. La capacidad de almacenamiento va en aumento y las interfases son cada vez más funcionales.

- **Publicación de páginas electrónicas** - Hace década y media, el número de páginas electrónicas era reducido y su atractivo era poco menos que inexistente. Hoy en día, prácticamente cualquier persona puede contar con una página personal (Blogs como Hi5 o faceBook) en la red. Las páginas web son un medio incomparable de difusión masiva en nuestros tiempos.

- **Mensajería Instantánea** - Los chats han sido una más de las prestaciones de la Internet que han revolucionado las comunicaciones. El lenguaje utilizado en las salas de chat incluso es materia de analisis y crítica. No solo es posible comunicar ideas por medio de texto, ahora los chats incorporan características como transmisión de Voz y Video, compartición de documentos e imágenes, todo en tiempo real, hacia cualquier parte del mundo y al alcance de un clic. Los servicios de mensajería instantánea más populares son: *ICQ*, *MSN Messenger*, *Yahoo! Messenger* y *Google Talk*.

- **Telefonía IP** - Una más de las aplicaciones que actualmente se encuentra en proceso de crecimiento y que se vislumbra como un nuevo servicio de red. Ejemplos de este servicio son: Vonage, Skype y Ekiga, por mencionar sólo algunos.

- **Comunidades virtuales** - Los internautas han encontrado una forma de colaboración organizada haciendo uso de las herramientas de la Internet, tales como las capacidades de Videoconferencia, las listas de correo electrónico, etc. A este tipo de organizaciones se les denomina comunidades u organizaciones virtuales y están en crecimiento. Las redes sociales se tejen vertiginosamente al mismo ritmo que lo hacen los adelantos tecnológicos en la Web.

- **Wikis y foros** - La forma en que el conocimiento se difunde también ha cambiado. Cada vez es más raro que los estudiantes consulten libros tradicionales para realizar algún trabajo escolar, por lo general consultan y localizan la información que requieren directamente en algún *Wiki* en un "*eBook*", o si se trata de algún problema técnico siempre pueden acudir a los foros para aprender de las experiencias de otras personas con el mismo problema.

- **Servicios de Media Streaming** - En esta categoría encontramos ejemplos como la radio por la Internet y la difusión de videos como ocurre con *youtube*.

- **Motores de búsqueda** - En este punto hemos de destacar la labor que realiza el portal de búsqueda más exitoso. Nos referimos a *google*. Existen otros motores, como el de *Yahoo!*; sin embargo, google es sin duda el más popular y eficaz.
- **Los Peer2Peer** - Hablando de compartición de la información, no existe mejor manera de distribuir archivos de música o video por la Web que los servicios de compartición de archivos como Ares, Bittorrent y Emule entre otros.

1.3. Convergencia de las redes de Voz y Datos

Hasta este momento, hemos visto como las redes tradicionales, tanto de voz como de datos, tenían una topología separada, es decir, la mayoría de las empresas o instituciones contaban o cuentan con una red de Datos y una red de Voz, las cuales usan dispositivos y cableado (infraestructura) separados. Las redes IP integran ambos mundos en una sola red. Sin embargo esta integración plantea diversos retos en si misma, por ejemplo, se requiere de una cuidadosa planificación para asegurar que la calidad de voz pueda ser mantenida correctamente sin pérdidas, ni retardos, esto por tratarse de un tráfico sensible que debe ser transportado en tiempo real.

El proceso de convergencia ha seguido un camino pausado, ya que *se deben proteger las inversiones de los clientes en cuestión de equipo e instalaciones*, de esta forma, se tiende a seguir un modelo híbrido donde conviven PBX tradicionales y PBX habilitados con soporte para redes IP. Sin embargo, esta convergencia de Voz, Datos y Video logrará en algún tiempo que la telefonía sea tratada como una aplicación más de redes. Hoy en día la industria de las telecomunicaciones ha decidido apostar fuerte por una plataforma común sobre el Protocolo de Internet. Para muchas organizaciones, incluyendo instituciones de educación, esto significa una oportunidad de fusionar las aplicaciones existentes con nuevas herramientas de comunicación.

La llegada de la telefonía IP significa una despedida definitiva para los PBX de la telefonía tradicional, estos apenas serán recordados, mientras dure la transición que significará la separación del hardware y el software en materia de telefonía. Lo que la industria ofrecerá a las empresas serán soluciones a partir de aplicaciones en un entorno de software localizado en servidores sobre una infraestructura de comunicaciones de redes convergentes. La tendencia es ofertar comunicaciones directamente hacia los clientes y no hacia las tecnologías propietarias.

En la telefonía IP un PBX puede interactuar con otro PBX sin importar que no sean de la misma marca, tan solo es necesario que utilicen los mismos protocolos de comunicación a través de la Internet. Por tal motivo la infraestructura es parte fundamental de las comunicaciones IP, ya que los sistemas deben conectarse entre sí sobre IP para poder hacer uso de las aplicaciones o servicios.

Por otro lado, la historia reciente nos ha enseñado que los oligopolios en el mundo de las telecomunicaciones son "necesarios" más no suficientes para mantener el ritmo de crecimiento tecnológico del mismo.

> "En condiciones de desarrollo tecnológico acelerado, la capacidad de las empresas tiende a excederse rápidamente, mientras sus márgenes de utilidad son reducidos por el desarrollo tecnológico mismo, tendencia exacerbada por la competencia intensa. Los participantes con poco capital son los primeros en retirarse o en ser absorbidos por aquellos con mayor resistencia, y sólo permanecen los que tienen capital suficiente"[17]

[17] Cota Meza, Ramón, "Informe Telecom" publicado en *Letras Libres* - julio de 2007

La emergencia de la telefonía sobre Internet VoIP y el rápido desarrollo tecnológico obligan a los prestadores de servicios y fabricantes a reemplazar equipo no obsoleto e infraestructura con márgenes de ganancia cada vez menores, en vez de representar una nueva fuente de ingresos. Así las cosas, los actores principales tienen que reducir sus costos de capital anteponiendo el ahorro en la adquisición de equipo nuevo a las ventajas que el mismo promete. El "Software Libre" se vislumbra como una alternativa ante esta situación y Asterisk junto con OpenSER son serias propuestas, dignas de ser tomadas en cuenta.

La convergencia es la impulsora de la telefonía IP.[18] El crecimiento de la telefonía IP en México ha comenzado con el surgimiento de la red de banda ancha y las soluciones IP en materia de telefonía, así como redes privadas virtuales. Aunque el rezago respecto a otros países es evidente, no necesariamente es algo malo, pues siempre se puede aprender de las experiencias de aquellos que van más rápido.

México ocupa uno de los primeros lugares en América Latina en telefonía IP, debido a que las organizaciones están optando por nuevas y mejores soluciones, aprovechando los beneficios de la convergencia. El mercado de la telefonía IP en México ha crecido notoriamente en los últimos años[19] y la tendencia es que ese crecimiento se mantenga constante en los próximos años.

Es importante reiterar que la adopción de soluciones de comunicaciones IP debe estar basada en un análisis profundo para considerar la mejor forma de migrar a la tecnología IP. La tecnología IP, además de la reducción de costos y mejorar los procesos, ofrece el valor agregado de la movilidad a través del acceso remoto, simplificación de la red, buena calidad así como la introducción de nuevas y mejores aplicaciones, lo cual es muy atractivo para las organizaciones.

Resumiendo. En este capítulo se bosquejó el crecimiento y evolución que han experimentado las redes de Voz y Datos. Se hizó enfasis en el hecho de que ambas, aunque separadas, tienen una historia en común. Se concluye que: actualmente se vive un proceso de convergencia tecnológica en el cual confluyen ambos mundos y que una de las aplicaciones de convergencia es la Telefonía IP, la cual es el tema de nuestro próximo capítulo.

[18] Olguín, Adán, "Las Telecomunicaciones y su base de IP", Artículo web sobre convergencia VoIP aparecido en *esemanal* - `http://www.esemanal.com.mx/enviar.php?type=2&id=350`, 2007

[19] el año 2003 era de $56 millones de dólares, para el año 2004 se estima que fue de $63 millones de dólares y la tendencia estima será de $141 millones de dólares para el año 2008.

Capítulo 2

Telefonía IP

La voz sobre redes IP *VoIP (Voice over IP)* inicialmente se implementó para reducir el ancho de banda por medio de procesos de compresión vocal diseñados para sistemas celulares en la década de los años 80. Como consecuencia, el costo del transporte internacional bajo. Luego tuvo aplicaciones en redes de servicios integrados sobre redes LAN y la Internet. Posteriormente, se migró de redes LAN (aplicaciones privadas) a redes WAN (aplicaciones públicas) con la denominación *IP-Telephony* o *ToIP (Telephony over IP)*. En este capítulo abordaremos las tecnologías, estándares y protocolos que soporta la telefonía IP.

2.1. VoIP y Telefonía IP

Llamamos Voz sobre IP al mero hecho de transportar la voz en forma de paquetes a través de una Red IP. VoIP es un término usado para referirnos a todo tipo de comunicación de voz que utiliza el protocolo de Internet (IP), llevando acabo el envío de la voz empleando conmutación por paquetes. *VoIP por lo tanto, no es un servicio como tal, sino una tecnología que permite encapsular la voz en paquetes para poder ser transportados sobre redes de datos* sin necesidad de disponer de circuitos conmutados como ocurre en un red de voz convencional (PSTN).

En el caso de la telefonía IP se debe realizar un conjunto de procesos más elaborados con el fin de brindar los mismos servicios que brinda la telefonía tradicional haciendo uso de la tecnología VoIP. Lo anterior significa que no es suficiente transportar la voz en paquetes, sino además es necesario establecer planes de numeración, métodos de control de tráfico de llamadas y de autenticación de abonados, establecer políticas de seguridad y de calidad de servicio (QoS) en la Red de Datos para dar prioridad al tráfico de Voz, entre otras medidas. La telefonía IP es una aplicación inmediata de VoIP en la cual una llamada telefónica ordinaria es transmitida a través de la Internet o una red privada de datos y puede o no hacer uso de la infraestructura de la red telefónica tradicional (PSTN).

La telefonía IP no utiliza circuitos físicos para establecer la conversación, sino que envía múltiples conversaciones (en forma de paquetes) a través del mismo canal (circuito virtual) codificadas en paquetes y en flujos independientes. Cuando se produce un silencio en una conversación, los paquetes de datos de otras conversaciones pueden ser transmitidos por la red, lo que implica un uso más eficiente de la misma.

2.2. Elementos de Telefonía IP

Para poder entrar de lleno al tema, es necesario que primero revisemos algunos conceptos e ideas en torno a la telefonia IP. En las siguientes secciones se abordan algunos de ellos con la finalidad de lograr un mejor entendimiento del tema.

2.2.1. Técnicas de digitalización de la Voz - Codec's

La denominación codec proviene de la contracción de las palabras Codificador - Decodificador y hace referencia al elemento encargado de convertir las señales analógicas de audio o video, en señales digitales listas para su transmisión a través de la Red para luego, en el otro extremo, realizar la tarea inversa y reproducir la señal original.

Además de digitalizar la voz y empaquetarla, los codec's pueden *comprimir* los paquetes de voz de manera que el tráfico de voz afecte lo menos posible al tráfico de datos en la Red. Otra funcionalidad de los codec's es la *encriptación* de los paquetes de voz a fin de que su viaje por la Red sea más seguro. Un codec se puede implementar en un DSP[1] que es un procesador diseñado específicamente para realizar operaciones sobre señales digitales o por medio de un programa en cualquier computadora (finalmente el programa se ejecuta en un procesador).

En el caso de la voz, el codec más empleado es el ITU-T G.711[2] también conocido como PCM [3] en sus dos variantes *Ley A y Ley* μ. A continuación, describiremos su funcionamiento y haremos mención de otras técnicas de digitalización y compresión de la voz empleadas actualmente.

Gracias al trabajo desarrollado por Harry Nyquist[4] en los Laboratorios Bell en la década de los años 20 sabemos que para representar de forma óptima una señal analógica por medio de muestras de la misma, tomadas a intervalos de tiempo regulares *es necesario que la tasa de muestreo*[5] *sea al menos el doble de la frecuencia máxima de la señal muestreada.*

El proceso de digitalización de la voz tiene las siguientes etapas: filtrado, muestreo, cuantificación y codificación (ver figura 2.1). La primera etapa consiste en filtrar la señal original para que tenga el ancho de banda deseado. En el caso de la voz humana se ha definido un rango de frecuencia estándar de 4[kHz]. Es por eso que en esta primera etapa se adecuá el rango mediante un filtro de 4 [kHz] de ancho de banda.

Ahora bien, tomando en cuenta el Ancho de Banda (BW por sus siglas en inglés *Band Width*) convencional para la Voz humana de 4 [kHz] y aplicando el *Teorema de Nyquist-Shannon*, esta claro que la tasa de muestreo debe ser de 8 [kHz] o lo que es lo mismo, 8[ksps] (8 mil muestras por segundo). Debemos recordar que todo proceso de muestreo implica una pérdida de información con respecto a la señal original. En ese sentido, la

[1] Digital Signal Processor - Procesador de Señales Digitales
[2] G.711 es un estándar de la ITU-T liberado en 1972 y empleado principalmente en telefonía.
[3] *Pulse Code Modulation* - Modulación por Codificación de Pulsos
[4] Teorema de Nyquist-Shannon, también conocido como teorema del muestreo.
[5] La frecuencia con que son tomadas las muestras.

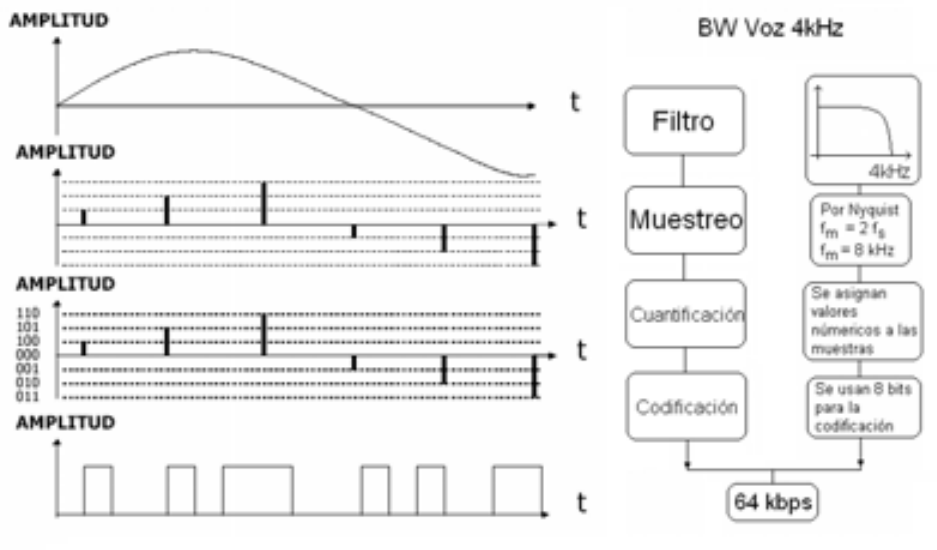

Figura 2.1: Proceso de digitalización de la voz

tasa de muestreo es un factor y determinante para la calidad y reconstrucción de la señal digitalizada. Si está es muy alta (más del doble del BW de la señal analógica) entonces tendremos más información de la necesaria; en cambio si la frecuencia de muestreo es baja, entonces corremos el riesgo de que ocurra un fenomeno llamado *Aliasing*, ejemplificado en la figura 2.2. El *aliasing* es la interpretación incorrecta de los puntos de muestra, lo que genera una señal falsa a la original. Por consecuencia no seremos capaces de reconstruir la señal original ante la insuficiencia de información.

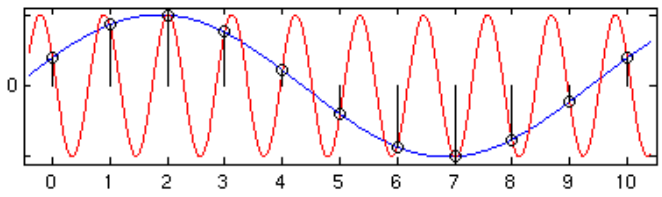

Figura 2.2: Aliasing. Dos senoidales que se ajustan al mismo conjunto de muestras

Una vez muestreada la señal se asignan valores numéricos a cada muestra. Tales valores se encuentran dentro de un rango arbitrario de posibles valores. Puesto que los valores reales de las muestras caen por encima y debajo de los valores que nosotros hemos establecido, es necesario *redondear* y/o aproximar los *valores reales infinitos* a un conjunto de valores discretos conocidos. En esta etapa al igual que en la etapa de filtrado se presentan pérdidas de información con respecto a la señal original. A esta pérdida en especial se le conoce como *Ruido de Cuantificación*. Es aquí donde surgen como alternativa la *Ley A y la Ley* μ(figura 2.3).

El problema de *ruido de cuantificación* es más notorio cuando el sistema de medición es lineal, es decir, cuando los valores asignados a las muestras se encuentran linealmente espaciados. La alternativa es emplear un sistema no lineal. ¿Por qué? Resulta que el oído humano distingue mucho mejor los cambios discretos de amplitud en volúmenes bajos que en volúmenes altos. En consecuencia, si procuramos cuantificar de mejor manera las muestras de baja amplitud (mayor densidad de posibles valores) en lugar de hacerlo por igual para todo el rango, entonces el *ruido de cuantificación* disminuye en términos subjetivos, pero efectivos.

La *Ley μ y la Ley A* son ambas, un modelo de sistema de cuantificación no lineal. Son modelos logarítimicos y de hecho son muy parecidos por no decir casi iguales, la diferencia más notable es geográfica. La *Ley μ* se emplea en Norte América y Japón, mientras que la *Ley A* es usada en Europa y el resto del mundo.

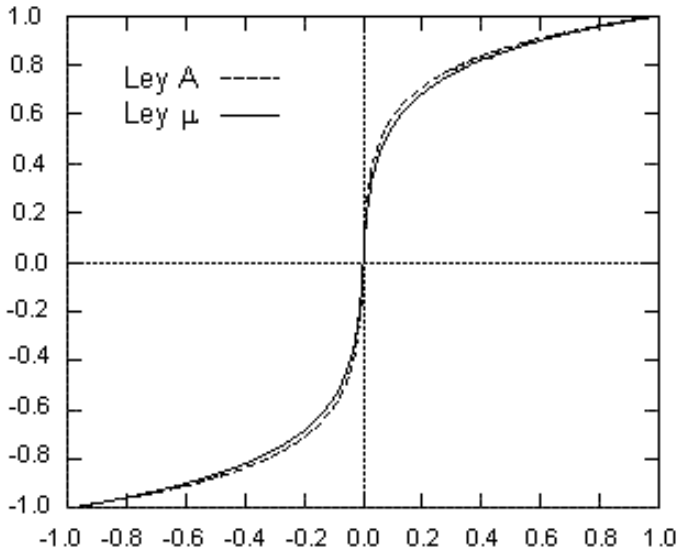

Figura 2.3: Ley A y Ley μ

El último paso en el proceso de digitalización de la voz es la Codificación. Este consiste en convertir en código binario los valores previamente asignados. Para el caso del codec G.711 se emplean 8 bits, es decir, en este punto ya sólo existen $2^8 = 256$ valores discretos posibles de aquel número infinito que existían en la señal original. El resultado final es un codec con una tasa de transmisión de:

```
4 [kHz] * 2 * 8 [bits/muestra] = 64 [kbps]
```

Aunque PCM es quizás el proceso de digitalización de voz mejor conocido, no es el único(ver referencia [12] para mayores detalles). Existen otros esquemas de digitalización que usan menor ancho de banda y proveen de una calidad comparable a la de PCM. En las líneas siguientes abordaremos estas otras alternativas.

Modulación por Codificación de Pulsos Diferencial Adaptativa - Adaptive Differential Pulse Code Modulation (ADPCM)

Con esta técnica es posible reducir la tasa de transmisión del codec G.711 a la mitad (32 [kbps]). En ADPCM no codifica cada muestra por separado, en cambio, se codifica únicamente la diferencia entre dos muestras, una real y otra predicha. Esto es posible gracias a que el habla humana es de comportamiento "*predecible*", lo cual permite reducir la cantidad de información requerida. La señal codificada en PCM es ingresada en un *transcoder ADPCM* que considera el comportamiento previo del flujo entrante para crear una predicción sobre el comportamiento de la siguiente muestra. Esta es la clave del proceso. En lugar de transmitir el valor real de la muestra predicha, se codifica y transmite la diferencia entre las muestras real y predicha con 4 bits dando por resultado una tasa de transmisión (*bitrate*[6]) de 32 kbps.

Algunos codec's que aprovechan esta técnica para disminuir el *bitrate* son: el G.721, el G.723 y el G.726, éste último sustituyó a los dos anteriores definiendo tasas de transmisión de 16, 24, 32 y 40 kbps correspondientes a tamaños de muestra (diferencial) de 2, 3, 4 y 5 bits respectivamente.

Modulación Delta de Pendiente Continuamente Variable - Continuously Variable Slope Delta (CVSD)

Mediante esta técnica se envía información sobre el *cambio en la pendiente de la forma de onda* en lugar de los valores en sí de cada muestra. En otras palabras, no se transmite el cambio en si de los valores, sino la tasa de cambio. Para realizar esto se emplea una muestra o voltaje de referencia contra la que se compara cada muestra entrante al codificador. Si el valor de la muestra entrante es mayor que el de la de referencia, entonces el codificador aumenta la pendiente de la curva de forma tal que se asemeje lo más posible a la señal original; de lo contrario, si el valor de la muestra entrante es menor que el valor de referencia, entonces el codificador disminuirá la pendiente. Con cada comparación se incrementa o disminuye una función escalón, lo cual provoca que la señal resultante tenga un aspecto dentado. Para reducir este efecto se aplican filtros pasa-bajas a la señal decodificada. De esta manera se suavizan las transiciones provocadas por la función escalón.

CVSD es empleado generalmente a una tasa de 32 kbps, aunque esta tasa puede descender hasta 9,600 bps. Mientras más baja es la tasa de transmisión, la calidad de la señal codificada con CVSD se empobrece notablemente.

Algunas aplicaciones de este tipo de codificación incluyen la transmisión de señales de voz entre dispositivos móviles (teléfonos celulares) y auriculares inalámbricos con tecnología Bluetooth, en la cual se utiliza CVSD a 64 kbps. Otra aplicación que ocupa menor ancho de banda la constituyen los radios de dos vías con línea encriptada de Motorola© en donde la tasa de transmisión es notablemente baja (12 kbps).

[6] En telecomunicación, el término bit rate (bitrate), define la cantidad de bits que un codificador utiliza por cada segundo de sonido, entre mayor sea el bitrate se lograra una mejor calidad de sonido.

Codificación Predictiva Lineal - Linear Predictive Coding (LPC)

Con esta técnica se logran resultados sorprendentes; sin embargo, la calidad de la señal codificada en LPC es de mediana a baja. La forma en que estos codec's funcionan es mediante un modelo matemático del tracto vocal. Con este modelo se predicen coeficientes que modifican la señal de salida. El nicho de aplicación de esta técnica son los juguetes con voces sintéticas o incluso los buzones de voz, debido a su gran capacidad de compresión. Con esta técnica se logran tasas de hasta 2,400 bps.

Una aplicación notable de esta técnica es el estándar GSM *(Global System for Mobile Communications)* utilizado en telefonía celular, en el cual junto con otros procesos es posible comprimir de forma sustancial los paquetes de Voz.

Interpolación Digital del Habla - Digital Speech Interpolation (DSI)

Esta técnica toma como ventaja un hecho poco percibido por la mayoría. Resulta que *en una conversación normal más del 50 % del tiempo de conversación, el canal permanece en silencio*. Éste hecho hace posible que el canal sea compartido por varias convesaciones simultáneas, interpolándolas en los momentos de silencio. Ésta técnica implementa una especie de multiplexación estadística y conforme aumenta la cantidad de usuarios es más eficiente, pues el comportamiento de las llamadas se vuelve más predecible. Comúnmente los canales se asocian a una conversación y durante el tiempo que esa conversación permanezca activa se reserva el canal exclusivamente para ella y nadie más. En DSI los canales no se asocian de esta manera, en lugar de ello, un gran número de usuarios comparten un conjunto de canales disponibles. Cuando un usuario comienza a hablar, el sistema DSI asigna una ranura de tiempo (canal en sistemas TDM) y notifica al extremo receptor sobre esta asignación. Sí durante la conversación existe una pausa, se reasigna esa ranura de tiempo a otro usuario, es decir, la asignación de canales es dinámica, de esta forma se aprovecha de mejor manera el recurso.

En la tabla 2.1 se resumen los principales codec's de Voz utilizados en telefonía IP[7]

[7] Referencias web consultadas: `http://www.itu.int/ITU-T/`, `http://en.wikipedia.org/` y `http://www.voipforo.com/codec/codecs.php`

Codec	[ksps]/[kbps]	Características
G.711μ	8 / 64	Utiliza técnica PCM. Estándar ITU-T G.711μ. Utilizado en E.U.
G.711a	8 / 64	Utiliza técnica PCM. Estándar ITU-T G.711a. Utilizado en Europa y México.
G.722	16 / (48 a 64)	Técnica ADPCM. Ahora esta libre de patentes y es estándar ITU-T G.722. Utiliza un BW para la voz de 7 kHz. Variante G.722.1 y G.722.2
G.723.1	8 / (5.3 y 6.3)	Al diseñar este códec, la principal aplicación considerada fue la telefonía visual a velocidad binaria muy baja como parte de la familia general de normas H.324. La técnica empleada es Codificación por Predicción Lineal (LPC).
G.726	8 / (16, 24, 32 y 40)	Emplea la técnica de compresión ADPCM. Reeplaza a G.721 y G.723. Las diferentes tasas de transmisión son resultado de los bits empleados para codificar la señal, es decir, 2, 3, 4 y 5 bits respectivamente.
G.729	8 / (6.4, 8 y 11.8)	La versión G.729a emplea menos recursos de procesamiento. Ambas son compatibles. G.729a utiliza técnica ACELP (Algebraic Code Excited Linear Prediction). Los derechos de propiedad intelectual pertenecen a Sipro Lab Telecom y VoiceAge. Se distribuye sin licencia para uso educacional.
GSM	8 / (5.6 y 13)	Global System for Mobile communication. Define un BW para la Voz de 3.1 kHz. Utiliza la técnica Regular Pulse Excitation Long-Term Prediction (RPE-LTP) que es una variante de LPC. Es el principal codec empleado en tecnología celular GSM.
iLBC	8 / (13.3 a 15.2)	Internet Low Bitrate Codec. Licencia de Global IP Sound. Definido en RFC 3951. Define tiempos de tramas de 30 y 20 ms, de ahí sus variantes iLBC-30 e iLBC-20 con tasas de transmisión de 13.3 y 15.2 kbps respectivamente. Emplea técnica "Block-Independent Linear-Predictive Coding" (LPC)
Speex	(8, 16 y 32) / (2-44)	Es Open Source. Emplea técnica "Code Excited Linear Prediction" CELP. Diseñado par VoIP transportada en UDP.

Tabla 2.1: Principales codec's utilizados en telefonía IP

2.2.2. IP-PBX

En la telefonía tradicional es necesario tener pleno control de las llamadas y de los canales de comunicación, lo mismo ocurre para el caso de la telefonía IP. En los sistemas convencionales de telefonía esa labor es desempeñada por el PBX. En el caso

de la telefonía IP el dispositivo que realiza esta labor se denomina IP-PBX[8] . Éste desempeña las funcionalidades de una central telefónica tradicional (PBX) haciendo uso de tecnologías y protocolos VoIP como son: SIP, H.323, IAX, etc.

2.2.3. Dispositivos cliente en Telefonía IP

Un cliente en telefonía IP se define como el dispositivo que actúa como terminal telefónica. Debemos hacer notar que en el caso de la telefonía tradicional las terminales telefónicas se consideran "tontas", ya que no requieren de configuración previa para interactuar con el PBX, mientras que en el caso de telefonía IP, cada terminal se considera "inteligente" porque posee una unidad de procesamiento (el DSP, al chip controlador del dispositivo y el chip para controlar la interfase de Red) e interactúa de forma dinámica con el IP-PBX para establecer las condiciones de cada llamada así como la llamada en sí.

Cada cliente debe *registrarse* ante un ITSP *(Internet Telephony Service Provider)* o en su defecto ante el servidor que brinde el servicio dentro de la Red local corporativa. Para poder registrarse el cliente requiere tener una cuenta previa en la base de datos del ITSP o del servidor VoIP local. los datos de esa cuenta son similares a los de una cuenta de correo electrónico, es decir, nombre de usuario (número de extensión en el caso de un cliente ToIP), una contraseña o password y la dirección IP o nombre de dominio del ITSP en cuestión, entre otros datos más. En los siguientes párrafos describiremos los tipos de clientes más comunes dentro de una Red ToIP.

Teléfonos IP por Hardware*(IPphones)*

Un teléfono IP es un dispositivo similar a un teléfono común, pero a diferencia de éste último, el teléfono IP digitaliza la voz y la empaqueta para poder ser transmitida sobre la Red a la cual esta conectada. En la figura 2.4 se puede observar un ejemplo de un teléfono IP marca Cisco©. Físicamente, un teléfono IP cuenta con un puerto de Red *(Ethernet RJ-45 de 4 pares)* en vez del tradicional RJ-11 de dos pares. Esto quiere decir, que no es posible conectar un teléfono IP en la roseta telefónica de nuestro hogar, sino que es necesario conectarlo a un dispositivo de Red, tal como un Switch. Esto también significa que por cada IPphone necesitamos un puerto adicional en nuestro Switch. Existen IPphones que cuentan con 2 puertos RJ-45, uno de ellos se conecta al Switch y el restante se "cascadea" hacia la PC en forma serial, también denominada Bridge o Daysychain para evitar el desperdicio de puertos en el Switch. Debemos tomar en cuenta también que al ser un dispositivo IP cada teléfono requerirá de su propia dirección IP. Esta deberá ser ajustada de forma manual o bien de manera automática a través de un servidor DHCP configurado en nuestro segmento.

