

UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



**PROPUESTA DE MEJORA PARA LA INTERCONEXIÓN ENTRE UN
OPERADOR DE LARGA DISTANCIA Y SUS CARRIERS INTERNACIONALES,
UTILIZANDO TECNOLOGÍA SBC EN MODO SIP-TRUNK**

**INFORME DE SUFICIENCIA
PARA OPTAR EL TÍTULO PROFESIONAL DE:
INGENIERO DE TELECOMUNICACIONES**

**PRESENTADO POR:
RODRÍGUEZ CASTILLO WILLIAM MAXIMILIANO**

**PROMOCIÓN
2005 – II**

**LIMA – PERÚ
2014**

**PROPUESTA DE MEJORA PARA LA INTERCONEXIÓN ENTRE UN
OPERADOR DE LARGA DISTANCIA Y SUS CARRIERS INTERNACIONALES,
UTILIZANDO TECNOLOGÍA SBC EN MODO SIP-TRUNK**

Dedicatoria:

A mis padres a quienes espero pueda enorgullecer, a mis hermanos a quienes amo mucho, a Gabriela por todo su apoyo y a mi facultad la FIEE que es mi orgullo.

SUMARIO

En el presente informe se propone la mejora en la tecnología de interconexión de un Operador de Larga Distancia (Americatel Perú SAC) con sus *Carriers* Internacionales, utilizando el protocolo de señalización SIP en modo *Trunk* (SIP-TRUNK) con equipamiento SBC (*Session Border Controller*).

En la primera etapa se realiza un reconocimiento de la tecnología SBC, abarcando conceptos de equipamiento y modelos, en esta etapa también se describen conceptos de protocolo SIP (*Session Initiation Protocol*) en la telefonía IP.

En la segunda etapa se desarrolla una topología de solución para el requerimiento propuesto, utilizando una determinada marca de equipo SBC, se detalla además la configuración aplicada al equipo SBC y centrales telefónicas a las que éste equipo se debe interconectar.

En la tercera etapa se realiza un estudio evaluativo con respecto al financiamiento del proyecto. Utilizando conceptos de VAN, TIR y los indicadores de gestión Capex y Opex se analiza la rentabilidad del proyecto a lo largo de 12 meses, demostrando que el proyecto es rentable.

El proyecto aporta una solución segura y viable para los Operadores de Telecomunicaciones que se encuentran en la necesidad de migrar sus Troncales Digitales TDM a Troncales SIP, los Operadores pueden estar en esta necesidad de migración buscando un ahorro económico o buscando estar a la vanguardia de las tecnologías actuales.

ÍNDICE

SUMARIO	v
INTRODUCCIÓN	1
CAPITULO I	
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA	2
1.1 Presentación	2
1.2 Descripción del problema	3
1.3 Objetivos del trabajo.....	4
CAPITULO II	
CONCEPTOS TEÓRICOS DE TELEFONÍA IP	6
2.1 Telefonía IP	6
2.1.1 Telefonía IP vs Telefonía Tradicional	6
2.1.2 Normas.....	8
2.1.3 Definición de VOIP	9
2.1.4 Funcionamiento de VOIP.....	10
2.1.5 Características de la Telefonía IP	12
2.1.6 Arquitectura	12
2.1.7 Beneficios.....	14
2.1.8 Protocolos de comunicación.....	14
2.1.9 Calidad de Servicio (QoS)	18
2.2 Sistemas de Gateways y SBC.....	20
2.3 Características SIP y beneficios sobre otros protocolos de señalización	21
2.3.1 Definición de Protocolo SIP	21
2.3.2 Funcionamiento de protocolo SIP.....	26
2.3.3 Protocolos RTP/RTCP y SDP.....	30
2.3.4 Comparación con protocolos MGCP, SCCP, H.323, IAX Y SS7	32
2.4 Protocolo SIP-TRUNK.....	35
CAPITULO III	
PLANEAMIENTO Y SOLUCIÓN DEL PROBLEMA	37
3.1 Objetivos de Servicio.....	37
3.2 Equipo <i>Session Border Controller</i>	37

3.2.1	Principales proveedores de equipos <i>Session Border Controller</i>	38
3.2.2	Modo Peering y Modo Access	40
3.3	Topología de la Solución	42
3.4	Equipamiento	44
3.4.1	<i>Acme Packet</i> Net-Net 3820	44
3.4.2	<i>Softswitch</i> Huawei SoftX3000.....	44
3.5	Configuración de Equipos.....	45
3.5.1	Configuración <i>Acme Packet</i> Net-Net 3820	45
3.5.2	Configuración en el <i>Softswitch</i> Huawei SoftX3000	49
CAPITULO IV		
CRONOGRAMA Y ESTUDIO ECONÓMICO DEL PROYECTO		51
4.1	Tiempo de Ejecución.....	51
4.2	Estudio económico del Proyecto.....	52
4.2.1	Análisis de CAPEX y OPEX	52
4.2.2	Evaluación económica del Proyecto	54
CONCLUSIONES Y RECOMENDACIONES		60
BIBLIOGRAFÍA.....		62
ANEXO A		
DATOS DE CONFIGURACIÓN DEL SBC <i>ACME PACKET</i>.....		63
ANEXO B		
PROPUESTA COMERCIAL - SBC <i>ACME PACKET</i>.....		69

ÍNDICE DE FIGURAS

Figura 1.1 Red de Telefonía del Operador de Larga Distancia	3
Figura 1.2 Diagrama actual de interconexión de <i>Carriers</i>	4
Figura 1.3 Diagrama propuesto de interconexión de <i>Carriers</i> con SBC	5
Figura 2.1 Red básica de un sistema de telefonía IP	7
Figura 2.2 Protocolos SIP, H.323, MEGACO y MGCP	9
Figura 2.3 Arquitectura de Telefonía IP	14
Figura 2.4 Estructura protocolar para sistemas VoIP según modelo OSI	21
Figura 2.5 Estructura de protocolo de “ <i>Redirect Server</i> ”	23
Figura 2.6 Estructura de trama mensaje SIP	24
Figura 2.7 Ejemplo de transacción	26
Figura 2.8 Ejemplo de diálogo	27
Figura 2.9 Diálogo de registro	28
Figura 2.10 Diálogo de Invitación de sesión	29
Figura 2.11 Diálogo de término de sesión	29
Figura 2.12 Diálogo de término de sesión con registro de ruta en “proxy”	29
Figura 2.13 Opciones de atributos ofrecidos por SDP para sesión	31
Figura 2.14 Opciones de atributos ofrecidos por SDP de tiempo	31
Figura 2.15 Opciones de atributos ofrecidos por SDP de media	31
Figura 2.16 Mensaje INVITE común, enmarcado en rojo ejemplo DSP	32
Figura 3.1 Diagrama de ejemplo para modo “ <i>Peering</i> ”	41
Figura 3.2 Diagrama de ejemplo para modo “ <i>Access</i> ”	42
Figura 3.3 Topología de Solución (Fuente: Elaboración propia)	43
Figura 3.4 <i>Acme Packet Net-Net 3820</i>	44
Figura 3.5 <i>Softswitch Huawei SoftX3000</i>	45
Figura 3.6 Jerarquía ACLI	45
Figura 3.7 Ingreso al SBC vía Telnet	46
Figura 3.8 Crear <i>Session Constraints</i>	46
Figura 3.9 Crear <i>Translations Rules</i>	46
Figura 3.10 Crear <i>Session Translation</i>	46
Figura 3.11 Crear <i>Realms</i>	47
Figura 3.12 Crear SIP Interface	47

Figura 3.13 Crear <i>Session Agent</i>	47
Figura 3.14 Crear <i>Session Group</i>	48
Figura 3.15 Crear Local <i>Policy</i>	48
Figura 3.16 Crear Access Control	48
Figura 3.17 Salvar y Activar	49
Figura 3.18 Performance Task Management	50
Figura 3.19 Task Management SOFTXV3 - SOFTX3000 Synchronize all tasks	50
Figura 4.1 Diagrama de Gantt parte 1	52
Figura 4.2 Diagrama de Gantt parte 2	52
Figura 4.3 Costo del Equipo SBC <i>Acme Packet Net-Net 3820</i>	54

ÍNDICE DE TABLAS

Tabla 2.1 Comparativa entre SIP y H.323	34
Tabla 3.1 Características del <i>Acme Packet</i> Net-Net 3820	44
Tabla 4.1 Proyección de cantidad de sesiones en el SBC vs tiempo	56
Tabla 4.2 Ingreso del Operador por minuto para diferentes destinos de Perú	57
Tabla 4.3 Promedio de tráfico de llamadas mensual de un <i>Carrier</i>	57
Tabla 4.4 Ganancia mensual de un <i>Carrier</i> de 100 sesiones de capacidad	57
Tabla 4.5 Flujo de caja mensual del Proyecto	58
Tabla 4.6 Flujo de caja mensual del Proyecto	58

INTRODUCCIÓN

Las redes de circuitos conmutados en el Perú han cumplido un importante ciclo en las comunicaciones telefónicas, pero es evidente la cantidad de antecedentes que muestran que esta tecnología está en su límite evolutivo, refiriéndose a términos de escalabilidad, costos, eficiencia de ancho de banda y flexibilidad de la red.

Es en el desarrollo de la Telefonía IP en donde se encuentra la respuesta a las debilidades de la Red de Telefonía Pública Conmutada (PSTN). La Telefonía IP es la red de voz paquetizada, que se soporta sobre redes WAN (redes de área Amplia), las cuales cumplen de forma parcial o total las veces de redes PSTN.

La Telefonía IP tiene ventajas y desventajas; ahora, se debe prestar atención a la ventaja de la convergencia, pues se refiere a unificar la red, es decir integración de todos los servicios en una eficiente red de transporte.

Ha sido importante para el desarrollo de la Telefonía IP el avance tecnológico en el transporte de información a nivel físico. Es así como el tema de las tecnologías SBC (*Session Border Controller*) amplía la visión de realización de toda idea de convergencia, administración, soporte, y costo sobre redes comunicaciones. Sin embargo se debe que rescatar conceptos de la tecnología actual como es el separar los canales de datos de información y señalización entre el transmisor y el receptor de estos datos. Es por esto que en el presente proyecto se toma como solución el protocolo de señalización SIP en modo *Trunk* (SIP-TRUNK) pues presenta características evolutivas altas para mantenerse vigente en el tiempo.

CAPITULO I

PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

1.1 Presentación

En el presente proyecto se propone una solución para un Operador Local que entre los distintos servicios que brinda a sus clientes está el servicio de llamadas larga distancia internacional. En adelante, a este Operador, se le denominará "Operador de Larga Distancia".

Los servicios de este Operador de Larga Distancia se soportan sobre tres grandes redes de fibra óptica y satelitales interconectadas entre sí: Una red local, con cobertura en todo Lima, una red nacional, que cubre los 24 departamentos del Perú y la red mundial, con interconexión directa a los principales operadores del mundo. Es precisamente en la red mundial en donde aplicaremos nuestra propuesta de mejora.

La red del Operador de Larga Distancia está compuesta por Interconexiones entre éste y diferentes *Carrier* Internacionales¹.

Actualmente el Operador de Larga Distancia tiene 2 tipos de interconexiones con sus *Carrier* internacionales:

- Troncal Digital TDM (con Sistema de Señalización por Canal Común o SS7)
- Troncal IP H.323 (con Señalización IP a través del protocolo H.323)

En la figura 1.1 se muestra un diagrama simple de la Red de Telefonía del Operador de Larga Distancia. De esta figura debemos destacar los siguientes dispositivos de Red:

- *Softswitch* y Mini UMG: Ambos dispositivos realizan el control de las líneas NGN² del Operador.
- Central Huawei C&C08: Dispositivo que realiza el control de las líneas de telefonía analógica (TA) y líneas primarias (PRI) del Operador.
- Central *Softswitch* SX3000: Central que se interconecta con los otros operadores como Telefónica del Perú y Claro; además de la Interconexión con los *Carrier* Internacionales por protocolo SS7.
- *Gateway* A8010: *Gateway* a través del cual se realiza la interconexión con los *Carrier* IP, utilizando el protocolo IP H.323.

¹ Los *Carrier* son las empresas de telecomunicaciones que permiten el tráfico de datos a otras empresas proveedoras de servicio (telefonía, internet, etc.).

² *Next Generation Networking* (Red de la próxima generación)

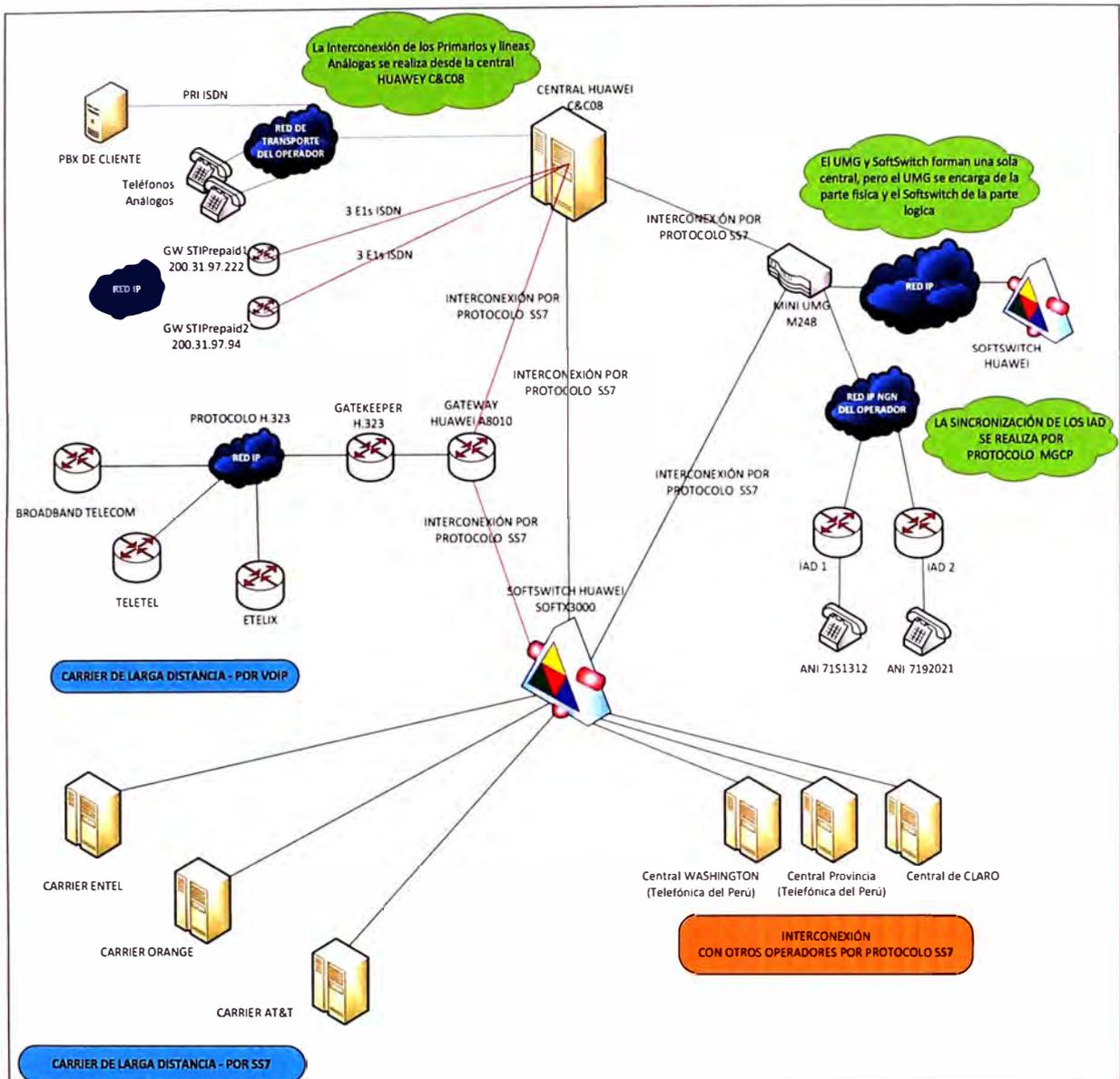


Figura 1.1 Red de Telefonía del Operador de Larga Distancia
(Fuente: Americatel Perú SAC)

1.2 Descripción del problema

De los dos tipos de interconexión que el Operador de Larga Distancia tiene actualmente con sus *Carrier* Internacionales (troncal digital TDM y troncal IP H.323), se afirma que:

- La troncal digital TDM por protocolo de señalización SS7, si bien es una tecnología aún vigente, ya se encuentra en su límite evolutivo. En los capítulos posteriores se fundamentará que la Telefonía IP es la respuesta a las debilidades de esta tecnología.
- La troncal IP H.323, si bien se trata de Telefonía IP, el protocolo de señalización H.323 es un protocolo que no garantiza la calidad de servicio, en los capítulos posteriores se fundamentará también que actualmente este protocolo ha sido desplazado por el protocolo de señalización SIP (*Session Initiation Protocol*).
- La troncal IP H.323, está actualmente utilizando un *Gateway* en su configuración, si bien los “gateways” cumplen una tarea muy importante en la traducción de llamadas

desde la PSTN³ a la red IP, el control, la seguridad y la calidad de las sesiones realizadas sobre IP punto a punto, no son respaldadas por estos equipos, lo que se traduce en puntos en contra para este sistema VoIP.

1.3 Objetivos del trabajo

De lo expuesto en el punto 1.2 se propone:

- Mantener la interconexión por troncal Digital TDM, debido a que existen aún en el mercado muchos *Carrier* que utilizan este tipo de interconexiones. Siendo además una interconexión que brinda muy buena calidad de servicio (calidad en las llamadas). Pero se debe tener claro que la tendencia de los *Carrier* es a las interconexiones IP.
- Migrar la interconexión por troncales IP H.323 a otro tipo de interconexión IP, que facilite un mayor control, seguridad y calidad de servicio. Cambiando el *Gateway* y *Gatekeeper* por el dispositivo de red SBC o "*Session Border Controller*" trabajando en protocolo SIP-*Trunk* (troncal SIP).

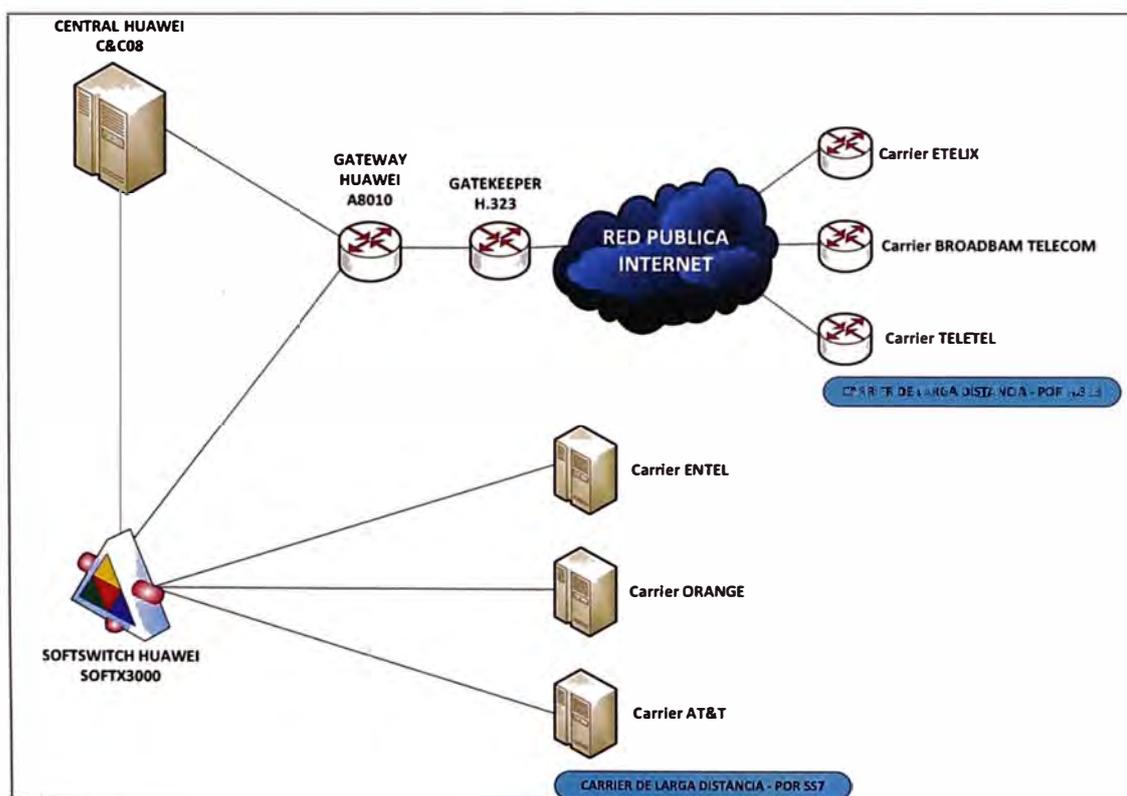


Figura 1.2 Diagrama actual de interconexión de *Carriers*
(Fuente: Americatel Perú SAC)

El SBC es un equipo controlador de sesiones optimizado para la interconexión entre redes VoIP. Este equipo tiene altas normas de seguridad para el tránsito de entrada y salida de todas las transmisiones de voz que viajan sobre la red.

El SBC puede pasar todo el tráfico telefónico de un punto a otro mediante una simple Troncal SIP (SIP-*Trunk*) con capacidad de entregar miles de llamadas simultáneas. Lo

³ Public switched telephone network (Red de telefonía pública conmutada)

que permitiría un gran ahorro, la eliminación paulatina de tramas E1 (debido a que cada vez hay menos *Carrier* con interconexión digital), y por supuesto mayor seguridad.

Además el SBC permite también la interconexión por protocolo H.323 si en caso uno de los actuales *Carrier* IP no tenga la facilidad de migrar a SIP-*Trunk*.

En la figura 1.2 se muestra el diagrama actual de interconexión con los *Carrier* Internacionales, se puede observar la troncal con protocolo H.323 y las troncales TDM con protocolo SS7.

En la figura 1.3 se muestra el diagrama de cómo sería la interconexión con los *Carrier* Internacionales utilizando el *Session Border Controller*, se puede observar la troncal con protocolo SIP-*Trunk* y también las troncales TDM por protocolo SS7 que aún se mantendrían vigentes pero con la opción de migrar a SIP-*Trunk*.

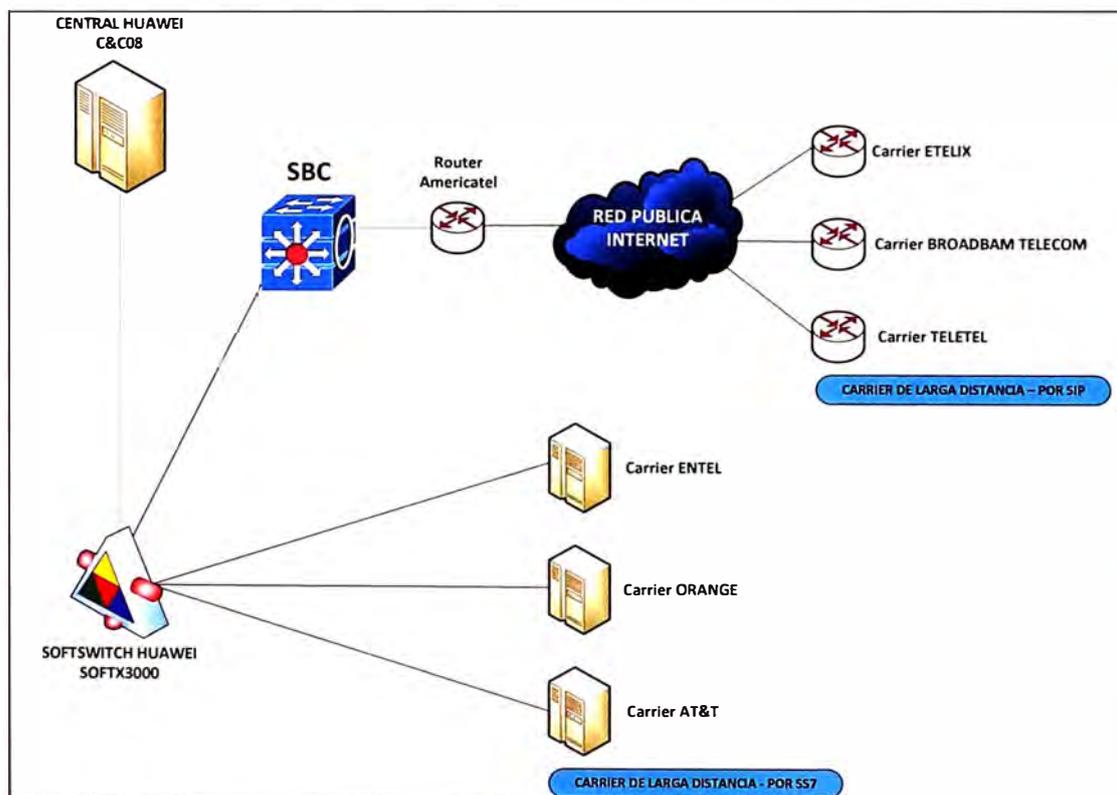


Figura 1.3 Diagrama propuesto de interconexión de *Carriers* con SBC
(Fuente: Elaboración propia)

CAPITULO II

CONCEPTOS TEÓRICOS DE TELEFONÍA IP

2.1 Telefonía IP

Los sistemas de telefonía tradicional están guiados por un sistema muy simple pero ineficiente denominado conmutación de circuitos. La conmutación de circuitos ha sido usada por las operadoras tradicionales por más de 100 años. En este sistema cuando una llamada es realizada la conexión es mantenida durante todo el tiempo que dure la comunicación. Este tipo de comunicaciones es denominado "circuito" porque la conexión está realizada entre 2 puntos hacia ambas direcciones. Estos son los fundamentos del sistema de telefonía convencional.

La telefonía IP (*Internet Protocol*) es una tecnología que reúne la transmisión de voz y de datos, posibilitando la utilización de redes informáticas para efectuar llamadas telefónicas. Desarrolla una red única, que se encarga de cursar todo tipo de comunicación, ya sea, de voz, datos o video, que se denomina Red Convergente o Red Multiservicios.

La telefonía IP surge como una alternativa a la telefonía tradicional, brindando nuevos servicios al cliente entre los que se cuentan una serie de beneficios económicos y tecnológicos.

2.1.1 Telefonía IP vs Telefonía Tradicional

Aunque en la telefonía IP se utiliza parte de la infraestructura de telecomunicaciones ya existente requiere de nuevos elementos.

Actualmente muchas organizaciones utilizan un entorno en el cual coexisten varias redes paralelas, como por ejemplo voz y datos.

Por el contrario en las nuevas redes, mediante la incorporación de unos elementos denominados VoIP GW (*Gateway* o Pasarela para Voz sobre IP) se pueden unificar ambas redes y por tanto se logra la Convergencia.

En la telefonía IP se necesita un elemento que se encargue de transformar las ondas de voz en datos digitales y que además los divida en paquetes susceptibles de ser transmitidos haciendo uso del protocolo IP. Este elemento es conocido como Procesador de Señal Digital (DSP), el cual está ya disponible y utilizan los Teléfonos IP o los propios *Gateways* (Pasarelas) encargadas de transmitir los paquetes IP una vez paquetizada la voz. Cuando los paquetes alcanzan el *Gateway* de destino se produce el mismo proceso a través del DSP pero a la inversa con lo cual el receptor podrá recibir la señal analógica

correspondiente a la voz del emisor. La figura 2.1 muestra una red básica de un sistema de telefonía IP.

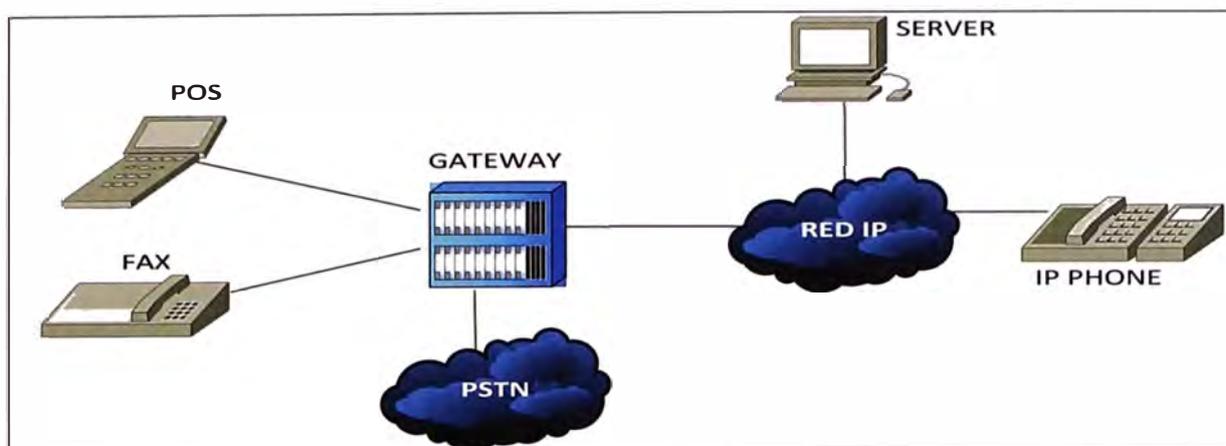


Figura 2.1 Red básica de un sistema de telefonía IP
(Fuente: Elaboración propia)

La transmisión de paquetes de voz según la forma expuesta, es similar a la transmisión de un correo electrónico desde el origen hasta el destino. El problema es que en las transmisiones IP de correo electrónico desde el origen hasta el destino no está garantizado el éxito, por lo cual si el correo no es legible o se "pierde" algún paquete, es necesario solicitar la retransmisión del mismo. Pero en el caso de la transmisión de voz esto no es así, ya que la necesidad de recibir los paquetes en un determinado orden, la necesidad de asegurar que no haya pérdidas y de conseguir una tasa de transmisión mínima hacen prácticamente necesaria la implantación de sistemas de Calidad de Servicio (QoS: *Quality of Services*). Estos sistemas suponen actualmente un gran reto en la industria ya que garantizar "Calidad de Servicio sobre IP" requiere la inmediata implantación de los sistemas de transmisión de voz.

- El servicio debe ser universal para todo el ámbito estatal.

Las redes de datos, basadas en la conmutación de paquetes, se identifican por las siguientes características:

- Para asegurar la entrega de los datos se requiere el direccionamiento de paquetes, sin que sea necesario el establecimiento de llamada.
- El consumo de los recursos de red se realiza en función de las necesidades, sin que sean reservados siguiendo un criterio de extremo a extremo.
- Los precios son determinados por la oferta y la demanda.
- Los servicios se prestan de acuerdo a los criterios impuestos por la demanda, variando ampliamente en cuanto a cobertura geográfica, velocidad y condiciones.
- Implementar una red convergente supone estudiar las diferencias existentes entre las características de las redes de voz y de datos, comprendiendo los problemas técnicos que implican dichas diferencias sin perder de vista la perspectiva del usuario final.

Las diferencias entre la operación de las redes de voz y datos requieren distintos enfoques de gestión.

Tradicionalmente, la industria de la telefonía trabaja con unas altas exigencias de fiabilidad, conocidas como los "cinco nueves": 99,999 por ciento. Esto se traduce en unos objetivos de diseño de centrales públicas de conmutación que garantizan niveles de caída del servicio de sólo dos horas cada cuarenta años de operación. Cuarenta años suponen aproximadamente 350.400 horas; y dos horas sin servicio representa un 0,0000057 de todo ese tiempo. O lo que es lo mismo, una disponibilidad del 99,9994 por ciento.

Gracias a la unificación de las redes de voz y datos se logran mejoras en la simplificación de la gestión, el control y reducción del mantenimiento y el mayor aprovechamiento de las líneas de datos.

2.1.2 Normas

Las normas ITU (Sector de Normas de Telecomunicaciones de la Unión Telegráfica Internacional) para VoIP han evolucionado de manera significativa. Hace cuatro años, parecía que el protocolo H.323, una norma desarrollada en 1996 para multimedia, se encaminaba hacia la aceptación universal como la norma principal para la señal y la configuración de llamadas VoIP.

Esta norma no se utilizó originalmente con este propósito, sin embargo, algunas de sus partes tuvieron mucho éxito entre los desarrolladores de productos VoIP. La segunda versión del protocolo H.323 agregó soporte WAN para VoIP; la norma H.323 más reciente, incluye un nuevo procedimiento para mejorar el tiempo de configuración.

A medida que los fabricantes de productos VoIP realizaron pruebas de interoperatividad para las operaciones más complejas, se percataron que necesitaban una norma sencilla y adaptable para el manejo de llamadas y el protocolo de transmisión. Con este fin, el IETF (Grupo de Trabajo de Ingeniería Internet) desarrolló el Protocolo de Iniciación de Sesión (SIP).

SIP contiene menos cantidad de códigos que el H.323, lo cual lo hace menos pesado. Debido a que es más pequeño que el HTML, utilizando texto ASCII para configuración, se puede adaptar con mayor facilidad a sistemas VoIP específicos. Tanto H.323 como SIP se consideran "clientes masivos", donde el control se conserva en los dispositivos finales como teléfonos IP. Así mismo, el H.323 tuvo varias ventajas, ya que la mayoría de los productos de primera generación, diseñadas con normas compatibles, soportan el H.323. Sin embargo, muchos proveedores desarrollan productos para soportar SIP, y, en muchos casos, los sistemas VoIP soportan tanto H.323 como SIP.

Los desarrollos actuales de VoIP incluyen los protocolos SIP, H.323, MEGACO/H.248 y

MGCP, los cuales constituyen la más completa suite de protocolos para las comunicaciones de voz y video sobre IP en tiempo real. De esta forma H.323 y SIP se usan para la comunicación entre los diferentes *gateways* (pasarelas) de un país y entre los *gateways* de diferentes países y Megaco y MGCP se usan para la comunicación entre los *gateways* y los *gatekeepers* o media gateway controlador; en la figura 2.2 se puede observar cómo interactúan estos protocolos.

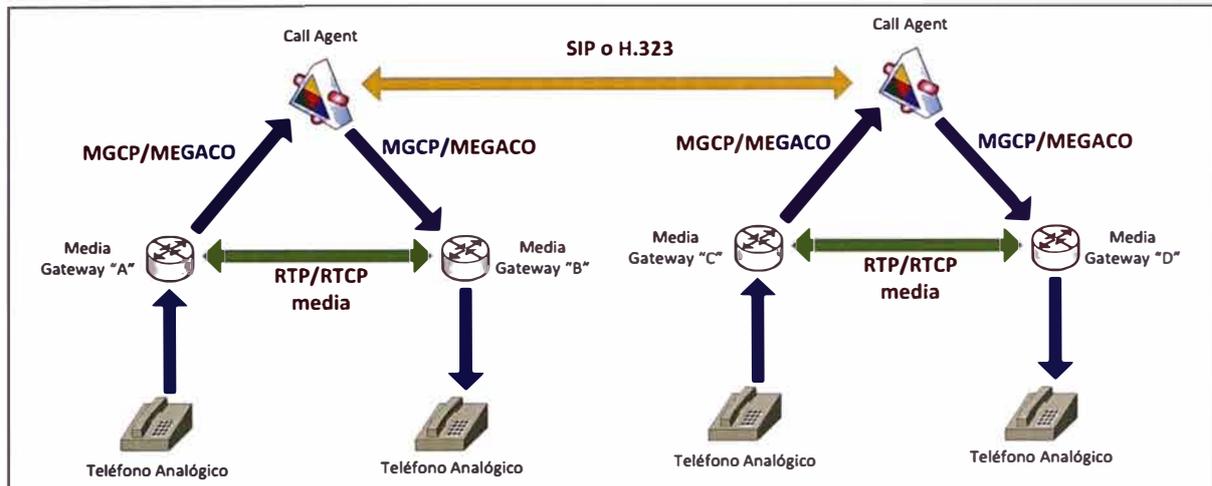


Figura 2.2 Protocolos SIP, H.323, MEGACO y MGCP
(Fuente: IP Telephony cookbook)

Todos los desarrollos de VoIP aseguran el nivel más alto de interoperabilidad y la máxima flexibilidad para todas las adaptaciones necesarias.

Los codificadores son usados para una utilización eficiente del ancho de banda. Diferentes técnicas de codificación para telefonía y voz paquetizada son normalizados por la ITU-T en sus recomendaciones de la serie G: G.723.1, G726, G729 etc.

Los esquemas de compresión de los codificadores-decodificadores (Codecs) son habilitados para ambos extremos de la conexión. Por tanto es lógico deducir que en la actualidad cualquier empresa que quiera trabajar en servicios de VoIP debe adoptar estas normas en todos sus desarrollos. De esta manera se garantizará una perfecta integración con plataformas hardware y software de distintos fabricantes cuyos productos sigan la misma norma.

2.1.3 Definición de VOIP

VoIP o Voz sobre IP, es una red de paquetes de datos para transportar tráfico de voz en tiempo real. Esta consiste de hardware y software y permite a las compañías y a las personas realizar conversaciones telefónicas sobre la red de datos. De acuerdo a un artículo escrito por Techguide.com, "VoIP puede definirse como la habilidad para hacer llamadas telefónicas (tal cual como en la red PSTN) y enviar fax sobre la red de datos basada en IP con una adecuada calidad de servicio (QoS) y a una relación costo/beneficio superior". Esto también es conocido como telefonía por internet. Sin

embargo, este último término es usado en referencia a las llamadas hechas sobre la red de internet pública y la VoIP es frecuentemente usada para referirse a las llamadas hechas en una red privada.

La red de voz tradicional o PSTN, usa técnicas de conmutación de circuitos. Esto significa que una comunicación particular usa un enlace dedicado durante la duración de la llamada. Aunque esta provee una conexión muy confiable para la transmisión de voz, hace un uso muy ineficiente del ancho de banda. Por otro lado, la red de datos generalmente usa conmutación de paquetes. Aquí se usa Conmutación de celdas estadísticas (STDM) con la finalidad de proveer un ancho de banda dinámico a una particular cadena de datos, basada en sus requerimientos y en los requerimientos y demandas de otros datos de la red. Esta provee un uso más eficiente de ancho de banda pero puede crear problemas para el tráfico de voz, el cual es sensible al retardo, debido a que cada paquete es enrutado individualmente a través de la red; esta conmutación de paquetes hace a la red menos eficiente en el tráfico de voz y presenta mayores retos a la calidad de la transmisión de voz. Esto incluye: pérdida de paquetes, retardo (eco), *Jitter* (variación en la velocidad de transmisión de paquetes de datos) y la entrega de paquetes poco confiable y fuera de orden debido a la naturaleza no orientada a conexión de la red de paquetes.

2.1.4 Funcionamiento de VOIP.

Para proveer un servicio de voz con una razonable calidad, existen técnicas que tratan con la congestión de la red y el retardo para hacer un mejor uso del ancho de banda. Este esquema de ahorro de ancho de banda incluye priorización, fragmentación, almacenamiento temporal (buffer) del *jitter*, compresión de voz, supresión de silencio y cancelación de eco. Es aquí donde protocolos, como H.323 juegan un papel importante, como norma para el control de la calidad en la transmisión de la voz en la red de datos.

Las técnicas de priorización están relacionadas con la calidad de servicios (QoS), como una forma de garantizar el rendimiento para cierto tráfico en la red. Este asegura el tráfico de voz sobre una red de datos a través de una alta prioridad. Esta priorización puede estar basada en una localidad, protocolo o tipo de aplicación. Los protocolos usados para asegurar esta QoS son RTP (*Real Time Protocol*) y RSVP (*Resource Reservation Protocol*).

La fragmentación, divide paquetes en fragmentos más pequeños de tal manera que su prioridad pueda ser asegurada. Esto ayuda a reducir el retardo en la entrega de la voz. Sin embargo, en las redes basadas en IP, esto puede crear encabezado adicional lo que incrementa el tamaño total del encabezado IP (20 bytes). Así aunque necesaria, la fragmentación sola no puede asegurar la entrega confiable de las aplicaciones de voz en tiempo real.

Por lo antes mencionado se hace necesaria la compresión. Para lo cual existen varias normas de codificación/decodificación. Por ejemplo la norma ITU G.723, hace posible un ancho de banda de 3.1 kbps en canales de 5.3 y 6.3 kbps, el mismo ha sido adoptado para su uso con VoIP.

En las redes basadas en IP, los paquetes que pertenecen a la misma transmisión (tanto voz como datos) no siempre llegan con la misma cantidad de retardo. Por ejemplo, paquetes del 1 al 5 de una determinada cadena de datos, pueden llegar todos con una cantidad de retardo consistente entre cada paquete, pero el retardo entre el paquete 5 y el 6 puede ser el doble de largo. Esta variación en retardo se conoce como "*jitter*". Como resultado las transmisiones de voz sonarán poco naturales. Cuando el próximo paquete en una cadena de voz no llega a tiempo, el paquete previo es retransmitido. Sin embargo esto puede crear conversaciones que carecen de una calidad natural. Con la finalidad de manejar esta variabilidad de retardo, se establece un almacenamiento temporal del *jitter*. Esto permite reunir los paquetes en un buffer y mantenerlos allí el tiempo suficiente para que lleguen los paquetes atrasados, luego todos ellos pueden ser entregados en la secuencia correcta y en el flujo natural de la voz. Esto proveerá el balance necesario entre el retardo del paquete y el retardo total, permitiendo las transmisiones de la voz con calidad.

En las conversaciones telefónicas, generalmente solo se utiliza el 50% del ancho de banda en ambas direcciones en un determinado tiempo. Esto sucede porque una persona escucha mientras la otra habla. En una conversación hay pausas naturales, pausas para respirar y pausas entre palabras, por lo que el ancho de banda total requerido para una conversación se reduce a un 10%. Esto significa que hay entre un 50% y 60% de ancho de banda disponible que no está siendo utilizado. Las técnicas de supresión de silencio toman ventaja de esto, detectando y suprimiendo los silencios de la transmisión. Esto resulta en un ahorro de ancho de banda el cual queda disponible para otras transmisiones. Sin embargo, como estos silencios son necesarios para el sonido natural de la conversación, el dispositivo receptor puede interpretar la falta de paquetes y reinsertar el punto de silencio en la salida.

Cuando el total de los retardos de extremo a extremo de una transmisión de voz es mayor de 150 milisegundos, el eco se convierte en un problema que puede desmejorar la calidad de la conversación. El dispositivo de cancelación de eco resuelve este problema ejecutando cancelación de eco en las señales.

Las Recomendaciones ITU G.165 o G.168 proveen las normas y requerimientos para cancelación de eco.

Cuando se trata la transmisión de los datos en una red IP, TCP (Protocolo de Control de

Transmisión) se encarga de los paquetes que se pierden debido a la congestión o por falla de enlaces, por aceptación del emisor y petición de retransmisión de los paquetes perdidos. Aunque este método trabaja bien para datos, no es eficiente para información sensible al tiempo como la voz. Con la finalidad de asegurar la calidad de la voz en la conversación, no es aceptable una cantidad de paquetes perdidos mayor de un 10% (*Techguide*). Para un 10% de paquetes perdidos, la interpolación (sonido pregrabado del último paquete) puede ayudar a mantener un flujo continuo de voz con un mínimo de pérdida de la calidad.

2.1.5 Características de la Telefonía IP

La convergencia de la telefonía y de la red de datos es una de las tendencias tecnológicas más importantes de esta década. Esta unión potencial comienza a ser de gran importancia, pudiendo producir ahorros y mejores desarrollos en las redes de las compañías de comunicaciones. Lo relevante en estos momentos es el de ofrecer al mercado IP, productos y soluciones con el fin de mejorar la efectividad y productividad en las compañías de comunicaciones, haciendo buen uso de la arquitectura de red.

La integración de las infraestructuras telefónica y de datos simplifica la administración de los recursos de red y facilita la capacidad de expansión. La ventaja real de la fusión de la telefonía y los datos es la potencialidad de soportar y ofrecer nuevas aplicaciones a los usuarios. El impulso tecnológico que hará posible la integración de las redes de voz y datos, es la evolución y la difusión de las redes IP.

2.1.6 Arquitectura

Las llamadas de VoIP requieren al menos dos *gateways* (pasarelas) de VoIP. Típicamente, un proveedor de servicios debería instalar *gateways* (o interactuar con otros proveedores de servicios y acceder a sus *gateways*) en todos los países o regiones hacia los cuales se realizan o se reciben llamadas. El resultado de la red de VoIP se compone de *gateways*, el acceso de la PSTN a cada *gateway* y la red IP que enlaza los *gateways*. En la red telefónica IP, la información de señalización es intercambiada entre los siguientes elementos funcionales. Estos mismos se tomarán en cuenta para las configuraciones de red que se plantearán más adelante.

- **Media Gateway:** La tecnología de VoIP permite que las llamadas originadas y terminadas en la PSTN, sean transportadas sobre la red IP, es decir, éste traduce TDM a paquetes. El *gateway* de VoIP sirve de puente entre la red PSTN y la red IP para ambos lados de origen y termino de la llamada. Para realizar una llamada, el abonado llamante accederá el *gateway* más cercano o por conexión directa o realizando una llamada sobre la red PSTN e ingresando el número telefónico de destino.

La tecnología de VoIP traduce el número telefónico de destino en la dirección de la red de datos ("dirección IP") asociada con el correspondiente *gateway* terminal más cercano al número de destino. Usando el protocolo apropiado y la transmisión de paquetes sobre la red IP, el *gateway* terminal iniciará una llamada al número telefónico de destino sobre la red PSTN para completar el establecimiento de la comunicación en ambos sentidos con los extremos finales (punto a punto). A pesar de la conexión adicional requerida, el tiempo total del establecimiento de la llamada no es significativamente más largo que con una llamada soportada por la PSTN.

Los *gateways* pueden emplear un protocolo común, por ejemplo, el SIP, H.323 o MGCP o un protocolo propietario, para soportar la norma de señalización telefónica. Los *gateways* emulan las funciones de la PSTN en respuesta a los estados de cuelgue y descuelgue, recibiendo o generando dígitos DTMF y recibiendo o generando tonos de llamadas en progreso. Las señales identificadas son interpretadas y mapeadas para la transmisión del mensaje apropiado hacia el *gateway* con la finalidad de soportar el establecimiento de la llamada, mantenimiento, facturación y finalización de la llamada.

- **Media Gateway Controlador o Gatekeeper:** Un *gatekeeper* (GK) maneja los registros y la gestión de los recursos de los media *gateways* de manera que no se produzcan situaciones de saturación en la red. Un *gatekeeper* intercambia mensajes ISUP con las centrales telefónicas vía un *gateway* de señalización. De esta forma el GK traduce direcciones telefónicas a direcciones IP.

La interpretación del número telefónico de destino en la dirección IP del media *gateway* terminal indicado es una función primordial del *gatekeeper*. La tabla de enrutamiento mantenida por el *gatekeeper* decide cual media *gateway* corresponde al número telefónico de destino con la finalidad de completar la llamada.