[8] La nomenclatura en telefonía IP aún no esta muy bien establecida y existen tantos términos como protocolos VoIP para referirse al elemento que controla el tráfico de llamadas. Recordemos que en el mundo de soluciones ToIP cada fabricante intenta "imponer" su solución

Un teléfono IP es un cliente y como tal requerirá, además de una configuración de Red, información pertinente para que sea capaz de registrarse, generar y recibir llamadas.

A diferencia de un teléfono convencional que recibe alimentación directamente del PBX a través de la roseta, un teléfono IP requiere de alimentación externa. Este es un tema determinante, pues aunque existen alternativas tales como PoE[9] que entregan Potencia Eléctrica sobre el mismo cable de Red (asignando pares específicos y sin interferencia con la señal de datos), no todos los dispositivos soportan este estándar y los que si lo hacen tienen un costo mayor.

Figura 2.4: Teléfono IP Cisco© 7960

Teléfonos IP por Software *(Softphones)*

Un softphone es un programa de computadora que emula a un teléfono IP. El caso de los softphones es distinto al de los teléfonos IP por hardware, pues al ser puramente software utilizan los recursos de la computadora en donde se encuentran instalados, además de sus periféricos. No tienen el problema de la fuente de potencia como ocurre en el caso de un teléfono IP por hardware, así mismo, no requieren de un puerto adicional en el Switch, ni de una dirección IP propia, pues utilizan la conexión a la Red de la computadora dónde estan instalados (sólo cambia el Socket)[10] . Lo anterior puede representar muchas ventajas; sin embargo, acarrea consigo otras desventajas, son un punto de vulnerabilidad, pues en este nodo convergen tanto el tráfico de datos, como el de voz lo cual no es una práctica recomendable, pues siempre se sugiere mantener por separado ambos tráficos aunque sea de forma lógica.

Existe una gran variedad de aplicaciones de Softphone en la Internet, por ejemplo: X-Lite©, Eyebeam©, ZoIPer©, etc. En la figura 2.5 se muestra un ejemplo de teléfono por software.

[9] Power over Ethenrnet. Estándar IEEE 802.3af

[10] Un socket es el identificador formado por una dirección IP y el puerto lógico de la computadora asignado a un servicio de red, por ejemplo HTTP (protocolo para navegación de páginas web) emplea el puerto 80 por lo tanto el socket que utiliza es de la forma: A.B.C.D:80 ó SSH A.B.C.D:22. Los sockets permiten la comunicación entre procesos ejecutándose en máquinas remotas

Figura 2.5: Softphone Eyebeam©

Adaptadores para Terminales Analógicas *(ATA's)*

Los adaptadores para terminales analógicas son dispositivos que convierten un teléfono convencional en un teléfono IP. Son dispositivos *externos* con puertos RJ-11 que permiten conectar teléfonos analógicos y un puerto RJ-45 *Ethernet* para conexión a Red. Internamente estan compuestos por convertidores A/D, DSP's para implementar los codec's, un chip controlador para la interfase de red y un CPU que controle y organice a los anteriores. Estos adaptadores permiten reutilizar los "viejos" teléfonos convencionales y evitar que caigan en desuso prematuramente. La ventaja de estos adaptadores es que utilizan un sólo puerto *Ethernet* para conectar desde 2 y hasta 32 clientes por el mismo puerto del Switch[11] .

Figura 2.6: ATA - Internet Phone Adapter Linksys Cisco

[11] El ejemplo de ATA más sencillo conocido por nosotros es el Internet Phone Adapter de Cisco© - Linksys© (figura 2.6) y el de mayor capacidad que conocemos es el BrainComm32© que maneja 32 clientes

2.3. Protocolos VoIP

Al igual que en la red telefónica convencional es necesaria la información relacionada con el establecimiento de la llamada, su mantenimiento y terminación, así como la información de control entre centrales telefónicas llamada *señalización*, en el mundo VoIP también es necesaria esta información. A continuación describimos tres de los protocolos ma utilizados en VoIP.

2.3.1. El conjunto de protocolos H.323

En un principio, las redes VoIP eran propietarias, cada fabricante diseñaba su propio conjunto de protocolos y definían los mecanismos de señalización, control y codificación de la voz con muy poca o sin ninguna interoperabilidad entre ellas. En 1996, la ITU-T emitió la recomendación H.323 titulada "Sistemas Telefónicos Visuales y Equipos para Redes de Área Local que proporcionan una Calidad de Servicio No Garantizada". Esta norma fue la base de los primeros sistemas de telefonía en la Internet.

H.323 surgió de la evolución de una serie de recomendaciones por parte del trabajo de la ITU-T sobre video-telefonía y conferencias multimedia. H.323 fue originalmente *diseñado para soportar servicios multimedia sobre redes LAN*. Su enfoque no incluía el soporte de QoS, pues aún no se desarrollaban mecanismos para ello en redes WAN. Conforme evolucionó, fue expandiendo su soporte hacia WAN y telefonía sobre Internet.

La versión inicial de H.323 fue aprobada por la ITU-T en junio de 1996. No se trata de un solo protocolo, sino de un sistema de protocolos[12] que incluye H.245 para operaciones de control, H.332 para el manejo de conferencias a gran escala, H.225 para gestionar la conexión, H.235 para soporte de seguridad, T.120 para intercambio de documentos en conferencias, entre otros.

H.323 ha tomado prestadas algunas de las mejores características de otros protocolos de señalización, ya en proceso de obsolescencia, como ISDN (H.320, H.321), PSTN (H.324), ATM (H.310), etc. Resultando en una amalgama de procedimientos rica en funciones y complejidad al mismo tiempo. La sintaxis que H.323 emplea es binaria.

Componentes de un sistema H.323 funcionales/lógicos

- **Terminal H.323** - Son los extremos finales compatibles con H.323 implementados en software (por ejemplo Softphones o programas como Microsoft NetMeeting) o dispositivos autónomos (por ejemplo IPphones H.323).

- **Guardián H.323 - *Gatekeeper*** - Es él responsable, entre otras cosas, del control de acceso, la resolución de direcciones, la gestión de la carga de red, además de ser donde se establecen las políticas de acceso y utilización del servicio. En resumen, el gatekeeper es el encargado de administrar los recursos. Todos los elementos de red que

[12] A H.323 se le llama también protocolo sombrilla y al conjunto de protocolos que abarca se le conoce como pila de protocolos H.323

componen un sistema H.323 se comunican con el gatekeeper utilizando el protocolo RAS H.225. Otras tareas a su cargo son: autenticación, enrutamiento del servidor de directorios, contabilidad de llamadas y determinación de tarifas, localización de los distintos gateways y MCU's cuando son requeridos, etc.

- **Puerta de enlace H.323 - *Gateway*** - Los gateway's H.323 interconectan entidades tales como MCU's, terminales u otros gateway's hacia otros ambientes de red o protocolos, es decir, traducen entre protocolos. El gateway tiene como misión enlazar la red VoIP con la red telefónica analógica PSTN o RDSI. La serie de recomendaciones especifica interfases de H.323 hacia H.320, ISDN/PSTN y Redes basadas en ATM. Últimamente se han incorporado especificaciones para troncales hacia redes telefónicas como SS7/ISUP, además de sistemas VoIP que utilizan protocolos H.323 con otros que usen SIP.

- **Controlador Multipunto - *Multipoint Controller* (MC)** - Es una entidad lógica que interconecta los canales de señalización de llamadas y control de conferencias de dos o más entidades H.323 en una topología de estrella. *Coordina el intercambio de medios entre todas las entidades involucradas en una conferencia.* Los MC *pueden estar en cualquiera de las entidades (Terminales, Gateway's y Gatekeeper's) o en entidades por separado.*

- **Procesador Multipunto - *Multipoint Processor* (MP)** - Estas entidades son requeridas en caso de conferencias multipunto en H.323. Este recibe flujos desde extremos individuales, los combina y los regresa a los extremos origen.

- **Unidad de Control Multipunto - *Multipoint Control Unit* (MCU)** - En el mundo H.323 un MCU es simplemente la combinación entre un MC y un MP en un solo dispositivo. El término se originó en el ambiente de videoconferencias ISDN en donde los MCU eran requeridos para crear conferencias multipunto de un conjunto de conexiones punto a punto.

Zonas H.323

Un ambiente H.323 esta dividido en zonas. Una zona H.323 es una colección de terminales H.323, MCU's, gateway's y un gatekeeper encargado de la zona. Cada zona (ver figura 2.8) es controlada por un gatekeeper primario (con gatekeepers de respaldo opcionales). Una zona puede o no ser congruente con la topología de red sobre la cual esta definida. La zona H.323 más sencilla se compone de una terminal y un gatekeeper, los gateway's y los MCU's no son necesarios.

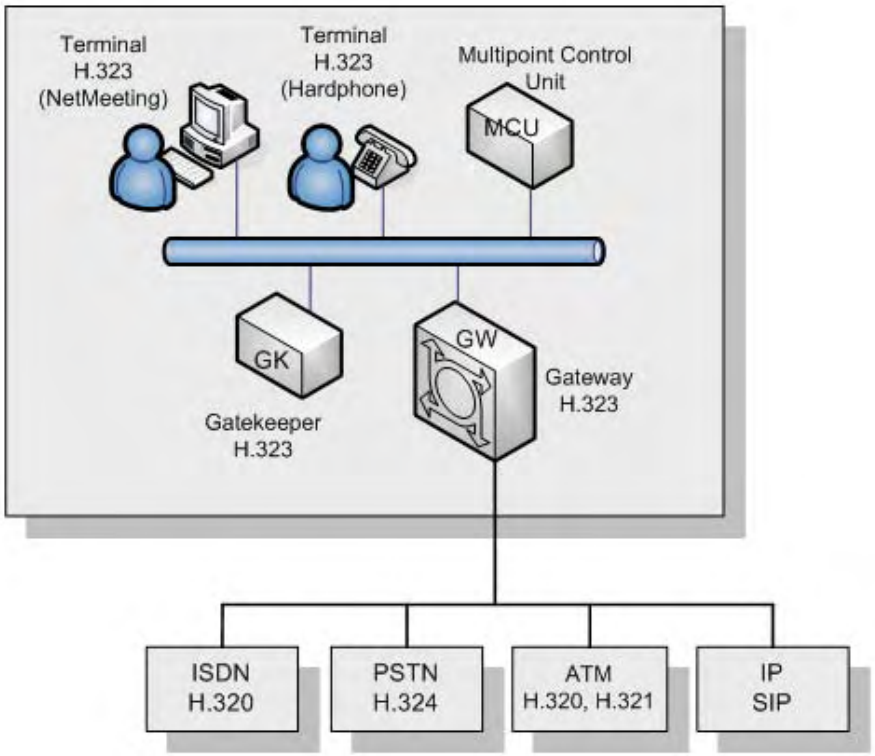

Figura 2.7: Componentes de un sistema H.323

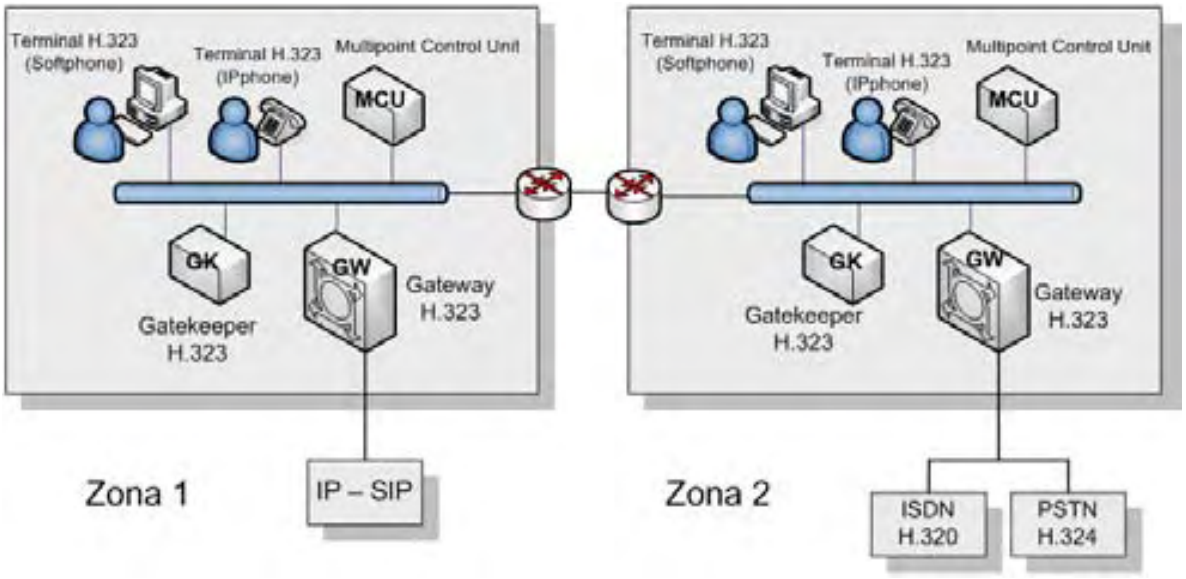

Figura 2.8: Zonas H.323

Protocolos H.323

H.323 comprende una serie de protocolos que son específicos para cada tarea específica. En la tabla 2.2 se detallan los mismos. En la figura 2.9 se esquematiza el

contenido de la tabla.

Función	Protocolo
Direccionamiento	RAS (Registration, Admision and Status): Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través del gatekeeper. DNS (Domain Name Service): Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS, pero a través de un servidor DNS.
Compresión de Voz	Requeridos: G.711 y G.723.1 Opcionales: G.728, G.729 y G.722
Compresión de Video	H.261 y H263
Señalización	H.225 (RAS): Protocolo que permite a las terminales hablar con el gatekeeper, solicitar y regresar ancho de banda y proporcionar actualizaciones de estado. Q.931: Protocolo de señalización de llamadas, para establecer y liberar las conexiones con la red telefónica RTC. H.245: Protocolo de control de llamadas, permite a los terminales negociar ciertos parámetros como: el tipo de codec, la tasa de bits.
Transmisión de voz y video	UDP "User Datagram Protocol": La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP. RTP "Real Time Protocol": Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.
Control de la transmisión	RTCP (Real Time Control Protocol): Es un protocolo de control de los canales RTP. Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

Tabla 2.2: Principales protocolos H.323

Descubrimiento y registro ante el gatekeeper

Existen dos posibles formas de contactar al gatekeeper desde una terminal H.323:

- Descubrimiento Multicast - El cliente envía una petición al gatekeeper (GRQ) hacia una dirección multicast bien conocida (224.0.1.41) y puerto 1718. Los GK que reciban la petición deberán confirmarla (GCF) o ignorarla.

- Por configuración manual - La terminal conoce la dirección IP del GK por configuración manual. En esta situación no es necesario el envío de una petición (GRQ) al GK preconfigurado; sin embargo, algunos clientes requieren este paso del protocolo y el GK tiene dos opciones ante la petición: confirmarla (GCF) o rechazarla (GRJ).

Figura 2.9: Protocolos que soportan a un sistema H.323

Cuando el procedimiento de descubrimiento es a través de paquetes multicast, el cliente puede enviar junto con el paquete un identificador del GK con el que desea contactar. Sólo el GK que posea el ID solicitado confirmará la recepción de la solicitud.

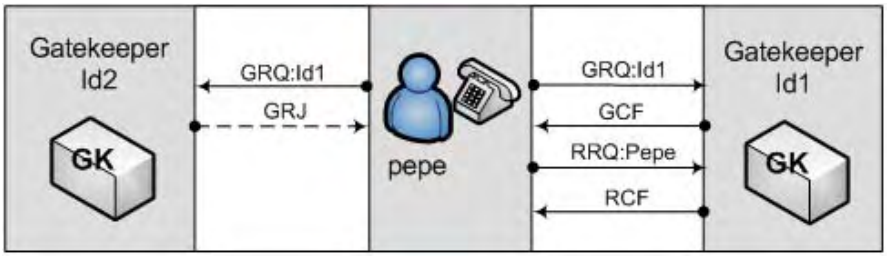

Figura 2.10: Trazado H.323 de un registro de usuario

Una vez que el cliente haya contactado al GK deseado, inicia el proceso de registro enviando mensajes RRQ. Entre otra información, el cliente envía los siguientes datos:

- Direcciones - Las direcciones del extremo (cliente); en el caso de una terminal sus ID's de usuario o número telefónico, etc.
- Prefijos - Si el solicitante es un gateway, entonces éste registrará prefijos de números telefónicos en lugar de direcciones.
- Tiempo de vida - El tiempo que el registro permanecerá en el GK sin expirar, aunque éste último puede sobre-escribirlo de acuerdo con sus propias políticas.

El GK verifica la información recibida y la confirma (RCF) en el caso de que sea correcta o la rechaza de no ser válida. En el caso de una confirmación, el GK asignará un identificador al "cliente" para que sea reconocido en las siguientes peticiones como registrado.

Proceso de una llamada H.323

Para entender mejor el funcionamiento del protocolo H.323, consideremos las diferentes fases de una llamada H.323[13] , mismas que se ilustran en la figura 2.11.

1. Establecimiento.

   Inicialmente observamos que una de las terminales se registra ante el gatekeeper utilizando el protocolo RAS (Registro, Admisión y Estado) con los mensajes ARQ y ACF. Posteriormente, utilizando el protocolo H.225 (control del establecimiento y liberación de la llamada) se manda un mensaje de SETUP para iniciar una llamada H.323. Entre la información que contiene el mensaje se encuentra la dirección IP, puerto y alias del llamante o la dirección IP y puerto del llamado. La terminal llamada contesta con un CALL PROCEEDING advirtiendo del intento de establecer una llamada. En este momento la segunda terminal tiene que registrarse con el gatekeeper utilizando el protocolo RAS de manera similar a la primera terminal. El mensaje ALERTING indica el inicio de la fase de generación de tono. Y por último CONNECT indica el comienzo de la conexión.

2. Señalización de control.

   En esta fase se abre una negociación mediante el protocolo H.245 (control de conferencia), el intercambio de los mensajes (petición y respuesta) entre las dos terminales establecen quién será MASTER y quién SLAVE, las capacidades de los participantes, codec's de audio y video a utilizar. Como punto final de esta negociación se abre el canal de comunicación(direcciones IP y puerto).

   Los principales mensajes H.245 que se utilizan en esta fase son:

   - TerminalCapabilitySet (TCS). Mensaje de intercambio de capacidades soportadas por los terminales que intervienen en una llamada.
   - OpenLogicalChannel (OLC). Mensaje para abrir el canal lógico de información que contiene información para permitir la recepción y codificación de los datos. Contiene la información del tipo de datos que serán transportados.

3. Audio.

   Las terminales inician la comunicación y el intercambio de audio (o video) mediante el protocolo RTP/RTCP.

[13] `http://www.voipforo.com/H323/H323ejemplo.php`

4. Desconexión.

   En esta fase cualquiera de los participantes activos en la comunicación puede iniciar el proceso de finalización de llamada mediante mensajes CloseLogicalChannel y EndSessionComand de H.245. Posteriormente utilizando H.225 se cierra la conexión con el mensaje RELEASE COMPLETE. Por último se liberan los registros con el gatekeeper utilizando mensajes del protocolo RAS.

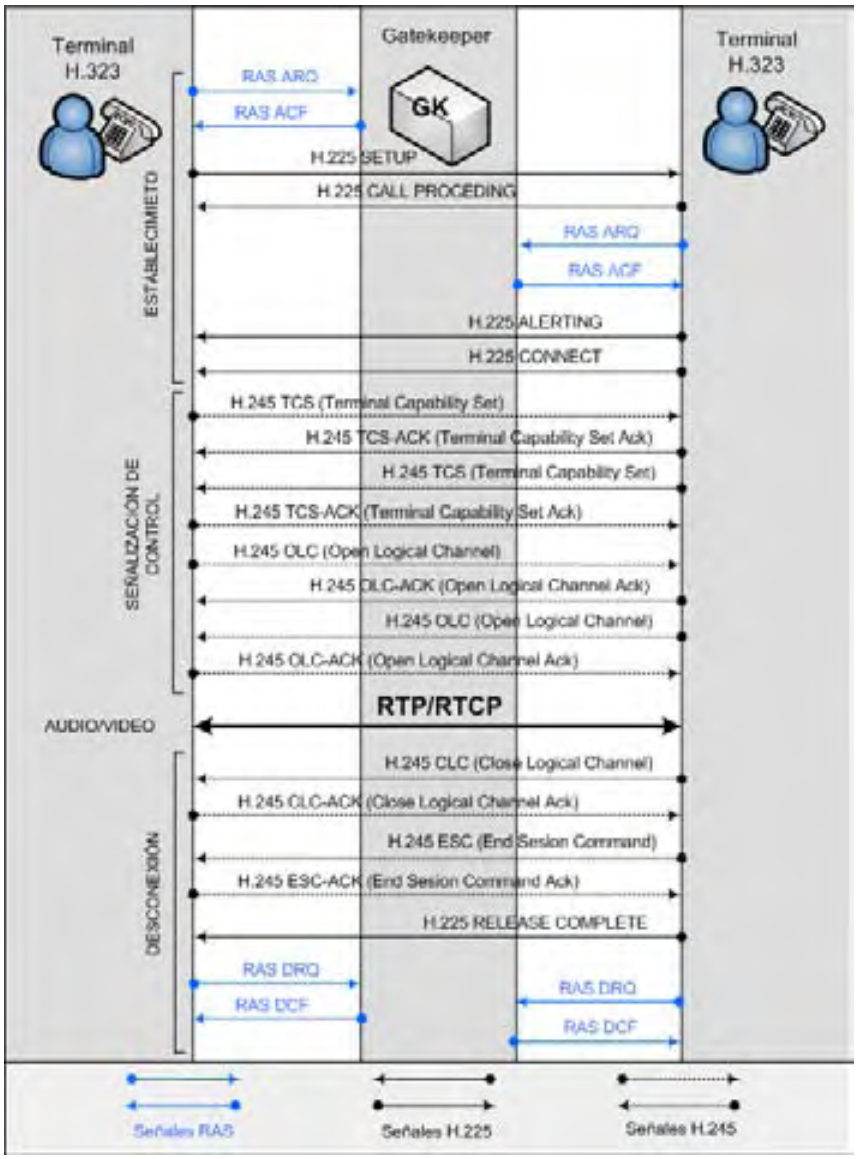

Figura 2.11: Llamada H.323

2.3.2. El Protocolo de Inicio de Sesión (SIP)

Este protocolo se definió por primera vez en el RFC 2543[14] , propuesto por la IETF(Veáse sección 1.2.1). En junio de 2002 se publicó la nueva versión de este protocolo en el RFC 3261. El propósito de SIP es la comunicación entre dispositivos multimedia. SIP hace posible esta comunicación por medio de dos protocolos los cuales son RTP/RTCP y SDP. El protocolo RTP se usa para transportar los datos de voz en tiempo real (igual que para el protocolo H.323, mientras que el protocolo SDP se usa para la negociación de las capacidades de los participantes, tipo de codificación, etc.) A diferencia del protocolo H.323, SIP no depende de otros protocolos para el control de la conferencia y no define ningún método para el transporte de tráfico de sesión. SIP soporta sesiones *Unicast y Multicast*.

SIP es un protocolo de señalización a nivel de aplicación (capa 7 del modelo OSI) para establecimiento y gestión de sesiones con múltiples participantes. Esta basado en mensajes de petición y respuesta, y reutiliza muchos conceptos de estándares anteriores como HTTP y SMTP.

Uno de sus atractivos es que soporta usuarios móviles (no clientes). La forma de identificar a una entidad SIP es similar a la empleada para definir una cuenta de correo electrónico. SIP utiliza las *URI's o URL's*[15] como método de localización de usuarios. Esta característica permite gran flexibilidad y compatibilidad con las aplicaciones Web.

Un servidor SIP puede funcionar en modo *stateful* o en modo *stateless*. Éste último permite que el protocolo tenga una gran escalabilidad, pues los servidores no mantienen información acerca del estado de la llamada. Una vez realizada la transacción, éste no necesita recordar nada sobre ella. De lo contrario el servidor mantiene la información y esto hace que su capacidad de procesamiento de llamadas se vea degradada.

Es un protocolo de señalización *extremo a extremo* que implica que toda la lógica es almacenada en los dispositivos finales (salvo el enrutado de los mensajes SIP)[4]. El estado de la conexión es también almacenado en los dispositivos finales. El precio a pagar por esta capacidad de distribución y su gran escalabilidad es una sobrecarga en la cabecera de los mensajes producto de tener que mandar toda la información entre los dispositivos finales.

Las funciones principales de éste protocolo son:

- Establecer, modificar y finalizar sesiones entre dos o más participantes.
- Registro y localización de participantes, y movilidad.
- Gestión del conjunto de participantes y de los componentes del sistema.
- Descripción de características de las sesiones y negociación de los participantes.

[14] Publicado en febrero de 1996

[15] Universal Resource Identifier o Universal Resource Locator del tipo sip:usuario@dominio, por ejemplo: sip:pumas@voip.unam.mx. Es de la misma manera en que se identifica un usuario de correo electrónico; por lo tanto, es posible iniciar una llamada SIP incluso desde un navegador Web.

Es el protocolo que en la actualidad presenta mayor auge por su simplicidad, su facilidad en la generación de nuevos servicios y su filosofía de arquitectura distribuida. Debido a esto, la mayoría de los dispositivos de VoIP están siendo desarrollados con soporte para protocolo SIP [16] .

Elementos del protocolo SIP

Los elementos básicos de un sistema SIP son los UA (Agentes de Usuario) y los servidores de Red. La configuración más simple para establecer una sesión SIP es utilizando sólo dos agentes de usuario (UA) conectados uno a otro. Estos últimos pueden ser de diferentes tipos, Proxies, Registrars y Redirect Servers. A menudo estos elementos son sólo entidades lógicas y comúnmente se sitúan en el mismo lugar.

- Agente de Usuario - SIP User Agent

  El agente de usuario se conforma por el UAS (User Agent Server) y el UAC (User Agent Client). Son estas entidades finales que usa SIP para contactar a cada usuario y definir las características de la sesión (Ver figura 2.12); por ejemplo, en un softphone, teléfonos celulares (SIP), Hard-IPphones, etc. El UAC se encarga de generar peticiones y recibir respuestas a esas peticiones, mientras que el UAS tiene como tarea el recibir peticiones y generar respuestas a las mismas.

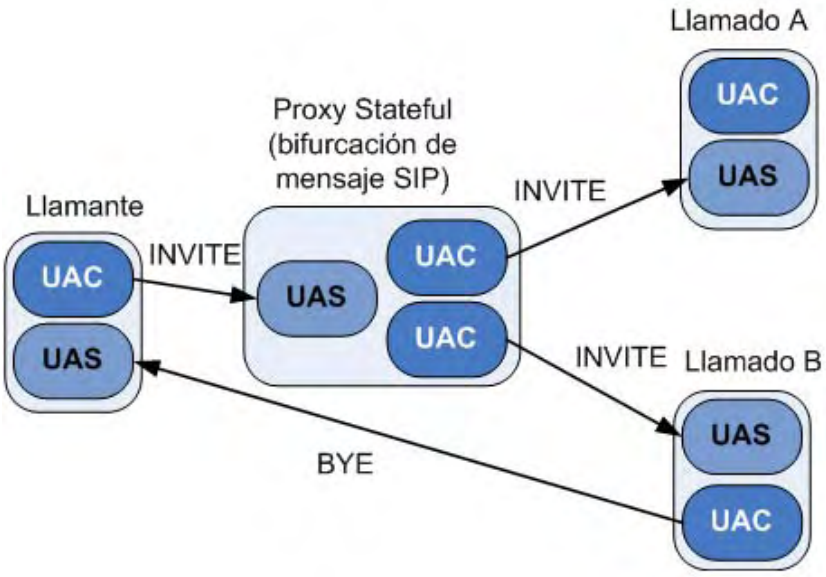

Figura 2.12: UAC y UAS

- Servidor - SIP Server

[16] K. Werbach, "Using VoIP to Compete". Harvard Business Review, September 2005.

Existen diversos programas de aplicación, llamados servidores, que aceptan peticiones de servicios y regresan respuestas a esas peticiones. En SIP, un servidor puede ser cualquiera de los siguientes tipos: Servidor Proxy, Servidor de Redirección, Servidor de Agente de Usuario y Servidor de Registro.

- Servidor Proxy - SIP Proxy Server

  Actúa tanto como servidor y cliente a la vez (ver figura 2.13). Es una entidad intermediaria que hace peticiones a nombre de los clientes. Un proxy Server tiene como trabajo el asegurarse de que las peticiones sean atendidas internamente o "enviada" a otra entidad más cercana al usuario destino, es decir, desempeña el papel del encaminamiento. Los proxies son también útiles para hacer cumplir ciertas políticas (por ejemplo, cerciorarse que un usuario pueda hacer una llamada). Un proxy interpreta y en caso necesario, reescribe partes específicas de un mensaje antes de reenviarlo.

  Los proxies SIP son los elementos que encaminan peticiones SIP a los UAS y respuestas SIP a los UAC. Una petición puede atravesar varios proxies en su camino hacia un UAS. Cada uno tomará decisiones de enrutamiento, modificando la petición antes de reenviarla al elemento siguiente. Las respuestas se encaminarán a través del mismo sistema de proxies atravesados por la petición, pero en el orden inverso. Existen dos tipos de SIP proxy Servers: stateful y stateless.

  Los *proxies stateful* guardan el estado de la transacción (llamada SIP), por lo que tienen un mayor control de la misma y pueden realizar tareas mas complejas, como: retransmisiones (no reenvíos) de mensajes, bifurcaciones de mensajes SIP, etc. Por otro lado, un *proxy stateless* no almacena información del estado que guardan las transacciones que atendió; por lo tanto posee una mayor escalabilidad en cuanto a la capacidad de procesamiento de peticiones SIP.

- Servidor de Registro - SIP Registrar Server

  Es el servidor que se encarga de aceptar peticiones de Registro (Ver figura 2.14) de los usuarios que se conectan a la Red (ejecuta su Softphone en su PC o enciende su IPphone), este envía un mensaje "REGISTER" hacía su proxy con el fin de que éste conozca su ubicación. La labor de un registrar proxy consiste en atender estos mensajes, validar y autenticar la cuenta contra una base de datos interna o externa y "registrar" la localización actual del usuario. Un registrar server es comúnmente sólo una entidad lógica y generalmente se encuentra en el mismo punto que un proxy o un Redirect Server y no puede ofrecer servicios de localización.

- Servidor de Redireccionamiento - SIP Redirect Server

  Es un servidor que acepta peticiones SIP, mapea las direcciones a nuevas y las regresa al cliente *(Respuestas 3XX)*. De esta manera ordena al cliente entrar en contacto con un sistema alterno (figura 2.15). A diferencia de un proxy SIP, *no genera sus propias peticiones SIP* y a diferencia de un UAS *no acepta llamadas*. En algunas arquitecturas puede ser deseable reducir la carga de proceso en los servidores proxy

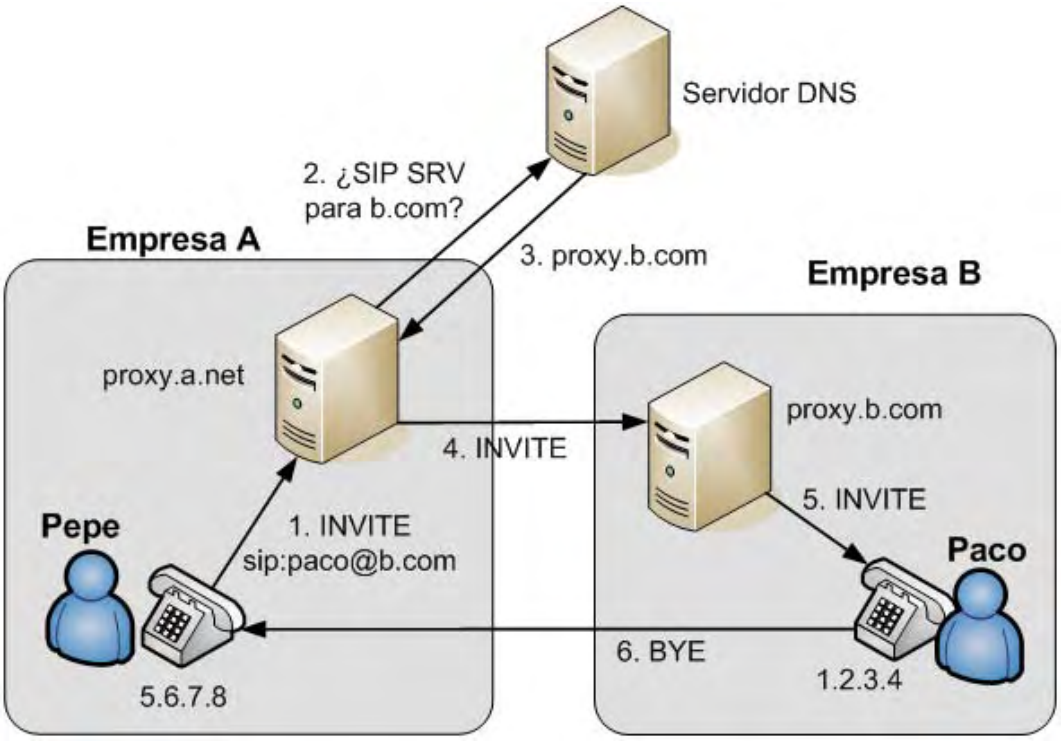

Figura 2.13: Invitación a Sesión

que son responsables de las peticiones de encaminamiento, y mejorar la robustez del recorrido de los mensajes de señalización, mediante redirecciones.

La redirección permite que los servidores envíen la información de encaminamiento para una petición como respuesta al cliente, de tal modo quitándose del camino de los subsiguientes mensajes para una transacción, mientras que ayudan en la localización de la petición. Cuando el autor de la petición recibe el cambio de dirección, enviará otra petición basada en la nueva URI o URI's que haya recibido. Propagando URI's desde el núcleo de la red hacia sus extremos, el cambio de dirección permite obtener una escalabilidad considerable en la red.

El usuario o proxy (cliente) que realizó la petición original extrae la información de la respuesta y envía otra petición directamente al resultado de la búsqueda.

- Proxy de Salida - Outbound proxy:

  Un proxy que recibe peticiones de un cliente, aunque puede o no ser el servidor resuelto por el Request-URI.

  Si el cliente configura su teléfono o su softphone, con un proxy de salida (outbound) este será capaz de procesar los mensajes del protocolo SIP e iniciar sesiones, es similar a la configuración de un web browser que utiliza un proxy web para navegar en la

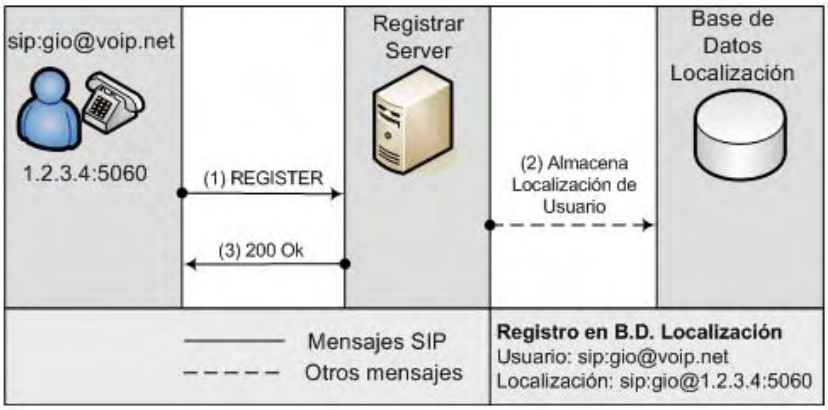

Figura 2.14: SIP registrar server

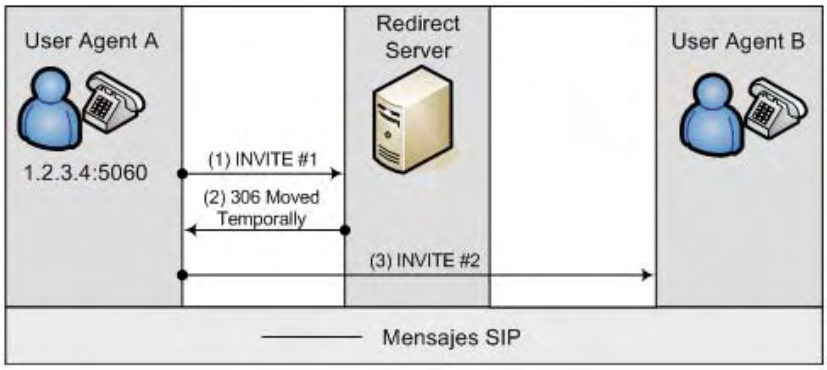

Figura 2.15: SIP redirect server

Red. En algunos casos, el proxy de salida se pone junto al firewall y *es la única manera de dejar pasar el tráfico SIP de la red interna hacia la Internet.*

El proxy de salida usado por un UA puede establecerse automáticamente por DHCP (éste se aplica sobre todo a los dispositivos SIP, no a los softphones SIP). Existen también soluciones de auto-descubrimiento, pero son utilizadas con poca frecuencia.

La división de estos servidores es conceptual, cualquiera de ellos puede existir físicamente en una única máquina, o como entidades independientes, lo cual permite una mayor escalabilidad y rendimiento del sistema en conjunto.

Los mensajes SIP

SIP utiliza una serie de mensajes para "señalizar" las sesiones. El mensaje SIP se conforma de una línea inicial (Start Line o Request Line), el encabezado del mensaje (Message Header) y el cuerpo del mensaje (Message Body).

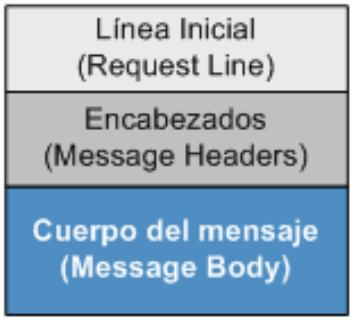

Figura 2.16: Estructura del mensaje SIP

- La línea inicial contiene la versión del protocolo SIP, el método y direcciones involucradas en la sesión si se trata de un mensaje de petición o bien, el estado de la sesión para el caso de los mensajes de respuesta.
- El encabezado contiene información relacionada con la llamada en forma de texto; por ejemplo: el origen y destino de la petición, el identificador de la llamada, etc.
- El cuerpo del mensaje o carga útil (payload) lleva información comúnmente SDP.

Existen dos tipos básicos de mensajes SIP, peticiones y respuestas. Las peticiones se emplean para iniciar alguna acción o para información. Las respuestas se usan para confirmar que una petición fue recibida y procesada, y contiene el estado del procesamiento.

En el ejemplo mostrado en la figura 2.17 puede ver un mensaje SIP correspondiente a una petición, se trata de una invitación para iniciar una sesión (INVITE). Delante de la palabra INVITE se encuentra la SIP URI, donde se especifica el brinco del mensaje, en este caso es 192.168.0.121. El campo VIA se usa para registrar la ruta que ha recorrido la petición o mensaje. En el caso de un mensaje INVITE, éste contendrá sólo un campo VIA, el cual registrará el origen de la petición. Los campos FROM y TO (De y Para), son transparentes por si solos. El campo CALL-ID identifica los mensajes que pertenecen a la misma llamada (sesión SIP), es así como el analizador de Red que utilizamos pudo reconocer todos los mensajes correspondientes a esta llamada. El campo Cseq se utiliza para mantener el orden de las peticiones. Éste identifica las transacciones dentro de un mismo diálogo SIP. El campo CONTACT contiene la IP y puerto en donde el emisor de la petición espera obtener respuesta a su mensaje. Existen otros campos que por el momento no describiremos a detalle. Finalmente, el cuerpo del mensaje INVITE contiene una descripción de los medios aceptados por el emisor codificados en SDP.

Otros mensajes de peticiones SIP que debemos considerar son los siguientes:

- ACK; Se usa para pedir la confirmación de que el extremo llamado recibió el INVITE. (3 Way Handshaking)

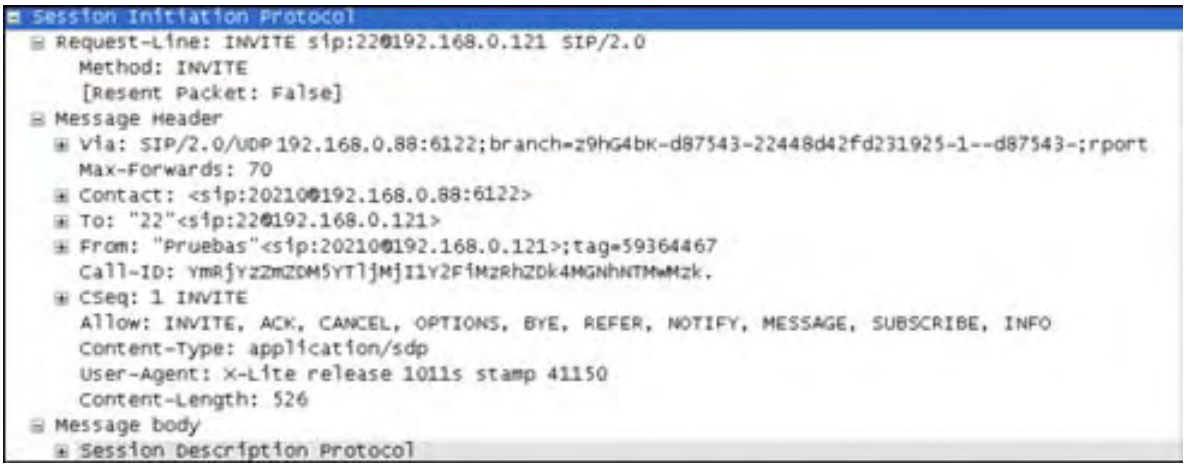

Figura 2.17: Mensaje SIP petición INVITE

- BYE; Empleados para finalizar una sesión.
- CANCEL; Para cancelar una sesión que no se ha completado del todo.
- REGISTER; Para que el proxy conozca la localización actual del emisor del mensaje.

Estas peticiones no contienen por lo general un cuerpo de mensaje, porque no lo requieren.

Cuando un proxy recibe una petición (excepto ACK), éste debe dar una respuesta. Un ejemplo puede ser observado en la figura 2.18

Figura 2.18: Respuesta SIP 200 Ok

Los mensajes de respuesta son similares a los de peticiones, excepto por la primera línea, la cual contiene la versión del protocolo y el código de la respuesta (200 = Ok). El primer dígito indica la clase de respuesta.

Existen 6 clases de respuesta:

- 1XX Son respuestas provisionales (La petición fue recibida, pero se desconoce aún el resultado del procesamiento). El emisor detiene el envío de retransmisiones después de recibir una respuesta de este tipo. Por ejemplo el código 180 = ringing o 100 = trying.
- 2XX Son respuesta finales positivas. La petición fue recibida y procesada de manera exitosa. Por ejemplo 200 = Ok significa que el extremo llamado aceptó la invitación a la sesión.
- 3XX Son usados para redireccionar llamadas. Dan información acerca de la nueva localización de un usuario o sobre un proxy alterno que pueda resolver satisfactoriamente alguna petición. El emisor del mensaje de petición debe reenviar su petición al otro lado para que sea atendida.
- 4XX Son respuestas finales negativas. Falla del lado del emisor, mala sintaxis del mensaje, etc.
- 5XX Falla del lado del servidor. Aparentemente la petición es válida, pero el proxy es incapaz de procesarla. El emisor debe reintentar después.
- 6XX La petición no puede ser atendida en ningún proxy. Falla general.

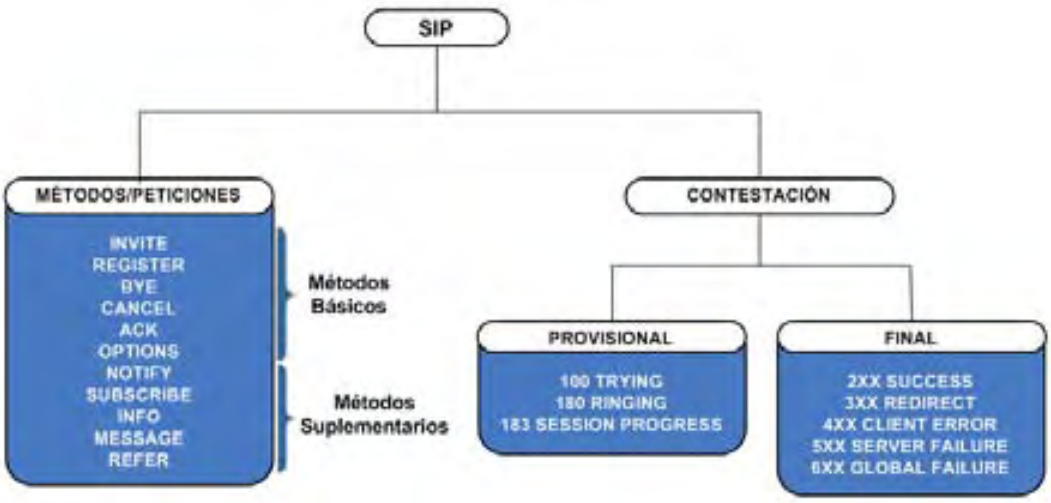

Figura 2.19: Mensajes SIP

Transacciones SIP

Una transacción SIP es una secuencia de mensajes SIP entre dos elementos de Red. Una transacción corresponde a una petición y todas las respuestas a esa petición, esto quiere decir, que una transacción incluirá cero o más respuestas provisionales y, una o más respuestas finales (en el caso de un mensaje INVITE, recuerde que este puede ser

dividido por un proxy, por lo tanto tendrá múltiples respuesta finales. Las entidades SIP que almacenan el estado de las transacciones son denominadas Stateful y lo hacen por medio del registro de cada transacción a través de un identificador contenido en el encabezado VIA[17] . La figura 2.20 ejemplifica una transacción perteneciente a una conversación SIP.

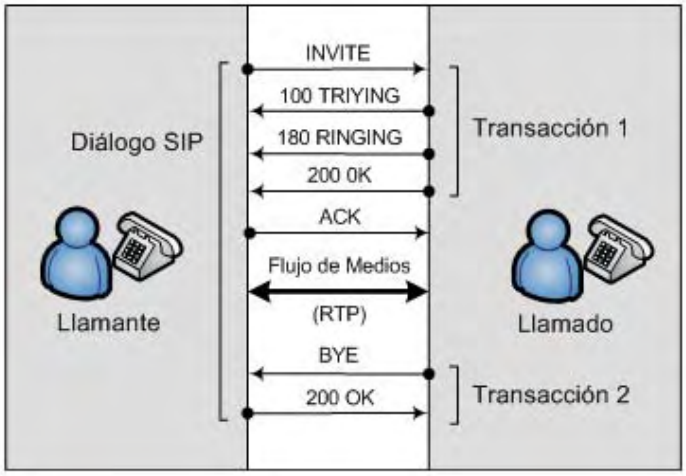

Figura 2.20: Ejemplo de transacciones SIP

Diálogo SIP

Un diálogo SIP es una conversación peer-to-peer entre dos UA (Agentes de Usuario). Los diálogos son identificados empleando los campos Call-ID (Identificador de llamada), From (De) y To (Para). Los mensajes con estos campos iguales pertenecerán a un mismo diálogo. El campo Cseq, del que hablamos anteriormente, es utilizado para ordenar los mensajes en un diálogo y representa el número de transacción. De forma breve podemos decir, que un diálogo es una secuencia de transacciones con el mismo campo Call-ID.

Escenarios clásicos de SIP

Registro.- Para que un usuario pueda ser llamado por otro, éste debe registrarse primero ante el proxy. El registro consiste en el envío de un mensaje REGISTER seguido de su correspondiente respuesta 200 (Ok). En caso de que el usuario no haya dado credenciales válidas recibirá por respuesta un mensaje 407, con lo cual tendrá que reenviar el mensaje de Registro hasta que tenga éxito.

[17] En la versión anterior del protocolo SIP (RFC-2543) éste identificador era calculado en base a los encabezados, pero resultaba bastante complicado y era fuente de problemas. A partir del RFC-3261 SIPv2 el identificador se incluye directamente en el mensaje.

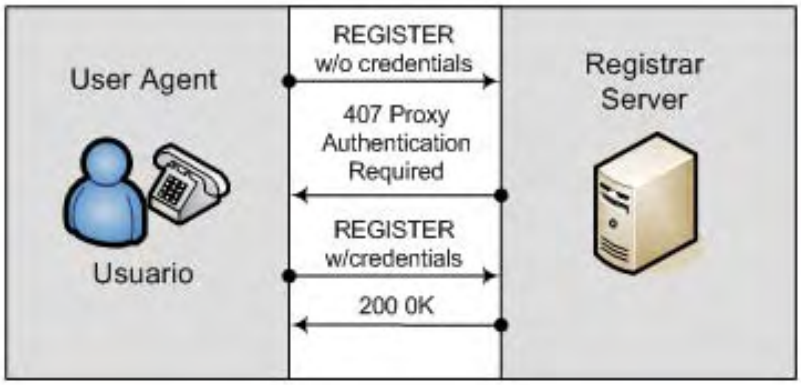

Figura 2.21: Registro de UA ante Registrar Server

Invitación a una sesión.- Una invitación inicia con el mensaje INVITE hacia el proxy. Éste responde con un TRYING (100) para detener las retransmisiones y reenvía las peticiones hacia el usuario llamado. Todas las respuestas provisionales generadas por el usuario llamado son regresadas al usuario origen. Por ejemplo, RINGING (180) que es un mensaje que se envía cuando el usuario llamado es contactado y comienza a timbrar, y una respuesta 200 (Ok) cuando éste contesta la llamada.

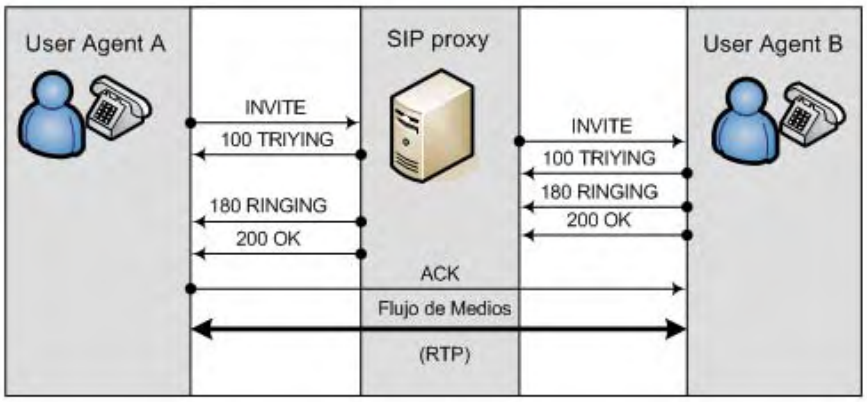

Figura 2.22: Invitación a Sesión

Terminación de sesión.- Una sesión es finalizada cuando uno de los usuarios envía el mensaje BYE, mientras que el otro extremo confirma el final de la sesión enviando por respuesta un mensaje 200 (Ok). La transacción para finalizar la sesión se realizará de un extremo a otro, sin pasar por el proxy a menos que en el mismo haya establecido un proceso de registro de ruta.

Registro de ruta.- Existen situaciones en las que el proxy requiere estar presente en la ruta de todos los mensajes con fines de control del tráfico, o por ejemplo cuando

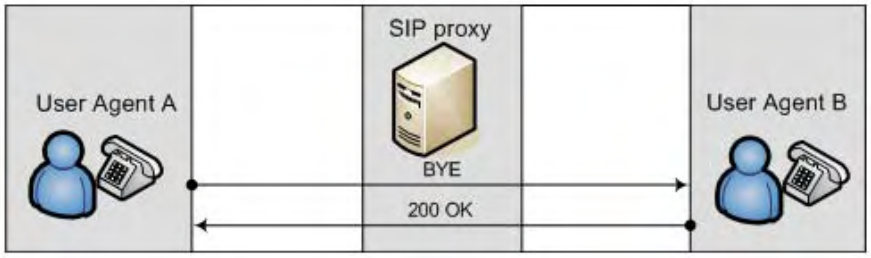

Figura 2.23: Finalización de sesión sin registro de ruta

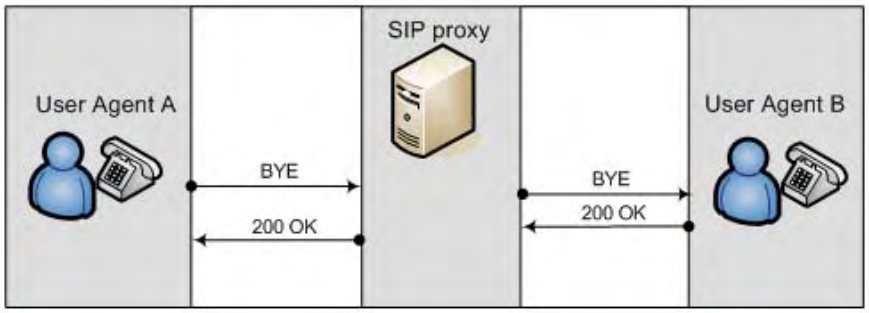

Figura 2.24: Finalización de sesión con registro de ruta

existe un servidor NAT[18] . El proxy o los proxies logran esto por medio de la inserción del campo RECORD ROUTE en los encabezados de los mensajes SIP.

El protocolo SDP Session Description Protocol

Es un protocolo que define un formato para describir sesiones multimedia en tiempo real. Proporciona la información suficiente para que los participantesde una sesión tengan conocimiento de las características de la misma y puedan unirse a ella.

Cada descripción SDP proporciona la siguiente información:

- El nombre y propósito de la sesión.
- Tiempos de inicio y fin de la sesión.
- Tipo y formato de los medios que la componen.
- Intervalo(s) temporal(es) de desarrollo de la sesión.
- Parámetros necesarios para poder recibir e interpretar los datos: direcciones IP's, los números de puertos involucrados, los esquemas de codificación, protocolo de transporte a ser usado, etc.

[18] Network Address Translation - Traductor de Direcciones de Red.

- Información complementaria relativa a los recursos de red necesarios para participar en la sesión; como por ejemplo, requisitos de ancho de banda e información de contacto del responsable de la sesión.

La especificación SDP define todos los tipos posibles de información que en la sesión son admitidos, el orden en el que deben aparecer y el formato, y las palabras reservadas para cada tipo que se ha definido.

Sin embargo, en la actualidad SDP es empleado para describir las capacidades de los sistemas y proporcionar varias alternativas de configuración a elegir, esto es, SDP se emplea actualmente para desempeñar la función de negociación de capacidades, tarea para la cual no está diseñado. Por tal motivo, se está desarrollando SDPng [1], el protocolo de descripción de sesiones y negociación de capacidades que se prevé sustituirá a SDP en el futuro. Siguiendo el modelo SDPng, una sesión multimedia consta de uno o más componentes de sesión, cada uno de los cuales describe un tipo de interacción que se puede llevar a cabo mediante diferentes aplicaciones y posiblemente con diferentes protocolos.

RTP/RTCP

El RTP[11] fue desarrollado por el grupo de trabajo de transporte de Audio y Video de la IETF, se publicó como estándar en 1996 (RFC 1889), y fue actualizado posteriormente, en el 2003 (RFC 3550). VoIP necesita de un protocolo de transporte, pero no es posible el uso del protocolo TCP debido a que este es demasiado lento para las aplicaciones de tiempo real, así es que para eso se usa el datagrama de UDP, pero éste no tiene control sobre el orden en que son recibidos los paquetes o cuanto tiempo les tomará llegar.

Así es como surgió el protocolo RTP con la finalidad de permitir que el receptor ponga los paquetes en el orden correcto y que no se tarde con los paquetes que se hayan perdido en el camino o que no se tarde demasiado al recibirlos, pues de ello depende bastante la calidad de la llamada.

RTP no ofrece garantías sobre la calidad del servicio, ni sobre el retraso en la entrega de datos, estos deben ser proporcionados por la Red subyacente. Aunque RTP halla su principal aplicación en videoconferencia y en la multimedia, es útil en aplicaciones de almacenamiento de datos continuos, simulación distribuida interactiva, etc.

El estándar RTP se define con dos protocolos, RTP (Real-time Transport Protocol) y RTCP (Real-time Transport Control Protocol). Siendo el primero utilizado para el intercambio de data multimedia, mientras que el segundo se usa para el envío periódico de información de control asociada a un determinado flujo de datos, proporciona una retroalimentación útil para mantener una calidad de distribución adecuada y también proporciona información de los usuarios.

RTP se considera un protocolo de capa de aplicación y tiene las siguientes funciones:

- Comunicar la elección del esquema de codificación de los datos.
- Determinar la relación temporal entre los datos recibidos.
- Sincronizar los distintos medios.
- Indicar la pérdida de paquetes.
- Indicar límites de frames en los datos.
- Identificación de usuarios.

RTCP tiene tres funciones básicas:

1. Informar el desempeño de la aplicación y la red, es decir, decide el uso de un esquema de compresión y con esto reducir la congestión, al igual que diagnóstica los problemas en la red.
2. Sincronización y correlación de diferentes streams que provienen de la misma fuente.
3. Un modo de transportar la identidad del usuario emisor para el despliegue en la interfase del usuario receptor.

Para cada clase de aplicación, RTP define un perfil (*profile*) y uno o más formatos (*formats*). El *perfil* entrega un información que asegura el entendimiento común de los campos en el encabezado de RTP, para tal clase de aplicación. La especificación del *formato* explica como deben ser interpretados los datos que siguen al encabezado de RTP.

Este protocolo hace uso eficiente del ancho de banda, principalmente mediante la restricción en la longitud del encabezado de RTP(Ver figura 2.25).

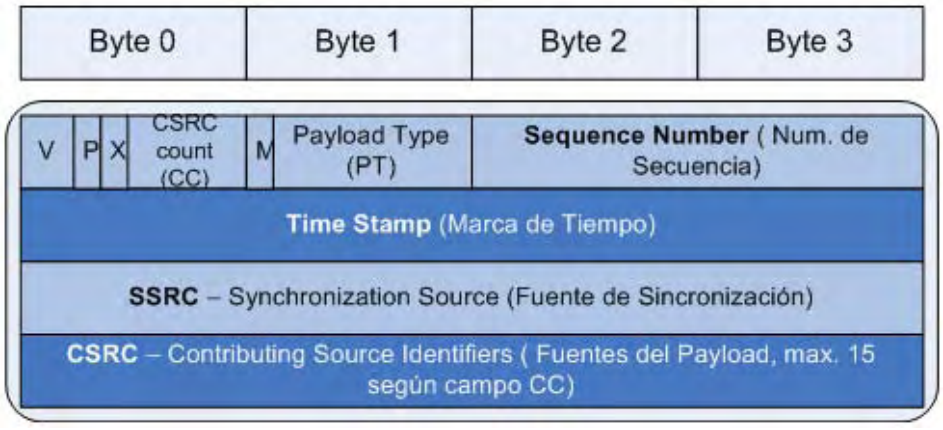

Figura 2.25: Encabezado RTP

La descripción de cada uno de los campos es la siguiente:

- Identificador de la versión de RTP (V): 2 bits.