La funcionalidad del *gatekeeper* puede ser distribuida entre todos los media *gateways* de la red de VoIP o puede ser centralizada en una o varias localidades. Cuando las funciones del *gatekeeper* están implantadas en cada media *gateway*, todos los *gateways* de toda la red de VoIP actúan independientemente para coordinar sus acciones. Cuando un *gatekeeper* es centralizado, todos los media *gateways* de la red coordinan sus acciones con respecto al *gatekeeper* centralizado en lugar de que actúen independientemente.

- **Gateway de Señalización o Signaling Gateway:** El *gateway* de señalización provee una traducción transparente de la señalización entre la conmutación de circuitos y la red IP. Un *gateway* de señalización puede señalizar en SS7 (señalización N° 7) o traducir y transmitir mensajes sobre una red IP a un media *gateway* controlador o a

otro *gateway* de señalización. Debido a su rol crítico en la integración de la red de voz, los *gateway* de señalización son normalmente desarrollados en grupos de dos o más para asegurar alta disponibilidad.

Las funcionalidades de *media gateway*, *gateway* de señalización y/o *media gatekeeper* pueden estar separadas en dispositivos diferentes o integrados en una sola unidad. La figura 2.3 muestra al *media gateway* como pasarela entre la red PSTN y la red IP.

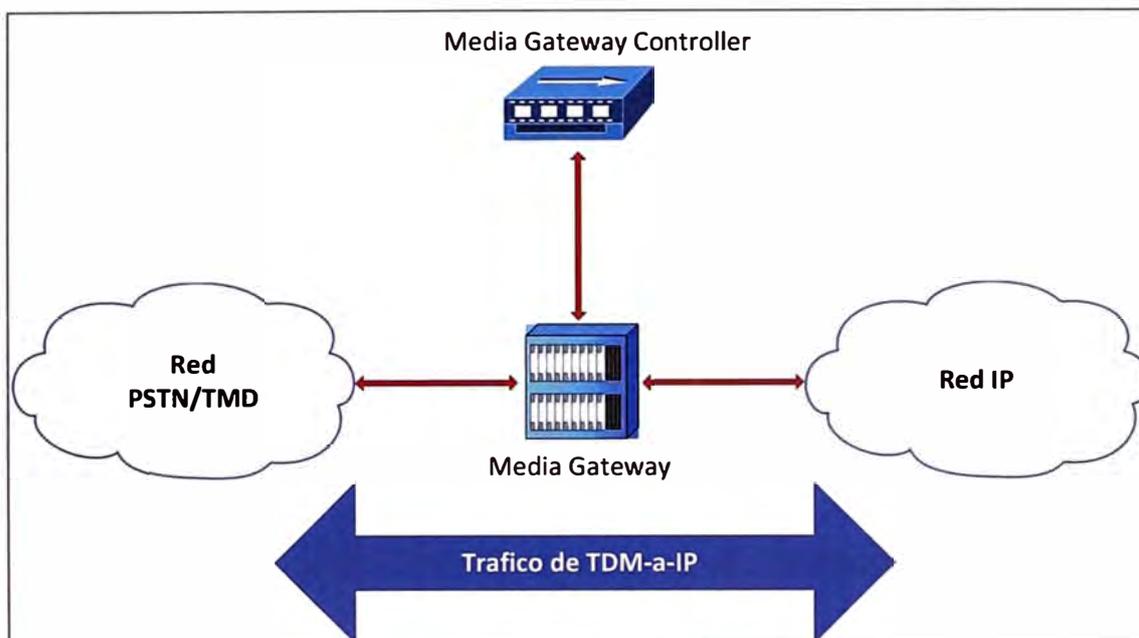


Figura 2.3 Arquitectura de Telefonía IP
(Fuente: IP Telephony cookbook)

2.1.7 Beneficios

Muchas compañías están viendo el valor de implementar VoIP en su red de datos por muchas razones. Esto incluye:

- Reducción de costos – bajo costo en llamadas telefónicas
- Convergencia en la red de datos/voz – unificación
- Simplificación y consolidación – gestión centralizada

Como la red de datos continúa creciendo, la implementación de VoIP es una opción muy atractiva que puede permitir reducir costos y proveer una mayor flexibilidad. Adicionalmente, para reemplazar las redes de voz corporativas, se puede utilizar una red de VoIP para conectar las sucursales a través de enlaces WAN existentes. Esto da a las compañías una alternativa con respecto a la red PSTN la cual puede continuar creciendo y adaptarse a las necesidades.

2.1.8 Protocolos de comunicación

Cuando un abonado realiza una llamada, primero marca un número telefónico o hace click sobre un nombre, la señalización determina el estatus del abonado llamado (si está disponible u ocupado) y establece la llamada. Luego cuando la conversación empieza,

las señales analógicas producidas por el micrófono son codificadas en un formato digital adecuado para su transmisión a través de la red IP. La misma red IP debe asegurar entonces que la conversación en tiempo real sea transportada a través de los medios disponibles en una forma que produzca una calidad aceptable de la voz.

En VoIP, el procesador de señal digital segmenta la señal de voz en tramas y las almacena en paquetes de voz. Estos paquetes de voz son transportados usando la red IP en conformidad con una de las especificaciones para transmitir multimedia (voz, video, fax y datos) a través de la red, entre ellas se encuentran: H.323 (ITU), MGCP (IETF), MEGACO (IETF), SIP (IETF).

a) H.323

El H.323 es una familia de normas definidos por el ITU para las comunicaciones multimedia sobre redes LAN. Está definido específicamente para tecnologías LAN que no garantizan una calidad de servicio (QoS). Algunos ejemplos son TCP/IP e IPX sobre Ethernet, *Fast Ethernet* o *Token Ring*. La tecnología de red más común en la que se está implementando H.323 es IP (*Internet Protocol*).

Esta norma define un amplio conjunto de características y funciones. Algunas son necesarias y otras opcionales. El H.323 define los siguientes componentes:

- Terminal
- *Media Gateway*
- *Gatekeeper*
- *Gateway* de señalización

El H.323 en perspectiva histórica: En Enero de 1996, un grupo de fabricantes de soluciones de redes y de ordenadores propuso la creación de una nueva norma ITU-T para incorporar videoconferencia en la LAN. Inicialmente, las investigaciones se centraron en las redes de área local, pues éstas son más fáciles de controlar. Sin embargo, con la expansión de Internet, el grupo tuvo que contemplar todas las redes IP dentro de una única recomendación, lo cual marcó el inicio del H.323.

El H323 es una norma que especifica los componentes, protocolos y procedimientos que proveen unos servicios de comunicación multimedia para las comunicaciones de audio en tiempo real, vídeo y datos en redes ya sean LANs, WANs, MANs a través de IP.

Soporta así mismo Internet e intranets. En Mayo de 1997, el Grupo 15 del ITU redefinió el H.323 como la recomendación para "los sistemas multimedia de comunicaciones en aquellas situaciones en las que el medio de transporte sea una red de conmutación de paquetes que no pueda proporcionar una calidad de servicio garantizada.

Normas del Protocolos H.323: El H.323 comprende a su vez una serie de normas y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

Direccionamiento, Señalización, Compresión de Voz, Transmisión de Voz, Control de la Transmisión.

1. Direccionamiento:

- RAS (*Registration, Admission 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.

2. Señalización:

- Q.931 Señalización inicial de llamada.
- H.225 Control de llamada: señalización, registro y admisión, y paquetización / sincronización del *stream* (flujo) de voz.
- H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para *streams* de voz.

3. Compresión de voz:

- Requerido: G.711
- Opcionales: G.728, G.729 y G.723

4. Transmisión de voz:

- UDP. 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. UDP provee a los usuarios acceso a los servicios IP. Los paquetes UDP son entregados como paquetes IP no orientados a conexión, los cuales pueden ser descartados antes de alcanzar su objetivo.
- 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*). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

b) SIP

El protocolo "*Session Initiation Protocol*" (SIP) es una norma emergente para establecer, enrutar y modificar sesiones de comunicaciones a través de redes *Internet Protocol* (IP). Utiliza el modelo de Internet y lo convierte al mundo de las telecomunicaciones, utilizando protocolos Internet existentes tales como HTTP (*Hypertext Transfer Protocol*) y SMTP (*Simple Mail Transfer Protocol*). También usa una estructura de dirección URL (*uniform resource locator*). Usa estas direcciones de tipo correo electrónico para identificar a los usuarios en lugar de los dispositivos que los utilizan. De esta forma SIP no depende del

dispositivo y no hace distinción alguna entre voz y datos, teléfono u ordenador. Como se describe a continuación, SIP es usado más para el manejo de servicios, mientras que H.323 se usa prácticamente para la conversión del número telefónico en paquetes IP.

Ejemplos de Aplicaciones Diseñadas para SIP:

- *Call Back* (Devolución de llamada). Mediante SIP, los usuarios pueden indicar su presencia en una red. Puesto que SIP usa una dirección independiente de la ubicación, sería posible encontrar un individuo en la red, independientemente de si está en un PC o en un teléfono móvil y avisarle cuando se dé la oportunidad o pedirle que devuelva la llamada
- *Conference on Demand* (Conferencia por demanda). Usando la información de presencia, puede detectarse y contactarse instantáneamente con un individuo e introducirlo en conferencias multimodo, donde los participantes pueden asistir a una conferencia usando distintos dispositivos/medios que están funcionando en redes diferentes.
- Servicios de traducción en los que los correos electrónicos o de voz se traducen automáticamente al idioma preferente predefinido por un usuario, en base a un perfil controlado dinámicamente.
- *Call Re-Routing* (Re-enrutamiento automático de llamadas).

Ventajas: Para la empresa, SIP creará una infraestructura tecnológica capaz de abarcar comunicaciones unificadas basadas en IP. Esta infraestructura incorporará soluciones de localización y movilidad.

Para el proveedor de servicios, SIP proporciona un conjunto de herramientas que permite ampliar el alcance y ámbito de sus ofertas. El proveedor de servicios que utilice SIP se beneficiará de servicios de comunicaciones más flexibles para aumentar la productividad personal, abrir muchas posibilidades de integración de soluciones de comunicación con aplicaciones comerciales y permitir que el cliente indique por sí mismo sus preferencias. Cuando los clientes tengan puntos finales habilitados para SIP, los proveedores de servicios podrán ofrecer a los clientes el variado conjunto de aplicaciones que actualmente existen en las redes del proveedor de servicios.

c) Megaco

Este protocolo se define en la Recomendación H.248 de la ITU-T. El protocolo H.248 o Megaco permite la conmutación de llamadas de voz, fax y multimedia entre la red PSTN y las redes IP de siguiente generación. El protocolo Megaco, que tiene su origen en el protocolo MGCP (protocolo de control de puerta de enlace al medio), proporciona un control centralizado de las comunicaciones y servicios multimedia a través de redes basadas en IP. Megaco permite una mayor escalabilidad que H.323, y da respuesta a las

necesidades técnicas y a las funciones de conferencia multimedia que se pasaron por alto en el protocolo MGCP.

Funcionalmente, Megaco es un protocolo de señalización utilizado entre los elementos de una arquitectura distribuida que incluye media *gateway* y controladores de media *gateway* (conocidos a menudo como *softswitches*, *gatekeeper* o *call server*).

d) MGCP

El MGCP fue concebido por un grupo conocido actualmente como el Consorcio Internacional *Softswitch*. Este grupo comenzó a trabajar en principio con las empresas Level 3 y Telcordia. A mediados de 1998, Level 3 creó un consejo de consultoría técnica, que publicó un protocolo llamado IDPC (Protocolo de Internet para el Control de Dispositivos). Telcordia creó el SGCP (Protocolo Sencillo de Control de Compuerta). Los Protocolos fueron unificados surgiendo así el MGCP.

El Protocolo de Control de Media *Gateway* (MGCP) es usado para controlar los *gateways* de telefonía desde los elementos de control de llamadas externos llamados Media *Gateways Controllers* (MGC) o *Gatekeepers*. Un *gateway* de telefonía es un elemento de red que provee conversión entre las señales de audio transportadas sobre los circuitos telefónicos y los paquetes de datos transportados sobre internet o sobre otra red de paquetes.

MGCP asume una arquitectura de control de llamada, donde el control de la llamada está fuera de los *gateways* y manejada por un elemento de control de llamada externo. El MGCP asume que estos elementos de control de llamadas o MGC, se sincronizarán entre sí para enviar comandos coherentemente a los *gateways* que están bajo su control. El MGCP es, en esencia, un protocolo maestro/esclavo, donde se espera que los *gateways* ejecuten comandos enviados por el MGC.

2.1.9 Calidad de Servicio (QoS)

Esta función tiene primordial importancia en relación con la QoS experimentada por el usuario final. En esto influyen dos factores fundamentales:

- La calidad de la voz extremo a extremo, determinada por los sucesivos procesos de codificación – decodificación, y las pérdidas de paquetes en la red.
- La demora extremo a extremo, debido a las sucesivos procesos de codificación – decodificación, paquetización y "encolados". Afecta la interactividad en la conversación, y por tanto a la QoS.

Las redes IP son redes del tipo *best-effort* (el mejor esfuerzo) y por tanto no ofrecen garantía de QoS, pero las aplicaciones de telefonía IP si necesitan algún tipo de garantía de QoS en términos de demora, *jitter* y pérdida de paquetes.

La preparación de los medios en los terminales para ser enviados y transferidos por la

red IP involucra varios procesos: digitalización, compresión y empaquetado en el extremo emisor, y los procesos inversos en el extremo receptor. Todo esto se lleva a cabo mediante un complejo procesamiento que sigue determinado algoritmo, lo cual a su vez se desarrolla en cierto intervalo de tiempo, esto es, implica demora de procesamiento y demora de empaquetado:

- Demora de procesamiento: demora producida por la ejecución del algoritmo de codificación, que entrega una corriente de bytes listos para ser empaquetados.
- Demora de paquetización: es el tiempo que se requiere para formar un paquete de voz a partir de los bytes codificados. Debe señalarse que el resultado de esta codificación–paquetización incide directamente en la QoS, y también la forma en que se lleve a cabo. Así, cuando se reduce la velocidad de codificación los requerimientos de ancho de banda también se reducen, lo que posibilita de cara a la red poder manejar más conexiones simultáneas, pero se incrementa el retardo y la distorsión de la señales de voz. Lo contrario ocurre al aumentar la velocidad de codificación.

Otro aspecto a considerar es el compromiso entre el retardo de paquetización y la utilización del canal (relación entre bytes de información y bytes de cabecera en cada paquete de voz), es decir, la búsqueda de mayor utilización del canal conduce a mayor demora de paquetización para cierta norma de codificación. Claro está, según la norma de codificación que se utilice será la demora resultante en relación con la utilización del canal, diferencias que se acentúan cuando la utilización del canal está por encima del 50%, con un crecimiento de la demora en forma exponencial en el caso de los *codecs* de baja velocidad como el G.723.1. La demora de paquetización también puede ser reducida mediante multiplexación de varias conexiones de voz en el mismo paquete IP.

A las demoras de procesamiento y empaquetado se suma también la demora que introduce el proceso de *buffering* (almacenamiento temporal de datos) en los terminales, y la demora de "encolado" en la red. Todo esto da una demora extremo a extremo que percibe el usuario final en mayor o menor medida.

Aspectos que afectan la QoS en las redes de VoIP:

- Retardo: Los excesivos retardos punto a punto hacen conversaciones difíciles y poco naturales. Cada componente en el camino de transmisión (emisor, red y receptor) añaden retardo. ITU-TG.114 (tiempo de transmisión en un solo sentido) recomienda 150mseg como el máximo retardo deseado en un sentido para lograr alta calidad de la voz.
- Jitter: Cuantifica el efecto del retardo total en la red ocasionado por los paquetes que llegan al receptor. Los paquetes transmitidos a intervalos iguales desde el *gateway* de

la izquierda llegan al *gateway* de la derecha a intervalos irregulares. El excesivo *jitter* hace que la voz sea entrecortada y con dificultades para entenderse. El *jitter* es calculado basado, en las horas de llegada entre paquete y paquete de los paquetes exitosos.

Para una alta calidad de voz, el promedio de las horas de llegada entre los paquetes en el receptor debería ser casi igual a la diferencia entre los paquetes en el transmisor y la norma de desviación debería ser baja. El *jitter* buffer (el buffer mantiene paquetes entrantes por una determinada cantidad de tiempo) es usado para neutralizar los efectos de las fluctuaciones de la red y crear un fácil flujo de paquetes en la recepción.

- Pérdida de paquetes: Típicamente ocurre en ráfagas o periódicamente debido a una red regularmente congestionada. La pérdida periódica en exceso de 5% a 10% de todos los paquetes de voz transmitidos puede degradar significativamente la calidad de voz. La pérdida ocasional de grupos de paquetes puede también hacer difícil la conversación.
- Errores de secuencia: La congestión en la conmutación de paquetes de la red puede causar paquetes que toman diferentes rutas para alcanzar el mismo destino. Los paquetes pueden llegar fuera de orden resultando una conversación distorsionada.

2.2 Sistemas de Gateways y SBC

Es claro que como muchas tecnologías, la telefonía IP ha mostrado durante las últimas décadas un avance increíble en su evolución como sistema de comunicación. Es cierto como se aprecia en la figura 1.1 los “*gateways*” cumplen una tarea muy importante en la traducción de llamadas desde la PSTN a las redes IP, pero el control, la seguridad, y la calidad de las sesiones realizadas sobre IP punto a punto, no son respaldadas por los “*Gateways*”, lo que se traduce en puntos en contra para los sistemas VoIP. Es así que la idea de un controlador diseñado no sólo para servir de pasarela entre el mundo PSTN y el VoIP, se materializa en los “*Session Border Controller*” (SBC).

Si se desarrolla una comparación conceptual entre ambos métodos. Los SBC son una respuesta evolutiva en el camino hacia la telefonía IP sin tramos de comunicación con telefonía convencional. La mayor ventaja es por supuesto el costo de realizar una llamada netamente IP y una llamada hacia la PSTN, la primera opción tiene un costo cero actualmente, por otra parte la capacidad de realizar llamadas desde cualquier parte con una conexión a Internet, muy atractivo para usuarios que viajan bastante, no necesitan de servicios externos para compatibilizar un usuario VoIP al estar en una red mundial como lo es Internet, con ello mismo la telefonía IP presenta más servicios extras sin cobrar por ellos, por ejemplo; identificación de llamadas, servicio de llamada en espera, servicio de transferencia de llamada. La principal razón de reconocer como superior el sistema VoIP

en todo el tramo de comunicación por sobre la telefonía dual es la modularidad y escalabilidad, ósea, la capacidad de dar cada vez mayor valor agregado al sistema por estar ligado a la red de datos (Internet), y la facilidad de crear, trasladar o eliminar líneas de comunicación telefónica dentro de estas redes.

2.3 Características SIP y beneficios sobre otros protocolos de señalización

SIP, o *Session Initiation Protocol* es un protocolo de control y señalización cuyas mayores ventajas recaen en su simplicidad y consistencia. SIP tiene ciertas características y beneficios que lo resaltan por sobre los otros protocolos de señalización.

2.3.1 Definición de Protocolo SIP

Es un protocolo desarrollado por el grupo de trabajo MMUSIC del IETF con la intención de ser la norma para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual.

Actualmente está definido por la RFC 3261, y se encuentra definido por OSI en la capa de aplicación. En la figura 2.4 se muestra como es la forma de interactuar de SIP en el medio VoIP.

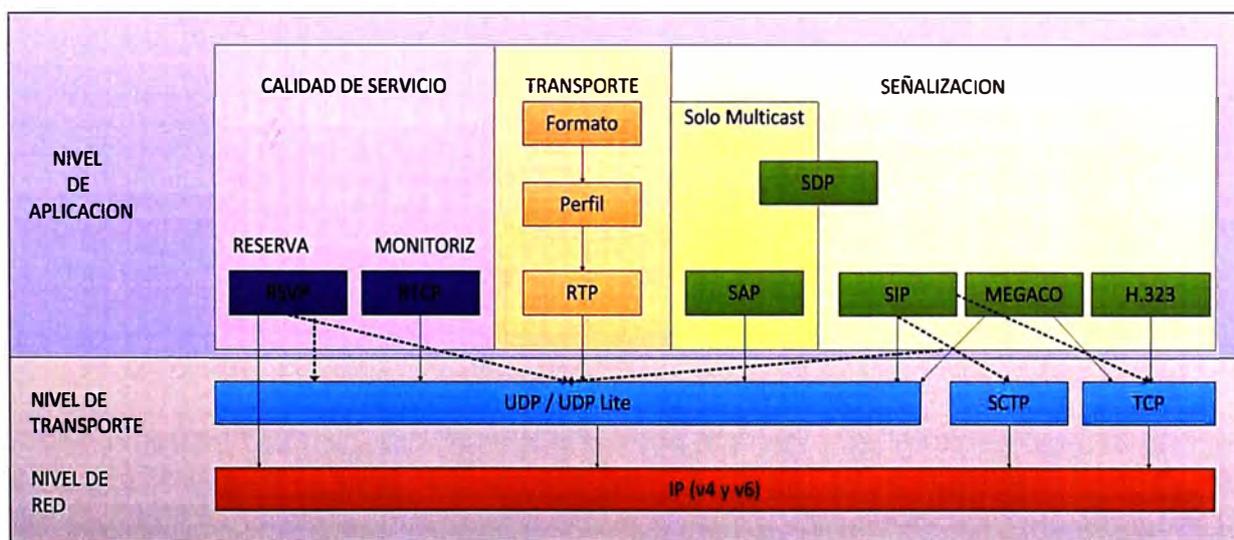


Figura 2.4 Estructura protocolar para sistemas VoIP según modelo OSI
(Fuente: IP Telephony cookbook)

Las características principales del protocolo son:

- Basado en texto.
- Sintaxis similar a HTTP o SMTP.
- Uso de URIs (con esquemas *sip*, *sips* y *tel*).
- Métodos básicos: "INVITE", "ACK", "BYE", "CANCEL", "REGISTER", "REFER", "OPTIONS".
- Los mensajes se agrupan en transacciones y llamadas.
- Generalmente, el cuerpo de los mensajes contiene descripciones de sesiones de

multimedia (SDP).

- Códigos de respuesta similares a los de HTTP (Ejemplo: 200 – OK).
- Localización basada en DNS.
- Cabeceras como método de ampliación.

a) Entidades SIP

En la configuración más simple para establecer una sesión SIP se utilizan dos agentes de usuario (“*User Agents*” o UA) conectados uno a otro. Los elementos básicos de un sistema SIP son los UA y los servidores de Red. 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.

- *User Agent*: El agente de usuario se conforma por el UAS (“*User Agent Server*”) y UAC (“*User Agent Client*”), estas son las entidades finales que usa SIP para contactarse de extremo a extremo entre dos terminales físicas en una misma red o diferentes y definir las características de la sesión. Se entiende por terminal, por ejemplo, un “*softphone*”, teléfonos celulares (SIP), “*Hard-IPphones*”, y similares.

El UAC es la parte del UA que 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. Esto se ejemplifica en la figura 2.7.

- SIP proxy server: IP Proxy Server es aquel que realiza una petición a nombre de un UA hacia otro Proxy u otro UA. La tarea más importante de un Proxy Server es encaminar las invitaciones de sesión para llevarlas hasta el UA llamado, se ejemplifica en la figura 2.10. Una invitación de sesión atravesará comúnmente un conjunto de “*Proxies*” hasta encontrar a aquel que conozca la localización exacta del UA buscado. Existen dos tipos de SIP Proxy Servers: “*stateful*” y “*stateless*”.
 - “*Stateful Proxy*”: Este tipo de servidor crea un estado de petición y lo mantiene hasta que la transacción finalice.
 - “*Stateless Proxy*”: Sólo reenvía los mensajes SIP.