Figura 2.26: Encapsulamiento RTP

- Padding (P): 1 bit. Indica si hubo que efectuar un relleno de bits para cumplir con algún requerimiento mínimo (por ejemplo, para un algoritmo de encriptación).
- La extensión (X): 1 bit. Señala la presencia de extensiones del encabezado. Este mecanismo permite añadir información extra al encabezado RTP.
- Conteo CSRC (CC): 4 bits. El número de fuentes de flujo multimedia(Contributing Source).
- Marcador (M): 1 bit. Se utiliza para indicar frames.
- Payload Type (PT): 7 bits. Nos indican el tipo de datos multimedia que transporta el paquete.
- El número de secuencia (sequence number): 16 bits. Permite al receptor de un stream RTP detectar paquetes perdidos o en desorden. El emisor incrementa el valor en una unidad por cada paquete transmitido. Notar que RTP no hace nada al detectar un paquete perdido, sino que deja que la aplicación decida que hacer cuando se pierde un paquete.
- Marca de tiempo (Time Stamp): 32 bits. Permite al receptor la reproducción de las muestras en los intervalos apropiados, y ayuda a la sincronización de diferentes streams.
- La fuente de sincronización (SSRC): 32 bits. Identifica la fuente de un stream RTP. Permite también que un nodo con múltiples fuentes distinga entre ellas.
- El campo CSRC (Contributing Source): 32 bits cada uno. Es usado sólo cuando streams RTP pasan por un mezclador, éste puede ser usado para reducir los requerimientos de ancho de banda.

2.3.3. El Protocolo de Intercambio Inter-Asterisk - IAX

El protocolo IAX[10], proporciona control y transmisión de media streaming sobre el protocolo de Internet (IP). Además, puede usarse para transmitir video, pero esta asignado principalmente al control de llamadas de Voz sobre IP. Su diseño fue en primera instancia para las conexiones de VoIP entre servidores Asterisk, posteriormente se utilizó como protocolo de conexión entre usuarios.

Los objetivos principales del protocolo IAX son:

1. Minimizar el uso del ancho de banda (BW) usado en las transmisiones de control y en el establecimiento de una llamada de voz.

2. Proporcionar soporte transparente a dispositivos NAT (Network Address Translation) usando como protocolo de transporte UDP (usualmente el puerto 4569), en donde tanto información de señalización como datos viajan conjuntamente. IAX no se sirve de RTP para el transporte del flujo de Voz como lo hace SIP.

3. Capacidad para soportar el envío de información del plan de marcación.

IAX es un "protocolo de señalización y transporte de VoIP" *peer-to-peer*. El componente de señalización del protocolo IAX posee características similares al SIP, en comparación al MGCP, que es tipo maestro-esclavo.

IAX es un protocolo binario al igual que H.323 y a diferencia de SIP que esta basado en texto. Esta elección de diseño fue hecha para hacer un uso más eficiente del ancho de banda para las llamadas de voz.

Trazado de una llamada IAX

En una llamada IAX2 se presentan tres fases:

1. **Establecimiento de la llamada.-**La Terminal A inicia la llamada enviando un mensaje "NEW" para la Terminal B. La Terminal B inmediatamente envía de regreso un mensaje "ACCEPT", indicándole a la Terminal A que ha recibido la solicitud y esta comenzando el servicio. La Terminal A envía un mensaje "ACK" para la Terminal B para confirmar la recepción del mensaje. Una vez que el teléfono de la Terminal B comienza a timbrar, este le envía de regreso a la Terminal A un mensaje "RINGING". La Terminal A envía de regreso un mensaje "ACK" para la Terminal B lo cual indica que ha recibido el mensaje "RINGING". Finalmente, cuando el teléfono de la Terminal B es contestado, está envía un mensaje "ANSWER" a la Terminal A y la llamada se establece completamente.

2. **Flujo de datos o flujo de audio.-**En la figura 2.28 se ilustra un solo sentido del flujo de datos de IAX, pero para una llamada de voz se presentan en ambos sentidos. Cada flujo está compuesto de "Mini Frames" (M), que contienen solo una cabecera de 4 bytes, cuyo objetivo es optimizar el ancho de banda. El flujo es complementado por "Full Frames" periódicos (F) que incluyen información de sincronización.

3. **Liberación de la llamada o desconexión.-**La Terminal A inicia la liberación de la llamada enviando un mensaje de "HANGUP" para la Terminal B. Está a su vez devuelve un mensaje "ACK" indicando que a recibido la petición de la liberación y confirma que la llamada ha sido liberada.

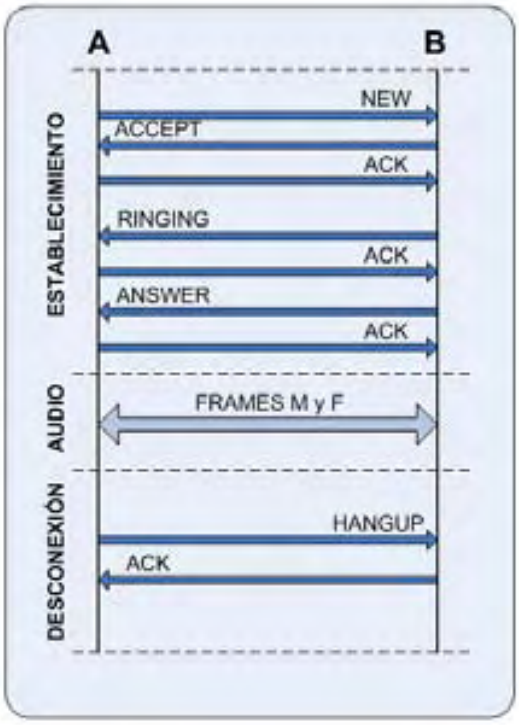

Figura 2.27: Trazado de mensajes IAX

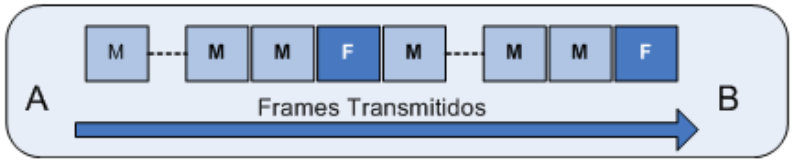

Figura 2.28: Frames IAX

El Frame IAX

IAX utiliza "frames" para enviar la información. Existen varios tipos de frames IAX, la estructura básica es la siguiente:

Un bit F es usado para indicar que se trata de un full frame o no. Cuando se tienen un valor de 1 dentro de este campo indica que el frame es un full frame y un valor de 0 indica que se trata de otro Frame excepto un full frame.

Los campos *"Source Call Number"* y *"Destination Call Number"* tienen 15 bits de longitud cada uno y son enteros no signados que identifican el origen y destino de la conexión (llamada). Se puede ver que existen dos valores diferentes para cada dirección de la llamada. Un valor cero es un número especial de llamada que indica que el número de la llamada es desconocido.

Un Timestamp puede ser un valor completo de 32 bits o una versión abreviada de 16 bits. En el caso de un campo de 16 bits, el valor está formado realmente por los 16 bits menos significativos de uno completo de 32 bits, esto es mantenido por la Terminal final.

Full Frame

Un full frame puede ser usado para el envío de la señalización, audio o video. *Los full frames son el único tipo de frames IAX que se transmiten de forma confiable.* Esto significa que el destinatario enviará algún tipo de mensaje de regreso inmediatamente después de la recepción. En algunos casos, el protocolo puede requerir un tipo específico de mensaje de regreso, de otro modo el destinatario solo envía un acuse de recibo. En la figura 2.27, en la parte del establecimiento de la llamada muestra ambos casos. Después de recibir un nuevo mensaje, el destinatario debe regresar un mensaje de aceptación de inmediato. En este caso, se requiere un ACK no explícito. Después, cuando un mensaje de timbrado es enviado, la Terminal A debe enviar de regreso un mensaje ACK explícito, puesto que el protocolo IAX no requiere que otro mensaje sea enviado de regreso en ese momento.

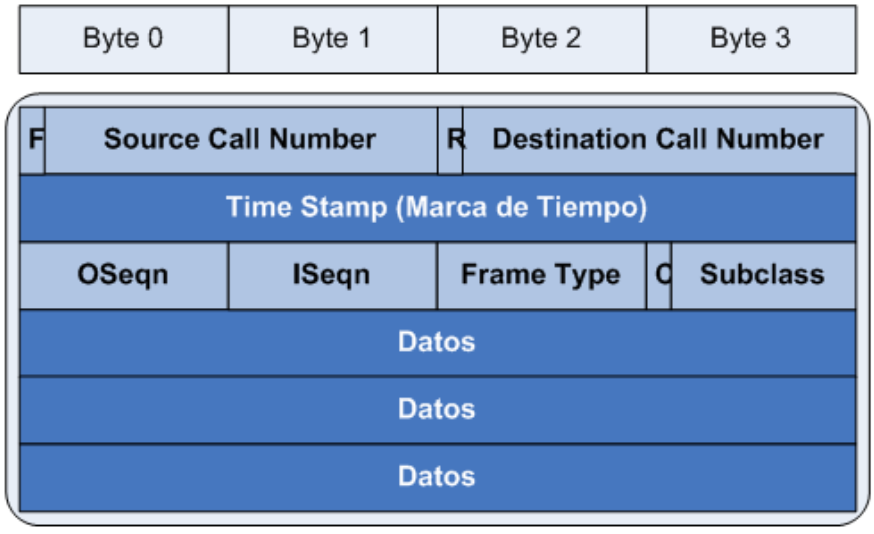

Figura 2.29: Formato binario del Full Frame

En la tabla 2.3 se describe cada uno de los campos de la figura 2.29, donde se detallará a través de una descripción su funcionamiento.

Campo	Descripción
F	Se establece el valor de 1 indicando que este es un full frame y si tiene el valor 0 indica que no es un full frame.
Source Call Number	El número de llamada de origen del full frame transmitido: 15 bits que identifican la conversación de origen, ya que puede haber varias comunicaciones multiplexadas por la misma línea.
R	Se establece el valor de 1 si este frame comienza a retransmitir y el valor de cero para la transmisión inicial.
Destination Call Number	El número de llamada destino del full frame: 15 bits que identifican la conversación del destino, ya que puede haber varias comunicaciones multiplexadas por la misma línea.
Timestamp	Trama de 32 bits, marca el tiempo de cada paquete.
OSeqno	Numero de secuencia de salida con 8 bits. Comienza en 0 y se va incrementando por cada mensaje.
ISeqno	Número de secuencia de entrada con 8 bits. Comienza en 0 y se va incrementando por cada mensaje.
Frame Type	Tipo de frame, identifica la clase de frame con 8 bits
C	Formato del valor de la subclase: Puesto a 0 indica que el campo subclase debe tomarse como 7 bits (un solo mensaje), si esta en 1 indica que el campo subclase se obtiene con 14 bits (dos mensajes consecutivos).
Subclass	Subclase del mensaje
Data	Datos que se envían en formato binario.

Tabla 2.3: Descripcion de campos del datagrama IAX

El campo "*Frame Type*" (Tipo de frame), junto con el campo de subclass determinan la función de cada paquete que se esta enviando o recibiendo, y sirve por tanto como señalización de control. En la tabla 2.4 se muestran los valores del campo "*Frame Type*" de las tramas F o full frame

Tipo	Descripción	Descripción de Subclase	Descripción de Datos
0x01	DTMF	0-9, A-D, *,	
0x02	Datos de voz	Formato de compresión de Audio	Datos de la Voz
0x03	Video	Formato de compresión de Video	Datos del Video
0x04	Control	Tipos de frame de control	
0x05	No usado		
0x06	Control IAX	Mensajes del Protocolo IAX	Información Elemental
0x07	Texto		Texto
0x08	Imagen	Formato de compresión de la Imagen	Datos de la Imagen
0x09	HTML	Tipos de frame HTML	Mensaje especifico

Tabla 2.4: Valores del Campo Frame Type

El campo subclase para el caso de un "*Frame Type*" de transmisión de voz, puede

tener cualquiera de los valores listados en la tabla 2.5 para el formato de compresión de Voz.

Subclase	Descripción	Cálculo de Longitud
0x0001	G.723.1	4, 20 y 24 byte de frames de 240 muestras
0x0002	GSM Tasa llena	33 byte cortos de 160 muestras o
		65 byte cortos de 320 muestras
0x0004	G.711 ley-mu	1 byte por muestra
0x0008	G.711 ley-a	1 byte por muestra
0x0010	MP3 (desaprovado)	
0x0020	IMA ADPCM	1 byte por 2 muestras
0x0040	16-bit Lineal	2 bytes por muestra
	little-endian	
0x0080	LPC10	Tamaño de frame variable de 172 muestras
0x0100	G.729	Segmento de 20 bytes por 172 muestras
0x0200	Speex	Variable
0x0400	ILBC	50 bytes por 240 muestras

Tabla 2.5: Formato de Compresión de la Voz

Hay dos tipos de información de control que se pasa entre "peers"que usan full frames, estos son *Frames de Control*, tabla 2.6 y *Frames de Control IAX* tabla 2.7. Los frames de control proporcionan el control de la sesión, por lo que controlan a los dispositivos conectados en puntos finales del IAX. Los frames de control IAX proporcionan al protocolo IAX la dirección de puntos finales específicos, es decir, que es usado para manejar interacciones con el protocolo IAX que son generalmente independientes del tipo de puntos finales.

Subclase	Descripción
0x01	Hangup
0x02	Ring
0x03	Ringing (Timbrado)
0x04	Answer
0x05	Busy Condition
0x08	Congestion Condition
0x0a	Wink (Parpadeo)
0x0b	Option
0x0c	Key Radio
0x0d	Unkey Radio
0x0e	Call Progress

Tabla 2.6: Frame de Control

Subclase	Código Mnemotécnico	Descripción
0x01	NEW	Iniciar una nueva llamada
0x02	PING	Enviar un Ping
0x03	PONG	Responder un Ping
0x04	ACK	Respuesta afirmativa “Acknowledgement”
0x05	HANGUP	Inicio de la liberación de la llamada
0x06	REJECT	Rechazar
0x07	ACCEPT	Aceptación
0x08	AUTHREQ	Petición de autenticación
0x09	AUTHREP	Respuesta de autenticación
0x0a	INVAL	Llamada inválida
0x0b	LAGRQ	Petición de retraso
0x0c	LAGRP	Respuesta de retraso
0x0d	REGREQ	Petición del registro
0x0e	REGAUTH	Autenticación del registro
0x0f	REGACK	Respuesta afirmativa del registro
0x10	REGREJ	Denegación del registro
0x11	REGREL	Liberación del registro
0x12	VNAK	Petición para retransmitir Video/Voz
0x13	DPREQ	Petición del plan de marcación
0x14	DPREP	Respuesta del plan de marcación
0x15	DIAL	Marcado
0x16	TXREQ	Petición de la transferencia
0x17	TXCNT	Conexión de la transferencia
0x18	TXACC	Aceptación de la transferencia
0x19	TXREADY	Transferencia preparada
0x1a	TXREL	Liberación de la transferencia
0x1b	TXREJ	Rechazar la transferencia
0x1c	QUELCH	Interrumpir transmisión de Audio/Video
0x1d	UNQUELCH	Continuar transmisión de Audio/Video
0x1e	POKE	Petición activar
0x1f	PAGE	Compaginar la descripción de la llamada
0x20	MWI	Indicador de mensaje en espera
0x21	UNSUPPORT	Mensaje no permitido
0x22	TRANSFER	Petición de la transmisión remota

Tabla 2.7: Frame de Control IAX

Trama M o Mini Frames

Un mini frame es usado para enviar un mínimo de información en la cabecera del protocolo.

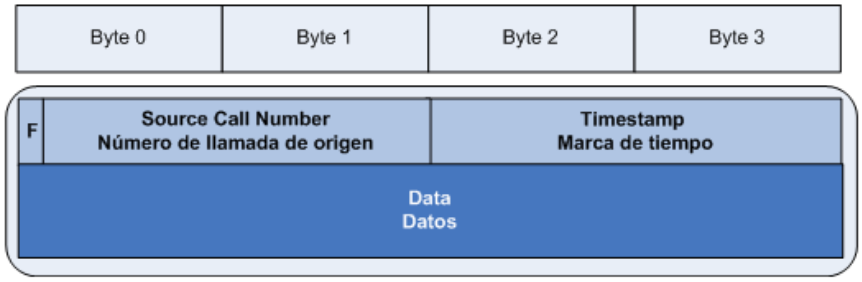

Figura 2.30: Formato binario del Mini Frame

Campo	Descripción
F	Establece el valor de 0 indicando que este no es un full frame.
Source Call Number	Número de llamada del lado que esta transmitiendo el mini frame.
Timestamp	Marca el tiempo solo tiene 16 bit para aligerar la cabecera.

Tabla 2.8: Trama M o Mini Frame

Tabla comparativa entre el Protocolo IAX y el Protocolo SIP

	Protocolo IAX	Protocolo SIP
Ancho de Banda	Menor.	Mayor.
Codificación	Binaria.	Texto.
Envió de información	La señalización y los datos viajan conjuntamente.	La señalización y los datos viajan en forma separada.
NAT	Sin problemas.	Con problemas.
Estandarización	Se encuentra en proceso de estandarización.	Protocolo estandarizado por la IETF.
Utilización de puertos	IAX usa únicamente el puerto 4569 para mandar la información de señalización y los datos de todas las llamadas.	SIP utiliza el puerto 5060 para señalización y 2 puertos RTP por cada conexión de audio.
Flujo de audio	La señalización como los datos al viajar conjuntamente necesariamente el tráfico pasa por el servidor IAX.	La señalización de control siempre pasa por el servidor, pero la información de audio (RTP) viajar de extremo a extremo sin tener que pasar necesariamente por el servidor SIP.
Real Time Protocol (RTP)	No lo utiliza.	Si lo utiliza.

Tabla 2.9: Tabla Comparativa de Protocolos

2.4. Seguridad en Redes ToIP

> *La transmisión de VoIP (Voice over IP — envío de paquetes de voz a través de redes conmutadas mediante el protocolo de Internet o IP) es una de las tecnologías con un auge considerable en las telecomunicaciones en la actualidad. Como muchas de las nuevas tecnologías presenta situaciones favorables, así como algunos riesgos o inconvenientes.*
> Ortega Aceves, Israel. "*Seguridad de Voz sobre IP*"[3]

En una Red Telefónica Pública Conmutada (PSTN) no se requiere la encriptación de la información. La violación de la confidencialidad en las redes convencionales se presenta cuando se interviene la línea, por lo tanto, es necesario estar conectado físicamente a la red. Con la tecnología VoIP, el propio protocolo facilita la identificación de la llamada desde cualquier lugar de la red. Al transmitir Voz junto con el tráfico de datos dentro de una Red IP, en donde, por naturaleza se comparte el medio, ésta se encuentra expuesta a los mismos riesgos de seguridad que cualquier otro tipo de información. La disponibilidad de las herramientas que permiten realizar monitoreo y captura de voz es amplia.

Algunas de las amenazas de seguridad mas comunes para redes VoIP se enlistan enseguida:

- Phishing - Literalmente es "salir a pescar" contraseñas, con todo lo que eso implica.
- Spoofing (Robo de identidad) - Utilizando técnicas de desvío de tráfico como *ARP poissoning*, un analizador de protocolos de red (*sniffer*) y herramientas para el "*cracking*"de contraseñas por fuerza bruta, es posible obtener toda la información necesaria para hacerse pasar por algúien mas.
- Captura de conversaciones - Una vez que se consigue ingresar a una parte clave de la infraestructura, como una puerta de enlace de VoIP (Gateway), un atacante puede capturar paquetes sin que la conversación se vea afectada. Una vez capturada la llamada IP, dada su naturaleza digital, es fácil almacenarla y reproducirla.
- Ataques de negación de servicios (Denial of Service *DoS*) - Los ataques de negación de servicios (DoS) pueden ocurrir cuando la red o el dispositivo se encuentran sobrecargados con tráfico sin sentido (p. ej. *UDP flooding*), o se envía una orden específica que la deshabilita, dejando a la red sin disponibilidad. La telefonía IP es vulnerable a los ataques de DoS al compartir la misma red con datos convencionales. La tecnología VoIP también es vulnerable a los ataques de virus. Estos ataques de virus están directamente relacionados con el sistema operativo.
- Realización de llamadas sin autenticar - Debido a la flexibililidad de los protocolos de señalización VoIP, es posible realizar llamadas IP sin necesidad de hacer un registro riguroso ante el ITSP (véase el glosario). Esto permite que alguién mas, haga uso no

autorizado de los recursos de nuestra red VoIP (*fraude telefónico*), con la consecuente pérdida económica que eso representa.

La demanda en las redes de ToIP ha propiciado el desarrollo de políticas de seguridad, donde se definen los procedimientos, las responsabilidades, los controles y las medidas de seguridad necesarios para proteger la información transmitida en un entorno convergente[19] .

Algunas de las mejores prácticas para disminuir los riesgos de seguridad en redes VoIP son:

- Separar la voz y datos en diferentes redes lógicas formando VLAN's (Redes de Área Local Virtuales) y segmentar la red. Cada red tendrá sus propias reglas sin afectarse una a la otra. Es como dividir un campo de fútbol en dos partes, A y B, para formar dos campos más pequeños, donde nadie de la mitad B puede jugar en la mitad A, ya que pertenecen a partidos diferentes.

- Habilitar protocolos de cifrado de datos para la protección de información sensible, como contraseñas, certificados de autenticación, etc. Ejemplo de técnicas de cifrado es AES (Advanced Encryption Standard), que emplea algoritmos matemáticos con diferentes operaciones de sustitución, desplazamiento, mezcla de estado, etcétera; con la finalidad de garantizar un cifrado fuerte.

- El uso de la tecnología VPN para establecer un circuito virtual seguro entre dos nodos, reduce el riesgo de intervenciones. Sin embargo, si la encriptación no se realiza entre los extremos adecuados (gateways) esta no es efectiva. O bien, podemos recurrir a otros métodos como son IPsec (IPsegura) o SRTP (Secure RTP).

- Es importante el uso de *contraseñas seguras* con el empleo de la mayor variedad de símbolos posible.

- Establecer sistemas de autenticación mas robustos para los usuarios, tales como el uso de certificados de seguridad, llaves compartidas, LDAP, RADIUS, etc.

- La señalización puede cifrarse a través de TLS (Transport Layer Security). TLS autentica y avala la identidad de los servidores ITSP; Para lograr lo anterior, se usan entidades certificadoras independientes como VeriSign que verifican las identidades, garantizando al usuario plena confianza en el servidor o servicio en cuestión, por medio de la generación de llaves privadas y públicas.

- Implementar sistemas de redundancia y respaldo en nuestra red, tanto físicos como logicos, por ejemplo: redundancia de potencia eléctrica, de enlaces de comunicación, respaldo de la información clave, etc.

[19] La información aquí expuesta sobre la seguridad de VoIP es de índole general y no pretendemos entrar en detalles al respecto, puesto que representa un tema aparte. Nuestro objetivo es, mas bien, dar a conocer que existen vulnerabilidades que deben ser tomadas en cuenta para garantizar la seguridad de la información.

2.5. Calidad de Servicio

En un principio las redes solo estaban diseñadas para la transmisión de datos, conforme crecieron en tamaño y capacidad se comenzó a transmitir voz y video, lo que llevó al aumento en la demanda de los recursos en la red.

La Calidad de Servicio - Quality of Service (QoS) es un conjunto de medidas a nivel protocolos de comunicación diseñado para establecer distintos niveles de prioridad a diferentes tipos de tráfico en una red IP, está característica no es inherente a una infraestructura de red, sino que se debe implementar de forma estratégica en la misma. Sin QoS, sería imposible garantizar que el tráfico de voz sea transmitido correctamente y recibido con la calidad requerida. Por lo tanto, una red a la que le ha sido implementada la calidad de servicio dará mayor prioridad al tráfico de aplicaciones de tiempo real (Voz) y en segundo término quedarán aplicaciones que no son sensibles a los efectos de retardo (p. ej. Datos).

Figura 2.31: Diagrama QoS

Las aplicaciones de datos basadas en TCP pueden reenviar paquetes que se han perdido, esto induce un retraso, lo cual no es deseable en aplicaciones de flujo de medios en tiempo real como voz y video. Este tipo de tráficos se transmiten mediante UDP donde solo se cancelan los paquetes perdidos.

Los parámetros de la calidad de servicio (QoS) son: El retardo (delay), la variación del retardo (Jitter) y la pérdida de paquetes (Packetloss). Una red debe garantizar un cierto nivel de calidad de servicio para un cierto tipo de tráfico que sigue un conjunto específico de parámetros, también se debe tomar en cuenta la implementación en la propia Red de Políticas de Calidad de Servicio (Ver tabla 2.10).

La Calidad del Servicio puede medirse a partir de aspectos como la integridad de la información recibida, así como de la disponibilidad del servicio.

- **Integridad.-**Los paquetes de VoIP se transmiten de forma independiente unos de otros, y como cualquier paquete de datos es vulnerable a pérdidas, por lo que pueden afectar la calidad de la voz en la comunicación.

  El control del jitter mantiene los paquetes de VoIP en la memoria hasta que llegan los

Políticas de Calidad de Servicio
Asignar ancho de banda en forma diferenciada.
Evitar y/o administrar la congestión en la red.
Manejar prioridades de acuerdo al tipo de tráfico.
Modelar el tráfico de la red.
Tiempo de espera reducido.
Ausencia de pérdidas de paquetes.

Tabla 2.10: Tabla de Servicios Diferenciados

paquetes más lentos y posteriormente, los transmite en la secuencia correcta[20] , ésto ayuda a mantener el orden de los paquetes de voz, sin embargo, aún así es necesario dar mayor prioridad a los paquetes de voz respecto a los datos convencionales en la red.

- **Disponibilidad.-**Al compartir el mismo medio de transmisión la voz y los datos, aumenta el riesgo de la disponibilidad del medio y se debe analizar cuanto ancho de banda se necesitará para satisfacer las necesidades de ambos paquetes. La transmisión de voz al ser una aplicación en tiempo real crítica, no se puede comprometer su calidad.

  Las amenazas de la disponibilidad varían desde errores en la calidad de la voz hasta la interrupción del sistema que afecta a la red en forma parcial o total.

Servicios Integrados

Provee a las aplicaciones una calidad de servicio basada en la reserva de recursos de red. Utiliza el protocolo RSVP (Resorce reSerVation Protocol). Son los dispositivos de red, tales como los propios routers, quienes generan un estado en cada flujo para que se efectúe la reserva de los recursos, algo equivalente a un circuito virtual.

En la arquitectura IntServ se definen tres tipos de servicio:

- **Servicio Garantizado:** Garantiza un caudal mínimo y un retardo máximo.
- **Servicio de Carga Controlada:** Este servicio debe ofrecer una calidad comparable a la de una red de datagramas poco cargada.
- **Servicio Best Effort:** Este servicio no tiene ninguna garantía.

[20] Achieving voice quality in packet networks, Sandeep Sharma, Express Computer, 11 de Octubre de 2002.

Servicios Diferenciados

La técnica denominada Servicios Direfenciados (DiffServ), surge de la necesidad de controlar la forma de compartir los recursos de la red para satisfacer los requisitos de cada servicio. Una solución es permitir que los enrutadores y conmutadores de la red se comporten de forma distinta en función de los distintos tipos de servicios (voz, datos y video).

En DiffServ se definen tres tipos de servicio, que son los siguientes:

- **Servicio Expedited Forwarding o Premium:** Este servicio es el de mayor calidad. Debe ofrecer un servicio equivalente a una línea dedicada virtual.
- **Servicio Assured Forwarding:** Este servicio asegura un trato preferente, pero no garantiza caudales, retardos, etc.
- **Servicio Best Effort:** Este servicio se caracteriza por tener cero los tres primeros bits del DSCP (Differentiated Services Code Point). En este caso los dos bits restantes pueden utilizarse para marcar una prioridad, dentro del grupo 'best effort'. En este servicio no se ofrece ningún tipo de garantías.

2.6. Ventajas y Desventajas de la Telefonía IP

Si bien es cierto que el uso de la tecnología VoIP en telefonía IP trae consigo innumerables ventajas, una de ellas y quizás la más mencionada es la reducción de costos en el transporte de la voz como datos, también es necesario reflexionar sobre las desventajas que representa transportar datos junto con voz en una misma red. A continuación mencionamos algunas de las ventajas y desventajas que trae consigo la telefonía IP, estableciendo claramente cuales son las fortalezas y debilidades de la telefonía IP.

Ventajas
Flexibilidad en el uso de las comunicaciones Mediante el uso de la Internet como plataforma de comunicación, es posible establecer comunicaciones desde cualquier sitio donde seamos capaces de conectarnos.
Portabilidad del número Los números de extensiones al estar asociados a cuentas VoIP fijas, permiten la movilidad geográfica, por lo que el usuario dispondrá del servicio telefónico en cualquier punto donde haya conexión a la Internet de alta velocidad.
Existen gran diversidad de dispositivos IP Con el surgimiento de nuevos proveedores que comienzan a integrarse al mercado de la telefonía IP han generado una diversidad de dispositivos IP, capaces de sustituir a los viejos teléfonos analógicos.
Se reducen los costos de transporte de la voz El tráfico de voz sobre redes IP, puede reducir o eliminar los cargos asociados con el transporte de llamadas sobre la red telefónica publica conmutada (PSTN). El ahorro en llamadas de larga distancia no dependerá de la duración de la llamada, sino del precio de la conexión a la Internet. Es decir, el servicio de voz será tarifado como un servicio más de datos, como lo es el mandar e-mails, navegar en páginas Web, etc.
Envió de información simultánea de datos, voz, fax y video La tecnología VoIP, permite transmitir la voz sobre una red de datos de manera que el coste por enviar y recibir voz por la red sea 0 (cero, significa mayor prioridad). La red de comunicaciones se verá enormemente simplificada, esto debido a que no habría que cablear por duplicada la red, sino que se agruparían todos los servicios.
Permite trabajar remotamente El servidor presenta la flexibilidad de ser administrado remotamente a través de programas de control y automatización como SSH, Telnet o Putty que se encuentran solicitando peticiones a la Internet o de la red local.