Los “*proxies stateful*” pueden desempeñar tareas mucho más complejas; por ejemplo hacer retransmisiones como lo sería el caso del servicio “*sígueme*” o re-emitir un mismo mensaje SIP hacia dos “*proxies*” diferentes con el fin de localizar a un usuario en específico.

- Registrar Server: Cuando un usuario se conecta a la Red (ejecuta su “*Softphone*” en su PC o enciende su “*IP-phone*”), este envía un mensaje “*Register*” hacia su “*Proxy*” con el fin de que éste conozca su ubicación.

La labor de un registrar “*Proxy*” consiste en atender estos mensajes, autenticar y validar la cuenta contra una base de datos interna o externa y registrar la localización

actual del usuario, se ejemplifica en la figura 2.9. Un “Registrar Server” es comúnmente sólo una entidad lógica y la mayoría de las veces se localiza junto con el “Proxy SIP Server”.

- **Redirect Server:** Entidad que escucha peticiones y regresa (no reenvía mensajes) respuestas que contienen la localización actual de un usuario en particular. Este servidor escucha las peticiones y realiza la búsqueda en la Base de Datos creada por el “Registrar Server”. Este tipo de Server contesta con mensajes SIP de clase 3XX, se muestra un ejemplo de la estructura en la figura 2.5.

El usuario o “Proxy” que realizó la petición original extrae la información de la respuesta y envía otra petición directamente al resultado de la búsqueda.

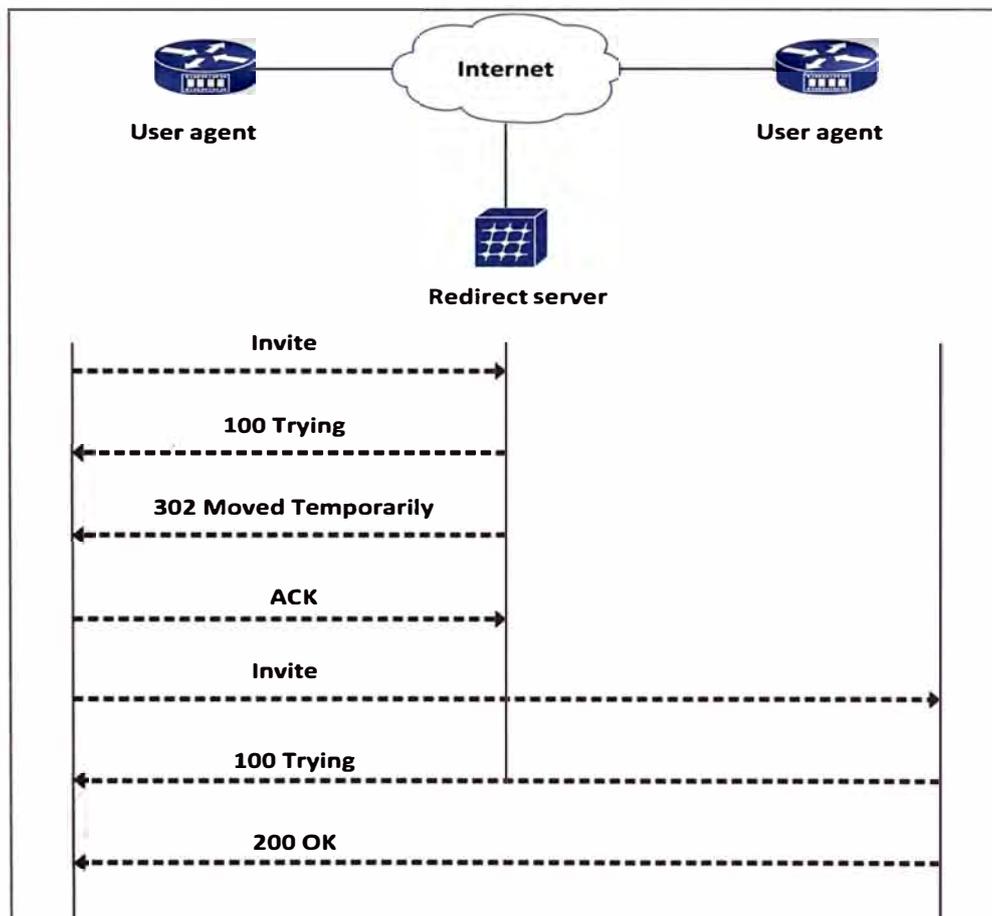


Figura 2.5 Estructura de protocolo de “Redirect Server”
(Fuente: IP Telephony cookbook)

b) Mensajes SIP

SIP utiliza una serie de mensajes para señalar las sesiones. El mensaje se conforma de una línea inicial, el encabezado del mensaje y el cuerpo del mensaje, se muestra en la figura 2.6 el formato de mensaje SIP.

La línea inicial contiene la versión del protocolo SIP, el método y direcciones involucradas en la sesión para las peticiones.

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 y otros tipos de información adicional. Todos ellos son definidos a continuación.

- “VIA”: Se usa para registrar (grabar) 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.
- “From”: Es la dirección del origen de la llamada.



Figura 2.6 Estructura de trama mensaje SIP
(Fuente: IP Telephony cookbook)

- “To”: Es la dirección del destino de la llamada.
- “ID-Call”: Identifica mensajes que pertenecen a la misma llamada. Así es por ejemplo un analizador de red que puede reconocer todos los mensajes correspondientes a una llamada determinada.
- “Cseq”: Se inicia en un número aleatorio e identifica en forma secuencial a cada petición.
- “Contact”: Contiene la IP y puerto en dónde el emisor de la petición espera respuesta a su mensaje.

El cuerpo del mensaje o carga útil: Lleva información comúnmente SDP o ISUP en caso de una troncal hacia la PSTN.

Existen 2 tipos de mensajes SIP, los métodos o peticiones, y las respuestas. Los métodos 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.

i) Métodos SIP

Existen varios métodos en la señalización SIP, dependiendo del estado la llamada. Los métodos más importantes y generalmente en uso (todos definidos en la RFC 3261) son definidos a continuación.

El método “INVITE” es usado con el fin de establecer una sesión entre UAs. INVITE corresponde al mensaje ISUP IAM o al mensaje Q.931 SETUP y contiene las

informaciones sobre el que genera la llamada y el destinatario así como sobre el tipo de flujos que serán intercambiados (voz, video, entre otros).

Cuando un UA que emitió el método SIP INVITE recibe una respuesta final a la invitación (ejemplo: 200 OK), el confirma la recepción de esta respuesta por medio de un método "ACK". Una respuesta del tipo ocupado o con respuesta es considerada como final, mientras una respuesta tipo "*ringing*" significa que el destinatario ha sido avisado es una respuesta provisoria.

El método "BYE" permite la liberación de una sesión anteriormente establecida. Corresponde al mensaje de liberación de los protocolos ISUP y Q.931. Un mensaje BYE puede ser emitido por el que genera la llamada o el que la recibe.

El método "REGISTER" es usado por una UA con el fin de indicar al "Registrar" la correspondencia entre su Dirección SIP y su dirección de contacto (ejemplo: dirección IP).

El método "CANCEL" es utilizado para pedir el abandono de la llamada en curso pero no tiene ningún efecto sobre una llamada ya aceptada. De hecho, solo el método "BYE" puede terminar una llamada establecida.

El método "OPTIONS" es utilizado para interrogar las capacidades y el estado de un "*User Agent*" o de un servidor. La respuesta contiene sus capacidades (ejemplo: tipo de "media" siendo soportado, idioma soportado) o el hecho de que el UA sea indisponible.

ii) Respuestas SIP

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 (ejemplo 200 = Ok) y una frase que explica, en términos más humanos, la razón de la respuesta. Los códigos de respuesta son enteros entre 100 y 699. El primer dígito indica la clase.

Existen 6 clases de respuestas:

- 1XX: Provisionales (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. Un ejemplo es el código 180 = "*ringing*" o 100 = "*trying*".
- 2XX: Son respuesta finales positivas. La petición fue recibida y procesada exitosamente. Por ejemplo 200 = "Ok" significa que el extremo llamado aceptó la invitación a la sesión.
- 3XX: Son usados para re-direccionar llamadas. Dan información acerca de la nueva localización de un usuario o sobre un Proxy alternativo que pueda resolver satisfactoriamente alguna petición. El emisor del mensaje de petición debe reenviar su petición a otro lado para que su petición sea atendida.
- 4XX: Son respuestas finales negativas. Falla del lado del emisor, mala sintaxis del

mensaje, entre otros.

- 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".

2.3.2 Funcionamiento de protocolo SIP

SIP es basado en arquitectura cliente/servidor similar al HTTP, con el que comparte muchos códigos de estado y sigue una estructura de petición-respuesta, estas peticiones son generadas por un cliente y enviadas a un servidor, que las procesa y devuelve la respuesta al cliente.

El par petición-respuesta recibe el nombre de transacción. Al igual que el protocolo HTTP, SIP proporciona un conjunto de solicitudes y respuestas basadas en códigos.

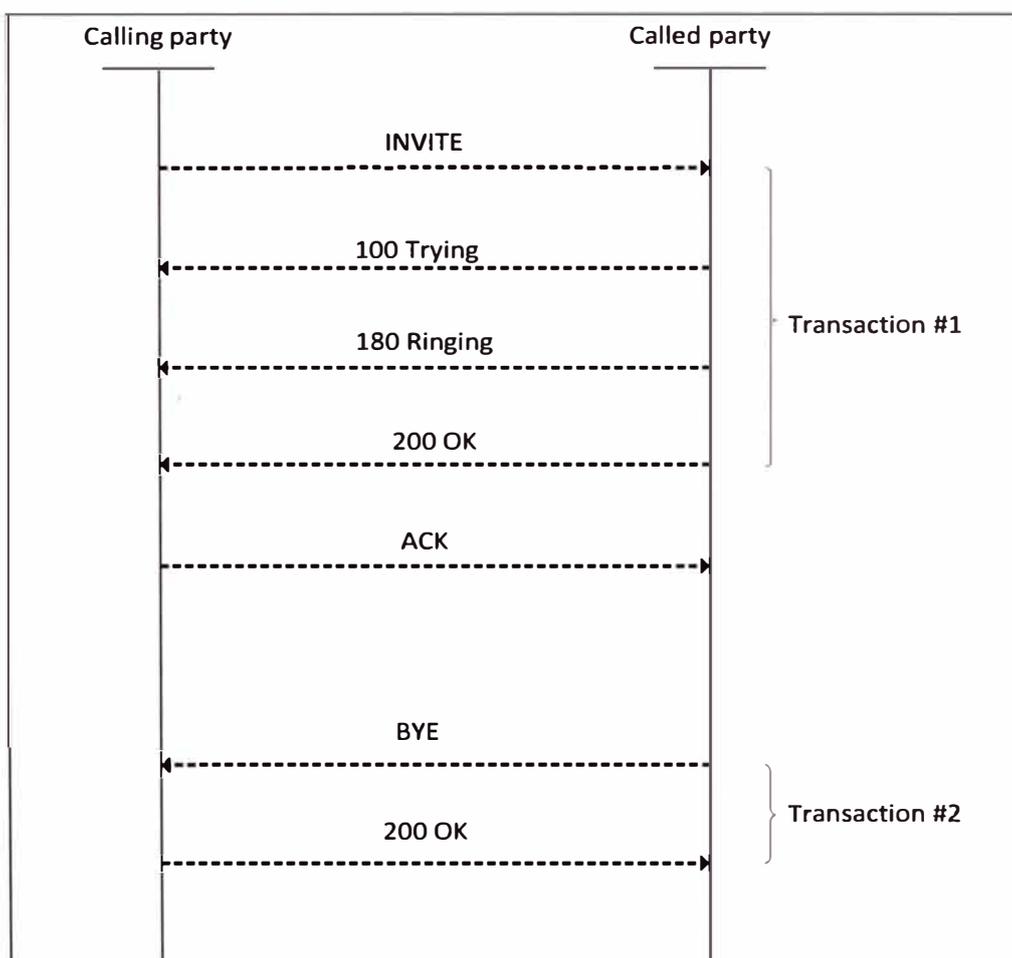


Figura 2.7 Ejemplo de transacción
(Fuente: IP Telephony cookbook)

A continuación se detallan los procesos de funcionamiento SIP.

a) Transacciones SIP:

Una transacción SIP es una secuencia de mensajes entre dos elementos de Red. Una transacción corresponde a una petición y todas las respuestas a esa petición.

De esta forma una transacción incluirá cero o más respuestas provisionales y una o más

respuestas finales (en el caso de un mensaje INVITE, recordar 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". Lo hacen por medio del registro de cada transacción a través de un identificador contenido en el encabezado VIA.

En la figura 2.7 se muestra un ejemplo los mensajes que pertenecen a una misma transacción dentro de una conversación SIP.

b) Diálogos SIP

Un diálogo SIP es una conversación "peer-to-peer" entre dos UA, esto se aprecia en la figura 2.8. Los diálogos son identificados usando los campos "Call-ID", "From" y "To". Los mensajes con estos campos iguales pertenecerán al mismo diálogo. El campo "Cseq", del que se habla anteriormente, es utilizado para ordenar los mensajes en un diálogo. De hecho el Cseq representa el número de transacción. De forma breve se puede decir que un diálogo es una secuencia de transacciones.

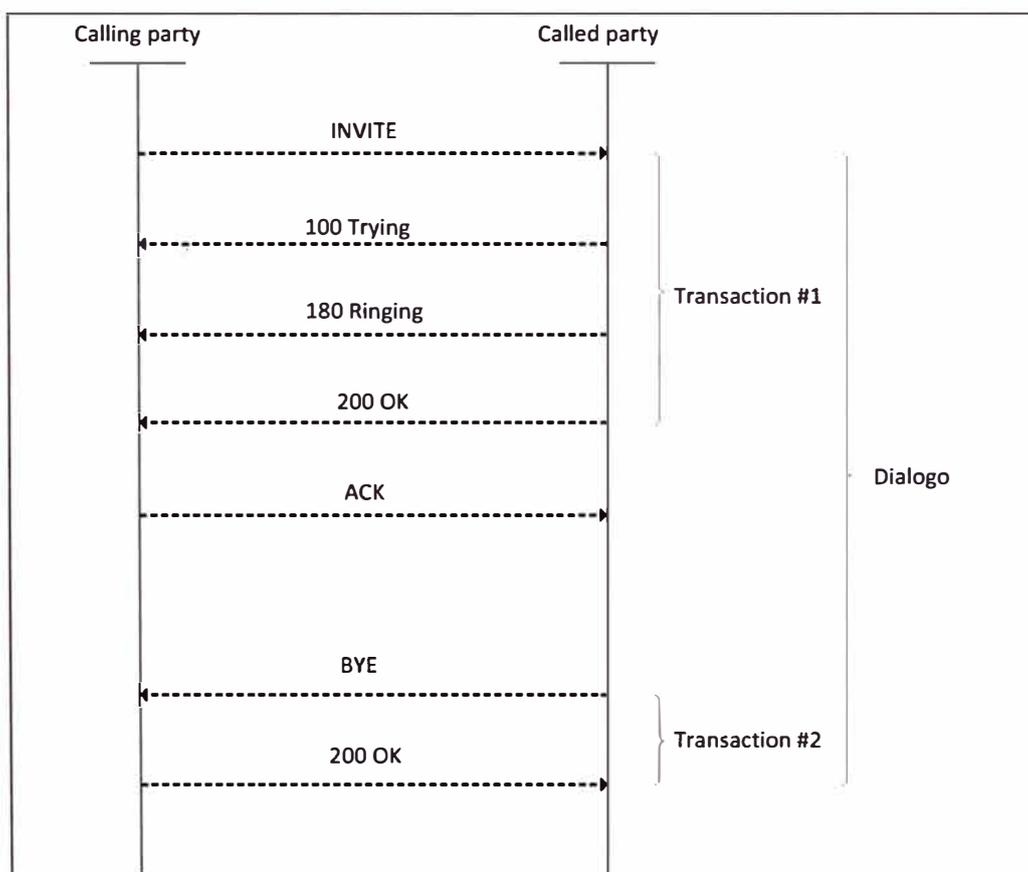


Figura 2.8 Ejemplo de diálogo
(Fuente: IP Telephony cookbook)

c) Esquema de señalización de una llamada SIP

Una vez analizados los conceptos de señalización, se procede a explicar los procesos típicos de diálogos SIP, estos son: registro, invitación a sesión, término de sesión, y registro de ruta.

- Registro: Para que un usuario pueda ser llamado por otro, este debe registrarse primero ante el "proxy", así este método se muestra en la figura 2.9.
El registro consiste en el envío de un mensaje "REGISTER" seguido de su correspondiente respuesta "200 OK". En esta primera instancia si el usuario no envía credenciales válidas, recibirá por respuesta un mensaje 407 que indica que son requeridas las credenciales de registro, con lo cual tendrá que reenviar el mensaje de Registro pero con credenciales válidas.
- Invitación a sesión: Una invitación inicia con el mensaje "INVITE" dirigido comúnmente al "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. Una respuesta "200 OK" es generada en cuanto el usuario llamado descuelga el auricular. Para ejemplificar se muestra un diagrama en la figura 2.10, este explica de forma gráfica el proceso.
- Término de sesión: Una sesión es finalizada cuando uno de los usuarios envía el mensaje "BYE" al otro extremo. El otro usuario confirma el final de la conversación enviando por respuesta un mensaje "200 OK", esto se ejemplifica en la figura 2.11.
La transacción para finalizar la sesión se realiza de un extremo a otro sin pasar por el "Proxy" a menos que en el mismo se haya establecido un proceso de Registro de ruta.
- Registro de la 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 existe un NAT. El "Proxy" o los "Proxies" logran esto por medio de la inserción del campo "RECORD ROUTE" en los encabezados de los mensajes SIP.
El diagrama que muestra la figura 2.12, explica de forma secuencial el proceso.

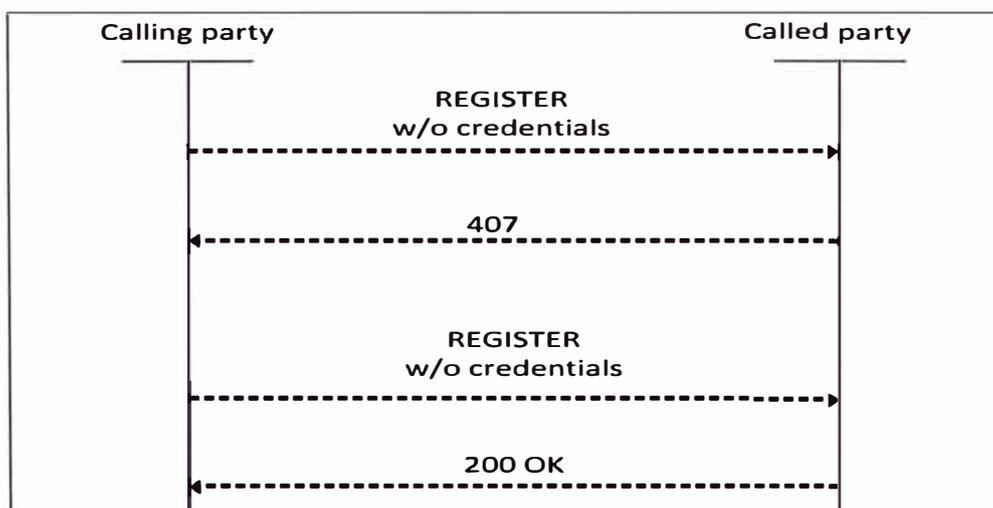


Figura 2.9 Diálogo de registro
(Fuente: IP Telephony cookbook)

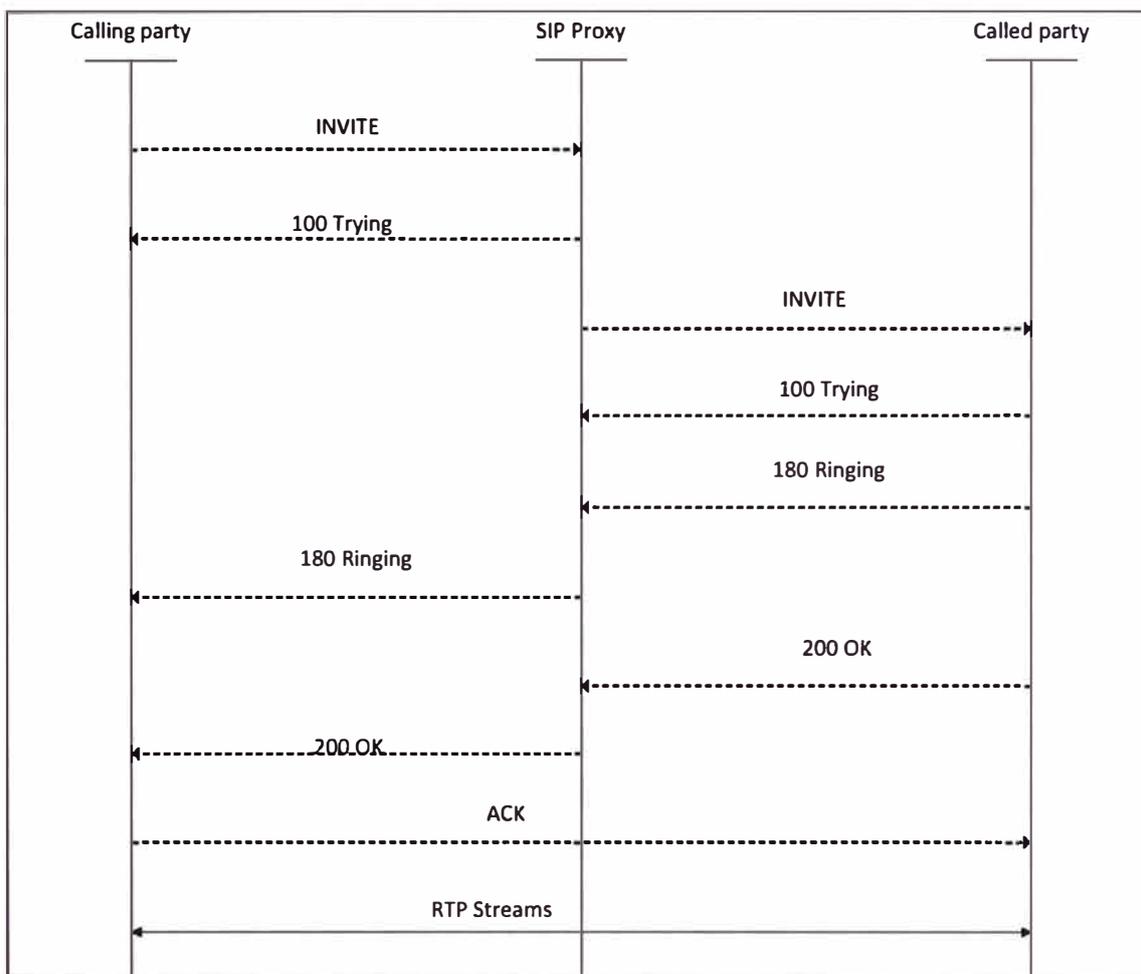


Figura 2.10 Diálogo de Invitación de sesión
(Fuente: IP Telephony cookbook)

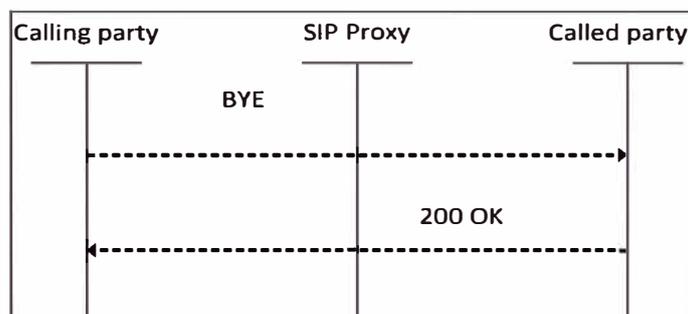


Figura 2.11 Diálogo de término de sesión
(Fuente: IP Telephony cookbook)

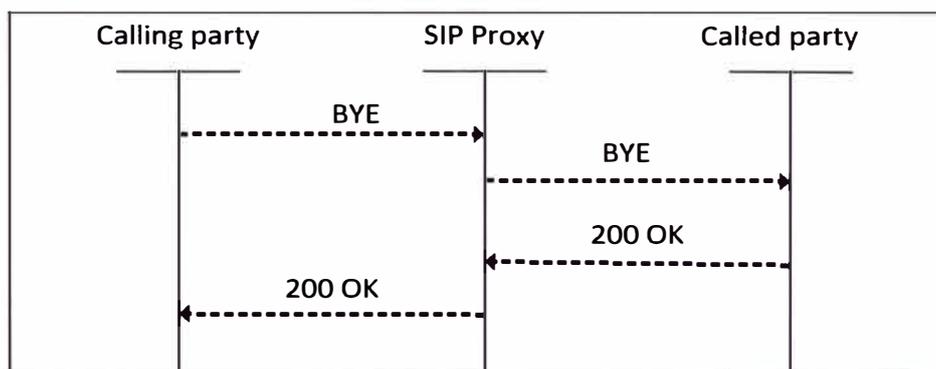


Figura 2.12 Diálogo de término de sesión con registro de ruta en "proxy"
(Fuente: IP Telephony cookbook)

2.3.3 Protocolos RTP/RTCP y SDP

Como se explica en la definición de protocolo SIP, este es sólo un protocolo pensado para enlazar en modo cliente – servidor a dos dispositivos y/o usuarios y establecer un canal entre ellos, pero no transportar la información ni mucho menos controlar cómo se transporta, es así como SIP se respalda en RTP y SDP.

a) Protocolo RTP/RTCP

Son los protocolos usados para transportar flujos de medios en Telefonía IP. Ambos fueron definidos en la RFC 1889. El primero para transportar flujos en tiempo real y el segundo para monitorear la calidad de servicio, así como para transportar información acerca de los participantes en la sesión.

Sus funciones son:

- Identificación del tipo de carga útil transportada (*Codecs* de Audio/Video)
- Verificar la entrega de los paquetes en orden (Marca de tiempo) y si resulta necesario reordenar los bloques fuera de orden.
- Transporte de información de sincronización para la codificación y decodificación.
- Monitoreo de la entrega de información.

RTP (*Real-time Transport Protocol*) utiliza UDP para el transporte de la información y aprovecha la suma de verificación del mismo, para que haya concordancia íntegra de los datos. Es importante resaltar que RTP no posee ningún método para garantizar la QoS ni la entrega ordenada de paquetes. Por otro lado RTCP utiliza el mismo protocolo que RTP para enviar paquetes de control hacia todos los participantes de una sesión.

Los servicios que provee RTCP (*RTP Control Protocol*) son los siguientes:

- Dar seguimiento a la calidad en la distribución de los datos, así como mantener el control de los “*codecs*” activos.
- Transportar un identificador constante para la fuente RTP (CNAME).
- Anunciar el número de participantes por sesión con el fin de ajustar la tasa de transmisión de datos.

b) Protocolo SDP

SDP, significa “*Session Description Protocol*” (Protocolo Descriptivo de Sesión), es un formato para describir parámetros de inicialización de flujo de medios. Ha sido publicado por la IETF como RFC 4566.

SDP está diseñado para transportar información de la sesión hacia los destinatarios, así como información de los medios referentes a la misma. Éste permite además asociar más de un flujo de medios a una misma sesión; por ejemplo en una misma sesión puede existir un flujo para audio y uno más para video o transferencia de documentos.

SDP es exclusivamente para propósitos de descripción y negociación de los parámetros

de sesión. No transporta el medio en sí. Fue pensado para trabajar en conjunto con otros protocolos como SIP, Megaco o HTTP. El transporte de información acerca de los flujos de medios permite a los destinatarios participar en la sesión si ellos soportan dichos flujos. Además, SDP permite la negociación de los parámetros del flujo tales como la tasa de muestreo de la señal, el tamaño de los paquetes, entre otros. En la figuras 2.13, 2.14 y 2.15 se muestran todas la opciones de SDP de información, por defecto u opcionales (diferenciadas por un *).

La información que SDP incluye en sus paquetes de forma general es la siguiente:

- La versión del protocolo.
- El nombre de la sesión y su propósito.
- El tiempo que la sesión esta activa.
- Los medios relacionados con la sesión (Video, Audio y formatos para Video o audio, entre otros).
- Las direcciones IP y los puertos pertinentes para el establecimiento de la sesión.
- Los atributos específicos a la sesión o a los medio dentro de ella.
- a= <atributo>, a=<atributo>:<valor>

```

Descripción de la sesión
v= (Versión del protocolo)
o= (Origen e identificador de sesión)
s= (Nombre de sesión)
i=* (Información de la sesión)
u=* (URI de descripción)
e=* (Correo electrónico)
p=* (Número telefónico)
c=* (Información de conexión)
b=* (Cero o más líneas con información de ancho de banda)
Una o más líneas de descripción de tiempo (Ver abajo "t=" y "r=")
z=* (Ajustes de zona horaria)
k=* (Clave de cifrado)
a=* (Cero o más líneas de atributos de sesión)
Cero o más descripciones de medios

```

Figura 2.13 Opciones de atributos ofrecidos por SDP para sesión
(Fuente: Elaboración propia)

```

Descripción de tiempo
t= (Tiempo durante el cual la sesión estará activa)
r=* (Cero o más veces de repetición)

```

Figura 2.14 Opciones de atributos ofrecidos por SDP de tiempo
(Fuente: Elaboración propia)

```

Descripción de medios, si está presente
m= (Nombre de medio y dirección de transporte)
i=* (Título)
c=* (Información de conexión)
b=* (Cero o más líneas con información de ancho de banda)
k=* (Clave de cifrado)
a=* (Cero o más líneas de atributos de sesión)

```

Figura 2.15 Opciones de atributos ofrecidos por SDP de media
(Fuente: Elaboración propia)

Los mensajes SDP están codificados como texto plano (ISO 10646 UTF-8), así se comprueba en la figura 2-13. Los nombres de campo y atributos usan US-ASCII pero lo demás es ISO 10646. Se eligió el formato texto plano para aumentar la "portabilidad" hacia sistemas basados en Web.

```

-----
(src=ipv4,[10.24.150.226]:5061;dest=ipv4,[10.0.0.32]:5060)
INVITE sip:18292137475@10.0.0.32;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.24.150.226:5061;branch=z9hG4bKd2q0811qrw84pqwdr2481qv38
Call-ID: zr22q232prv428vww213xppr1rt3dv3v4@SoftX3000
From: <sip:14368814@10.24.150.226;user=phone>;tag=4vytw00v-CC-23-TRC-544
To: <sip:18292137475@10.0.0.32;user=phone>
CSeq: 1 INVITE
Contact: <sip:14368814@10.24.150.226:5060;user=phone>
Min-SE: 90
Session-Expires: 3600
Allow:
INVITE,ACK,OPTIONS,BYE,CANCEL,REGISTER,INFO,PRACK,SUBSCRIBE,NOTIFY,UPDATE,MESSAGE,
REFER
User-Agent: HuaweiSoftX3000 V300R010
Diversion: <sip:19770018292137475@10.24.150.226;user=phone>;reason=do-not-
disturb;counter=2
Supported: 100rel,timer
Max-Forwards: 70
Content-Length: 299
Content-Type: application/sdp

v=0
o=HuaweiSoftX3000 99693643 99693643 IN IP4 10.24.150.226
s=Sip Call
c=IN IP4 10.24.160.2
t=0 0
m=audio 3264 RTP/AVP 8 0 18 4 97
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=rtpmap:4 G723/8000
a=rtpmap:97 telephone-event/8000
a=fmtp:97 0-15
a=fmtp:18 annexb=yes

```

Figura 2.16 Mensaje INVITE común, enmarcado en rojo ejemplo DSP
(Fuente: Elaboración propia)

2.3.4 Comparación con protocolos MGCP, SCCP, H.323, IAX Y SS7

A continuación una breve descripción de cada protocolo y un tabla comparativa demostrando sus fortalezas y debilidades dentro de parámetros para comunicación VoIP.

- **SS7:** El sistema de señalización de canal común numero 7 (es decir, SS7 o C7) es una norma global para las telecomunicaciones definidas por el sector de normalización de las telecomunicaciones (ITU-T) de la unión de telecomunicaciones Internacionales (ITU). La norma define el protocolo y los procedimientos mediante los cuales los elementos de la PSTN intercambian información sobre una red digital para efectuar el ruteo, establecimiento y control de llamadas. La definición de ITU para SS7 permite variantes nacionales tales como el Instituto de Normas Nacionales Americanos (ANSI) y Bell *Communications* usados en Norteamérica y el Instituto de Normas de Telecomunicaciones Europeos (ETSI) usado en Europa.
- **MEGACO (MGCP):** Es un protocolo de control de dispositivos, donde un *gateway* esclavo (MG) es controlado por un maestro (MGC, también llamado “*Call Agent*”). MGCP, “*Media Gateway Control Protocol*”, es un protocolo interno de VoIP cuya arquitectura se diferencia del resto de los protocolos VoIP por ser del tipo cliente – servidor. MGCP está definido informalmente en la RFC 3435, y aunque no ostenta el

rango de norma, su sucesor, MEGACO está aceptado y definido como una recomendación en la RFC 3015.

Está compuesto por:

- Un MGC, "*Media Gateway Controller*"
- Uno o más MG, "*Media Gateway*"
- Uno o más SG, "*Signaling Gateway*".

Un "*Gateway*" tradicional, cumple con la función de ofrecer conectividad y traducción entre dos redes diferentes e incompatibles como lo son las de Conmutación de Paquetes y las de Conmutación de Circuitos. En esta función, el *gateway* realiza la conversión del flujo de datos, y además realiza también la conversión de la señalización, bidireccionalmente.

MEGACO separa conceptualmente estas funciones en los tres elementos previamente señalados. Así, la conversión del contenido multimedia es realizada por el MG, el control de la señalización del lado IP es realizada por el MGC, y el control de la señalización del lado de la red de Conmutación de Circuitos es realizada por el SG.

MEGACO introduce esta división en los roles con la intención de aliviar a la entidad encargada de transformar el audio para ambos lados de las tareas de señalización, concentrando en el MGC el procesamiento de la señalización.

El control de calidad de servicio QoS se integra en el *gateway* GW o en el controlador de llamadas MGC. Este protocolo tiene su origen en el SGCP (de Cisco y *Bellcore*) e IPDC. *Bellcore* y Level3 plantearon el MGCP a varios organismos.

- **SCCP**: "*Skinny Client Control Protocol*" es un protocolo propietario de control de terminal desarrollado originariamente por *Selsius Corporation*. Actualmente es propiedad de Cisco Systems, Inc. y se define como un conjunto de mensajes entre un cliente ligero y el "*Call Manager*". Ejemplos conocidos de clientes ligeros son la serie Cisco 7900 de teléfonos IP como el Cisco 7960, Cisco 7940 y el Cisco 7920 802.11b inalámbricos. *Skinny* es un protocolo ligero que permite una comunicación eficiente con un sistema Cisco "*Call Manager*". El "*Call Manager*" actúa como un proxy de señalización para llamadas iniciadas a través de otros protocolos como H.323, SIP, RDSI o MGCP. Un cliente *skinny* utiliza TCP/IP para conectarse a los "*Call Managers*" en un *cluster*. Para el tráfico de datos (flujo de datos de audio en tiempo real) se utiliza RTP/UDP/IP. SCCP es un protocolo basado en estímulos y diseñado como un protocolo de comunicación para puntos finales hardware y otros sistemas embebidos, con restricciones de procesamiento y memoria significativas.

Cisco adquirió la tecnología SCCP cuando compró la empresa Selsius a finales de los años 1990. Como una reminiscencia del origen de los actuales teléfonos IP Cisco, el

nombre por defecto de los teléfonos Cisco registrados en un *CallManager* es SEP (Selsius Ethernet Phone) seguido de su MAC.

- **IAX2:** Protocolo desarrollado por Digium, con el objetivo de permitir la comunicación entre servidores Asterisk. Este protocolo ha sido desarrollado para solucionar problemas de NAT (por ejemplo con H.323) y mejorar el *trunk* entre sistemas basados en este protocolo (sólo se reserva el ancho de banda necesario en cada comunicación, a diferencia de otros como TDM/VoIP que reservan un determinado ancho de banda).
- **H.323:** El H.323 es una familia de normas para las comunicaciones multimedia sobre redes LAN. Está definido específicamente para tecnologías LAN que no garantizan una calidad de servicio. El protocolo de red más común en el cual se está implementando H.323 es IP. H.323 hace referencia a otras recomendaciones. La serie H.323 incluye recomendaciones como: H.225 referente a paquetización y Sincronización, H.245 relacionada a Control, H.261 y H.263 como “codecs” de video, G.711, G.722, G.728, G.729 y G.723 como “codecs” de audio y la serie T.120 de protocolos de datos.

Tabla 2.1 Comparativa entre SIP y H.323
(Fuente: IP Telephony cookbook)

Característica	Protocolo	
	H.323	SIP
Codificación	Binaria (ASN.1)	Textual (SigComp)
Formato	Serie G.XXX y H.XXX, MPEG, GSM	Tipos MIME – IANA
Ampliabilidad	Campos reservados	Métodos, cabeceras
Autenticación	H.235 (puede usar TLS)	Análogo a http
Localización	Gatekeeper (puede usar DNS)	DNS
Transporte	TCP, UDP	TCP, UDP, SCTP, DCCP, etc.
Arquitectura	Monolítica	Modular
Implementación	Costosa	Más sencilla
Negociación de parámetros	H.245	SDP
Vigencia	En declive	En auge
Numeración	Número de teléfono	URIs
IM	No	Si
Cantidad de estándares	Amplia	Reducida
Servicios	H.450	SIP CGI/CPL
Seguridad	Si	SI
Conferencias multimedia	Si	No
QoS	Gatekeepers	Externo (RSVP)

Las normas que se comparan en la tabla 2-1 son entre H.323 y SIP, ya que SS7 es un protocolo predecesor que no viene al caso para comparar, si toma mucha importancia en la implementación de los protocolos sucesores por un tema de migración hacia ellos, por otra parte IAX2 no es un protocolo de confiabilidad profesional o dicho de otra forma apoyado por alguna institución que dicte recomendaciones de renombre mundial, como lo son IETF o ITU, además de ser un protocolo muy vulnerable en cuanto a seguridad se refiera. Por otra parte MEGACO es un protocolo complementario a H.323 y SIP, además de ser un protocolo para controlar “media Gateway” y no señalización, y SCCP queda descartado por ser un protocolo propietario, así que claramente no es configurable en la variedad de equipos SBC a tratar en este tema.

2.4 Protocolo SIP-TRUNK

La definición de “SIP-*Trunk*” está basada en SIP, excepto por la propiedad de troncal. La definición de troncal telefónica es un concepto antiguo que data de PSTN la cual trata de un circuito entre centrales telefónicas de conmutación o de otro tipo equipos, a diferencia de los circuitos de bucle de abonado que se extienden desde el intercambio de equipo de conmutación telefónica para teléfonos de información individual o de inicio/termino de equipo.

Una definición global para SIP- *Trunk* es pues, una entidad SIP virtual en un servidor (UAS, UAC o proxy) limitado por un conjunto predefinido de políticas y normas que determinan la forma de procesar las solicitudes. El comportamiento del troncal está condicionado a un contrato, un acuerdo entre el cliente y el servidor, que siempre y cuando las solicitudes sean basadas en el formato del contrato, entonces la petición recibe el tratamiento que se especifica.

SIP permite resolver a nivel de servidor, en el tratamiento que se aplica a una solicitud SIP entrante. Como se transfieren las llamadas, como se autentifica, si se conecta a la PSTN, si los encabezados se agregan o quitan, si se termina la sesión, y así sucesivamente, son todas tratadas en la discrecionalidad del servidor. Un troncal SIP se define como un particular conjunto de la lógica de procesamiento de solicitudes, un sistema de autenticación específico, así como una lógica de enrutamiento específicas, además de adición y extracción de cabeceras determinadas.

Los siguientes son ejemplos de troncales SIP que pueden ser definidos en un servidor SIP, mostrando así las funcionalidades y comportamientos de SIP-*Trunk*:

- Interconexión PSTN/Troncal: Este es un troncal SIP que sería utilizado por las empresas que se conectan a un proveedor de servicios. El troncal utiliza la autenticación TLS mutua para determinar la identidad de interés en la empresa. Las solicitudes se aceptan sólo si el resultante de identidad coincide con un usuario de la

empresa antes de la provisión; todos los otros causan el cierre inmediato de la conexión TLS. Luego las solicitudes entrantes son aceptadas por los terminales hacia la PSTN. El URI de solicitud debe contener un número de teléfono en la parte de usuario, y la parte de dominio contiene el dominio del proveedor. Los números deben estar en formato E.164. El servidor utiliza configuración de tablas de enrutamientos localmente para enviar la invitación a una puerta de enlace PSTN basado en el número marcado.

- **Filtrado Troncal:** Este es un troncal SIP que puede ser proveído por un "*Session Border Controller*" (SBC) u otro servidor de borde. Esta *SIP-Trunk* se ejecuta a través de TCP y no es securizado con TLS. La petición URI puede estar basado en cualquier formato RFC oficial; la parte de dominio representa el destino de las solicitudes no el servidor en sí. El servidor examina la solicitud SIP y compara los encabezados en ella frente a unos pre-configurados, con encabezados permitidos. Los encabezados que no se encuentran en la lista son eliminados por el servidor antes de que la solicitud se envíe.
- **Troncal de correo de voz:** Este es un troncal SIP que puede ser proveído por un "Voicemail Server". Se ejecuta a través de TCP y es securizado con TLS; los clientes deben presentar certificados de un conjunto permitido. El URI de la solicitud debe tener el formato basado en las convenciones de la RFC 4458.
- **Troncal de publicación:** Este es un troncal SIP que puede salir en un servidor presente. Es compatible con TLS sobre TCP solamente, y se utiliza expresamente para PUBLICAR peticiones, la RFC3903 contiene los documentos presentes. Sólo un cierto conjunto de extensiones de documentos presentes cuentan con soporte, en particular, los documentos necesitan cumplir con la RFC 4480.

CAPITULO III

PLANEAMIENTO Y SOLUCIÓN DEL PROBLEMA

3.1 Objetivos de Servicio

A través de la recabación de datos realizada como primera parte del proyecto, se toman como objetivos técnicos específicos lograr los siguientes puntos:

- Solución base de “Troncal SIP” interconectado a *Carrier VoIP*.
- Solución avanzada para empresas que aún no poseen una estructura telefónica IP, y desean una mejora de servicios, estar a la vanguardia, o disminuir aún más sus costos gracias a *SIP-Trunk*.
- Solución experimental que da la existencia a costos diferenciales variables desde origen o destino, este es uno de los fines en los equipos SBC, la cual resulta una gran ventaja con respecto a la red pública conmutada de telefonía.

3.2 Equipo *Session Border Controller*

El “*Session Border Controller*” (SBC) es un equipo controlador de sesiones optimizado para la interconexión entre redes VoIP de diferentes dueños: corporaciones, ISPs o *Carriers* con NGN. Con éste, las empresas podrán pasar su tráfico telefónico en uno o más puntos de su red a múltiples proveedores mediante un simple troncal SIP con capacidad de entregar hasta miles de conversaciones simultáneas. Esto permite un gran ahorro, la eliminación de las tramas E1, mayor seguridad y una amplia disponibilidad de oferentes para dirigir su tráfico por la alternativa más económica.

Al mismo tiempo en que los ISP y “*Carriers*” implementan redes de VoIP y otros protocolos, aparecen desafíos que incluyen temas básicos de seguridad en la red, compatibilizar señalizaciones entre diferentes redes e interoperabilidad en un ambiente de múltiples proveedores.

“*Session Border Controller*” permite que los proveedores de VoIP públicos y privados interconecten sus redes vía IP con las redes basadas en SIP y H.323 de los clientes VoIP corporativos, implementando una conexión segura, y dejando en el pasado las antiguas tramas TDM de la red tradicional.

El SBC es un equipo que controla, con altos niveles de seguridad, el tránsito de entrada y salida de todas las transmisiones de voz que viajan sobre su red.

Este dispositivo tiene la capacidad de vigilar todas las comunicaciones desde y hacia su red diferenciando que es voz y que no, evitando ataques que puedan poner en peligro el

servicio. Además, es escalable sin necesidad de invertir en equipos, dado que puede trabajar con 250 hasta 10 mil sesiones simultáneas con sólo una actualización de licencia.

3.2.1 Principales proveedores de equipos *Session Border Controller*

Entre los principales proveedores de equipos SBC se encuentran: *Acme Packet*, Cisco, Juniper, *NexTone*, *Genband*, *Ditech*, e *InGate*. Cada empresa contempla una visión común con respecto a esta tecnología, y al mismo tiempo reservan sus propios puntos de vista de cómo encajar los SBC en función de un mejor desempeño de los actuales sistemas de telefonía IP.

Para el proyecto se utilizará el equipo de la marca *Acme Packet* debido a que es un equipo con el que se tiene buenas referencias de parte de diferentes proveedores de telefonía.

Acme Packet

Tanto la gente de negocios como usuarios necesitan mucho más que un correo electrónico, mensajería instantánea basada en texto y servicios de datos para comunicarse entre sí. También necesitan servicios interactivos con verdadera comunicación en tiempo real, como las llamadas de voz, PBX/servicios Centrex, la presencia con voz instantánea o llamadas de video/conferencias, colaboración multimedia, videoconferencias, educación a distancia, el Cliente interactivo/"*Supplier Relationship Management*" (C/SRM), multimedia para sitios de atención al cliente web y más.

Expuestas las necesidades de los clientes, *Acme Packet* clasifica las soluciones en cuatro grandes módulos:

- Empresa: Soluciones actualmente implementadas en Chile, en un formato de demostración y prueba para grandes empresas nacionales, todo esto con el protocolo SIP-trunk. Como idea principal de la solución, se da un servicio telefónico IP a menor costo de normal, gracias a una mayor eficiencia en el uso del ancho de banda con SIP-trunk.
- Móvil: Solución que extiende la solución "Empresa" a una unificación geográfica para el cliente, lo que se traduce a utilizar el servicio VoIP en cualquier lugar físico con condiciones de conectividad razonables.
- Línea Fija: Solución que pretende escalar el mercado SBC a los proveedores de servicio, dando un salto en el público objetivo, actualmente empresas, a usuario individuales.
- Capa más alta y aplicaciones para proveedores de servicio: Solución que apunta a la integración total al mundo IP, en cuanto a servicios de comunicación, lo que se

denomina IMS (Subsistema Multimedia IP), esto brinda una infinidad de servicios agregados a las comunicaciones telefónicas actuales.

Las soluciones de *Acme Packet* idealmente no cumplen todos sus propósitos, aunque es el que se acerca más a la solución final. Las redes IP actuales son incapaces de soportar estas comunicaciones. ¿Por qué?, debido a que cualquier proveedor de servicios de red por sí solo no llega lo suficientemente lejos y de manera global, Internet carece de la necesaria QoS y de los mecanismos de contabilidad para ofrecer una calidad alta.