Tabla 2.11: Tabla de Ventajas

Ventajas
Permite compatibilidad de tecnologías La compatibilidad de la tecnología VoIP entre diferentes tecnologías ha permitido su desarrollo y su implementación de forma masiva.
Cableado estructurado convergente Con la innovación de la telefonía IP es necesario mejorar el cableado estructurado y migrarlo a la categoría 6 que trae consigo mejoras en la gestión de calidad de la red.
Reduce costos de mantenimiento y capacitación La aplicación y la infraestructura al ser menos compleja, permiten que los costos por mantenimiento y soporte permanezcan inferiores a los sistemas tradicionales de voz.
Estándares abiertos e interoperabilidad VoIP puede adoptar estándares abiertos e incluso estándares propietarios, esto permite la integración de equipos de múltiples fabricantes y elimina la dependencia de las soluciones propietarias. Al utilizar un estándar abierto es posible desarrollar aplicaciones innovadoras e implantarlas rápidamente.
Productividad de la tecnología Las aplicaciones y servicios IP mejoran la productividad al añadir, eliminar, mover o cambiar en menos tiempo la configuración de un usuarios en la red, además de la pronta instalación de nuevos servicios.
Permite utilizar arquitecturas centralizada o distribuida En un principio las redes de voz se encontraban construidas sobre una arquitectura centralizada, donde los teléfonos eran controlados por los conmutadores. Con la tecnología VoIP, las redes de voz pueden estar construidas sobre una arquitectura centralizada o bien distribuida. Esta flexibilidad permite construir redes caracterizadas por una administración simplificada e innovación de Endpoints (Los Endpoints pueden ser Gateways VoIP, teléfonos IP, servidores media, o cualquier dispositivo que pueda iniciar y terminar una llamada VoIP.), dependiendo del protocolo usado. La arquitectura Centralizada (protocolos MGCP o MEGACO), permite centralizar la administración, el aprovisionamiento y el control de llamadas. Simplifica el flujo de llamadas repitiendo las características de voz. Sin embargo, contar con está arquitectura suprime las innovaciones de las características de los Endpoints y llega a presentar problemas cuando se pretende programar servicios VoIP. La arquitectura distribuida (protocolos H.323 y SIP), permite que las aplicaciones de VoIP sean tratadas como cualquier otra aplicación IP, proporcionando mayor flexibilidad para añadir inteligencia a cualquier dispositivo de control de llamadas (Los dispositivos de control de llamadas son llamados Gatekeepers en una red H.323, y servidores proxy o servidores Redirect en una red SIP.o Endpoints, dependiendo de los requerimientos tecnológicos y de la propia red.

Tabla 2.12: Tabla de Ventajas

Desventajas
La Disponibilidad Hablando en términos de disponibilidad, las soluciones de telefonía IP tienen aún, un largo camino por recorrer. Mientras los sistemas de telefonía tradicional son capaces de asegurar una disponibilidad del 99.999 % en un periodo de un año (esto significa una interrupción del servicio de 5 minutos al año, lo cual es imperceptible por el usuario común), los sistemas ToIP se encuentran sujetos a las mismas condiciones que las redes de datos y no puede ofrecer, por ahora, los mismos niveles de ininterrupción del servicio.
No existe un estándar universal VoIP es una tecnología que aún no cuenta con un estándar universal, por lo que en ausencia de estándares globales, los fabricantes han creado sus propios protocolos lo que ha hecho difícil la interoperabilidad e integración entre dispositivos. A pesar de ello, han surgido protocolos estándares de señalización, como son: H.323, SIP, Megaco (H.248) y MGCP, siendo los dos primeros los más utilizados en la actualidad.
La seguridad La seguridad es un tema de importancia en las redes VoIP. Tal y como se menciona en Seguridad de voip[3], existen técnicas como el *ARP poissoning* que junto con otras herramientas, hacen relativamente fácil la tarea de grabar conversaciones VoIP. También existen softwares capaces de provocar loop's en los servidores, es decir, el servidor recibe peticiones que al incrementarse ocasionan que esté se sature y empiece a perder gestión con la llamadas
El tema de la potencia (evaluación costo-beneficio) Para cuantificar los beneficios con respecto a los costos, es necesario conocer que esperamos obtener con su implementación y si está cumple nuestras expectativas. En un principio el costo superará los beneficios, puesto que es una tecnología nueva requiere una mayor inversión en equipo y esto acarrea mayores costos. Un buen servicio Voip no esta restringido solo al costo, sino también a la operatividad, calidad, soporte local, escalabilidad e incluso a la posibilidad de la convergencia.
Inversión inicial representativa La inversión en materia de infraestructura e innovación tecnología es alta, pero, la implementación de una red VoIP atraerá beneficios a corto y largo plazo que amortizarán esa inversión inicial.

Tabla 2.13: Tabla de Desventajas

Capítulo 3

Software Libre y Telefonía IP

El mundo del "Software Libre" ha creado una nueva manera de hacer las cosas. Este movimiento se ha desarrollado a la par de los servicios de la Internet, mismos que proporcionan las condiciones idóneas para la creación de ideas novedosas y sin restricciones. Asterisk y OpenSER son ejemplo de como el trabajo organizado en comunidades virtuales da lugar a un círculo virtuoso y creador. Asterisk y OpenSER son dos de las principales plataformas utilizadas en la actualidad para implementar soluciones de VoIP como telefonía IP. En este capítulo describiremos las principales características de Asterisk y OpenSER, así como sus ventajas y desventajas. Esperamos que al lector le resulte de utilidad la información que aquí incluimos.

3.1. Software Libre

El movimiento del software libre ha permeado en casí todos los ámbitos tecnológicos modernos. La prueba más palpable del éxito que ha alcanzado este movimiento es el Sistema Operativo Linux; sin embargo, no es la única, ya que existen numerosos casos de éxito, incluso en terrenos como el hardware. La filosofía del "Software Libre" es transparente y el fín que persigue es el progreso en comunión, pero, ¿qué características son las que determinan el que un programa sea considerado como software libre?

El "Software Libre" es cuestión de libertad, no de precio. Para entender el concepto, debemos pensar en "libre" como en "libertad de expresión", no como en "cerveza gratis"[1] . El término "Software Libre" nos refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. El software libre garantiza las cuatro libertades del usuario, estás son los siguientes:

- La libertad de usar el programa, con cualquier propósito (libertad 0).
- La libertad de estudiar como funciona el programa, y adaptarlo a tus necesidades (libertad 1). El acceso al código fuente es una condición previa para esto.
- La libertad de distribuir copias, con el proposito de difusión (libertad 2).
- La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie. (libertad 3). El acceso al código fuente es un requisito previo para esto.

Un programa es considerado "software libre" si los usuarios tienen todas estas libertades. Así, pues deberíamos tener la libertad de distribuir copias, sea con o sin modificaciones, sea gratis o cobrando una cantidad por la distribución, a cualquiera y en cualquier lugar. El ser libre significa (entre otras cosas) que no tenemos que pedir o pagar permisos.

Para que estas libertades sean reales, deben ser irrevocables, mientras no hagas nada incorrecto; si el desarrollador del software tiene el poder de revocar la licencia, aunque no le hayas dado motivos, el software no se considera libre. Sin embargo, son aceptables ciertos tipos de reglas sobre la manera de distribuir software libre, mientras no entren en conflicto con las libertades centrales. Por ejemplo, copyleft ["copia permitida"] es la regla que implica que, cuando se redistribuya el programa, no se pueden agregar restricciones para denegar a otras personas las libertades centrales. Esta regla no entra en conflicto con las libertades centrales, sino que más bien las protege.

El software libre se distribuye bajo una licencia conocida como GNU/GPL[2] que garantiza las libertades del mismo. "software libre" no significa "no comercial". Un

[1] En inglés la palabra *free* significa tanto libre como gratis, lo que ha dado lugar a cierta confusión.

[2] Se puede encontrar la última versión de esta licencia directamente en la página electrónica `http://gplv3.fsf.org/`. Recomendamos la versión en inglés, puesto que la versión traducida al castellano aún no es reconocida oficialmente y puede dar lugar a interpretaciones legales incorrectas.

programa libre debe estar disponible para uso, desarrollo y distribución comerciales. El desarrollo comercial del software libre ha dejado de ser inusual.

Cuando se habla de software libre, es mejor evitar términos como: "regalar" o "gratis", porque esos téminos implican que lo importante es el precio, y no la libertad.

Para obtener un mejor conocimiento acerca del software libre, las categorias existentes y los organismos involucrados en su promoción, recomendamos consultar los siguientes sitios en la Internet:

- `http://www.gnu.org/`
- `http://www.fsf.org/`
- `http://gplv3.fsf.org/`

En las secciones subsecuentes a esta, expondremos dos de los principales ejemplos de soluciones para telefonía IP basados en "Software Libre". Nos referimos a Asterisk y OpenSER

3.2. Asterisk

Asterisk es de acuerdo con "Jared Smith, Leif Madsen y Jim Van Meggelen"[8], un completo IP-PBX basado en Software Libre. Esto quiere decir, que Asterisk brinda todos los servicios de un PBX convencional; por ejemplo: Matra, Nortel, etc. En palabras nuestras lo hemos definido como un Conmutador Híbrido[3] basado en Software Libre. Fue creado por Mark Spencer, fundador de la compañía Linux Support Services, Inc. ahora Digium©, empresa que sigue siendo la principal desarrolladora de las versiones estables. Asterisk se distribuye en dos versiones: la comercial (*Business Edition*) y la de código abierto (*Open Source*), en la versión comercial (basada en la libre), se eliminan aquellos elementos susceptibles de ocasionar fallos y pérdida de estabilidad, además, la empresa Digium© brinda soporte durante un año.

En cuanto a la versión "Open Source", ésta cuenta con una activa comunidad[4] que la respalda. Existen multitud de desarrolladores que han aportado funciones y nuevas aplicaciones al proyecto. En su versión libre, Asterisk se distribuye bajo licencia GNU-GPL (General Public License). Esta licencia nos permite distribuir libremente el software Asterisk tanto en código fuente como en binario, con o sin modificaciones y; por lo tanto, sin responsabilidad alguna por parte de quien lo distribuye. Actualmente, existen dos "releases" principales, las versiónes 1.2.X y la 1.4.X. El 18 de enero de éste año (2008), Digium© anunció la liberación de la versión 1.6.0-beta1 la cual esta bajo prueba y actualmente puede probarse el beta4. La idea detrás de Asterisk es simplicidad y poderio[9].

Asterisk puede ser ejecutado en diversas plataformas UNIX como Linux, Open BSD, MacOS-X y Sun[5] . El costo total de implementar una solución para telefonía IP basada en Asterisk comparado con las soluciones propietarias es mucho menor. Asterisk nos permite construir aplicaciones de comunicaciones tan complejas o avanzadas como se desee, por su naturaleza de ser exclusivamente software.

Como mencionamos anteriormente, Asterisk posee todas las capacidades de un PBX convencional e incorpora algunas funcionalidades complejas que en soluciones propietarias son muy costosas e incluso se distribuyen como productos por separado. Algunos de los servicios que Asterisk es capaz de brindar son: Correo de Voz, Conferencia Telefónica, Directorio Corporativo, IVR (Interactive Voice Response), Colas de Llamadas, Servicio de Identificación de Llamadas (CallerID), Video-Llamadas (en modo "Passthrough"[6]), etc. Además, Asterisk es multiprotocolos, es decir, que soporta diversos protocolos de señalización VoIP como son: SIP, H.323, MGCP, SCCP/Skinny, IAX (Inter Asterisk eXchange Protocol), entre otros.

En líneas arriba se describió a Asterisk como un conmutador híbrido y en realidad

[3] Se emplea el término hibrido en alusión a que este conmutador es capaz de convivir tanto con redes IP como con redes TDM

[4] `http://www.asterisk.org/community`

[5] `http://www.asterisk.org/support/about`

[6] Se espera que en la versión 1.6.X cuente con soporte completo para video

lo es, puesto que es capaz de interactuar con la Red Telefónica tradicional (PSTN) por medio de la interfase Zapata[7] . Se pueden adquirir tarjetas con módulos FXS/FXO para conectar DID's que sirvan como *troncales analógicas* entre Asterisk y la PSTN. Por otro lado, usando interfases digitales T1/E1, Asterisk es capaz establecer enlaces hacia otros PBX por medio de señalización RDSI (ISDN PRI), Q.SIG (limitado a emisión y recepción de llamadas con recuperación de poca información extra) y MFCR2[8] (Para el caso de México y otros países de Asía y América Latina).

3.2.1. ¿Qué se puede hacer con Asterisk?

El limite en cuanto a las aplicaciones que puede tener Asterisk lo impone el propio desarrollador o integrador, según sea el caso. Aquí mostramos algunos de los esquemas más comunes en los cuales se emplea un servidor Asterisk.

Asterisk como un PBX tradicional

Bajo este esquema mostrado en la figura 3.1, el servidor Asterisk funciona como un PBX convencional y maneja tráfico "analógico" entre la PSTN y los clientes conectados al servidor vía interfases FXS/FXO. Este esquema saca poco provecho de las capacidades IP del servidor.

Asterisk como un IP-PBX

En la figura 3.2, se muestra un servidor Asterisk funcionando como un IP-PBX, bajo este esquema el servidor se comporta como un PBX tradicional, pero en vez de conmutar en el mundo TDM lo hace en el de IP. En estas circunstancias, tampoco son aprovechadas todas las capacidades del servidor.

---

[7] El proyecto ZAPATA fue conducido por Jim Dixon, cofundador de Digium© y ahora responsable del desarrollo de hardware de esa empresa. Debemos resaltar el hecho de que el hardware también es abierto y puede ser reproducido por cualquier empresa (Digium©, Sangoma, Varion, etc.). La historia del proyecto puede ser vista en: `http://www.asteriskdocs.org/modules/tynicontent/index.php?id=10`. El nombre del proyecto en palabras del propio Dixon surgió así:

> Since this concept was so revolutionary, and was certain to make a lot of waves in the industry, I decided on the Mexican revolutionary motif, and named the technology and organization after the famous Mexican revolutionary Emiliano Zapata. I decided to call the card the "tormenta" which, in Spanish, means "storm", but contextually is usually used to imply a big storm, like a hurricane or such.

[8] Asterisk no soporta de forma nativa la señalización MFCR2, para implementarla es necesario incorporar algunas librerías extra como libmfcr2, libunicall, libsupertone, posteriormente es necesario recompilar Asterisk; sin embargo, el soporte para estos protocolos de señalizacíón TDM aún es experimental y no se garantiza su buen funcionamiento.

Figura 3.1: Asterisk como un PBX tradicional

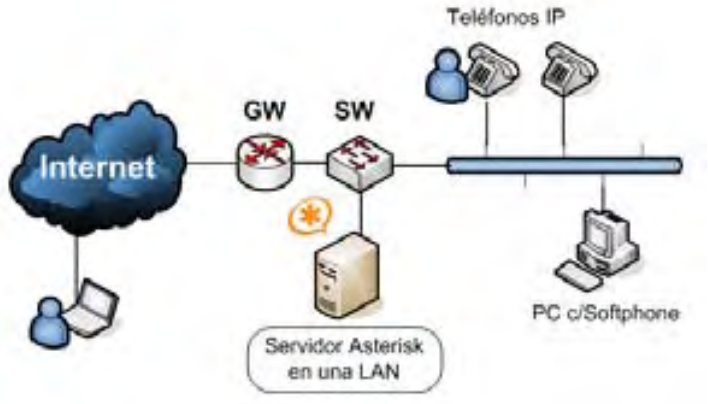

Figura 3.2: Asterisk como un IP-PBX

Asterisk como complemento de un PBX convencional

Tal y como se muestra en la figura 3.3, podemos hacer uso de Asterisk como complemento para un PBX convencional. De esta forma es posible sacar provecho de las prestaciones y capacidades tanto IP como TDM del mismo. Es notable ver que Asterisk tiene la capacidad de integrar ambos mundos de forma sencilla y transparente para el usuario final, ya que estos no notarán diferencia alguna entre hablar desde su softphone hacia alguien en su misma red local o hacia una persona en la red pública. Así mismo, el usuario final se beneficia de las prestaciones que implica el mundo IP tal como poder consultar el Buzón de Voz en su Correo Electrónico o iniciar una llamada IP con un sólo "clic" sobre la liga de uno de sus contactos en un navegador Web, etc.

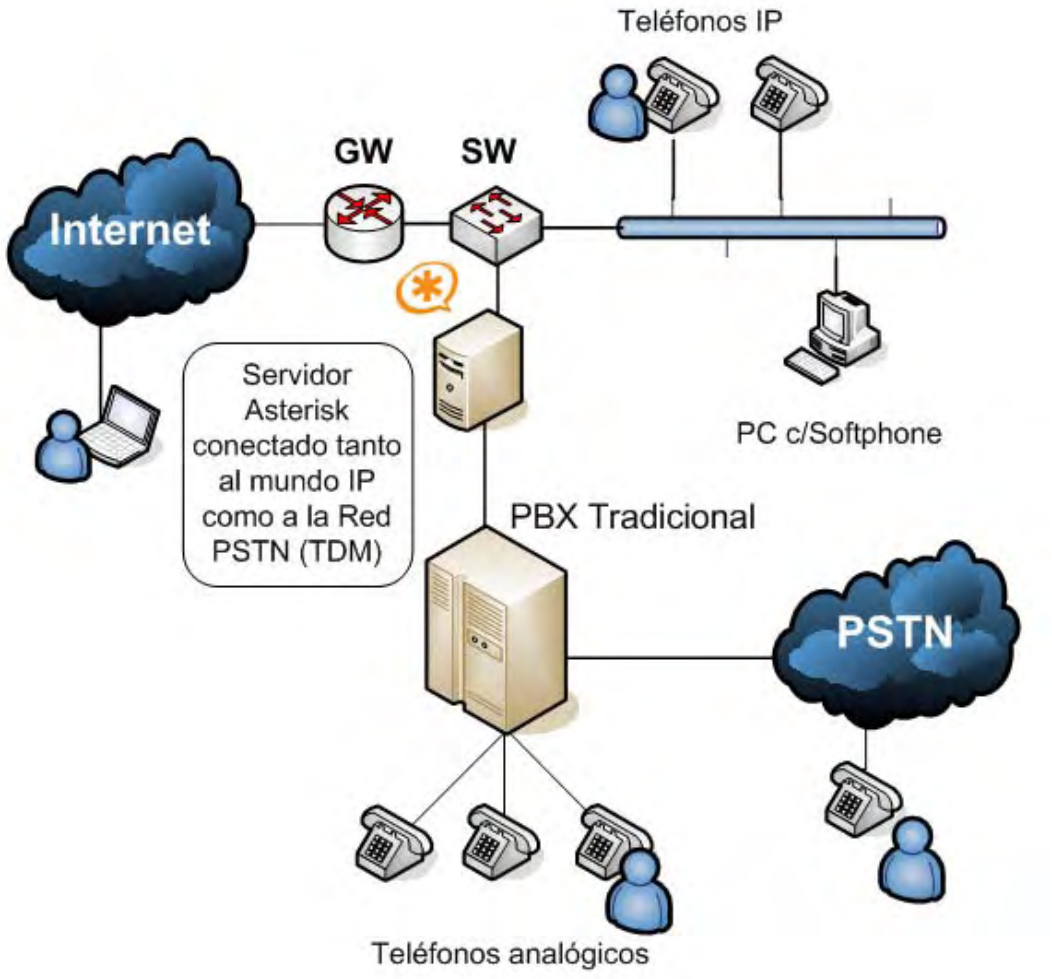

Figura 3.3: Asterisk como complemento de un PBX convencional

Asterisk como Gateway VoIP/PSTN

Ahora mostramos por medio de la figura 3.4, el empleo de Asterisk como gateway entre una Red de datos IP y una Red TDM. El uso más común de este esquema es el de un servidor de acceso remoto hacia la PSTN. Nóte como el servidor Asterisk no tiene ningún cliente directamente conectado. Su labor únicamente es la de "puente" entre ambos mundos.

Además de los esquemas aquí presentados, podemos incluir Asterisk en sistemas distribuidos de telefonía IP que facilitan las comunicaciones en empresas con múltiples sedes, tanto locales como foráneas. Pensemos por ejemplo, en una compañía cuya planta se encuentra en un estado de la república y cuyas oficinas centrales se sitúan en la capital del país. Las comunicaciones entre ambas sedes se verían sumamente beneficiadas con un servidor Asterisk en cada localidad y conectados por medio de un enlace dedicado

Figura 3.4: Asterisk como gateway PSTN/VoIP

con lo cual no hay necesidad de hacer llamadas de larga distancia entre la planta de producción y las oficinas centrales.

3.2.2. Interfases gráficas para Asterisk

Existen diversas interfases gráficas que hacen amigable la configuración de Asterisk, por ejemplo Asterisk NOW o Trixbox. Ésta última es un compilado que incluye Asterisk sobre una distribución de linux (CentOS) que sirve como Sistema Operativo y demás aplicaciones como FreePBX, Munin, SugarCRM, Meetme, etc. FreePBX es una aplicación Web escrita en PHP y MySQL para configurar Asterisk utilizando un navegador Web lo que facilita la administración del sistema. Estas aplicaciones forman en conjunto una solución para telefonía IP compatible con tecnología TDM.

Asterisk NOW!

Esta distribución (figura 3.5), se obtiene en `http://www.asterisknow.org/` y, de acuerdo con la empresa que lo distribuye (la propia Digium©), es la manera más fácil de iniciar con Asterisk, pues se instala en "cuestión de minutos".

Figura 3.5: Pantalla de instalación Asterisk NOW!

Desde su página Web oficial es posible descargar la *imagen del CD de instalación*. Esta imagen instalará una distribución "modificada" de linux (comúnmente CentOS), el software Asterisk, la interfase GUI y demás aplicaciones para el correcto funcionamiento de Asterisk.

Si bien este CD instalará y configurará Asterisk en cosa de minutos, le bastará también unos cuantos minutos para borrar el contenido de nuestro disco duro. Por ello es importante considerar que esta distribución no convive con otros Sistemas Operativos en la mísma computadora.

Trixbox

Está es otra opción. La pantalla de arranque se muestra en la figura 3.6. La página oficial de trixbox es: `http://www.trixbox.org/` y desde ella podemos descargar una *imagen ISO del CD de instalación*.

Figura 3.6: Pantalla de instalación de Trixbox

3.2.3. Arquitectura

Asterisk fue diseñado para tener flexibilidad total[9] . Su estructura consiste en un núcleo y varios módulos que se ejecutan alrededor de él. Asterisk funciona como un *middleware*[10] entre aplicaciones. En la base se encarga de comunicarse con las tecnologías de telefonía (TDM, SIP, IAX, etc.) y en la parte superior se encarga de administrar las aplicaciones que brindan los servicios de telefonía en sí, por ejemplo: IVR, Voicemail y otros.

El núcleo de Asterisk, (ver figura 3.7), esta conformado por múltiples aplicaciones, cada una de ellas desempeña una tarea en especial. Dos aplicaciones muy importantes son: el Cargador Dinámico de Aplicaciones "*Dynamic Module Loader*" y el Lanzador de Aplicaciones "*Application Launcher*". Cuando se inicia Asterisk, el Cargador de Módulos se encargá de añadir los controladores para canales, formatos de archivo, instancias

[9] `http://www.asterisk.org/support/architecture`
[10] Software intermediario

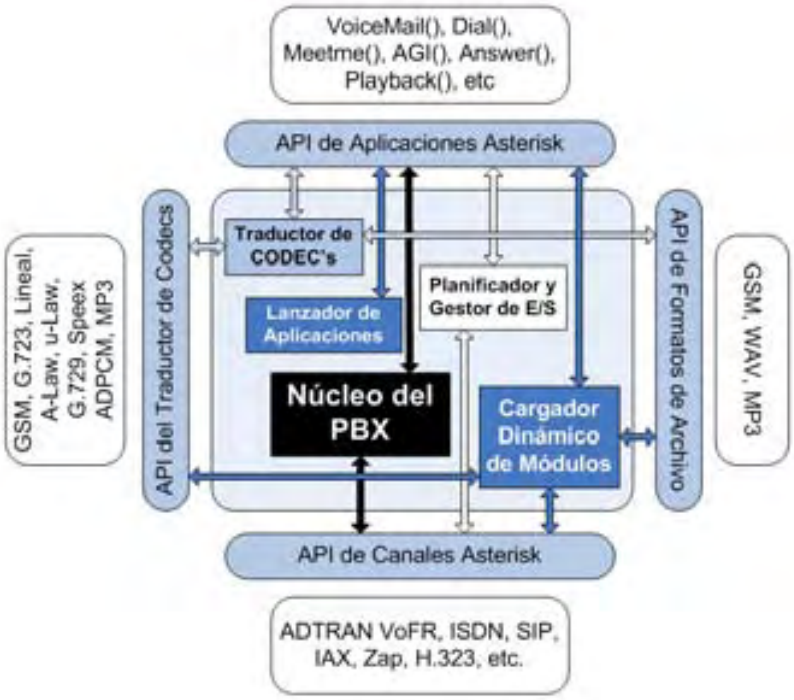

Figura 3.7: Arquitectura modular de Asterisk

para el procesamiento del registro detallado de llamadas (CDR Backends), codec's, aplicaciones y más, los enlaza con las APIs[11] internas correspondientes. En este momento el sistema es capaz de hacer y recibir llamadas. Cuando esto sucede, entra en acción el *Lanzador de Aplicaciones* quien es el encargado ejecutar los programas encargados de hacer sonar los teléfonos, conectar las llamadas entre sí, conectar al usuario con el Buzón de Voz, enlazar una llamada con una troncal, etc.

El núcleo de Asterisk desempeña la tarea esencial de conmutación, interconectando las llamadas unas con otras. Por su parte el traductor de codec's se encargan, precisamente de la traducción entre distintos codec's. Alrededor de éste núcleo se encuentran las API's de Asterisk. Se definieron cuatro API's, son los siguientes:

API de canales.- Encargada de adaptar o acondicionar el tipo de conexión sobre la cual llega una llamada, ya sea VoIP, ISDN, Zap o alguna otra tecnología.

API de aplicaciones.- La API de aplicación, permite que se ejecuten diversas tareas de módulos necesarias para desempeñar distintas funciones, tales como conferencias (MeetMe), Buzón de Voz (VoiceMail), etc.

[11] El término API *Application Program Interface* es usado aquí para hacer referencia al conjunto de programas desarrollados para apoyar la interacción del sistema principal (núcleo de Asterisk) con las aplicaciones (módulos) que rodean a dicho sistema principal.

API del traductor de codec's.- Carga los módulos necesarios para soportar la codificación y decodificación de audio en formatos tales como: GSM, Mu-Law, A-law, e incluso MP3.

API de Formato de Archivos.- Se encarga de la lectura y escritura en distintos formatos, para el almacenamiento de datos dentro del sistema de archivos.

3.2.4. Configuración

Archivos de configuración Asterisk

Asterisk emplea para su funcionamiento diversos archivos de configuración localizados en la carpeta `/etc/asterisk`. Son los llamados archivos "`.conf`". Estos archivos controlan el comportamiento del IP-PBX y en ellos se configuran los servicios y prestaciones telefónicas. Entre otras cosas, en los archivos "`.conf`" se configura el *plan de numeración*, el *plan de marcación*, los servicios tales como: *Buzón de Voz* (VoiceMail), *Conferencia*, *Transferencia de Llamadas*, etc. En esta sección presentamos una clasificación de estos archivos, su uso y el propósito de cada uno de ellos.

Existen otras alternativas para configurar el Asterisk, por ejemplo mediante una interfase Web como lo es *Trixbox* o *Asterisk Now*. La alternativa de utilizar los archivos "`.conf`" es quizás, la que requiere un grado mayor de abstracción; sin embargo, es que proporciona mayor conocimiento para saber como funciona Asterisk y eso resulta útil cuando queremos configurar acciones muy especializadas o específicas.

Podemos clasificar los archivos de configuración Asterisk de la siguiente manera[14]:

- Archivos de Configuración Maestra
  `asterisk.conf`
- Archivos de Configuración de Canales Asterisk
  `h323.conf, iax.conf,mgcp.conf,sip.conf,skinny.conf,zapata.conf,...`
- Archivos de Configuración del Plan de Marcación
  `extensions.conf,features.conf,...`
- Archivos de Comandos Específicos del Plan de Marcación
  `alarmreceiver.conf,enum.conf,dundi.conf,festival.conf,`
  `meetme.conf,musiconhold.conf,queues.conf,voicemail.conf,...`
- Archivos Varios
  `codecs.conf,modules.conf,...`
- Archivos agregados por otros Módulos de Asterisk
  `ldap.conf,/etc/zaptel.conf,...`

La mayoría de estos archivos se localizan en el subdirectorio `/etc/asterisk/` salvo algunas excepciones, en cuyo caso se especificará la ruta completa. Como se mencionó anteriormente, ellos determinan el comportamiento de nuestro IP-PBX y por tal

motivo es importante conocer el propósito de cada uno de ellos, es por ello que en adelante describiremos algunos de ellos.

Archivo de Configuración Maestra (`asterisk.conf`)

Archivo de configuración general. Contiene la ruta de los directorios útiles para el Asterisk (donde residen aplicaciones, módulos y demás archivos de configuración). Es el primer archivo que Asterisk busca al iniciar. Es posible establecer por medio de línea de comandos otro archivo de configuración maestra. Esto resulta útil cuando se quieren hacer pruebas sin cambiar los archivos originales. Este archivo sirve para:

- Ubicar la localización de los directorios importantes para el Asterisk
- Ajustar opciones por defecto para la Interfase de Línea de Comandos CLI.
- Establecer permisos y propietarios de los archivos importantes.

Archivos de Configuración de Canales

A este grupo de archivos pertenecen `sip.conf`, el `h323.conf`, `iax.conf`, entre otros, cuyo propósito es definir los parámetros de configuración para cada canal en específico.

Algunos de los archivos más comúnmente utilizados son: `iax.conf, sip.conf y zapata.conf`. En ellos se configuran los canales de tipo IAX2, SIP y Zapata respectivamente. Este último en particular tiene la función de establecer los parámetros de las interfases pseudo-analógicas Zapata. Por medio de este tipo de canales nos es posible configurar líneas analógicas[12] que nos sirvan como troncales hacia la PSTN.

Archivos de Configuración del *Plan de Marcación*

Es el archivo `extensions.conf` el más importante de todos, en cuanto a que define el comportamiento del IP-PBX. En éste archivo se describe por medio de comando la secuencia de acciones que Asterisk ha de llevar a cabo en cuanto una extensión sea marcada. Podemos contar con múltiples canales configurados de tipo SIP, IAX, Zaptel, etc; pero si no se incluye una línea correspondiente a cada uno de ellos dentro del archivo `extensions.conf` entonces no seremos capaces de hacer o recibir llamadas hacia ellos.

Otro archivo importante dentro de esta categoría es el `features.conf`, en él se describen y configuran algunas facilidades teléfonicas de Asterisk, por ejemplo: el lote de estacionamiento para llamadas, la extensión de "parkeo" de llamadas, transferencia de llamadas con y sin supervisión, entre otras.

[12] Para ello requerimos de tarjetas FXS/FXO o T1/E1 marca Digium© o de algún otro fabricante que sea compatible.

Archivos de Comandos *Específicos del Plan de Marcación*

En esta categoría encontramos archivos que sirven para configurar funciones específicas de Asterisk como el correo de voz (`voicemail.conf`), la música en espera (`musiconhold.conf`), el manejo de las colas de llamadas (`queues.conf`), las salas de conferencias (`meetme.conf`), etc. Estos son sólo algunos de los archivos.

Archivos Varios

Existen también archivos que son muy importantes para Asterisk, pero que no se encuentran dentro de las categorías anteriores. Ejemplos de ellos son: el `modules.conf` que nos sirve para definir que módulos deberán ser cargados por asterisk para su buen funcionamiento. De esta manera podemos aligerar la carga de procesamiento y de memoria de trabajo al sistema quitando aquellos módulos que no nos interesan y dejando aquellos que sí.

Por otro lado, en el archivo `codecs.conf` se determinan los codec's que el sistema reconocerá y con los cuales trabajará.

Archivos Agregados por otros Módulos.

A este conjunto de archivos pertenecen algunos como `ldap.conf`, el cual pérmite manejar métodos de "Autentificación" para los abonados y el archivo `/etc/zaptel.conf` que nos permite establecer los parámetros de funcionamiento de los módulos pseudoanalógicos Zapata.

3.3. OpenSER

OpenSER es un servidor SIP (SIP Express Router). De acuerdo con la página del proyecto OpenSER [13], éste puede ser implementado tanto en sistemas con recursos limitados, como en sistemas de nivel carrier estableciendo hasta varios miles de llamadas por segundo. Esta escrito en *lenguaje C para sistemas UNIX/Linux* y es sumamente flexible. Puede ser configurado como servidor de registro, de localización, proxy server, servidor de redirección, gateway hacia SMS/XMPP o servidor de aplicaciones avanzadas de VoIP.

Como cualquier otro desarrollo *"Open Source"*, OpenSER tiene una comunidad que lo respalda. Cualquiera, que así lo desee, puede realizar contribuciones al proyecto con el único fin de entregar servicios de VoIP de calidad. Las áreas de colaboración son las siguientes:

- Desarrollo de Código (Ya sea para el núcleo de OpenSER, módulos o aplicaciones adyacentes);
- Documentación (Mejorandola o escribiendola);
- Miscelaneas (Por ejemplo, mantenimiento a la página) y;
- Por supuesto contribución de nuevas ideas.

OpenSER no puede ser considerada como una central tradicional. A diferencia de Asterisk, OpenSER no tiene prestaciones de "Media Gateway" (servicios), es decir, no podría remplazar o sustituir una central avanzada. Sin embargo, está considerado como el servidor SIP más avanzado sobre software libre, lo que permite una gran escalabilidad, esta basado en sistemas abiertos, y facilita la conexión de gran cantidad de usuarios de forma concurrente.

Resumiendo, *OpenSER* puede actuar como:

- Servidor Proxy SIP
- Servidor de Registro SIP
- Servidor de Localización SIP
- Servidor de Aplicaciones SIP
- Servidor Despachador SIP

3.3.1. Breve historia de OpenSER

La historia de *OpenSER* tiene sus orígenes en Alemania entre los años 2001 y 2002, especificamente en el Instituto de Investigación FhG FOKUS de Berlín. El proyecto original se denominó *SIP Express Router* (SER), y fue liberado como de *"Código Abierto"* bajo licencia GPL en el otoño de 2002. Hasta 2005, el proyecto se desarrolló en múltiples direcciones, pero fue en junio de 2005 que dos de los principales desarrolladores junto con uno de los más importantes contribuyentes iniciaron el proyecto OpenSER. Entonces se formó un buró de administración para definir políticas sobre las contribuciones, la periodicidad de los *releases*, etc; con el objetivo de iniciar rápidamente el nuevo proyecto.

Algunos de los antiguos colaboradores de *SER* se unieron al nuevo proyecto y luego de año y medio el proyecto contaba con 80 colaboradores de código, 20 de ellos, desarrolladores registrados. El primer *release* de *OpenSER*, llegó el *14 de junio de 2005* como la versión 0.9.4 derivado de la versión 0.9.0 de *SER*.

De ahi a la fecha han existido otros *releases*. Actualmente se distribuye la versión 1.3.0 (*Black Cat*).

3.3.2. Arquitectura

La arquitectura de OpenSER es, al igual que Asterisk, modular. La parte fundamental se denomina núcleo (core) y alrededor de esta se cargan módulos que añaden funcionalidad a todo el conjunto. Por medio de los módulos podemos determinar el comportamiento específico de OpenSER. Por su parte los módulos contienen dos partes importantes: los parámetros exportados y las funciones exportadas. Estos parámetros y funciones son utilizados (invocados) en el archivo de configuración de OpenSER (generalmente `/etc/openser/openser.cfg`).

Los parámetros exportados determinan el comportamiento de los módulos ejecutados por OpenSER, mientras que las funciones exportadas nos permiten programar la forma en que se procesan los mensajes SIP. Algunos módulos dependen de otros para poder funcionar, por ejemplo: el módulo de registro depende, entre otros, del módulo de localización de usuarios.

Los archivos de configuración de OpenSER son la clave para que el servidor funcione como nosotros lo deseemos. Existen tres archivos fundamentales para OpenSER:

- `/etc/openser/openser.cfg`
- `/etc/openser/openserctlrc`
- `/etc/default/openser`

La localización de estos archivos depende del prefijo al momento de compilar OpenSER. En el caso de Debian, al instalar los paquetes .deb, los archivos usan "/" como prefijo. En otros casos el prefijo puede ser "/usr/local/".

A continuación describiremos algunos de los módulos de OpenSER, así como la funcionalidad que estos añaden al sistema cuando son integrados.

La lista completa de los módulos disponibles de OpenSER se puede consultar en su sitio oficial `http://www.openser.org`, en la sección de documentación.

Figura 3.8: OpenSER y sus distintos módulos

- **Módulo de Contabilidad - Accounting (ACC)** - Es usado para llevar el registro detallado de las transacciones hacia diferentes sistemas *"backends"* como syslog, SQL, RADIUS y DIAMETER. Podemos usar este módulo para llevar la "contabilidad" (facturación) de las llamadas y demás servicios del sistema.

- **Módulo de Autenticación - Authentication (AUTH)** - Éste es un módulo que contiene funciones comunes de autenticación, útiles para otros módulos como AUTHDB (Autenticación ante Bases de Datos), AUTHRAD (Autenticación usando servidor de certificados RADIUS).

- **Módulo de Valor Avanzado de Par de Opciones - Advanced-Value-Pairs Options (AVPOPS)** - En este módulo se incluye un conjunto de funciones de script, las cuales permiten la manipulación de AVP's. Un AVP puede ser visto como una variable cuyo identificador es numérico o una cadena de caracteres, y su valor también.

  En OpenSER un AVP esta relacionado a una petición o transacción SIP, esto se lleva acabo cuando OpenSER esta en modo "Stateful". El AVP es automáticamente desechado en cuanto el proceso de la transacción que le dió origen, finaliza.

  Los AVP son una herramienta poderosa para implementar servicios o preferencias por usuario o dominio. Son usadas directamente desde el script de configuración. El módulo AVPOPS incluye funciones para interactuar con recursos de Bases de Datos (carga, almacenamiento y borrado de elementos de la Base de Datos), funciones

para intercambiar información entre AVPs y mensajes SIP, funciones para verificar y comprobar el valor de un AVP.

- **Módulo Despachador - DISPATCHER** - Se utiliza para actuar como balanceador de carga ("Loadbalancer"), esto es, equilibrar la carga de transacciones SIP entre un conjunto proxies disponibles. La lista de proxies disponibles es leída desde un archivo de texto.

- **Módulo de Trazado de Números Telefónicos - tElephone NUmber Mapping (ENUM)** - Implementa funciones para realizar consultas ENUM (Veáse sección 1.2.7), basadas en la parte de usuario de la URI, se encuentra en proceso. Se asume que la parte de usuario es un número telefónico internacional (*ITU-T E.164*) de la forma [+digitos_decimales] (por ejemplo +35831234567), donde el número de digitos varía entre 2 y 15.

- **Módulo de Ejecución de Comandos Externos (EXEC)** - El módulo EXEC permite iniciar un comando externo a OpenSER desde el script de configuración (openser.cfg). El comando pueden ser cualesquiera de los comandos de shell disponibles. Adicionalmente, OpenSER entrega información suficiente sobre las peticiones SIP en forma de variables de ambiente.

- **Módulo de Conferencia de Mensajería Instatánea (IMC)** - Ofrece soporte para conferencias de mensajería instatánea. Sigue la arquitectura de los canales IRC (Internet Relay Chat).

- **Módulo para Soporte de Sistemas de Presencia (JABBER)** - Ofrece soporte para sistemas de presencia e interacción con otros sistemas de mensajería instantánea como Jabber, ICQ, MSN, AIM y Yahoo.

- **Módulo LDAP (Protocolo Ligero de Acceso a Directorios)** - Implementa una interfase de búsqueda, almacenamiento y autenticación usando *Lightweight Directory Access Protocol*. Puesto que las implementaciones LDAP son óptimas para un rápido acceso de lectura, son una buena elección para almacenar datos SIP sensibles o importantes. En pruebas de desempeño se ha observado que el uso de este módulo logra menores tiempos de acceso a datos y mayores tasas de llamadas que otros módulos para bases de datos, como MySQL o Postgress.

- **Módulo de Reenvíos Máximos (MAXFWD)** - Este módulo incluye funciones para el procesamiento del campo de encabezado `MaX-Forward`. Estas funciones pueden ser de verificación del valor del campo, así como incremento y decremento del mismo.

- **Módulo Proxy de Medios (MEDIAPROXY)** - Esta diseñado para que casi cualquier cliente SIP sea capaz de atravesar ambientes de red que se encuentran detrás de un NAT.

- **Módulo para Servidor de Bases de Datos (MYSQL)** - En este módulo, OpenSER puede conectarse con un servidor de bases de datos MySQL. Las funciones que se añaden al incluir este módulo, proporcionan un API para realizar consultas y editar la Base de Datos de OpenSER. Al igual que este módulo, existen módulos para soportar otros manejadores de bases de datos, como son, POSTGRES y UNIXODBC.

- **Módulo para Extensiones basadas en el Lenguaje de Programación Perl (PERL)** - Provee de las funciones necesarias para desarrollar nuestras propias extensiones para OpenSER basadas en este lenguaje de programación.

- **Módulo de Administración de Sistemas de Presencia (PRESENSE)** - Junto con los módulos PRESCENCE_MWI y PRESCENCE_XML, aportan un conjunto de funciones y variables útiles para la conformación de un sistema de presencia, parecido al de Windows Messenger.

- **Módulo de Registro (REGISTRAR)** - Éste es uno de los módulos más importantes de todos. Debe ser incluido en la configuración básica de OpenSER. Esto debido ha que cuenta con las funciones necesarias para realizar procedimientos de registro de usuarios. El registro es importante, pues provee de los elementos necesarios para la localización de los usuarios.

- **Módulo Registro de Ruta - Record Route (RR)** - En ocasiones es imprescindible que el proxy tenga mayor control sobre todos los diálogos SIP. La solución es implementar un proceso de registro de ruta con el fin de que los mensajes SIP contengan dentro del campo VIA, la ruta exacta por donde han pasado, con el fin de que las respuestas sigan el mismo camino, pero en sentido opuesto.

- **Módulo Short Message Service (SMS)** - Con las funciones contenidas en este módulo, OpenSER tiene la posibilidad de actuar como un gateway SIP - SMS en ambas direcciones. El módulo SMS requiere del uso de un modem GSM capaz de enviar y recibir mensajes SMS. Comúnmente este tipo de modems son externos, conectados a la PC por medio de un cable serial. El modem puede ser dedicado (por ejemplo, los de marca FALCOM), o puede ser un teléfono GSM que tenga un modem interno (NOKIA, ERICSSON).

- **Módulo Text Options (TEXTOPS)** - Puesto que SIP es un protocolo basado en texto, el módulo TEXTOPS cuenta con funciones de procesamiento y formato de texto que son útiles para el procesamiento de los mensajes SIP a nivel texto plano.

- **Módulo Transaction Manager (TM)** - El módulo de administración de transacciones permite al núcleo de OpenSER realizar procesamiento "statefull" de las operaciones SIP.

- **Módulo User Location (USRLOC)** - Este módulo mantiene una tabla en donde registra la localización de los usuarios y permite a otros módulos el acceso a la misma.

El módulo USRLOC no exporta funciones que puedan ser usadas por los scripts de configuración.

- **Módulo XLOG** - Las funciones y variables de este módulo, permiten al usuario de OpenSER puede imprimir mensajes de log o debugging con formato desde los scripts de OpenSER. Su funcionamiento es similar a la función printf del lenguaje C.

Aquí se han presentado sólo algunos de los módulos con los que se puede añadir funcionalidad al núcleo de OpenSER. Consideramos importante reiterar la gran flexibilidad de OpenSER y la enorme versatilidad de sus módulos. La lista de los módulos disponibles para la versión 1.3.0 de OpenSER se puede encontrar en la página oficial del proyecto `http://www.openser.org/docs/modules/1.3.x/`.

3.3.3. Configuración

El archivo `openser.cfg` es considerado el cerebro del enrutador SIP. Se divide en siete secciones, son las siguientes:

1. Sección de definición de parámetros globales: Esta sección usualmente contiene la dirección IP y el puerto a escuchar, niveles de depuración, etc. Las configuraciones de esta sección afectan al mismo demonio de OpenSER.

2. Sección de carga de módulos: En esta sección se encuentran contenidas las librerías externas necesarias para ofrecer las funcionalidades no provistas por el núcleo. Estos módulos son archivos de objetos compartidos "`*.so`" y se cargan con el comando "`load module`".

3. Sección de configuración de parámetros de módulos: Las librerías externas especificadas en la sección de módulos, necesitan configurar parámetros para que funcionen adecuadamente. Estos parámetros de módulos son ajustados utilizando el comando "`modparam`".

4. Bloque de lógica primaria de ruteo (MRB): Este es análogo a los programas principales de función de C. Este es el punto de entrada para el procesamiento de mensajes SIP. Determina la forma en que serán tratados los mensajes recibidos por OpenSER.

5. Bloque de ruteo secundario (SRB): En adición al *Main Route Block* el archivo de configuración puede contener bloques de enrutamientos adicionales que pueden ser invocados desde el MRB u otros SRB. Un SRB es parecido a una subrutina.

6. Bloque de ruteo de repetición (RRB): "opcional", pueden utilizarse para manejar respuestas de mensajes SIP. A menudo estos son mensajes OK.

7. Bloque de ruteo en caso de falla (FRB): "opcional", pueden ser usados cuando es necesario un procedimiento especial, para manejar condiciones de falla en el servidor, tales como: Ocupado, Fuera de tiempo, etc.

Capítulo 4

Protocolo de Pruebas

En este capítulo describimos los escenarios de pruebas sobre los que se probaron las soluciones Asterisk y OpenSER descritas en el capítulo anterior. Estas pruebas tienen como objetivo final, el caracterizar ambas plataformas. Tanto Asterisk como OpenSER ofrecen la posibilidad de probar y evaluar las tecnologías ToIP sobre software libre.

Se pretende que los sistemas OpenSER y Asterisk se lleven a un entorno de producción dentro de la propia Universidad Nacional Autónoma de México, aunque los cambios en la metodología de implementación merecen una evaluación y una planeación cuidadosa.

Cada plataforma esta diseñada para soportar servicios múltiples, es decir, además de la Voz, la plataforma también es capaz de brindar soporte extensivo a los servicios de Mensajería Unificada y Video. A través de cada escenario queremos mostrar las características más sobresalientes de estas dos propuestas para telefonía IP, así como el ambiente en que se desenvuelven.

4.1. I - Pruebas Asterisk

El conjunto de pruebas que a continuación describimos tuvo como propósito, el caracterizar la solución Asterisk en cuanto a los siguientes parámetros:

1. Facilidades y servicios de telefonía para el usuario final;
2. Facilidades y servicios de valor agregado (Video-Llamadas, etc.);
3. Flexibilidad para la creación de nuevas facilidades y servicios;
4. Servicios de administración y mantenimiento del sistema;
5. Interoperatividad con las tecnologías existentes.

Las pruebas se planearon de forma tal, que el primer escenario corresponde al caso más sencillo, esto es, Asterisk como un IP-PBX aislado en un ambiente de red local. Los siguientes escenarios fueron añadiendo complejidad al sistema, en el segundo escenario se agregó la posibilidad de conectarse con redes externas TDM mediante troncales analógicas. Subsecuentemente, se pusieron a prueba las capacidades del sistema para manejar troncales digitales, troncales IP y por último se integraron todos los escenarios de manera que el sistema en su conjunto representara en la medida de lo posible un caso de aplicación real.

En la tabla 4.6 se enlistan los recursos utilizados en el laboratorio para la realización de estas pruebas. Tales forman parte de un protocolo más extenso que tiene como finalidad el integrar un IP-PBX prototipo que brinde servicio a dependencias universitarias, cuyas necesidades de servicios de comunicación empaten con los objetivos de este trabajo. Aquí sólo se resumen algunos de los resultados obtenidos y en el apendice B se muestran las configuraciones necesarias para la reproducción de estas pruebas.

Para corroborar que muestra red telefónica de pruebas no presentará ningún problema en la interconexión, ya sea para llamadas internas, llamadas de entrada y llamadas de salida, se utilizó una matriz de llamadas. La matriz de llamadas planeada tuvo como objeto, verificar que efectivamente todas y cada una de las extensiones conectadas al sistema fueran capaces de acceder a servicios, realizar llamadas internas y, realizar llamadas hacia redes externas. En la sección de resultados se muestra tal matriz, así como el registro de los resultados de las pruebas.

La evaluación de las prestaciones para la administración y mantenimiento del sistema fue también tomada en cuenta. Para ello se verificó que el sistema fuese capaz de tener diferentes categorías de usuarios para administración y monitoreo, capacidad para respaldar información del estado del sistema, capacidad de llevar un registro detallado de las llamadas (CDR) para efectos de tarificación y facilidad de gestión por medio de interfases gráficas de usuario (GUI), entre otras. Nuevamente, los resultados obtenidos se resumen al final de esta sección.

Equipo/Software	Descripción
Servidor Asterisk	Dell PowerEdge 840. Intel® Pentium® D CPU 2.80GHz, 2 GB RAM de 667 MHz. D.D. SATA 7200 RPM de 160 GB, Tarjeta de Red 10/100/1000
Tarjetas Digium	TDM400P (2FXS y 2FXO), TE110P (T1/E1)
Sistema Operativo	CentOS 5.0 kernel 2.6.18-8.el5
Asterisk	Versión 1.4.19
Zaptel	Versión 1.4.9.2
Libpri	Versión 1.4.3
PBX NEC	NEAX 7400 ICSa
Tarjeta ISDN NEC	30PRST
Teléfonos Analógicos	Aastra Bell Modelo Be70T NEC DTP-1HM-2(WH) TEL
Teléfonos IP	Cisco IP 7960 (SIP phone) v.2
	Grand Stream GXP2000 (SIP phone) v.2
Softphones	Eyebeam v1.5.16.1 build 43069 CounterPath SIP
	X-lite v3.0 build 41150 CounterPath SIP
	ZoIPer v2.0.6 Atractel IAX2/SIP
Switches	3COM SuperStark II switch 3300 c/24 puertos 10/100 Mbps Administrable
ATA	Cisco Linksys Internet phone Adapter PAP2T
Cableado	UTP Norma A CAT 5
Balun	Adaptador de impedancias BNC - RJ45
Codec's Utilizados	
G.711 Ley A	Es el codec usado para la compresión de las señales de audio
H.263	Es el codec usado para la compresión de las señales de video
Protocolos de señalización VoIP	
Protocolo SIP	Es usado para las llamadas en ambiente IP
Protocolo IAX	Es usado para las llamadas en ambiente IP
Protocolo Zap	Es usado para señalizar las llamadas entrantes y salientes de las tarjetas Digium (Zapata Pseudo-Analog Interface Telephony)
Protocolos de señalización TDM	
ISDN PRI-Q.SIG	Señalización CCS Red - Red 30B + D.
MFC/R2	Señalización CAS Red - Red 30 canales de Voz, 1 canal de señalización y 1 de sincronía.
Interoperatividad con la telefonía tradicional	
DID's	55506095 (Telmex) ext. 28530 y rango de exts. 29901-29930 (RUV) p/pruebas de enlaces digitales
Enlace digital E1	Interfase TDM con 32 canales de 64 kbps c/u, con un ancho de banda total de 2.048 Mbps

Tabla 4.1: Recursos de Hardware y Software empleados

4.1.1. Escenario I.I - Facilidades y Servicios

Descripción de la prueba

En esta prueba se registraron los servicios de telefonía, así como aquellos servicios de valor agregado que la solución Asterisk entrega al usuario final. Además, esta prueba nos

sirvió para verificar como Asterisk soporta múltiples dispositivos, de diferentes marcas y diferentes protocolos. Esta prueba fue la base para los siguientes escenarios.

En la figura 4.1 se muestran los elementos involucrados en la prueba. Se utilizaron distintos tipos de clientes para telefonía IP, así como un equipo de administración y monitoreo remoto desde donde se configuró y supervisó el desempeño del servidor.

Maqueta de la prueba

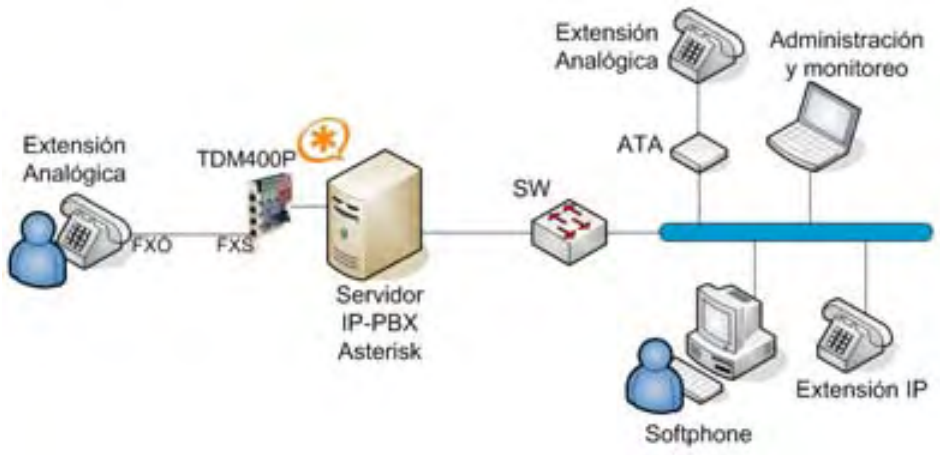

Figura 4.1: Maqueta para prueba de facilidades y servicios

Para interactuar con sistemas de telefonía tradicional se utilizó la tarjeta Digium TDM400P. Esta tarjeta cuenta con dos interfases FXS y dos FXO que pueden ser configuradas en Asterisk para recibir terminales analógicas (dispositivos con puertos FXO como teléfonos o faxes), o bien para recibir líneas directas (FXS) desde otros sistemas, tal y como veremos en el siguiente escenario. En esta prueba se utilizaron únicamente los puertos FXS de la tarjeta para conectar dos extensiones analógicas que utilizan tecnología Zapata.

4.1.2. Escenario I.II - Troncales Analógicas

Descripción de la prueba

Mediante esta prueba se comprobó la interoperatividad del sistema con los sistemas de telefonía tradicionales (TDM). Para ello se hizó uso de troncales analógicas. Se utilizarón DID's[1] provenientes de la PSTN (Telmex) y de la Red Universitaria de Voz (RUV). Estas líneas se conectaron a la tarjeta Digium TDM400P (Puertos FXO). Se configuraron prefijos para toma de troncal de la manera siguiente: [9] para toma de troncal hacia la PSTN (Telmex) y [0] para toma de troncal hacia cualquier extensión de la RUV. Se verificó el correcto procesamiento de tráfico entrante y saliente, y se comprobó el acceso a servicios internos desde redes externas, así como el uso de restricciones para toma de troncal desde extensiones internas.

Maqueta de la prueba

Figura 4.2: Maqueta para prueba de troncales analógicas

[1] Direct Inward Dialing - Línea directa proveniente, generalmente de la compañia telefónica. Contiene el número de origen y destino para que el PBX de la empresa sea capaz de procesar y enrutar la llamada internamente.

4.1.3. Escenario I.III - Troncales Digitales

Descripción de la prueba

En este escenario se conectó el servidor Asterisk con un PBX convencional NEC (modelo NEAX 7400ICSa) para comprobar la interoperatividad de Asterisk con los sistemas de telefonía tradicional (TDM). Los enlaces digitales utilizados fueron E1's con señalización ISDN (PRI-Q.SIG), así como MFC/R2. Del lado de Asterisk se utilizó una tarjeta Digium TE110P, la cual sirve como interfase para enlaces T1/E1. El PBX NEC funcionó como Switch Tandem para dar salida hacia RUV y PSTN (Telmex) respectivamente. Se verificó el correcto procesamiento de tráfico entrante y saliente, y se comprobó el acceso a servicios internos desde las redes de voz externas, así como el uso de restricciones para toma de troncal desde extensiones internas.

Diagrama

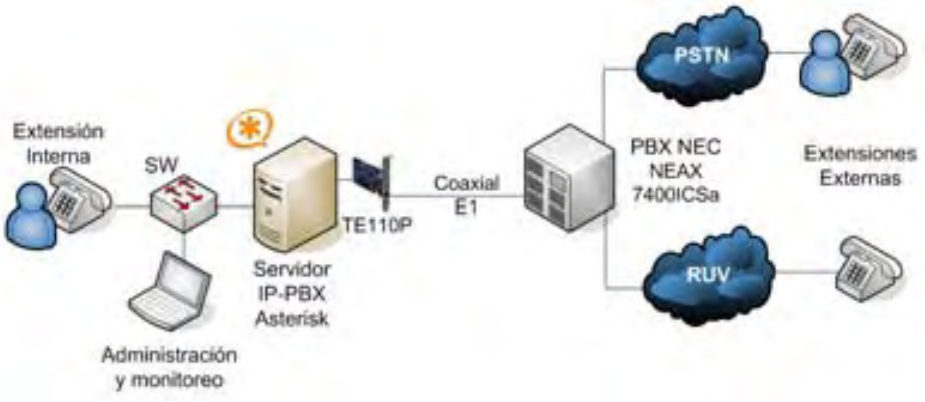

Figura 4.3: Maqueta para prueba de troncales digitales

4.1.4. Escenario I.IV - Troncales IP (SIP e IAX)

Descripción de la prueba

A través de esta prueba confirmamos que Asterisk soporta troncales IP usando los protocolos SIP e IAX. La prueba consistió en interconectar dos servidores Asterisk (A y B) utilizando troncales IP de tal forma que las extensiones pertenecientes al servidor A pudiesen llamar a las del sistema B y viceversa. También se comprobó cual de los dos protocolos (SIP o IAX) resultan más aptos para la troncal.