La entrega de alta calidad de voz interactiva, el vídeo y las comunicaciones multimedia a través de las fronteras de la red IP representan una gran oportunidad de ganancias para los proveedores de servicios. Esto es a lo que *Acme Packet* apunta, dejar atrás el desarrollo aislado de la telefonía IP, y convertir a Internet, en la red de telefonía IP más grande del mundo.

Principales modelos Acme Packet 3820 y 4500

Soporte de SCPs: SIP, H.323, interoperabilidad SIP/H.323, MGCP/NCS, H.248, RTCP.

Control de sesión: Completa en las áreas de seguridad, aplicaciones/maximización de alcance del servicio, garantía de SLA (“*Service Level Agreement*”).

DoS: Autoprotección contra capas 3 y 4, IPsec, protocolos de señalización contra ataques de sobrecarga.

Administración: Aplicación NET-NET EMS y SAS, CLI, telnet, ssh, FTP, XML, RADIUS, SNMP, syslog.

Interoperabilidad (probadas): Principales centralitas IP, plataformas de comunicaciones unificadas, Servidores SIP, servidores de aplicación, *gateways* de medio de comunicación, “*softswitches*”, elementos de IMS CSFC, “*gatekeepers*” H.323.

- Capacidad para 4000 sesiones de señalización.
- Alta disponibilidad (H.A.), redundancia 1:1, restablece estado configuración y “media” para no tener perdida de servicio.
- QoS.
- Encriptación: Opciones de sesión - Túnel IPsec y TLS, Opciones de tráfico: IPsec y SRTP. 1000 túneles con llaves manuales, 5000 túneles con IMS-AKA.
- Entradas de rutas locales: 1.000.000 de rutas configurables.
- Interfaces de red: 4 activas 10/100/1000 Mbps con interfaces Ethernet.
- Rendimiento de sistema: 5 Gbps.

Especificaciones Físicas/programables:

Chasis:

- 1U, para montaje en rack.
- Panel frontal: LED de estado para energía y H.A., “pinhole” para restauración del

sistema, interfaces de consola y almacenamiento local.

- Panel Trasero: Un unidad "slot" de interfaz de red (señalización, "media" e interfaces de administración), una fuente de alimentación fija, escape de aire de salida.

Memoria:

- 1 GB para la configuración activa y operación.
- 256 MB de memoria flash interna para almacenar archivos (sistema operativo, configuración, "accounting", "log").
- Contenido de memoria *direccionable* (CAM): 128KB para ACL estática y dinámica, reglas de control de "media" y entradas ARP.
- Una interfaz serial RS-232 con interfaz de consola RJ-45 (sólo por detrás o delante de interfaz se puede utilizar en cualquier momento).
- Una interfaz de alarma con conector RJ-45.
- Panel de gestión de interfaces frontal.
- Una interfaz USB 2.0.
- Voltaje: 100-240 VAC entrada "autoranging" de ancho, con corrección de factor de potencia.
- Frecuencia: 50/60 Hz.
- Corriente: 1,5 A a 115 VAC y 0,75 como máximo a 230 VAC.

3.2.2 Modo Peering y Modo Access

Estos dos conceptos se introducen para tener un mayor entendimiento de los tipos de redes que implementen y evalúen en laboratorio con el objetivo principal de integración de tecnología para servicios VoIP / Datos / Multimedia / Control.

a) Modo "Peering"

En primer lugar un escenario "peering" típico es cuando participan dos operadores de red que intercambian tráfico entre sí. Un ejemplo sería el escenario de interconexión que se ilustra en la figura 3.1. Un "Gateway" de origen (GW-A1) en el operador A de la red envía un INVITE que se dirige al operador de SBC en el operador B de la red. Entonces el SBC envía el INVITE al *softswitch* (SS-B).

En una segunda etapa del proceso, el "softswitch" responde con una redirección (3xx) mensaje de nuevo al SBC que apunta al Gateway terminal adecuado (GW-B1) en el operador de red de B. Si el operador B no tuviera un SBC, el mensaje de redirección iría al "Gateway" procedente del operador "A". Después de recibir el mensaje de redirección, el SBC envía la invitación al "Gateway" finalmente.

Desde la perspectiva del SBC es el operador A la red exterior, y el operador B es la red interna. El operador B puede utilizar el SBC, por ejemplo, para controlar el acceso a su red, proteger sus puertas y conmutadores de software de uso no autorizado y ataques de

denegación de servicio (DoS), supervisar la señalización y el tráfico de los medios de comunicación. También simplifica la gestión de la red, reduciendo al mínimo el número de ACL (“Access Control List”) en la entrada del “Gateway”. Los “Gateway” ya no deben estar expuestos a la red de otros pares, y pueden restringir el acceso (tanto los medios de comunicación y señalización) al SBC.

El SBC ayuda a garantizar que sólo los medios de comunicación de sesiones autorizadas en el SBC lleguen a la puerta de enlace.

Como definición más ortodoxa se tiene que el concepto de “peering” es la interconexión voluntaria entre dos redes en Internet administrativamente independientes, con el propósito de intercambiar tráfico entre usuarios de cada una de las redes.

La definición estricta significa "libre acuerdo" o "el remitente se hace cargo", esto es, ninguna de las partes paga a la otra por el intercambio de tráfico, sino que cada una deriva el crédito de sus propios clientes.

La comercialización y las presiones comerciales han llevado al uso rutinario de esta palabra toda vez que hay un cierto acuerdo implicado, aunque no se trata de su sentido técnico exacto. La frase “peering de libre acuerdo” se utiliza a veces para reflejar esta realidad y para describir sin lugar a dudas que se trata de un intercambio de información sin costo. El “peering” requiere la interconexión física de las redes, un intercambio de la información de encaminamiento con el protocolo de encaminamiento del *Border Gateway Protocol* (BGP) y, a menudo, va acompañado por acuerdos que implican diversa formalidad que varía, del simple “handshake” a conexiones más complejas.

Así existen 2 tipos de “peering”, público y privado.

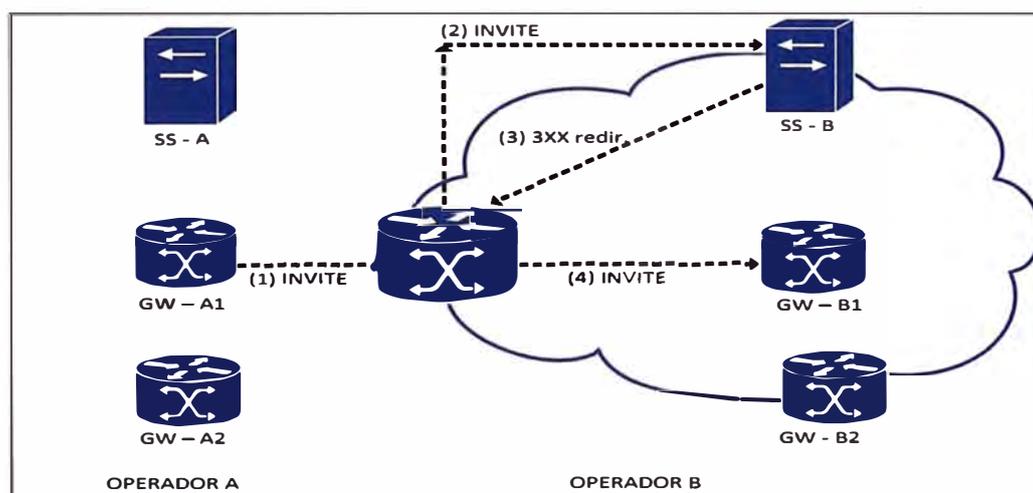


Figura 3.1 Diagrama de ejemplo para modo “Peering”
(Fuente: IP Telephony cookbook)

b) Modo “Access”

En un escenario de acceso, presentado en la figura 3.2, el SBC se coloca en la frontera entre la red de acceso (red exterior) y la red del operador (red interna) para controlar el

acceso a la red del operador, proteger sus equipos (servidores de medios, servidores de aplicaciones, pasarelas, entre otros), restringir el acceso no autorizado, los ataques DoS, supervisar la señalización y el tráfico de los medios de comunicación. Además, como el SBC es un evaluador de llamadas, puede ofrecer funciones de control de acceso para evitar sobresuscripción de los enlaces de acceso.

Los extremos están configurados con el SBC como su dirección de proxy de salida.

El SBC enruta peticiones a uno o más proxies en la red del operador.

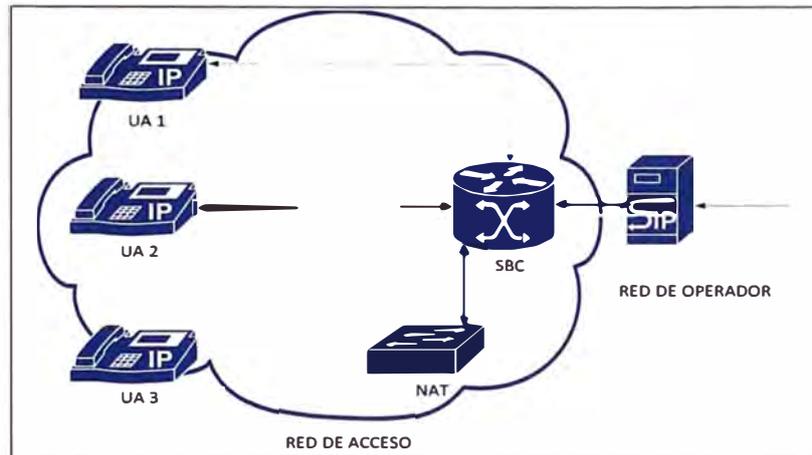


Figura 3.2 Diagrama de ejemplo para modo "Access"
(Fuente: Elaboración propia)

El SBC puede ser configurado en la red de acceso (esto es común cuando el acceso a la red es una red de la empresa), o en la red de operador (esto es común cuando la red de acceso es un residencial o una pequeña red de empresa).

A pesar de desde donde el SBC se configura, siempre es administrado por la organización de mantenimiento de la red del operador.

Algunos "endpoints" pueden estar detrás de NATs de empresa o residencial. En los casos en que la red de acceso es una red privada, el SBC es un NAT para todo el tráfico. Cabe señalar que el tráfico de SIP puede requerir recorrer más de un NAT.

El proxy usualmente realiza autenticación y/o autorización de registro y llamadas de salida.

El SBC modifica la petición REGISTER de modo que las solicitudes posteriores a la dirección registrada de record se enrutan a la SBC.

Esto se hace con un campo de "path" de la cabecera, o modificando el punto de contacto en el SBC.

3.3 Topología de la Solución

La topología de solución es la que se muestra en la figura 3.3. Como se puede ver en la figura la solución trata de la instalación de un equipo *Session Border Controller* interconectado al *Softswitch* del Operador de Telefonía.

El equipo *Session Border Controller* utiliza la configuración "Reino Core" y "Reino Peer".

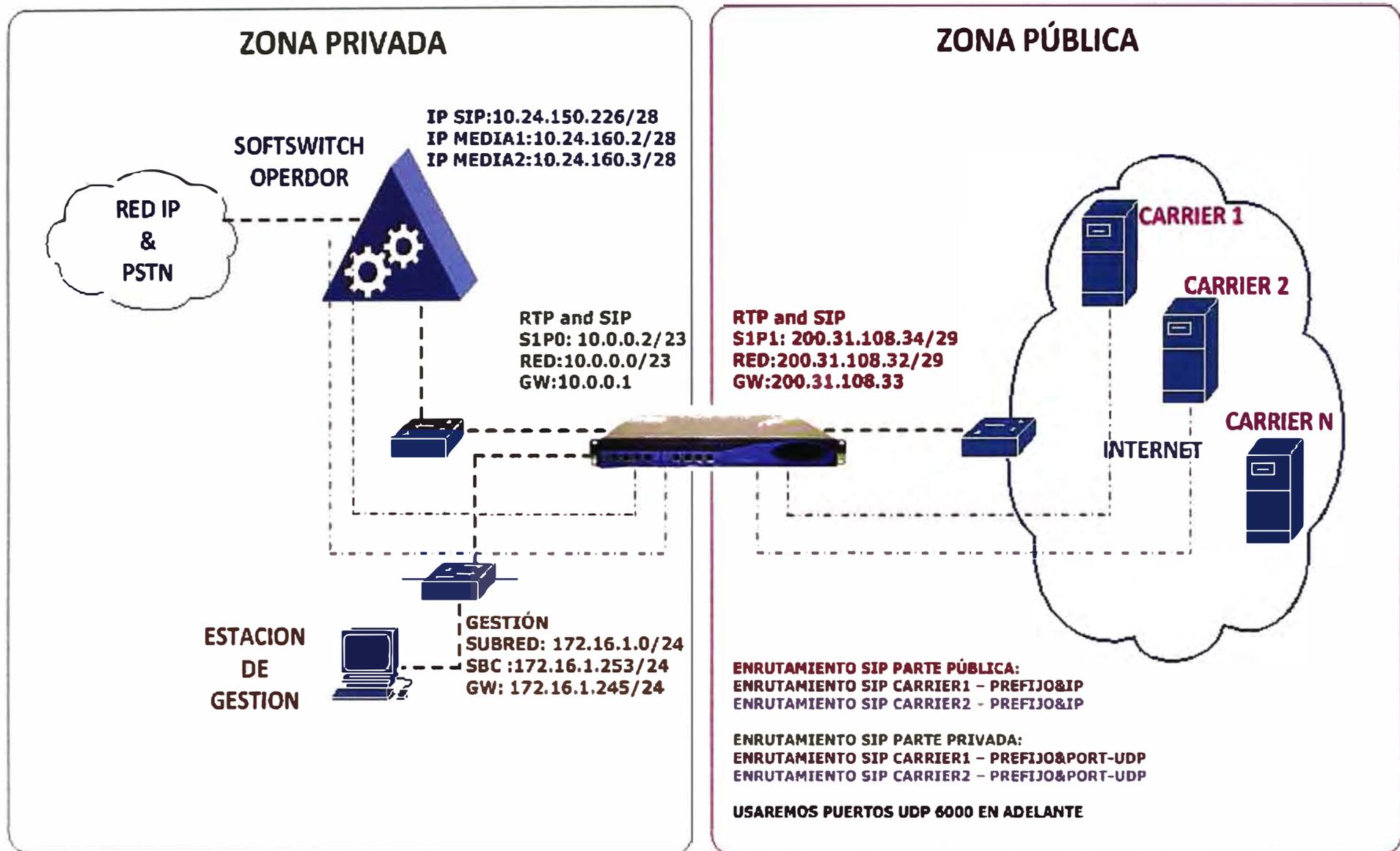


Figura 3.3 Topología de Solución
 (Fuente: Elaboración propia)

El “Reino Core” es la “Zona Privada” que como se ve en el gráfico contiene a la Red PSTN del Operador y la Red de Gestión del *Session Border Controller*.

El “Reino Peer” es la “Zona Pública” que como se ve en el gráfico contiene la interconexión del equipo *Session Border Controller* con los *Carrier*.

3.4 Equipamiento

Para la solución se va a utilizar el equipo *Session Border Controller* de la marca “Acme Packet”, el modelo del equipo escogido es el “Net-Net 3820”.

3.4.1 Acme Packet Net-Net 3820

Acme Packet 3820 es una unidad de rack (1U), plataforma que cuenta con hardware especialmente diseñado por Oracle integrado con Acme Packet OS, para proporcionar los controles críticos para la entrega de confianza, de primera clase en tiempo real con las comunicaciones de voz, video y multimedia sesiones a través de Internet *Protocol* (IP) de las fronteras de la red. En la figura 3.4 se muestra el equipo Acme Packet 3820 y en la tabla 3.1 se muestra las características técnicas.

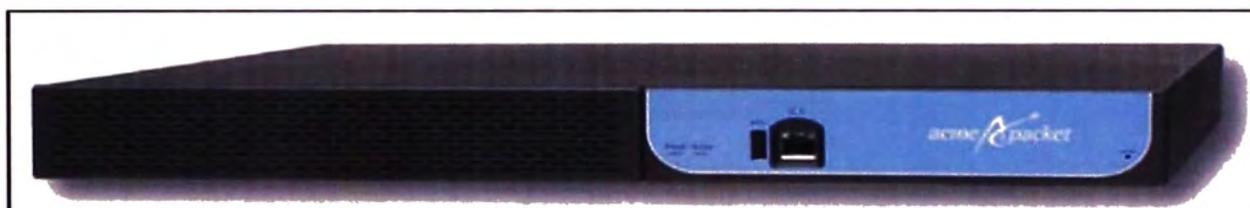


Figura 3.4 Acme Packet Net-Net 3820
(Fuente: Acme Packet)

Tabla 3.1 Características del Acme Packet Net-Net 3820
(Fuente: Acme Packet)

	Net-Net 3820
Licensed Session Capacity Range	150 – 8K
System Throughput	5Gbps
Network Interface (# active)	(4) 1Gbps
IPsec Tunnel Capacity	120K
Transcoding Session Capacity	0-7200
Local Route Table Capacity (# of Router)	1M

3.4.2 Softswitch Huawei SoftX3000

El SoftX3000, que actúa como central de tránsito (C4), central de llamadas sub urbanas y central *gateway*, procesa señalización diversificada y proporciona servicios tales como el punto de conmutación del servicio (SSP), listas negras y blancas de gran capacidad, autenticación, cobro e igualdad de acceso. Asimismo, interopera con dispositivos de otras redes, tales como la red de multiplexación por división de tiempo (TDM), la red AS de terceros, la red inteligente (IN), la red de protocolo de inicio de sesión/H323 (SIP), la red

móvil terrestre pública (PLMN), la red del subsistema IP multimedia (IMS), el acceso inalámbrico WLL con acceso múltiple por división de código (CDMA) y la red de acceso coaxial por fibra híbrida (HFC). Para el presente caso, el Operador ya cuenta con un *Softswitch* pero se le menciona pues en él se realizarán también configuraciones. En la figura 3.5 se muestra una foto del equipo *Softswitch* Huawei SoftX3000.

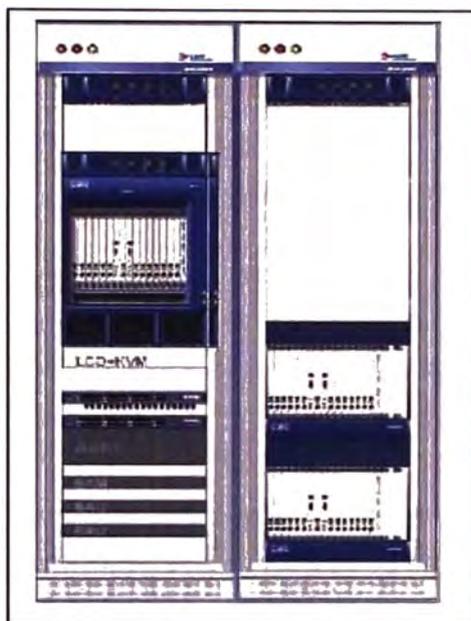


Figura 3.5 *Softswitch* Huawei SoftX3000
(Fuente: Huawei)

3.5 Configuración de Equipos

El proyecto consiste en la implementación de un equipo SBC en modo SIP-*Trunk* para un Operador de Larga Distancia, a continuación se mostrará la configuración que este equipo SBC de la marca *Acme Packet* debe tener para su correcto funcionamiento; también se mostrará la configuración en el *Softswitch* (marca Huawei, modelo SoftX3000).

3.5.1 Configuración *Acme Packet* Net-Net 3820

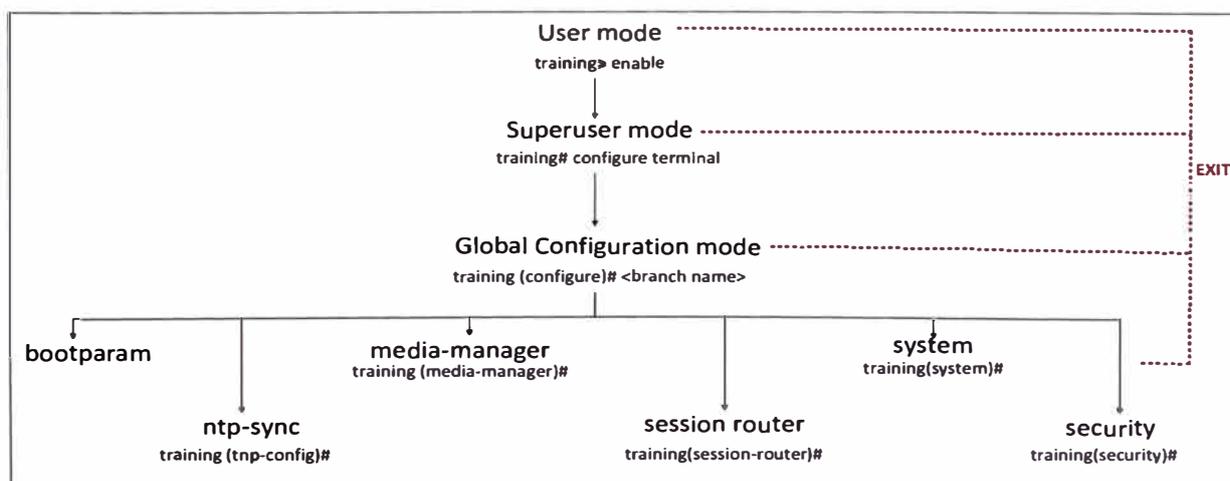


Figura 3.6 Jerarquía ACLI
(Fuente: *Acme Packet*)

- Ingresar vía telnet (solo desde la red Interna)

```
Host ~ $ telnet 172.16.1.253
Trying 172.16.1.253...
Connected to 172.16.1.253.
Escape character is '^]'.
Password: *****
SBCSUR01A> en
Password: *****
SBCSUR01A#
```

Figura 3.7 Ingreso al SBC vía Telnet
(Fuente: Elaboración propia)

- Crear *Session-Constraints* (limitante de sesiones)

```
SBCSUR01A(configure)# session-router
SBCSUR01A(session-router)# session-constraints
SBCSUR01A(session-constraints)# name sesConst_carrier1
SBCSUR01A(session-constraints)# max-sessions 30
SBCSUR01A(session-constraints)# done
```

Figura 3.8 Crear Session Constraints
(Fuente: Elaboración propia)

- Crear *Translations Rules* (tratamiento de prefijos)

```
##Agregar prefijo
SBCSUR01A(configure)# session-router
SBCSUR01A(session-router)# translation-rules
SBCSUR01A(translation-rules)# id addpref281000
SBCSUR01A(translation-rules)# type add
SBCSUR01A(translation-rules)# add-string 281000
SBCSUR01A(translation-rules)# done
##Eliminar prefijo
SBCSUR01A(translation-rules)# id delpref6051
SBCSUR01A(translation-rules)# type delete
SBCSUR01A(translation-rules)# delete-string 60#51
SBCSUR01A(translation-rules)# done
```

Figura 3.9 Crear Translations Rules
(Fuente: Elaboración propia)

- Crear *Session Translation* (vistos desde lado Core)

```
##De entrada [[BR]]
##De entrada
SBCSUR01A(configure)# session-router
SBCSUR01A(session-router)# session-translation
SBCSUR01A(session-translation)# id Carrier1_In
SBCSUR01A(session-translation)# rules-called addpref281000
SBCSUR01A(session-translation)# done
##De salida
SBCSUR01A(session-translation)# id Carrier1_Out
SBCSUR01A(session-translation)# rules-called delpref6051
SBCSUR01A(session-translation)# done
```

Figura 3.10 Crear Session Translation
(Fuente: Elaboración propia)