Diagrama

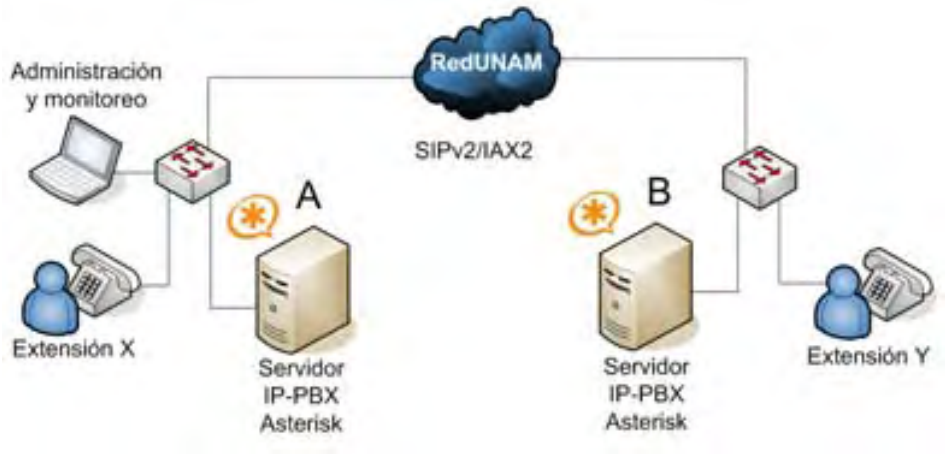

Figura 4.4: Maqueta para la prueba de troncales IP (SIP e IAX)

4.1.5. Escenario I.V - Esquema General

Descripción de la prueba

En esta última prueba se integraron todos los anteriores escenarios, de forma tal que pudimos apreciar al máximo todas las posibles alternativas de uso del servidor Asterisk. Se simuló un ambiente de trabajo lo más cercano a un entorno de aplicación real.

Diagrama

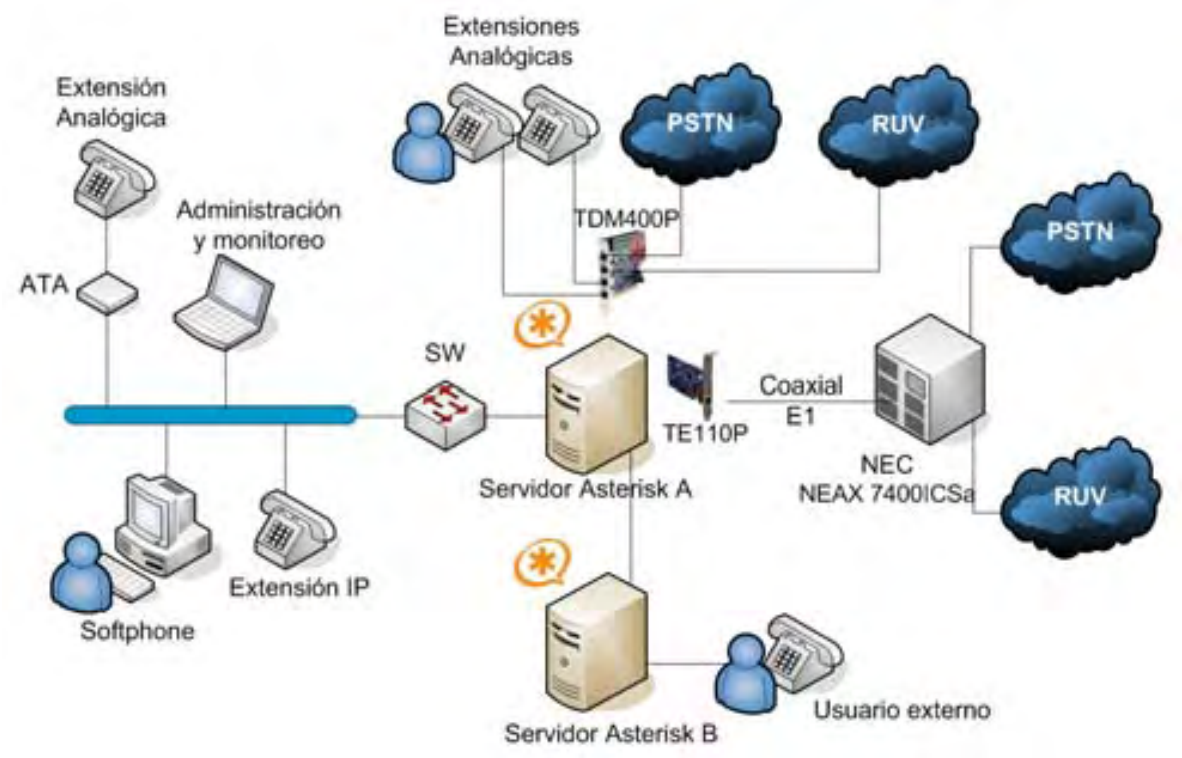

Figura 4.5: Esquema General

4.1.6. Resultados Obtenidos

Conexiones de Llamadas Internas		
Origen	Destino	Resultado
IPphone	IPphone	Ok
IPphone	Extensión Analógica (Zap)	Ok
IPphone	Extensión c/ATA	Ok
IPphone	Softphone SIP	Ok
IPphone	Softphone IAX	Ok
Extensión Analógica (Zap)	Extensión Analógica (Zap)	Ok
Extensión Analógica (Zap)	IPphone	Ok
Extensión Analógica (Zap)	Extensión c/ATA	Ok
Extensión Analógica (Zap)	Softphone SIP	Ok
Extensión Analógica (Zap)	Softphone IAX	Ok
Extensión c/ATA	Extensión c/ATA	Ok
Extensión c/ATA	IPphone	Ok
Extensión c/ATA	Extensión Analógica (Zap)	Ok
Extensión c/ATA	Softphone SIP	Ok
Extensión c/ATA	Softphone IAX	Ok
Softphone SIP	Softphone SIP	Ok
Softphone SIP	IPphone	Ok
Softphone SIP	Extensión Analógica (Zap)	Ok
Softphone SIP	Extensión c/ATA	Ok
Softphone SIP	Softphone IAX	Ok
Softphone IAX	Softphone IAX	Ok
Softphone IAX	IPphone	Ok
Softphone IAX	Extensión Analógica (Zap)	Ok
Softphone IAX	Extensión c/ATA	Ok
Softphone IAX	Softphone SIP	Ok

Tabla 4.2: Matriz de Llamadas Internas

Conexiones de Llamadas de Entrada/Salida		
PSTN/RUV	Extensión IP	Ok
PSTN/RUV	Extensión Analógica (Zap)	Ok
PSTN/RUV	Extensión c/ATA	Ok
PSTN/RUV	Softphone SIP	Ok
PSTN/RUV	Softphone IAX	Ok
Extensión IP	PSTN/RUV	Ok
Extensión Analógica (Zap)	PSTN/RUV	Ok
Extensión c/ATA	PSTN/RUV	Ok
Softphone SIP	PSTN/RUV	Ok
Softphone IAX	PSTN/RUV	Ok

Tabla 4.3: Matriz de Llamadas Externas

Facilidades	Disponible (s/n)	Usuario accede por:		
		Tecla	Código	Otro
Identificador de Llamadas (Caller-ID)	SI			
Transferencia de Llamadas c/supervisión (Transfer)	SI	X	X	
Transferencia de Llamadas s/supervisión (Transfer)	SI	X	X	
Estacionamiento de Llamadas (Call Park)	SI		X	
Grupos de Timbrado (Ring Groups)	SI			Extensión
Grupos de Captura (Call Pick-Up)	SI	X	X	
Colas de Llamadas (Queues)	SI			X
Regreso de Llamada (Callback)	SI		X	
Servicios	**Disponible (s/n)**	**Usuario accede por:**		
		Tecla	Código	Otro
Llamada en Espera (act./desact.)	SI		X	
Desvío Automático de Llamadas (act./desact.)	SI		X	
Buzón de Voz (Voicemail)	SI		X	
+ Reenvío de Mensajes de Voz al Correo Electrónico	SI			
+ Consulta del Buzón de Voz vía Web	SI			Web
Contestadora Autómatica Interactiva de Voz (IVR)	SI			Externo
Cuartos de Audio-Conferencias	SI		X	
Acceso Directo al Sistema (DISA)	SI			Externo
Música en Espera	SI			
Envío y Recepción de Fax	SI			Externo
+ Reenvío de Fax Entrante al Correo Electrónico	SI			
Video-Llamada	SI			Configuración

Tabla 4.4: Lista de Facilidades y Servicios para el Usuario

Servicio de Administración y/o Monitoreo	Disponible (s/n)
Administración Remota vía SSH	SI
Administración Remota Web (HTTPS)	SI
Monitoreo del Sistema vía Web (HTTPS)	SI
Facturación y Registro detallado de Llamadas (CDR)	SI
Respaldo de la Información	SI
Panel de Operadora	SI

Tabla 4.5: Servicios de Administración

Como podemos observar, Asterisk ofrece una gran cantidad de servicios y facilidades telefónicas al usuario final. En las tablas anteriores se enlistan sólo los servicios y facilidades más representativas. Aún cuando Asterisk no cuente con un servicio, es posible configurarlo mediante su lenguaje de programación en el archivo `extensions.conf`. Además, Asterisk ofrece la posibilidad de reutilizar terminales analógicas, gracias a las tarjetas Digium (Zapata).

4.2. II - Pruebas OpenSER

En esta sección describimos los escenarios de pruebas sobre los cuales se examinaron las principales características del proxy SIP OpenSER. Puesto que OpenSER esta diseñado con base en el protocolo SIP, éste no ofrece como Asterisk, servicios de telefonía en sí, sino que ofrece servicios de comunicación en tiempo real soportados por el protocolo, debido a los métodos SIP básicos (INVITE, ACK, BYE, CANCEL, REGISTER, etc, definidos en el RFC-3261) y a los métodos suplementarios como MESSAGE, INFO, NOTIFY, REFER, PUBLISH y SUBSCRIBE (RFC-3265, RFC-3428, RFC-2976, RFC-3515 y RFC-3903).

Equipo/Software	Descripción
Servidor OpenSER	Dell Precison 380, Intel® Pentium® 4 CPU 3.0 GHz, 1 GB RAM, D.D. SATA 80 GB, Tarjeta de Red 10/100 Mbps
Sistema Operativo	Debian 4 Etch kernel 2.6.18-4-686
OpenSER	Versión 1.2.0
Teléfonos Analógicos	Aastra Bell Modelo Be70T NEC DTP-1HM-2(WH) TEL
Teléfonos IP	Cisco IP 7960 (SIP phone) v.2
	Grand Stream GXP2000 (SIP phone) v.2
Softphones	Eyebeam v1.5.16.1 build 43069 CounterPath SIP
	X-lite v3.0 build 41150 CounterPath SIP
	ZoIPer v2.0.6 Atractel IAX2/SIP
Switches	3COM SuperStark II switch 3300 c/24 puertos 10/100 Mbps Administrable
ATA	Cisco Linksys Internet phone Adapter PAP2T
Cableado	UTP Norma A CAT 5
Codec's Utilizados	
G.711 Ley A	Es el codec usado para la compresión de las señales de audio
H.263	Es el codec usado para la compresión de las señales de video
Protocolos de señalización VoIP	
Protocolo SIP	Es usado para las llamadas en ambiente IP
Protocolos de señalización TDM	
ISDN PRI-Q.SIG	Señalización CCS Red - Red 30B + D.
Interoperatividad con la telefonía tradicional	
Enlace digital E1	Interfase TDM con 32 canales de 64 kbps c/u, con un ancho de banda total de 2.048 Mbps

Tabla 4.6: Recursos de Hardware y Software empleados

4.2.1. Escenario II.I - OpenSER como Proxy SIP

Descripción de la prueba

En esta prueba se evaluarón los servicios de comunicación que OpenSER entrega al usuario final. Tales servicios incluyen tanto facilidades telefónicas, como servicios de Mensajería Instantánea y transmisión de Video. Siendo el protocolo SIP un protocolo estándar, esta prueba nos permitió además, verificar la compatibilidad existente de OpenSER con los diversos dispositivos tanto clientes como servidores.

En la figura 4.6 se presenta el diagrama de la prueba, con todos los dispositivos utilizados para la misma. Al igual que en los casos anteriores, se incluyeron distintos tipos de clientes, así como un equipo de monitoreo y administración remota.

Diagrama

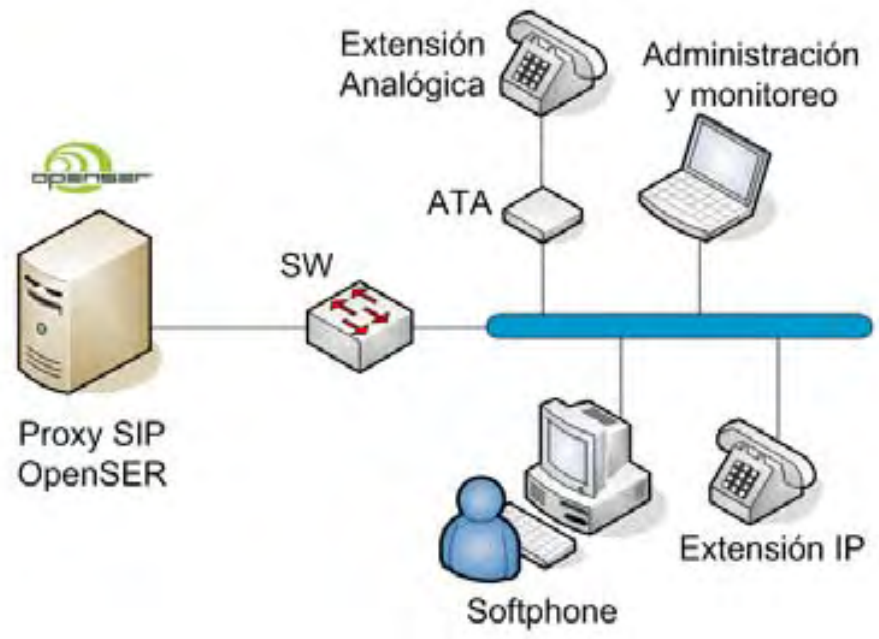

Figura 4.6: OpenSER como Proxy SIP

4.2.2. Escenario II.II - OpenSER con Gateway hacia PSTN

Descripción de la prueba

En este escenario se agregó conectividad hacia la Red telefónica tradicional (TDM). Esto se logró con la introducción de un elemento intermedio conocido como gateway. El gateway tiene la tarea de traducir entre protocolos de señalización TDM y protocolos de señalización VoIP, en este caso, traduce de SIP a Q.Sig y viceversa. Con esta prueba se comprobó que los usuarios internos establecieran llamadas hacia la PSTN y que pudieran recibir llamadas desde la red pública.

En el diagrama mostrado en la figura 4.7 se ilustra la manera en que fueron dispuestos los dispositivos para la realización de la prueba.

Diagrama

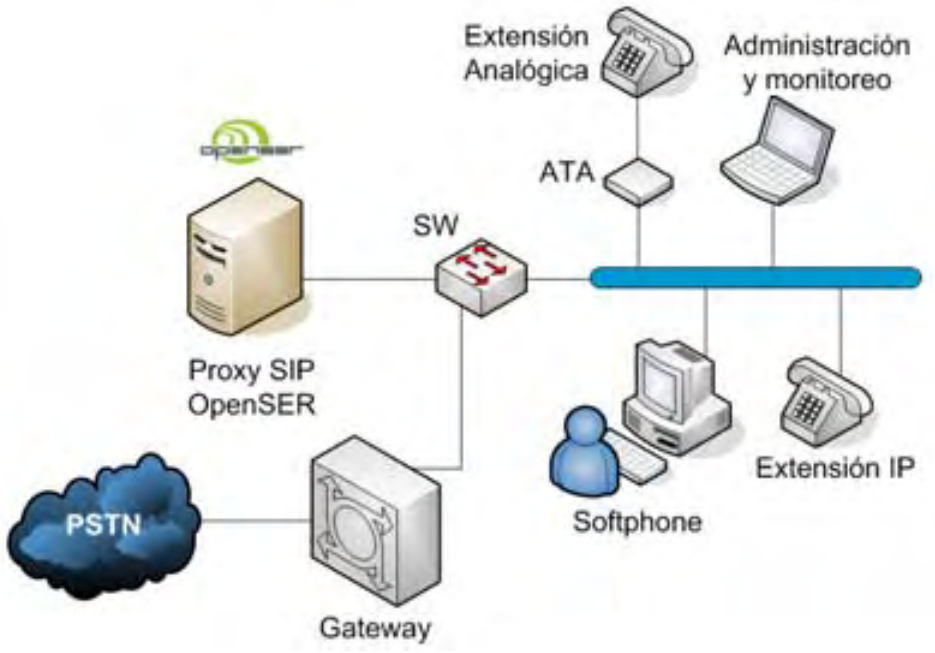

Figura 4.7: Maqueta para la prueba OpenSER con Gateway hacia PSTN

4.2.3. Resultados Obtenidos

Conexiones de Llamadas Internas		
Origen	Destino	Resultado
IPphone SIP	IPphone SIP	Ok
IPphone SIP	Extensión c/ATA	Ok
IPphone SIP	Softphone SIP	Ok
Extensión c/ATA	Extensión c/ATA	Ok
Extensión c/ATA	IPphone SIP	Ok
Extensión c/ATA	Extensión Analógica (Zap)	Ok
Softphone SIP	Softphone SIP	Ok
Softphone SIP	IPphone SIP	Ok
Softphone SIP	Extensión c/ATA	Ok
Conexiones de Llamadas de Entrada/Salida		
PSTN/RUV	Extensión IP (SIP)	Ok
PSTN/RUV	Extensión c/ATA	Ok
PSTN/RUV	Softphone SIP	Ok
Extensión IP (SIP)	PSTN/RUV	Ok
Extensión c/ATA	PSTN/RUV	Ok
Softphone SIP	PSTN/RUV	Ok

Tabla 4.7: Matriz de Llamadas

Facilidades	Disponible (s/n)	Usuario accede por:		
		Disp. Cliente	Código	Otro
Identificador de Llamadas (Caller-ID)	SI			
Transferencia de Llamadas c/supervisión (Transfer)	SI	X		
Transferencia de Llamadas s/supervisión (Transfer)	SI	X		
Servicios	**Disponible (s/n)**	**Usuario accede por:**		
		Disp. Cliente	Código	Otro
Llamada en Espera (act./desact.)	SI	X		
Desvío Automático de Llamadas (act./desact.)	SI			Conf. Cliente
Video-Llamada	SI			Conf. Cliente
Mensajería Instantánea	SI			Conf. Cliente
Manejo de Presencia	SI			Conf. Cliente

Tabla 4.8: Lista de Facilidades y Servicios para el Usuario

Es evidente que OpenSER no es una plataforma dedicada a la telefonía, mas bien esta estrechamente ligado al protocolo SIP y en la definición de este protocolo se establece que SIP es un protocolo de señalización y control de la capa de aplicación, que

Servicio de Administración y/o Monitoreo	Disponible (s/n)
Administración Remota vía SSH	SI
Administración Remota Web (HTTPS)	SI
Monitoreo del Sistema vía Web (HTTPS)	SI
Facturación y Registro detallado de Llamadas (CDR)	SI (Módulo ACC)
Respaldo de la Información	SI (B. de D. MySQL, Postgress y Unix ODBC
Panel de Operadora	No

Tabla 4.9: Servicios de Administración

sirve para crear, modificar y terminar sesiones con uno o más participantes, y que tales sesiones pueden ser, entre otras, llamadas telefónicas, conferencias multimedia y/o distribución de flujos multimedia. Por las razones anteriores, OpenSER no puede ser comparado con Asterisk en cuanto a los servicios que ofrecen uno y otro.

Podemos decir, que OpenSER es muy flexible por su adición de módulos y en las versiones más recientes se han agregado algunos que permiten la incorporación de servicios de telefonía como los que Asterisk ofrece (por ejemplo: el módulo SPEEDDIAL añadido desde la versión 1.3 entre otros).

4.3. III - Integración de Asterisk y OpenSER

4.3.1. Justificación

A lo largo de las pruebas realizadas, nos pudimos percatar de las ventajas que tenía Asterisk como solución de telefonía, pero al mismo tiempo sus carencias como proxy SIP. Tales carencias son resueltas por OpenSER, aunque este último no brinda todos los servicios de telefonía que ofrece Asterisk. Es por ello que en lugar de comparar ambas plataformas decidimos integrarlas, con el objetivo de subsanar las carencias de cada una y sumar las ventajas que ambas ofrecen. De este modo surgió el planteamiento de intentar comunicar Asterisk con OpenSER y el resultado se muestra en esta última sección.

Asterisk	
¿Qué es Asterisk?	**¿Qué no es Asterisk?**
Es una central pequeña de IP	No es una plataforma escalable de comunicaciones IP
Es modular	No es una plataforma enfocada al usuario
Es multiprotocolos	No es un proxy SIP
Es un gateway	No es estándar
Es un correo de buzón de voz (Voicemail)	No cuenta con todo el stack de SIP
Es un servidor de medio / servidor de conferencias	No soporta TCP ni TLS
Es un IVR (Contestadora Automática)	No soporta “Outbound Proxy”

Tabla 4.10: Tabla de Asterisk

OpenSER	
¿Qué es OpenSER?	**¿Qué no es OpenSER?**
Es un proxy SIP	No es una plataforma enfocada al usuario
Es modular	No esta consciente de los codec’s
Es escalable	No es un servidor de medio, IVR, etc.
Manejo de presencia	No es un servidor de aplicaciones SIP
Soporta J2EE y Perl	No es un gateway

Tabla 4.11: Tabla de OpenSER

Descripción de la prueba

La prueba consistió en interconectar ambas plataformas mediante una troncal SIP. De esta manera, nos fue posible redirigir el tráfico que OpenSER no pueda manejar, es decir, servicios como Voicemail o extensiones especiales hacia Asterisk, mientras que OpenSER procesa las llamadas SIP de una forma mucho más eficaz que Asterisk.

Diagrama

Figura 4.8: Integración de Asterisk y OpenSER

Astesrik + OpenSER
Asterisk no es un proxy SIP, OpenSER sí
Asterisk no tiene un stack SIP completo, OpenSER sí
Asterisk no soporta TCP, OpenSER sí
Asterisk no es escalable, OpenSER sí
Asterisk actúa como b2bua, OpenSER no
Asterisk soporta multimedia, OpenSER no
Asterisk tiene Voicemail, Meetme, etc., OpenSER no
Asterisk dispone de interfases físicas, OpenSER no
Asterisk puede hacer de gateway, OpenSER no

Tabla 4.12: Astesrik + OpenSER

4.4. Resultados

Las pruebas son el mecanismo ideal para verificar que los sistemas se han capaces de cumplir con todos los requisitos precisados por el mercado.

Después de evaluar el servidor Asterisk se concluye que este posee un desempeño acorde a las expectativas que el mercado ha dictado y los servicios se distinguen por ser innovadores.

- Posee gran flexibilidad de extensión de servicios y funcionalidaes.
- Por medio de las interfases de administracíón basadas en web se facilita en mucho su administración y configuración.
- Las características de interoperabilidad mostradas son adecuadas para que un sistema Asterisk se integre prácticamente en cualquier entorno de telecomunicaciones moderno, tanto TDM como IP.
- Al ser una solución multiprotocolo, resulta transparente para el usuario final.
- Este tipo de soluciones es conveniente para aplicaciones de mediana escala, aunque existe la posibilidad de integrar varios servidores en un ambiente distribuido.
- Se deben realizar adecuaciones para que el sistema completo funcione como un dispositivo de propósito específico. Al final de cuentas, los recursos que Asterisk utiliza son administrados por el propio sistema operativo y son compartidos.
- La capacidad de "*transcoding*" representa una ventaja para el usuario final, pero sacrifica el rendimiento del sistema y su escalabilidad.

En lo que respecta a OpenSER, éste no nos ofrecen servicios de telefonía como tal, sino que nos aporta servicios de comunicación en tiempo real que el propio protocolo SIP soporta. Y, si el dispositivo conectado al proxy SIP implementa métodos SIP para la ejecución de facilidades básicas de telefonía como transferencias, call-pickup, etc, entonces, OpenSER es capaz de procesar y generar esos servicios.

- OpenSER presenta una mayor escalabilidad que Asterisk al estar basado en un único protocolo estandar (SIP).
- OpenSER es capaz de proveer servicios multimedia basados en SIP como Video llamada IP, Mensajería Instantánea, Sistemas de Manejo de Presencia, servidor de medios, etc.
- Al ser un proxy SIP, OpenSER no requiere que el tráfico de medios viaje a través del servidor, sino que sólo establece la conexión, la monitorea y la libera, dejando que sean los extremos quienes acuerden las características de la misma, reduciendo así la carga de trabajo para el propio servidor y aumentando su capacidad de procesamiento de llamadas.

- OpenSER esta basado en el protocolo estándar mas extendido en uso actualmente, lo cual le representa una gran oportunidad para incursionar en el mercado como un opción seria para la telefonía IP.
- Para entender el funcionamiento de OpenSER, es necesario entender al cien por ciento el funcionamiento del protocolo SIP y algunas cosas mas, por lo que la curva de aprenzaje de OpenSER es mas pronunciada que la de Asterisk.

Al ser ambos servidores desarrollados sobre software libre, éstos constituyen una opción favorable en cuanto a la configuración y por lo tanto, cuentan con una amplia gama de aplicaciones, debido fundamentalmente a las facilidades para vincularse a otras aplicaciones y servicios.

Capítulo 5

Conclusiones

Muchas son las conclusiones que podemos deducir de este trabajo. A continuación enlistamos aquellas que consideramos son las más importantes:

- El proceso de convergencia de las redes de Voz y Datos es irreversible y la telefonía convencional esta siendo desplazada por las tecnologías VoIP.
- La diferencia más notable entre los sistemas de telefonía tradicional y la telefonía IP es que en los primeros, se establece un circuito exclusivo para cada canal de Voz por cliente (Conmutación de circuitos), lo cual garantiza una alta calidad y confiabilidad en las llamadas, pero la ineficiencia en el aprovechamiento del canal es evidente en esta tecnología, mientras que en telefonía IP el uso del canal es más democrático y no existe una exclusividad del mismo (Conmutación de paquetes).
- El desarrollo de la tecnología VoIP ha propiciado el surgimieto de nuevos horizontes a medida que los recursos de la Red van incrementándose. Esto permite ofrecer algo más que un servicio básico de telefonía. La telefonía IP ofrece servicios inteligentes de comunicación basados en las necesidades de cada usuario y no en la oferta del proveedor del servicio.
- La ventaja que hace atractivo el uso de la telefonía IP por sobre la telefonía tradicional es la simplificación de la infraestructura de comunicaciones con la consecuente reducción de costos en el transporte de datos y en operación.
- La telefonía IP no es una solución mágica. Planear, diseñar e implementar una Red convergente plantea enormes retos y no es una tarea trivial; sin embargo, siguiendo una metodología de implementación adecuada es posible sacar enorme provecho de esta tecnología.
- Gracias a los modernos medios de comunicación hoy existentes, nos es posible trabajar en organizaciones virtuales sin importar las distancias, compartimos nuestras ideas con personas alrededor del mundo a través de listas de correo, foros de discusión, salas de conferencias, etc. El movimiento "Open Source" ha sido uno de los principales

benefiarios de los avances en el mundo de las comunicaciones globales y ha sabido corresponder a esos beneficios aportando ideas frescas y revolucionarias, lo cual genera un círculo virtuoso sumamente productivo.

- Con el uso de "Telefonía sobre Software Libre" como Asterisk y OpenSER se logra una independencia tecnológica con respecto a las grandes empresas de comunicaciones (por ejemplo Telmex), al desarrollar e innovar con servicios y aplicaciones.
- Tanto Asterisk como OpenSER poseen características y particularidades que los hacen diferentes entre sí, pero al mismo tiempo esas diferencias los convierten en plataformas complementarias.
- Al adoptar soluciones basadas en estándares abiertos se promueve la interoperatividad y se pueden integrar dispositivos o equipos de múltiples fabricantes y eliminar así la dependencia de un sólo fabricante. Asterisk y OpenSER, lejos de poder competir con las compañías que comercializan soluciones de VoIP Hw/Sw de alta calidad como son Alcatel-Lucent, Cisco, Avaya o Nortel, pretenden ser los mejores candidatos para evolucionar las redes telefónicas.

Apéndice A

Cronología histórica - Telefonía

En esta cronología se encuentran las fechas y sucesos que forman parte de los avances tecnológicos que desembocaron en las redes actuales de telefonía.

Fecha	Personaje	Hecho
1820	Hans C. Oersted	Descubre la generación de un campo magnético a partir de una corriente eléctrica (Relación entre Electricidad y Magnetismo). El resultado de sus experimentos fue publicado en un artículo en *Latín* bajo el título: "*Experimenta circa effectum conflictus electrici in acum magneticam*"
1820	André-Marie Ampere	Formula las *Leyes del Electromagnetismo*. Por vez primera se habla de ambos fenómenos como uno sólo.
1825	G. Stargeon	Fabrica un electroimán.
1835	Michael Faraday y Joseph Henry	Formulan de forma independiente y simultáneamente el *Principio de la Reciprocidad o Ley Faraday-Henry*. Éste principio establece que al igual que una corriente puede generar un campo magnético, un campo magnético *variable en el tiempo*, es capaz de producir una *F. E. M.* y ésta a su vez una corriente sobre un conductor.
1837	J. Henry y Page	Descubren que la Corriente Alterna circulando por un solenoide genera vibraciones.
1854	Charles Bourseul	Empleado del Correos y Telégrafos de Francia (*La Poste*). Presentó el primer reporte en donde proponía la transmisión de la Voz haciendo uso de medios electromagnéticos. Lamentablemente sus estudios no fueron tomados en serio.
1861	James Clerk Maxwell	Formulo cuatro ecuaciones, publicadas en *On Physical Lines of Force*. Estas formulas derivan de la ley de Faraday, la ley de Ampere y la ley de Gauss.
1867	Philip Reis	Presenta el artículo "*telefonía por medio de la corriente eléctrica*", en base a un modelo del oído. Construyó un aparato con el cual podía transmitir sonido a una distancia de hasta 100 [m]. El transmisor corresponde a las sugerencias de Bourseul y el receptor de las experiencias de Page. Con este aparato, nombrado por el mismo *teléfono*, consiguió reproducir sonidos a distancia, pero no así la palabra hablada, ya que el receptor permitía reproducir sólo el tono y no el timbre, y en modo muy imperfecto la intensidad.
1868	Icates	Modifica el *Teléfono* de Reis *modulando* la Corriente.
1871	Antonio Meucci	Es, desde 2001, reconocido como el verdadero inventor del *Teléfono*. En 1871 presentó la patente correspondiente. En 1872 presentó su invento al presidente de la NY Telegrap h Co. quien nunca lo devolvió. La Globe Telephone Co. emprendió un proceso en favor de la patente de Meucci en 1884, que fue interrumpida por una oferta de US$100,000. Meucci falleció antes del conocer el falló a su favor de la patente.
1876	Alexander Graham Bell y Elisha Gray	Se disputan la invención del *Teléfono*, inscribiendo patentes respectivas con dos horas de diferencia. Durante los siguientes noventa años el diseño del *Teléfono* no sufrió más que pequeñas modificaciones.
1878		Inauguración de la primera central telefónica en New Haven, EE.UU.
1879	Connelly y MacThige	Reciben la concesión por la patente de la primera *Central semiautomática* presentada en la Exposición Universal de Paris de aquel año.
1891	Almon Strowger	Recibió la patente por un Conmutador totalmente automático. Su sistema, desarrollado desde 1889, estaba basado en cinco hilos lo cual era poco eficiente. Poco después los científicos A. E. Keith, Frank A. Laundquist y los hermanos Erickson, John y Charles, lograron perfeccionar el sistema Strowger, reduciendo las líneas a dos hilos e integrando una batería más pequeña.