- Crear Realms

```

##Peer Realm
SBCSUR01A# conf t
SBCSUR01A(configure)# media-manager
SBCSUR01A(media-manager)# realm-config
SBCSUR01A(realm-config)# identifier peer_carrier1
SBCSUR01A(realm-config)# description "Realm for Peer Carrier1"
SBCSUR01A(realm-config)# addr-prefix 0.0.0.0
SBCSUR01A(realm-config)# network-interfaces M00:0
SBCSUR01A(realm-config)# parent-realm peers_SBC
SBCSUR01A(realm-config)# out-manipulationid ACME_NAT_TO_FROM_IP
SBCSUR01A(realm-config)# access-control-trust-level high
SBCSUR01A(realm-config)# constraint-name sesConst_carrier1
SBCSUR01A(realm-config)# done

##Core Realm
SBCSUR01A(realm-config)# identifier core_carrier1
SBCSUR01A(realm-config)# description "Realm for Core Carrier1"
SBCSUR01A(realm-config)# addr-prefix 0.0.0.0
SBCSUR01A(realm-config)# network-interfaces M10:0
SBCSUR01A(realm-config)# parent-realm core_SBC
SBCSUR01A(realm-config)# in-translationid Carrier1_In
SBCSUR01A(realm-config)# out-translationid Carrier1_Out
SBCSUR01A(realm-config)# out-manipulationid ACME_NAT_TO_FROM_IP
SBCSUR01A(realm-config)# access-control-trust-level high
SBCSUR01A(realm-config)# done

```

Figura 3.11 Crear Realms
(Fuente: Elaboración propia)

- Crear SIP Interface

```

SBCSUR01A(configure)# session-router
SBCSUR01A(session-router)# sip-interface
SBCSUR01A(sip-interface)# realm-id core_carrier1
SBCSUR01A(sip-interface)# description "Sip-interf for core_carrier1"
SBCSUR01A(sip-interface)# sip-ports
SBCSUR01A(sip-port)# address 10.0.0.8
SBCSUR01A(sip-port)# port 5060
SBCSUR01A(sip-port)# allow-anonymous all
SBCSUR01A(sip-port)# done
SBCSUR01A(sip-port)# exit
SBCSUR01A(sip-interface)# done

```

Figura 3.12 Crear SIP Interface
(Fuente: Elaboración propia)

- Crear Session Agent

```

##Session Agent 01
SBCSUR01A(configure)# session-router
SBCSUR01A(session-router)# session-agent
SBCSUR01A(session-agent)# hostname 194.183.68.100
SBCSUR01A(session-agent)# ip-address 194.183.68.100
SBCSUR01A(session-agent)# port 5060
SBCSUR01A(session-agent)# realm-id peer_carrier1
SBCSUR01A(session-agent)# description "SA Carrier1 01"
SBCSUR01A(session-agent)# ping-method OPTIONS;hops=0
SBCSUR01A(session-agent)# ping-interval 60
SBCSUR01A(session-agent)# ping-send-mode keep-alive
SBCSUR01A(session-agent)# done

##Session Agent 02
SBCSUR01A(configure)# session-router
SBCSUR01A(session-router)# session-agent
SBCSUR01A(session-agent)# hostname 194.183.68.101
SBCSUR01A(session-agent)# ip-address 194.183.68.101
SBCSUR01A(session-agent)# port 5060
SBCSUR01A(session-agent)# realm-id peer ''carrier1''
SBCSUR01A(session-agent)# description "SA Carrier1 02"
SBCSUR01A(session-agent)# ping-method OPTIONS;hops=0
SBCSUR01A(session-agent)# ping-interval 60
SBCSUR01A(session-agent)# ping-send-mode keep-alive
SBCSUR01A(session-agent)# done

```

Figura 3.13 Crear Session Agent
(Fuente: Elaboración propia)

- Crear Session Group

```
SBCSUR01A(session-agent-group)# group-name CARRIER1
SBCSUR01A(session-agent-group)# description "SAG CARRIER1"
SBCSUR01A(session-agent-group)# strategy RoundRobin
SBCSUR01A(session-agent-group)# dest (194.183.68.100 194.183.68.101)
SBCSUR01A(session-agent-group)# done
```

Figura 3.14 Crear Session Group
(Fuente: Elaboración propia)

- Crear Local Policy

```
##Softswitch to Peer
SBCSUR01A(configure)# session-router
SBCSUR01A(session-router)# local-policy
SBCSUR01A(local-policy)# from-address *
SBCSUR01A(local-policy)# to-address *
SBCSUR01A(local-policy)# source-realm core_carrier1
SBCSUR01A(local-policy)# description "Softswitch -> Carrier1"
SBCSUR01A(local-policy)# policy-attributes
SBCSUR01A(local-policy-attributes)# next-hop SAG:CARRIER1
SBCSUR01A(local-policy-attributes)# realm peer_carrier1
SBCSUR01A(local-policy-attributes)# done
SBCSUR01A(local-policy-attributes)# exit
SBCSUR01A(local-policy)# done

##Peer to Softswitch
SBCSUR01A(local-policy)# from-address *
SBCSUR01A(local-policy)# to-address 60
SBCSUR01A(local-policy)# source-realm peer_carrier1
SBCSUR01A(local-policy)# description "Carrier1 -> Softswitch"
SBCSUR01A(local-policy)# policy-attributes
SBCSUR01A(local-policy-attributes)# next-hop 10.24.150.226
SBCSUR01A(local-policy-attributes)# realm core_carrier1
SBCSUR01A(local-policy-attributes)# done
SBCSUR01A(local-policy-attributes)# exit
SBCSUR01A(local-policy)# done
```

Figura 3.15 Crear Local Policy
(Fuente: Elaboración propia)

- Crear Access Control (Se deben crear uno por IP del peer)

```
##IP 01
SBCSUR01A(configure)# session-router
SBCSUR01A(session-router)# access-control
SBCSUR01A(access-control)# realm-id peer_carrier1
SBCSUR01A(access-control)# description "ACL for SA Carrier1 01"
SBCSUR01A(access-control)# source-address 194.183.68.100
SBCSUR01A(access-control)# destination-address 200.31.108.34
SBCSUR01A(access-control)# application-protocol SIP
SBCSUR01A(access-control)# trust-level high
SBCSUR01A(access-control)# done

##IP 02
SBCSUR01A(configure)# session-router
SBCSUR01A(session-router)# access-control
SBCSUR01A(access-control)# realm-id peer_carrier1
SBCSUR01A(access-cont
rol)# description "ACL for SA Carrier1 02"
SBCSUR01A(access-control)# source-address 194.183.68.101
SBCSUR01A(access-control)# destination-address 200.31.108.34
SBCSUR01A(access-control)# application-protocol SIP
SBCSUR01A(access-control)# trust-level high
SBCSUR01A(access-control)# done
```

Figura 3.16 Crear Access Control
(Fuente: Elaboración propia)

- Salvar y Activar

```
#Verificar y Salvar
SBXSUR01A(configure)# done
SBXSUR01A# verify-config
-----
Verification successful! No errors nor warnings in the configuration
SBXSUR01A# save-config
checking configuration
Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
SBXSUR01A# activate-config
Activate-Config received, processing.
waiting for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
SBXSUR01A#
```

Figura 3.17 Salvar y Activar
(Fuente: Elaboración propia)

3.5.2 Configuración en el Softswitch Huawei SoftX3000

Los siguientes son comandos que deben ingresarse en el SoftX3000 para provisionar correctamente un SIPTRUNK para tráfico *wholesale* (tráfico masivo).

- Crear CSC

```
ADD CALLSRC: CSC=CSCindex, CSCNAME="TGname", LP=11, RSSC=RSSCindex;
```

Dónde: LP=11, es el LDNSET designado para todo tráfico *wholesale*.|

- Crear OFICINA

```
ADD OFC: O=OFCindex, ON="TGname", DOT=NATT, DOL=LOW, DOA=SPC;
```

- Crear SUB RUTA

```
ADD SRT: SRC=SRCindex, O=OFCindex, SRN="TGname", RENT=URT;
```

- Crear SIPTG

```
ADD SIPTG: TG=TGindex, CSC=CSCindex, SRT=SRCindex, TGN="TGname",
RCHS=0,HCIC=#canales, LCIC=#canales, ST=NGNN, NOAA=NO, EA=YES, ICR=LCO-
1&LC-1&LCT-1&NTT-1&ITT-1&INTT-1&IITT-1&IOLT-1&CCR1-1&CCR2-1&CCR3-1&CCR4-
1&CCR5-1&CCR6-1&CCR7-1&CCR8-1&CCR9-1&CCR10-1&CCR11-1&CCR12-1&CCR13-
1&CCR14-1&CCR15-1&CCR16-1, OCR=LCO-1&LC-1&LCT-1&NTT-1&ITT-1&INTT-1&IITT-
1&IOLT-1&CCR1-1&CCR2-1&CCR3-1&CCR4-1&CCR5-1&CCR6-1&CCR7-1&CCR8-1&CCR9-
1&CCR10-1&CCR11-1&CCR12-1&CCR13-1&CCR14-1&CCR15-1&CCR16-1, UHB=NO,
ACODEC=G729, VIDEOS=SUPPORT, CHBF=NO, E2833F=NSUPPORT, SELMODE=DIST;
```

- Crear LINK SIP

```
ADD SIIPPAIR: TG=TGindex, IMN=132, OSU="IP_realm_core_SBC:5060", DH=NO;
```

- Agregar funcionalidad TGAP para rel-rerouting

```
ADD TGAP: TG=TGindex, CDFP=NO, CNCM=ALLOW, CCICF=NO, CRF=YES, CLF=NO,
TRF=NP, TLF=NO, CNISUP=NO;
```

- Activar Heartbeat

```
MOD SIPTG: TG=TGindex, EA=YES, UHB=NORMAL, NHB=60, XHB=120;
```

Dónde: XHB=2xNHB=120, es la cantidad de segundos entre mensajes OPTIONS.

- Activar Medidas

- o Crear task en SOFTSWITCH

```
CRE TRFCROBJ: TSKN="TGGRP_BOTHWAY_TGindex_CARRIERname", MU=tkgbothway,
PRD=M30, ST1=00&00, ET1=00&00, CYCL=DAY, OPD=nmp, OPM=PP, tkg="TGindex";
```

o Sincronizar Task en N2000

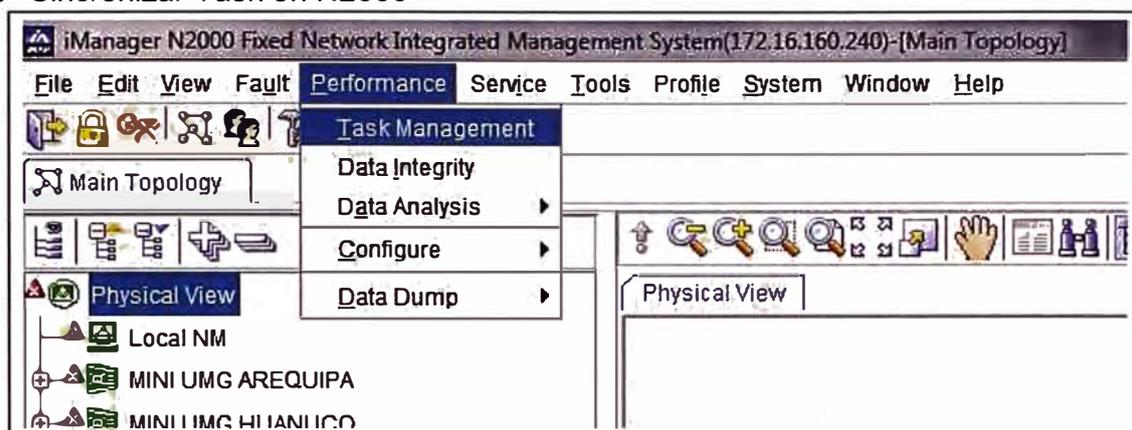


Figura 3.18 Performance Task Management
(Fuente: Americatel Perú SAC)

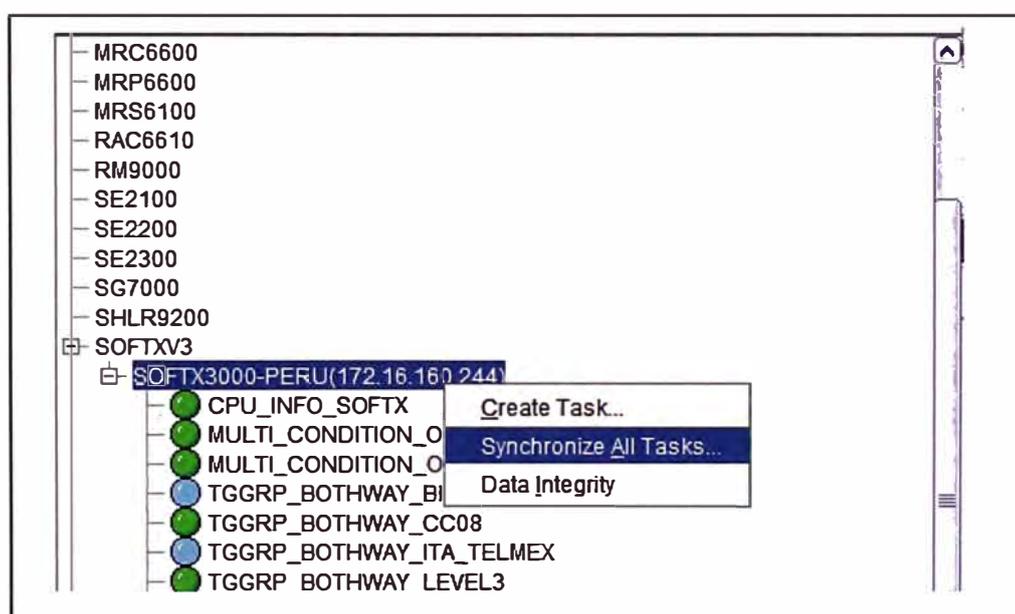


Figura 3.19 Task Management SOFTXV3 - SOFTX3000 (172.16.160.244) Synchronize all tasks
(Fuente: Americatel Perú SAC)

Observación: Es obligatorio que el peer responda el mensaje OPTIONS con 200 OK a fin de que el *Softswitch* sepa que la ruta esta activa.

CAPITULO IV

CRONOGRAMA Y ESTUDIO ECONÓMICO DEL PROYECTO

En este capítulo se detalla las fases de implementación del proyecto, entregando información de los costos del equipamiento para la implementación del mismo, el trabajo de la instalación y soporte del equipo *Session Border Controller* estaría a cargo de una empresa proveedora, los datos de costos y tiempos de ejecución son estimados de algunas propuestas comerciales recibidas. Posteriormente se hará una evaluación económica del proyecto buscando hallar el tiempo de retorno de la inversión.

4.1 Tiempo de Ejecución

El tiempo de ejecución estará dividido en 7 fases:

- Inicio.
 - Presentación de la solución.
 - Aceptación de la Oferta Técnica-Económica.
 - Revisión de los COSTOS/MARGEN del proyecto.
 - Apertura del proyecto.
- Adquisición:
 - Fabricación de equipos.
 - Despacho y nacionalización de equipos.
- Instalación.
 - Acondicionamiento en el Rack de Comunicaciones, tomas de energía.
 - Acondicionamiento de Red.
 - Instalación del SBC.
 - Configuración de Switches y Routers.
 - Configuración del SBC.
 - Configuración del SIP-*Trunk* de prueba.
- Pruebas.
 - Pruebas de llamadas con el nuevo *Carrier* SIP.
 - Verificación de las herramientas de medidas de tráfico.
- Capacitación.
 - Capacitación del equipo *Session Border Controller*.
 - Capacitación de la nueva red VoIP instalada.
 - Capacitación de las provisiones y desprovisiones de los nuevos *Carrier* SIP en el equipo SBC y el *Softswitch*.

- Cierre Técnico.
 - Confirmar que todo lo ofrecido se ha entregado.
 - Elaboración del informe final de implantación para los superiores.
- Cierre Administrativo.
 - Revisión final de los gastos del proyecto.

Las figuras 4.1 y 4.2 muestran el tiempo de ejecución del proyecto en un diagrama de Gantt.

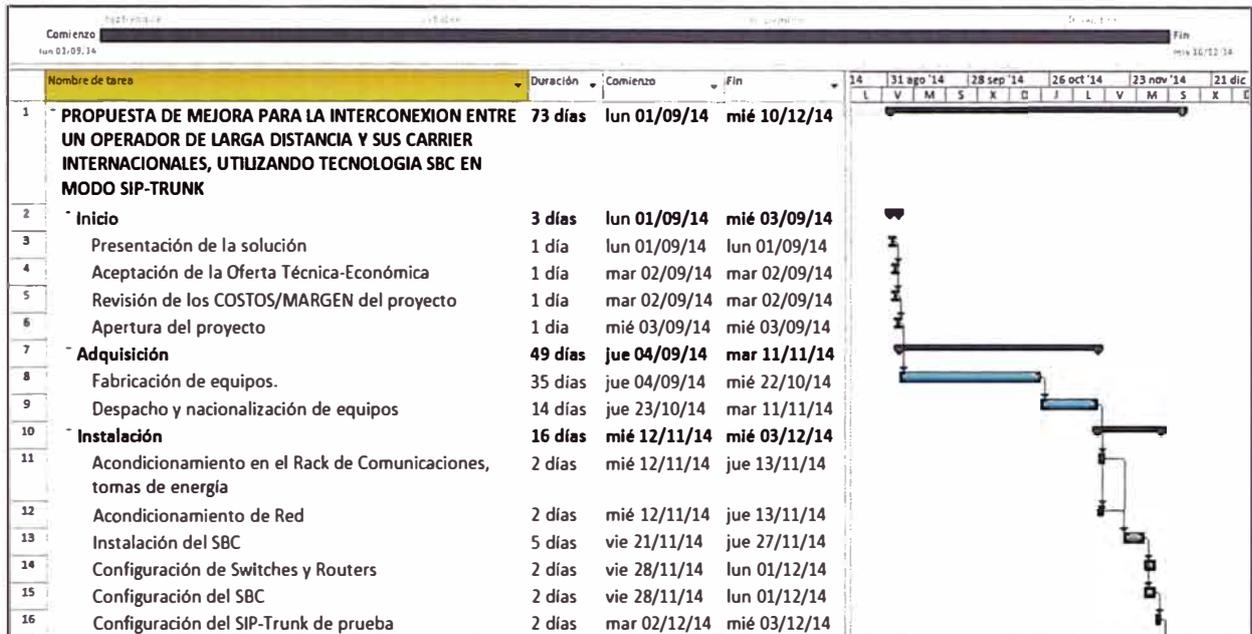


Figura 4.1 Diagrama de Gantt parte 1
(Fuente: Elaboración propia)

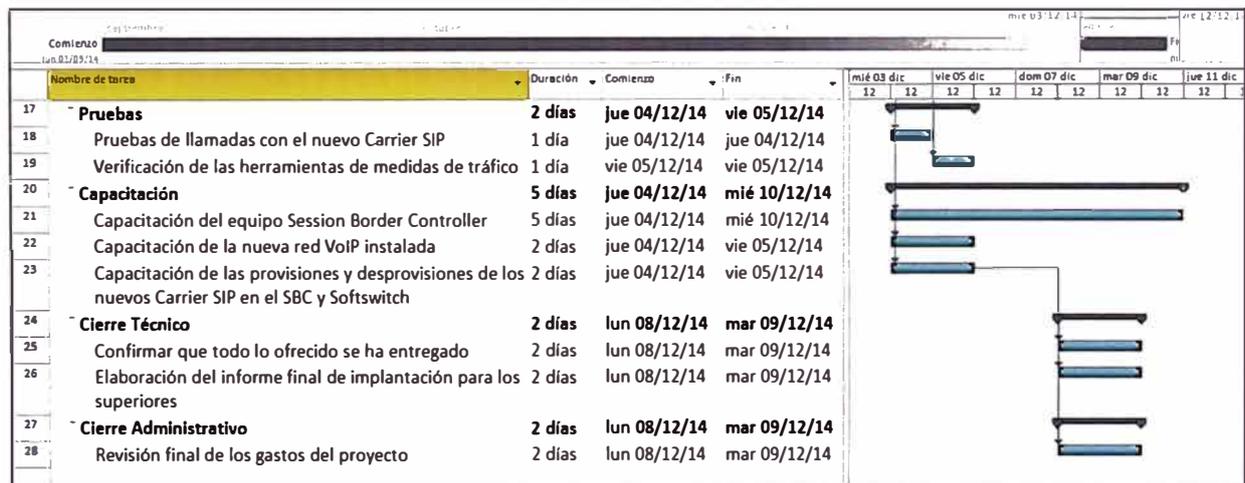


Figura 4.2 Diagrama de Gantt parte 2
(Fuente: Elaboración propia)

4.2 Estudio económico del Proyecto

Este apartado tiene como finalidad establecer la rentabilidad de la inversión en el proyecto a través de conceptos como CAPEX, OPEX, VAN y TIR.

4.2.1 Análisis de CAPEX y OPEX

CAPEX es la abreviatura de la expresión Inglés Capital Expenditure (en español, capex o

gastos de capital) y es la cantidad de dinero gastado en la adquisición (o mejora) de los bienes de capital de una empresa en particular. El CAPEX es por lo tanto la cantidad de inversiones en equipos e instalaciones con el fin de mantener la producción de un producto o servicio o para mantener funcionando un negocio o un sistema particular. En términos de contabilidad, un gasto se considera como CAPEX cuando el activo o la inversión realizada mejora la capacidad productiva o aumenta la vida útil de un activo productivo ya existente. Se refiere así a un gasto que será capitalizado en el activo, y será distribuido durante la vida útil del activo mediante su amortización.

Por el contrario, el OPEX, se refiere a los costos asociados con el mantenimiento de equipos y gastos de consumibles y otros gastos de funcionamiento necesarios para la producción y el funcionamiento del negocio o del sistema.

Por ejemplo, la compra de una máquina es CAPEX, mientras que el costo de mantenimiento es OPEX. Para el Proyecto se analiza cuáles son los Costos de Capital (CAPEX) y los Costos de Operación (OPEX).

a) Costo de Capital

En los Costos de Capital se ven involucrados los siguientes parámetros:

- Equipos
- Instalación de Equipos

El proyecto trata sobre la implementación de un equipo *Session Border Controller* para un Operador de Larga Distancia, para este caso el proveedor ya cuenta con el espacio donde instalará el equipo, con el acondicionamiento debido, los otros elementos de red (switches y *routers*), además de personal calificado (Ingenieros y técnicos que trabajan en la empresa Operadora de Larga Distancia).

El costo del proyecto representa el equipo SBC, es decir el costo que la empresa proveedora propondría por la venta e instalación del equipo además de las licencias y el soporte. En la figura 4.3 se muestra el cuadro de costos que está basado en una propuesta comercial de una empresa proveedora de Equipos *Session Border Controller* de la marca *Acme Packet*.

Se está cotizando un equipo SBC *Acme Packet* modelo Net-Net 3820, con licencia para 1000 llamadas simultáneas y un plan de soporte de un año.

Costo total del equipo es de **\$80,668.00**. Que para el proyecto es el mismo valor del Costo de Capital (CAPEX).

b) Costo de Operación

En los Costos de Operación se ven involucrados los siguientes parámetros:

- Planta Externa (mantenimiento de equipos)
- Consumo de Energía de los equipos.