Tabla A.1: Cronología

Fecha	Hecho
1894	Inauguración en la Porte (América) de la primera central autómatica.
1921	Conversación a 10,000[km] entre la Habana e Isla Catalina combinando telefonía ordinaria y radiotelefonía.
1935	Se desarrolla el sistema de conmutación crossbar con control común.
1960	Aparecen los primeros sistemas de transmisión digital.
1966	Desarrollo de la central electrónica con control por programa almacenado.
1968-1972	Desarrollo del sistema PCM.
1972	Por vez primera la CCITT define la ISDN (RDSI) en la recomendación G.702: "Red Digital de servicios Integrados". La cual es una Red digital utilizada para la transmisión de diversos servicios como Voz y Datos.
1980	Se desarrolla el sistema de conmutación basado en control distribuido por microprocesadores.
1984-1988	Se crea en Europa la ETSI (European Telecommunications Standard Institute). Se crea el Sistema de Señalización número 7 (SS7).
A la fecha	Se desarrollan nuevos sistemas de señalización y se comienza el desarrollo de la telefonía celular, y la telefonía por la Internet.

Tabla A.2: Cronología

Apéndice B

Archivos de Configuración

B.1. Asterisk

```
\#--------------------(/etc/asterisk/asterisk.conf)----------------------

   [directories]
   astetcdir => /etc/asterisk
   astmoddir => /usr/lib/asterisk/modules
   astvarlibdir => /var/lib/asterisk
   astdatadir => /var/lib/asterisk
   astagidir => /var/lib/asterisk/agi-bin
   astspooldir => /var/spool/asterisk
   astrundir => /var/run
   astlogdir => /var/log/asterisk

\#--------------------(/etc/asterisk/features.conf)---------------------

   [general]
   parkext => 700
   parkpos => 701-720
   context => parkedcall
   parkingtime => 45
   courtesytone = beep
   parkedplay = caller
   findslot => next
   parkedmusicclass=default
   transferdigittimeout => 3
   xfersound = beep
   xferfailsound = beeperr

   pickupexten = *8
```

```
   featuredigittimeout = 500
   atxfernoanswertimeout = 15

   [featuremap]
   ;blindxfer => #
   disconnect => *0
   automon => *1
   atxfer => *2
   parkcall => #72

\#--------------------(/etc/asterisk/indications.conf)--------------------

   [general]
   country=mx

   [mx]
   description = Mexico
   ringcadence = 2000,4000
   dial = 425
   busy = 425/250,0/250
   ring = 425/1000,0/4000
   congestion = 425/250,0/250
   callwaiting = 425/200,0/600,425/200,0/10000
   dialrecall = !350+440/100,!0/100,!350+440/100,!0/100,!350+440/100,!0/100,
   350+440
   record = 1400/500,0/15000
   info = 950/330,0/30,1400/330,0/30,1800/330,0/1000
   stutter =!350+440/100,!0/100,!350+440/100,!0/100,!350+440/100,!0/100,
   !350+440/100,!0/100,!350+440/100,!0/100,!350+440/100,!0/100,350+440

\#-----------------------(/etc/asterisk/meetme.conf)-----------------------

   [general]
   [rooms]
   conf => 1234
   conf => 2345,9938

\#--------------------(/etc/asterisk/musiconhold.conf)---------------------

   [default]
   mode=files
   directory=/var/lib/asterisk/moh
   random=yes

\#------------------------(/etc/asterisk/iax.conf)-------------------------
```

```
   [general]
   bindport = 4569
   bindaddr = 0.0.0.0
   disallow=all
   allow=ulaw
   allow=alaw
   allow=gsm
   mailboxdetail=yes
   autokill=yes

   [29906]
   type=friend
   secret=29906
   callerid=ZoIPer <29906>
   host=dynamic
   context=local-iax
   qualify=yes
   autokill=yes
   mailbox=29906@default

\#-------------------------(/etc/asterisk/sip.conf)---------------------------


[general]
context=default
bindport=5060
bindaddr=0.0.0.0
videosupport=yes
disallow=all
allow=alaw
allow=alaw
allow=gsm
allow=h261
allow=h263
allow=h263p
allow=h264
language=en
useragent=Asterisk-Tesis
promiscredir=yes
dtmfmode=rfc2833

register => mx-df:passwd@IP_serv_mty/mx-mty

[29901]
```

```
type=friend
secret=29901
context=local-sip
callerid="Ing. Giovanni Nopal (Cisco 7960)" <29901>
host=dynamic
dtmfmode=rfc2833
nat=no
careinvite=no
nat=yes
callgroup=0
pickupgroup=0
mailbox=29901@default

[29902]
type=friend
secret=29902
context=local-sip
callerid="Ing. Juan Zarraga (Grandstream)" <29902>
host=dynamic
dtmfmode=rfc2833
nat=no
careinvite=no
callgroup=0
pickupgroup=0
mailbox=29902@default

[29903]
type=friend
secret=29903
context=local-sip
callerid="Ing. Israel Ortega (ATA Lynksys)" <29903>
host=dynamic
dtmfmode=rfc2833
nat=no
careinvite=no
callgroup=0
pickupgroup=0
mailbox=29901@default

[mx-mty]
type=friend
secret=passwd
context=mty-incoming
host=dynamic
```

```
[3001]
type=friend
secret=3001
context=local-sip
callerid="test-trunk" <3001>
host=dynamic
dtmfmode=rfc2833
nat=yes
careinvite=no

\#--------------------(/etc/asterisk/unicall.conf)----------------------

   [Channels]
   language=en
   usecallerid=yes
   echocancel=yes
   rxgain=0
   callgroup=0
   pickupgroup=0
   amaflags=default
   musiconhold=default
   context=trk-r2
   group=11

   protocolclass=mfcr2
   protocolvariant=mx,0,4,7
   category=NATIONAL_SUBSCRIBER
   channel=>1-10

\#--------------------(/etc/asterisk/voicemail.conf)----------------------

   [general]
   format=wav49|gsm|wav
   serveremail=staff-lab@voip.unam.mx
   attach=yes
   maxmsg=10
   maxmessage=120
   minmessage=3
   maxgreet=60
   skipms=3000
   maxsilence=10
   silencethreshold=128
   maxlogins=3
   userscontext=default
```

```
emailbody=Estimado ${VM_NAME}:\n\n\tUsted ha recibido un nuevo mensaje de voz
en su buzon numero: ${VM_MAILBOX}.\nMensaje numero: ${VM_MSGNUM}\nDuracion:
${VM_DUR}\nRemitente: ${VM_CALLERID},\nRecibido el dia: ${VM_DATE}.
Le sugerimos revisarlo en cuanto tenga tiempo. Gracias!\n\n\t\t\t\t--Asterisk\n
emaildateformat=%A, %B %d, %Y at %r

  mailcmd=/usr/sbin/sendmail -t
  sendvoicemail=yes

  [zonemessages]
  eastern=America/New_York|'vm-received' Q 'digits/at' IMp
  central=America/Chicago|'vm-received' Q 'digits/at' IMp
  central24=America/Chicago|'vm-received' q 'digits/at' H N 'hours'
  military=Zulu|'vm-received' q 'digits/at' H N 'hours' 'phonetic/z_p'
  european=Europe/Copenhagen|'vm-received' a d b 'digits/at' HM

  [default]
  29901 => 29901,Ing. Giovanni,giovanni@voip.unam.mx,,|tz=central|attach=yes
  29902 => 29901,Ing. Juan,juan@voip.unam.mx,,|tz=central|attach=yes
  29903 => 29901,Ing. Israel,israel@voip.unam.mx,,|tz=central|attach=yes
  29906 => 29901,Ing. ZoIPer-IAX,giovanni.nopal@gmail.com,,|tz=central|attach=yes
  666 => 666,Buzon de sugerencias,giovanni@voip.unam.mx,,|tz=central|attach=yes

\#----------------------(/etc/asterisk/extensions.conf)------------------

[local-sip]

include => locales

exten => _2990[1-5],1,Dial(SIP/${EXTEN},10,Ttr)
exten => _2990[1-5],n,Voicemail(${EXTEN}|u)
exten => _2990[1-5],n,Hangup

[local-iax]

include => locales

exten => _2990[6-9],1,Dial(IAX2/${EXTEN},10,Ttr)
exten => _2990[6-9],n,Voicemail(${EXTEN}|u)
exten => _2990[6-9],n,Hangup

[trk-r2]

exten => _9.,1,Dial(Unicall/g11/${EXTEN:1})
exten => _9.,n,Hangup()
```

```
exten => s,1,goto(ivr-tesis,s,1)

[mty-incoming]

include => locales

[mty-outgoing]

exten => _75XXX,1,NoOp(Llamada SIP saliente)
exten => _75XXX,n,Dial(SIP/mx-mty/${EXTEN:1})
exten => _75XXX,n,Hangup()

[locales]

include => local-sip
include => local-iax
include => servicios
include => parkedcall
include => trk-r2
include => mty-outgoing

[servicios]

include => correo-voz
include => conf-libre
include => conf-pwd
include => graba
include => buzon-suger
include => directorio

[correo-voz]

exten => *98,1,Answer
exten => *98,n,Wait(1)
exten => *98,n,VoiceMailMain()
exten => *98,n,Hangup
exten => _*98.,1,Answer
exten => _*98.,n,Wait(1)
exten => _*98.,n,VoiceMailMain(${EXTEN:3})
exten => _*98.,n,Hangup

[conf-libre]
exten => *1234,1,MeetMe(1234);
```

```
[conf-pwd]
exten => *2345,1,MeetMe(2345,9938);

[graba]

exten => *80,1,Wait(1)
exten => *80,n,Record(%d:gsm|1|100|'skip')
exten => *80,n,Wait(1)
exten => *80,n,Playback(${RECORDED_FILE})
exten => *80,n,Hangup()

[buzon-suger]

exten => *666,1,Playback(deja_mensaje)
exten => *666,n,Voicemail(666|s)
exten => *666,n,Hangup

[directorio]

exten => *90,1,Directory(default,locales)

[ivr-tesis]

include => servicios

exten => s,1,Set(LOOPCOUNT=0)
exten => s,n,SetMusicOnHold(default)
exten => s,n,Set(TIMEOUT(digit)=2)
exten => s,n,Set(TIMEOUT(response)=5)
exten => s,n,Playback(bienvenida)
exten => s,n(otravez),Background(menu_princ)
exten => s,n,WaitExten(5)

exten => 1,1,Goto(directorio,*90,1)

exten => 2,1,Goto(conf-libre,*1234,1)

exten => 3,1,Goto(conf-pwd,*2345,1)

exten => 4,1,Goto(buzon-suger,*666,1)

exten => #,1,Goto(hang,1)

exten => t,1,Goto(loop,1)
```

```
exten => i,1,Playback(ext_invalida)
exten => i,n,Goto(loop,1)

exten => loop,1,Set(LOOPCOUNT=$[${LOOPCOUNT} + 1])
exten => loop,n,GotoIf($[${LOOPCOUNT} > 2]?hang,1:s,otravez)

exten => hang,1,Playback(adios)
exten => hang,n,Hangup

exten => h,1,Hangup

\#----------------------------(/etc/selinux)-------------------------------
SELINUX=disabled

\#---------------------------(/etc/zaptel.conf)----------------------------

# Span 1: WCT1/0 "Digium Wildcard TE110P T1/E1 Card"
   span=1,1,0,cas,hdb3
   cas=1-15:1101
   cas=17-31:1101
# Global data
   loadzone        = mx
   defaultzone     = mx

------------------------------------------------------------------------------
Enlace digital E1 con señalización ISDN
------------------------------------------------------------------------------

\#---------------------------(/etc/zaptel.conf)----------------------------

# Span 1: WCT1/0 "Digium Wildcard TE110P T1/E1 Card 0" (MASTER)
   span=1,1,0,ccs,hdb3,crc4
   bchan=1-6
   dchan=16

# Global data
   loadzone    = mx
   defaultzone = mx

\#----------------------(/etc/asterisk/zapata.conf)---------------------------
   [channels]
   echocancel=no
   echotraining=no
   rxgain=0.0
   txgain=0.0
```

```
   group=0
   context=e1
 ;;Para señalización Q.sig cambiar a signallingtype=qsig
   switchtype=euroisdn
   signalling=pri_net
   channel=>1-6
```

B.2. OpenSER

Estos son los tres principales archivos de OpenSER para conocer su compormiento:

```
\#--------------------------(/etc/default/openser)-----------------------------
   RUN_OPENSER=yes
   USER=openser
   GROUP=openser
   Memory=64M
   DUMP_CORE=no
\#-------------------------/etc/openser/openserctlrc)-------------------------
   SIP_DOMAIN=openser.voip.unam.mx
   DBENGINE=MYSQL
   DBHOST=localhost
   DBNAME=openser
   DBRWUSER=openser
   DBROUSER=openserro
   DBROOTUSER="root"
   CTLENGINE="FIFO"
   OSER_FIFO="/tmp/openser_fifo"
   VERBOSE=1
\#-------------------------/etc/openser/openserctlrc)-------------------------

\# - - - - - - - - - - Parámetros de configuración globales - - - - - - - - -

   debug=3
   fork=yes
   log_stderror=no
   Check_via
   fifo="/tmp/openser_fifo"
   port=5060

\# - - - - - - - - - - - - - - - - Carga de modulos - - - - - - - - - - - - - -

loadmodule "/usr/local/lib/openser/modules/mysql.so"
```

```
loadmodule "/usr/local/lib/openser/modules/sl.so"
loadmodule "/usr/local/lib/openser/modules/tm.so"
loadmodule "/usr/local/lib/openser/modules/rr.so"
loadmodule "/usr/local/lib/openser/modules/maxfwd.so"
loadmodule "/usr/local/lib/openser/modules/usrloc.so"
loadmodule "/usr/local/lib/openser/modules/registrar.so"
loadmodule "/usr/local/lib/openser/modules/textops.so"
loadmodule "/usr/local/lib/openser/modules/xlog.so"
# Si habilitas el módulo de autenticación, debes cargar mysql.so
loadmodule "/usr/local/lib/openser/modules/auth.so"
loadmodule "/usr/local/lib/openser/modules/auth_db.so"

\# - - - - - - - - - - - - Lógica de ruteo de peticiones - - - - - - - - - - - -

route{
    if (!mf_process_maxfwd_header("10")) {
       sl_send_reply("483","Too Many Hops");
       exit;
    };
    if (msg:len >=  2048 ) {
       sl_send_reply("513", "Message too big");
       exit;
    };
    if (!method=="REGISTER")
       record_route();
       if (loose_route()) {
          append_hf("P-hint: rr-enforced\r\n");
          route(1);
       };
          if (!uri==myself) {
             append_hf("P-hint: outbound\r\n");
             route(1);
          };
          if (uri==myself) {
             if (method=="REGISTER") {
                if (!www_authorize("openser.voip.unam.mx","subcriber"){
                   www.challenge("openser.voip.unam.mx","0");
                   exit;
                }
              save("location");
                 exit;
             };
             lookup("aliases");
                if (!uri==myself) {
                   append_hf("P-hint: outbound alias\r\n");
```

```
                route(1);
             };
             if (!lookup("location")) {
                xlog("L_ERR","hora: [$Tf] metodo <$rm> r-uri <$ru> \n");
                xlog("L_ERR","<----Llamada a Asterisk---->\n);
                rewritehostport("IP_asterisk:5060");
                xlog("L_ERR","hora: [$Tf] metodo <$rm> r-uri <$ru> \n");
                route(1)
                sl_send_reply("404", "Not Found");
                exit;
             };
          append_hf("P-hint: usrloc applied\r\n");
       };
       route(1);
 }
 route[1] {
   if (!t_relay()) {
      sl_reply_error();
   };
 exit;
}
```

Apéndice C

Glosario de Términos y Acrónimos

En este apéndice se encuentran algunos términos y acrónimos de uso común, con la finalidad de hacer más comprensible el funcionamiento y operación de los sistemas de telefonía IP.

A

Alaw	Algoritmo de codificación y decodificación de Voz, utilizado para optimizar sistemas de comunicación. Es empleado principalmente en Europa y México.
Asterisk PBX	Es un software de código abierto. Es un conmutador telefónico tanto TDM como IP.
ATA	Es el acrónimo de "Analog Terminal Adapter". Es un dispositivo usado para conectar un teléfono analógico a una línea IP.

B

Bit	Es el acrónimo de "Binary Digit" (dígito binario).
bps	Es el acrónimo de "Bits Por Segundo".
BRI	Es el acrónimo de "Basic Rate Interface". Es la interfase RDSI al acceso a la tasa básica. Incluye dos canales B (bearer o transportadores) de 64Kbps y un canal D (delta) de 16 Kbps para control y señalización.
BW	Es el acrónimo de "Band-Width". Es el rango de frecuencias asignadas a un canal de transmisión. El ancho de banda se mide como la diferencia entre dos puntos del espectro en freuencia donde la atenuación de la señal no es mayor a tres decibeles(dB).

C

CAS	Es el acrónimo de "Channel Associated Signaling" - Señalización por Canal Asociado, por ejemplo, la señalización MFC/R2.
Codec	Es la contracción de "Codificador - Decodificador". Es el elemento que convierte una señal analógica en digital, la comprime y la codifica para su transmisión y luego realiza la tarea inversa para recuperar la señal original.
Conmutador	Es el dispositivo que realiza la labor de reencaminar líneas de transporte punto a punto, mediante la unión de líneas de entrada a líneas de salida.

D

DHCP	Es el acrónimo de "Dynamic Host Configuration Protocol". Es un protocolo que es usado para asignar las direcciones IP y demás datos de Red a los hosts de forma dinámica(RFC 2131 y RFC 2132).
DID	Es el acrónimo de "Direct Inward Dialing". Es un número telefónico que podemos marcar desde el exterior para acceder a una extensión dentro de un sistema privado de forma directa.
Dirección IP	Son los identificadores dentro de una red TCP/IP. Están compuestas de cuatro números separados por puntos, los cuales están dentro del rango numérico de 0 a 255.
DISA	Es el acrónimo de "Direct Inward System Access". Es un servicio que nos permite llamar desde el exterior e ingresar a extensiones que sólo los usuarios internos pueden acceder.
DNS	Es el acrónimo de "Domain Name System". Es usado dentro de la Internet para traducir nombres de dominio a direcciones IP y viceversa. Ej. www.yahoo.com.mx $\leftrightarrow$ 68,180,206,184
DSL	Es el acrónimo de "Digital Suscriber Line" - Línea Digital de Abonado. Es un conjunto de normas para la conectividad de red de banda ancha sobre líneas telefónicas normales.
DTMF	Es el acrónimo de "Dual Tone Multifrecuency". Son los tonos generados a distintas frecuencias, que utiliza la telefonía para identificar el marcado de un número u opción ingresados desde el teclado del teléfono.

E

E1	Es un protocolo de capa física para transmisiones de líneas dedicadas. Es un enlace digital con una tasa de transmisión de 2.048 Mbps, el cual lleva 32 canales de 64kbps, donde el canal 1 es utilizado para sincronía y el canal 16 se emplea para señalización.

F

Firewall	Es un dispositivo o programa encargado de filtrar la información al aplicar políticas de tráfico entre las fronteras de dos o más redes, es un requerimiento de seguridad de la red.
FreePBX	Es una interfase WEB para la configuración, administración y monitoreo de un sistema Asterisk.
FXO	Es el acrónimo de "Foreing eXchange Office". La interfase FXO es el dispositivo o elemento que recibe la llamada.
FXS	Es el acrónimo de "Foreing eXchange Subscriber". La interfase FXS se ubica en un PBX o dispositivo de la central telefónica y es la interfase para conectar un equipo terminal de usuario.

I

IAX2	Es el acrónimo de "Inter-Asterisk eXchange protocol". Es el protocolo propio de Asterisk para la señalización de llamadas VoIP.
ISDN	"Integrated Services Digital Network". Red Digital de Servicios Integrados. Es una tecnología que permite la transmisión de Voz, Video y Datos punto a punto utilizando la infraestructura de la Red de telfonía convencional.
ITSP	Es el acrónimo de "Internet Telephony Service Provider". Se denomina de esta forma a los proveedores del servicio de telefonía a través de la Internet.
IVR	Es el acrónimo de "Interactive Voice Response". Es una aplicación que permite reproducir un menú de voz, con el cual el llamante puede interactuar desde el teclado telefónico.

J

Jitter	Variaciones en el tiempo de arribo entre paquetes IP, causados por la congestión de la red o cambios en el ruteo.

L

LAN	Es el acrónimo de "Local Area Network" - Red de Área Local. Una LAN es una red que conecta computadoras y otros dispositivos (impresoras, escanners, etc), en una área geográfica pequeña. Cada dispositivo conectado a una LAN se denomina nodo.

M

MAN	Es el acrónimo de "Metropolitan Area Network" - Red de Área Metropolitana. Una MAN es una red de alta velocidad (banda ancha) que cubre un área geográfica extensa.
MGCP	Es el acrónimo de "Media Gateway Control Protocol". Este protocolo tiene su origen en el SGCP (de Cisco y Bellcore) e IPDC.
MULTICAST	Multidifusión a través del envió de la información en una red a múltiples destinos de manera simultánea.

N

NAT	Es el acrónimo de "Network Address Translation Protocol". Es un protocolo de traducción de direcciones de red.

P

Paquete	Unidad de datos que se rutea entre un origen y un destino en la Internet u otra red de intercambio de paquetes.
PBX	Es el acrónimo de "Private Branch eXchange" o "Private Business eXchange". Es un conmutador telefonico *privado*.
POST	Es el acrónimo de "Plain Old Telephone Service". Es el servicio de telefonía básica brindado por la PSTN.
PRI	Acrónimo de "Primary Rate Interface". Es la interfase RDSI de acceso a la tasa primaria. Incluye treinta canales B (bearer o transportadores) de 64kbps y un canal D (delta) de 16 kbps para control y señalización.
Protocolo de comunicación	Conjunto de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.
PSTN	Es el acrónimo de "Public Switched Telephone Network". Es la Red Telefónica Pública Conmutada mundial de Voz.

R

RFC	Es el acrónimo de "Request for Comments", representa una serie de documentos numerados e informales que buscan construir consensos en favor de la estandarización de protocolos y servicios para la Internet
RJ11	RJ es un acrónimo de "Registered Jack". Es una interfase física usada para conectar aparatos telefónicos convencionales, donde se suelen utilizar generalmente sólo los dos pines centrales para una línea simple o par telefónico.
RJ45	RJ es un acrónimo de "Registered Jack". Posee ocho "pines" o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado. Es una interfase física usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e y 6).
RTCP	Es el acrónimo de "Real time Transport Control Protocol". Está definido en el RFC 3550. Es utilizado para enviar paquetes de control a los participantes en una llamada. La función primaria es proveer realimentación de la calidad de servicio provista por RTP.
RTP	Es el acrónimo de "Real time Transport Protocol'". El cual define un formato de paquete estándar para el envío de audio y video sobre la Internet. Está definido en el RFC 1889.

S

Script	Es un conjunto de sentencias de control e instrucciones que generan un programa.
SIP	Es el acrónimo de "Session Initiation Protocol". Es un protocolo de señalización para la telefonía IP utilizado para establecer, modificar y terminar llamadas de VOIP. SIP fue desarrollado por el IETF y publicado en el RFC 2543.
SNMP	Es el acrónimo de "Simple Network Management Protocol". Es un protocolo estándar de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la suite de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.
Softphone	Es la combinación de términos (Software y Telephone). Es un software que simula un teléfono convencional, este puede ser instalado en un dispositivo electrónico como la computadora o una PDA (Agenda electrónica).
SSH	Es el acrónimo de "Secure Shell". Es un software que permite realizar comunicaciones o transferencia de datos de manera remota y segura.
Switch	Dispositivo que conduce los datos de entrada, desde una serie de puertos de entrada múltiple al puerto de salida específico que conducirá los datos hacia el destino indicado.

T

TCP	Es el acrónimo de "Transmission Control Protocol". El protocolo que garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.
TDM	Es el acrónimo de "Time Division Multiplexing". Es la intercalación en el tiempo de muestras de diferentes fuentes de tal forma que la información de todas sea transmitida en serie sobre un mismo canal de comunicación.
TFTP	Es el acrónimo de "Trivial File Transfer Protocol". Es un protocolo de transferencia de archivos asociado al puerto 69 y basado en UDP que no proporciona ninguna seguridad.
TrixBox	Es un compilador sobre la distribución de CentOS está basado su desarrollo sobre software de código abierto. Trixbox es una solución hibrida confiable, ya que nos proporciona compatibilidad con los sistemas de telefonía-IP y las telefonía convencional.
Trunk	Es el medio de transmisión por el que se puede manejar varias comunicaciones o canales. Siendo un canal que opera entre dos puntos distantes.

U

UDP	Es el acrónimo de "User Datagram Protocol". Es un protocolo del nivel de transporte basado en el intercambio de datagramas, al no presentar confirmación de entrega o de recepción, ni control de flujo, no es posible saber si el envió fue exitoso.
Ulaw	Ley Mu es un sistema de cuantificacion logaritmica de una señal de audio utilizado principalmente en EEUU y Japon.
UPS	Es el acrónimo de "Uninterruptible Power Supply". Fuente de alimentación ininterrumpida. Están diseñadas para proteger los equipos de un amplio rango de disturbios que pueden ocurrir.
UTP	Es el acrónimo de "Unshielded Twisted Pair". Es un tipo de cableado utilizado principalmente para comunicaciones, normalizado sobre la norma Americana TIA/EIA-568-B y a la internacional ISO-11801.

V
W

VoIP	Es el acrónimo de "Voice Over Internet Protocol". Es la tecnología que permite el enrutamiento de conversaciones de voz a través de redes de datos o de la Internet.
VPN	Es el acrónimo de "Virtual Private Networks". Es una red privada virtual la cual realiza la conexión de usuarios de distintas redes a través de un túnel que se construye sobre la Internet o sobre cualquier red pública.
WAN	Es el acrónimo de "Wide Area Network". Una WAN es una red que conecta los ordenadores en un área geográficamente dispersa. Este tipo de redes suelen ser públicas, es decir, compartidas por muchos usuarios.

Bibliografía

[1] *SDPng transition*. 2003. Trabajo en desarrollo bajo el nombre draft-ietf-mmusic-sdpng-trans-04.txt.

[2] 3com. Understandign ip addressing: Everything you ever wanted to know. White paper.

[3] Juán Israel Ortega Aceves. Seguridad de voip. *Suplemento Enter@te*, 55, 2007. `http://www.enterate.unam.mx/`.

[4] Uyless Black. *IP Telephony*. Prentice Hall, 2005. United States - First Edition.

[5] Comisión Federal de Telecomunicaciones COFETEL. Nom-em-012-sct1-199412dic1994, centrales telefónicas digitales parte 2 - transmisión. In *Diario Oficial de la Federación*, 12 dic 1994.

[6] Comisión Federal de Telecomunicaciones COFETEL. La norma oficial mexicana nom-151-sct1-1999 , interfaz a redes públicas para equipos terminales. In *Diario Oficial de la Federación*, pages 65–66, 1999.

[7] Sunrise Telecom Incorporated. Introduction to mfc-r2 signaling. technology series. Publication Number TEC-GEN-002 Rev. B, 2001.

[8] Leif Madsen Jim Van Meggelen, Jared Smith. *Asterisk The future of Telephony*. O'Reilly, 2007. Segunda Edición.

[9] Christopher Rodes & The Asterisk Documentation Team Mark Spencer, Mack Allison. The asterisk handbook version 2. Copyright Digium© Inc., 2003.

[10] Frank W. Miller Mark Spencer. Inter-asterisk exchange (iaxv2). Copyright Digium© Inc. y Cornfed Systems, LLC.

[11] Stephen L.; FREDERICK Ron; JACOBSON Van. SCHULZRINNE, Henning; CASNER. Rtp: A transport protocol for real time applications. In *RFC 1889*, enero 1996.

[12] Steven Shepard. *Voice over IP Crash course*. McGraw-Hill, 2005. United States - First Edition.

[13] www.openser.org. Página del proyecto OpenSER. `http://www.openser.org`, 2007.

[14] www.voip info.org. Wiki de VoIP-info.org. `http://www.voip-info.org/wiki/view/Asterisk`, 2007.