CODIGO	DESCRIPCION	Unit Price US\$ - DDP - US	250 sessions - Etapa Inicial		Upgrade 250 to 350 sessions		Upgrade 350 to 500 sessions		Upgrade 500 to 1000 sessions	
			Qty	Extended Price	Qty	Extended Price	Qty	Extended Price	Qty	Extended Price
priceNN3820-SD-S.25-MSE4	Net-Net 3820 SD, up to 250 sessions	\$31,730.00	1	\$31,730.00						
NN3800-SD-BP-SHI-B	SIP w/software-based TLS, H.323 and SIP-H.323 interworking base protocol; QoS and accounting feature groups	\$0.00	1	\$0.00						
NN3820-PWR-DC	(-)48 volt DC power option (single supply)	\$0.00	1	\$0.00						
NN3820-O-PS-DC	300 watt DC power supply	\$1,058.00	1	\$1,058.00						
NN3800-SD-R-.25	Routing license - 250 session	\$1,210.00	1	\$1,210.00						
NN3800-SD-LB-.25	Load balancing license - 250 session system	\$1,210.00	1	\$1,210.00						
NN3800-SD-BP-SIP-C	Sip Base protocol	\$0.00	1	\$0.00						
NN3800-SD-UP-S-.25-.35	Session license upgrade from 250 to 350 sessions	\$3,910.00			1	\$3,910.00				
NN3800-SD-UP-R-.25-.35	Routing license upgrade from 250 to 350 sessions	\$108.00			1	\$108.00				
NN3800-SD-UP-LB-.25-.35	Load balancing license upgrade from 250 to 350 sessions	\$108.00			1	\$108.00				
NN3800-SD-UP-S-.35-.5	Session license upgrade from 350 to 500 sessions	\$2,700.00					1	\$2,700.00		
NN3800-SD-UP-R-.35-.5	Routing license upgrade from 350 to 500 sessions	\$194.00					1	\$194.00		
NN3800-SD-UP-LB-.35-.5	Load balancing license upgrade from 350 to 500 sessions	\$194.00					1	\$194.00		
NN3800-SD-UP-S-.5-1	Session license upgrade from 500 to 1000 sessions	\$14,569.00							1	\$14,569.00
NN3800-SD-UP-R-.5-1	Routing license upgrade from 500 to 1000 sessions	\$1,890.00							1	\$1,890.00
NN3800-SD-UP-LB-.5-1	Load balancing license upgrade from 500 to 1000 sessions	\$1,890.00							1	\$1,890.00
	648Subtotal system Net Price			\$35,208.00		\$4,126.00		\$3,088.00		\$18,349.00
SER-STD	Standard service support plan - 1 Subtotal Support Year 1		1	\$6,760.00	1	\$842.00	1	\$630.00	1	\$3,743.00
				\$6,760.00		\$842.00		\$630.00		\$3,743.00
SER-INST-D	Installation - 8 hours - during business day (including T&E)	\$2,934.00	3	\$7,922.00						
	Subtotal Installation			\$7,922.00						
GRAN TOTAL				\$49,890.00		\$4,968.00		\$3,718.00		\$22,092.00

Figura 4.3 Costo del Equipo SBC Acme Packet Net-Net 3820
(Fuente: Itelecom)

4.2.2 Evaluación económica del Proyecto

Existen dos parámetros muy usados si se requiere calcular la viabilidad de un proyecto y estos son el VAN (Valor Actual Neto) y el TIR (Tasa Interna de Retorno). Ambos conceptos se basan en lo mismo, y es la estimación de los flujos de caja que tenga la empresa (simplificando, ingresos menos gastos netos).

En este punto se va a sustentar que el proyecto es viable y tiene un retorno de inversión en 10 meses; para esto se debe proyectar el flujo de caja mensual de la empresa Operadora para luego obtener el VAN el cual debe generar un resultado positivo.

a) El VAN y el TIR

El VAN es un indicador financiero que mide los flujos de los futuros ingresos y egresos que tendrá un proyecto, para determinar, si luego de descontar la inversión inicial, quedaría alguna ganancia. Si el resultado es positivo, el proyecto es viable.

Basta con hallar VAN de un proyecto de inversión para saber si dicho proyecto es viable

o no. El VAN también permite determinar cuál proyecto es el más rentable entre varias opciones de inversión.

La fórmula del VAN es:

$$VAN = BNA - Inversión \quad (4.1)$$

Donde BNA es el valor actual del flujo de caja o beneficio neto proyectado, el cual se ha actualizado a través de una tasa de descuento.

La tasa de descuento (TD) con la que se descuenta el flujo neto proyectado, es el la tasa de oportunidad, rendimiento o rentabilidad mínima, que se espera ganar; por lo tanto, cuando la inversión resulta mayor que el BNA (VAN negativo o menor que 0) es porque no se ha satisfecho dicha tasa. Cuando el BNA es igual a la inversión (VAN igual a 0) es porque se ha cumplido con dicha tasa. Y cuando el BNA es mayor que la inversión es porque se ha cumplido con dicha tasa y además, se ha generado una ganancia o beneficio adicional.

$VAN > 0 \rightarrow$ el proyecto es rentable.

$VAN = 0 \rightarrow$ el proyecto es rentable también, porque ya está incorporado ganancia de la TD.

$VAN < 0 \rightarrow$ el proyecto no es rentable.

Entonces para hallar el VAN se necesitan:

- Tamaño de la inversión.
- Flujo de caja neto proyectado.
- Tasa de descuento.

El BNA se calcularía con la siguiente fórmula:

$$BNA = \sum_{n=1}^N \frac{Q_n}{(1+r)^n} \quad (4.2)$$

Donde Q_n es el flujo de caja del mes n , r es la tasa de interés con la que se está comparando (TD) y N son los meses de inversión.

Entonces la fórmula de VAN que utilizará es la siguiente:

$$VAN = I - \sum_{n=1}^N \frac{Q_n}{(1+r)^n} \quad (4.3)$$

La TIR es la tasa de descuento (TD) de un proyecto de inversión que permite que el BNA sea igual a la inversión (VAN igual a 0). La TIR es la máxima TD que puede tener un proyecto para que sea rentable, pues una mayor tasa ocasionaría que el BNA sea menor que la inversión (VAN menor que 0).

b) Cálculo del VAN y el TIR en el proyecto

Para hallar el VAN se necesita el tamaño de la inversión, el flujo de caja neto proyectado y la tasa de descuento. En el apartado 4.2 se determinó el tamaño de la inversión que es

de \$80,668.00. La tasa de descuento normal que se usa es 12% o 1% mensual. Faltaría identificar el flujo de caja proyectado.

A continuación se determinará el flujo de caja proyectado, para esto se consideran los siguientes puntos:

- i) En el proyecto se implementa una solución para interconexiones SIP-*Trunk* entre un Operador de Telecomunicaciones y sus *Carriers* internacionales. Desarrollar la solución le permitirá al Operador añadir a su cartera a nuevos clientes, *Carrier* por protocolo SIP-*Trunk*, a estos *Carriers* se le facturará por el tráfico de llamadas que le entreguen al Operador, este tráfico de llamadas puede ser a fijos (Lima o provincias) o móviles.
- ii) El equipo SBC que se instalará en este proyecto presenta una capacidad de 1000 sesiones simultáneas, es decir que todos los *Carrier* que se interconecten a él realizarán en conjunto 1000 llamadas simultáneas.
- iii) Para proyectar el flujo de caja se estima que una vez ejecutado el proyecto se generaran acuerdos comerciales con 3 *Carrier* de 100 sesiones cada uno; por supuesto que con el correr de los meses los acuerdos comerciales deben ir aumentando, ya sea aumento de los *Carriers* o aumento de la cantidad de sesiones de los mismos. La tabla 4.1 muestra la proyección de la cantidad de sesiones que le Operador de Larga Distancia tendrá con los *Carrier* Internacionales.

Tabla 4.1 Proyección de cantidad de sesiones en el SBC vs tiempo
(Fuente: Elaboración Propia)

Meses	Proyección de cantidad de Sesiones de todos los <i>Carriers</i>
Enero 2015	300
Febrero 2015	300
Marzo 2015	300
Abril 2015	500
Mayo 2015	500
Junio 2015	500
Julio 2015	700
Agosto 2015	700
Septiembre 2015	700
Octubre 2015	800

- iv) El Operador de larga Distancia factura al *Carrier* por el tráfico de llamadas que recibe de él, pero éste tráfico, a su vez, es entregado a otros operadores locales y el

Operador debe pagar por eso, la diferencia de estos dos valores es lo que el Operador gana por minuto. La tabla 4.2 muestra las tarifas que el Operador de Larga Distancia factura al *Carrier* y paga al Operador Local.

Tabla 4.2 Ingreso del Operador por minuto para diferentes destinos de Perú
(Fuente: Americatel Perú SAC)

Destinos		Se le cobra al <i>Carrier</i> (por minuto)	Se le paga al Operador (por minuto)	Diferencia
Llamadas a fijos	Lima	\$0.009200	\$0.008270	\$0.000930
	Provincia	\$0.009300	\$0.008260	\$0.001040
Llamadas a móviles	Claro	\$0.050000	\$0.047630	\$0.002370
	Movistar	\$0.065000	\$0.047311	\$0.017689
	Nextel	\$0.065000	\$0.032530	\$0.032470

- v) También se necesita saber cuánto trafica un *Carrier* en promedio, la tabla 4.3 muestra el promedio mensual del tráfico de llamadas de un *Carrier* cuya interconexión tiene 100 sesiones de capacidad.

Tabla 4.3 Promedio de tráfico de llamadas mensual de un *Carrier*
(Fuente: Elaboración Propia)

Destinos		Tráfico de llamadas mensual de un <i>Carrier</i> de 100 sesiones de capacidad (minutos)
Llamadas a fijos	Lima	1553500
	Provincia	500
Llamadas a móviles	Claro	26482
	Movistar	25355
	Nextel	45078

- vi) De las tablas 4.2 y 4.3 se obtiene el promedio de la ganancia mensual por una interconexión de 100 sesiones de capacidad. Se muestra en la tabla 4.4.

Tabla 4.4 Ganancia mensual de un *Carrier* de 100 sesiones de capacidad
(Fuente: Elaboración Propia)

Destinos		Ganancia por minuto	Tráfico de llamadas mensual de un <i>Carrier</i> de 100 sesiones (minutos)	Ganancia Mensual de un <i>Carrier</i> de 100 sesiones
Llamadas a fijos	Lima	\$0.000930	1553500	\$1,444.76
	Provincia	\$0.001040	500	\$0.52
Llamadas a	Claro	\$0.002370	26482	\$62.76

móviles	Movistar	\$0.017689	25355	\$448.49
	Nextel	\$0.032470	45078	\$1,463.68
TOTAL MENSUAL				\$3,420.21

vii) De las tablas 4.1 y 4.4 se obtiene la proyección del flujo mensual de caja del Proyecto. Se muestra en la tabla 4.5.

Tabla 4.5 Flujo de caja mensual del Proyecto
(Fuente: Elaboración Propia)

Meses	Proyección de cantidad de Sesiones de todos los <i>Carrier</i>	Ganancia Mensual por Interconexión de 100 sesiones	Proyección de la ganancia mensual
Enero 2015	300	\$3,420	\$10,260
Febrero 2015	300	\$3,420	\$10,260
Marzo 2015	300	\$3,420	\$10,260
Abril 2015	500	\$3,420	\$17,100
Mayo 2015	500	\$3,420	\$17,100
Junio 2015	500	\$3,420	\$17,100
Julio 2015	700	\$3,420	\$23,940
Agosto 2015	700	\$3,420	\$23,940
Septiembre 2015	700	\$3,420	\$23,940
Octubre 2015	800	\$3,420	\$27,360

Calcular el VAN del proyecto:

- Tamaño de la inversión = \$80,668.00
- Tasa de descuento = 1% mensual
- Flujo de caja neto proyectado:

Tabla 4.6 Flujo de caja mensual del Proyecto
(Fuente: Elaboración Propia)

Meses	n	Q
Enero 2015	1	\$10,260
Febrero 2015	2	\$10,260
Marzo 2015	3	\$10,260
Abril 2015	4	\$17,100
Mayo 2015	5	\$17,100
Junio 2015	6	\$17,100
Julio 2015	7	\$23,940
Agosto 2015	8	\$23,940

Septiembre 2015	9	\$23,940
Octubre 2015	10	\$27,360
		\$181,260

- Formula:

$$VAN = I - \sum_{n=1}^N \frac{Q_n}{(1+r)^n} \quad (4.3)$$

El beneficio neto nominal es de \$181,260 y la utilidad lógica es \$100,592 (\$181,260 - \$80,668.00), pero este beneficio o ganancia no es real (sólo nominal) porque no se está considerando el valor del dinero en el tiempo, por lo que cada periodo debe actualizarse a través de una tasa de descuento (tasa de rentabilidad mínima que se espera ganar).

De la formula se calcula el VAN y es igual a:

VAN = \$89,414 (es un valor positivo, proyecto viable)

De igual forma se calcula el TIR y su valor es igual a:

TIR = 15% mensual

CONCLUSIONES Y RECOMENDACIONES

Del proyecto se obtienen las siguientes conclusiones:

- 1.- En el proyecto se detallan las múltiples ventajas que tiene sobre otros protocolos (como el protocolo SS7), por lo tanto se concluye que es la mejor opción a escoger para la implementación de la interconexión que se está proponiendo.
- 2.- Se explica conceptualmente como el sistema de interconexiones por troncales de telefonía, están evolucionando a troncales SIP y una de las soluciones más seguras y viables es mediante de los equipos SBC, por lo tanto se concluye que el presente proyecto es un proyecto que está a la vanguardia de las tecnologías actuales.
- 3.- El nicho de mercado para este proyecto son los nuevos *Carriers* con los que el Operador de Larga Distancia establecerá negocio una vez implementada la interconexión SIP-*Trunk*. Se concluye que el presente proyecto tiene un nicho de mercado definido.
- 4.- La condición que se toma en cuenta para aceptar o rechazar la inversión es que el valor del VAN sea positivo. El proyecto tiene un cálculo de VAN positivo, por lo tanto es un proyecto viable.
- 5.- Los cálculos para la evaluación económica del Proyecto se hicieron con unidad de tiempo mensual para un periodo de 10 meses, se justifica con las variables económicas que hay un retorno de inversión por lo que se concluye que se trata de un proyecto rentable que generará ganancias en menos de un año.

Para el proyecto se dan las siguientes recomendaciones:

- 1.- Se recomienda, para la problemática del Operador en este proyecto, la migración de sus actuales troncales IP (con protocolo H.323) a la nueva solución SIP-*Trunk* y luego diseñar una estrategia para ir captando nuevos clientes (*Carrier*), pues con esta implementación queda abierta una nueva ventana para los negocios con *Carriers* internacionales.
- 2.- El equipo SBC 3820 del proyecto fue propuesto con una capacidad de 1000 sesiones, pero puede extenderse a 2000, 4000 o hasta 8000 sesiones. Se recomienda continuar la búsqueda de negocios con nuevos *Carrier* y seguir explotando las capacidades del equipo SBC.
- 3.- Se recomienda la posterior inversión en un equipo backup para garantizar la calidad del servicio.
- 4.- Se recomienda analizar la posibilidad de incorporar el equipo SBC a la infraestructura de la red NGN del Operador de telefonía, con el fin de brindar mayor seguridad a la red NGN.

BIBLIOGRAFÍA

- [1] Trans-European Research and Education Networking Association – TERENA “IP Telephony cookbook” Marzo 2004.
- [2] Uyles Black “Voice over IP” – 1999.
- [3] SIPPING Working “Group Requirements from Session Initiation *Protocol* (SIP) Session Border” - draft-ietf-sipping-sbc-funcs-09.txt - Febrero 18, 2010.
- [4] SIPPING Working “What is a Session Initiation *Protocol* (SIP) *Trunk* Anyway?”- Draft-rosenberg-sipping-siptrunk-00.txt - Febrero 15, 2010
- [5] Huawei Technologies, <http://www.huawei.com>, *Carrier Network*, 2014.
- [6] *Acme Packet* Page, <http://www.acmepacket.com>
- [7] *Acme Packet* Support, <https://support.acmepacket.com/>, “acme-packet-3820-ds-1990147.pdf”
- [8] Manual de instalación *Acme Packet* 3820,
http://docs.oracle.com/cd/E50394_01/doc/acmepacket3820_installation.pdf
- [9] Manual de configuración *Acme Packet* 3000/4000,
http://community.acmepacket.com/acmepacket/attachments/acmepacket/ops/1498/1/PartnerConfigGuide_Acme_Packet_Net-Net_3000-4000_Series%20R18.pdf
- [10] Propuesta comercial *Acme Packet* 3000/4000, <http://www.itelecom.cl>
- [11] Roscoe Davis, *Contabilidad Financiera* ,1998.
- [12] Jonh A. Tracy, *Fundamentos de Contabilidad* 1999.

ANEXO A
DATOS DE CONFIGURACIÓN DEL SBC ACME PACKET

- PHY-interface

```

SBCSUR01A(configure)# system
SBCSUR01A(system)# phy-interface
SBCSUR01A(phy-interface)# select
<name>:
1: M00
2: M10

selection: 1
SBCSUR01A(phy-interface)# show
phy-interface
  name           M00
  operation-type  Media
  port           0
  slot           0
  virtual-mac
  admin-state    enabled
  auto-negotiation  enabled
  duplex-mode    FULL
  speed          100
  overload-protection  disabled
  last-modified-by  admin@200.31.103.59
  last-modified-date 2012-06-25 20:12:33

selection: 2
SBCSUR01A(phy-interface)# show
phy-interface
  name           M10
  operation-type  Media
  port           0
  slot           1
  virtual-mac
  admin-state    enabled
  auto-negotiation  enabled
  duplex-mode    FULL
  speed          100
  overload-protection  disabled
  last-modified-by  admin@200.31.103.59
  last-modified-date 2012-06-25 20:13:37

```

- Network-interface

```

SBCSUR01A(system)# network-interface
SBCSUR01A(network-interface)# select
<name>:<sub-port-id>:
1: M00:0 ip=200.31.108.34 gw=200.31.108.33
2: M10:0 ip=10.0.0.2 gw=10.0.0.1

selection: 1
SBCSUR01A(network-interface)# show
network-interface
  name           M00
  sub-port-id    0
  description    Access for Peers
  hostname
  ip-address     200.31.108.34
  pri-utility-addr
  sec-utility-addr
  netmask        255.255.255.248
  gateway        200.31.108.33

  last-modified-by  admin@181.65.2.23
  last-modified-date 2012-12-07 19:11:27

selection: 2
SBCSUR01A(network-interface)# show
network-interface
  name           M10
  sub-port-id    0
  description    Network Interface Core
  hostname
  ip-address     10.0.0.2
  pri-utility-addr
  sec-utility-addr
  netmask        255.255.254.0
  gateway        10.0.0.1
  last-modified-by  admin@172.16.129.144
  last-modified-date 2012-12-17 12:25:27

```

- Media manager

```

SBCSUR01A# configure terminal
SBCSUR01A(configure)# media-manager
SBCSUR01A(media-manager)# media-manager
SBCSUR01A(media-manager-config)# select
SBCSUR01A(media-manager-config)# show
media-manager
  state                enabled
  latching              enabled-----El SBC escucha el primer paquete
  flow-time-limit       86400                RTP y desde ahí solo deja pasar
  ---                                     RTP del mismo origen
  media-policing        enabled
  max-signaling-bandwidth 1041040
  max-untrusted-signaling 1
  min-untrusted-signaling 1
  app-signaling-bandwidth 0
  tolerance-window      30
  rtcp-rate-limit       0
  ---
  last-modified-by      admin@10.10.1.187
  last-modified-date    2012-08-16 15:53:51

```

- SIP config

```

SBCSUR01A(configure)# session-router
SBCSUR01A(session-router)# sip-cobn
SBCSUR01A(session-router)# sip-config
SBCSUR01A(sip-config)# sel
SBCSUR01A(sip-config)# show
sip-config
  state                enabled -----SIP activado
  operation-mode        dialog-----Control sobre todas las sesión
  dialog-transparency   enabled----- Oculta topología
  refer-src-routing     disabled
  add-ucid-header       disabled
  proxy-sub-events      disabled
  pass-gruu-contact     disabled
  sag-lookup-on-redirect disabled
  set-disconnect-time-on-bye disabled
  last-modified-by      admin@172.16.129.144
  last-modified-date    2012-11-19 15:19:11

```

- Realm padre Peer

realm-config	
identifier	peers_SBC
description	Parent Realm for Peers
addr-prefix	0.0.0.0
network-interfaces	
	M00:0 -----Nateo para headers From y To
parent-realm	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	ACME_NAT_TO_FROM_IP
access-control-trust-level	high
hide-egress-media-update	disabled
last-modified-by	admin@10.10.1.187
last-modified-date	2012-08-16 12:46:36

- Realm padre Core

realm-config	
identifier	core_SBC
description	Parent Realm for Core
addr-prefix	0.0.0.0
network-interfaces	
	M10:0 -----Nateo para headers From y To
parent-realm	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	ACME_NAT_TO_FROM_IP
access-control-trust-level	high
hide-egress-media-update	disabled
last-modified-by	admin@172.16.129.124
last-modified-date	2012-08-20 11:37:12

- Steering-pool Realm padre

```

SBCSUR01A(steering-pool)# show
steering-pool
  ip-address          200.31.108.34
  start-port          10000 -----IP y puertos habilitados para
  end-port            19999                       tráfico RTP en los peer realms
  realm-id            peers_SBC
  network-interface   M00:0
  last-modified-by    admin@172.16.129.124
  last-modified-date  2012-08-20 11:14:25

SBCSUR01A(steering-pool)# show
steering-pool
  ip-address          10.0.0.2
  start-port          10000 -----IP y puertos habilitados para
  end-port            19999                       tráfico RTP en los core realms
  realm-id            core_SBC
  network-interface   M10:0
  last-modified-by    admin@172.16.129.124
  last-modified-date  2012-08-20 11:41:07

```

- SIP-interface Realm padre

```

SBCSUR01A(configure)# session-router
SBCSUR01A(session-router)# sip-interface
SBCSUR01A(sip-interface)# select
<realm-id>:
  1: peers_SBC          200.31.108.34:5060
      -----
  20: core_broadband    10.0.0.21:5060
  21: core_crossfone_usa 10.0.0.22:5060
selection: 1
SBCSUR01A(sip-interface)# show
sip-interface
  state          enabled
  realm-id       peers_SBC
  description     Sip-interf for Peers SBC
  sip-port
    address       200.31.108.34 -----SIP interface hacia los Carriers
    port          5060
    transport-protocol UDP
    tls-profile
  allow-anonymous agents-only --Solo permite llamadas de session agent
  Carriers
      -----
  last-modified-by    admin@172.16.129.144
  last-modified-date  2012-10-04 12:11:51

```

- Comandos esenciales

```
SBCSUR01A# show sipd sessions  
SBCSUR01A# verify-config  
SBCSUR01A# save-config  
SBCSUR01A# activate-config  
SBCSUR01A(license)# show
```



Equipos SBC 3820 SA

CODIGO	DESCRIPCION	Unit Price US\$ - DDP - US	250 sessions - Etapa Inicial		Upgrade 250 to 350 sessions		Upgrade 350 to 500 sessions		Upgrade 500 to 1000 sessions		Upgrade 1000 to 2000 sessions		Upgrade 2000 to 4000 sessions		Upgrade 4000 to 8000 sessions	
			Qty	Extended price	Qty	Extended price	Qty	Extended price	Qty	Extended price	Qty	Extended price	Qty	Extended price	Qty	Extended price
NN3820-SD-S-25-MSE4	Net-Net 3820 SD, up to 250 sessions	\$31.730	1	\$31.730												
NN3800-SD-BP-SHI-B	SIP w/software-based TLS, H.323 and SIP-H.323 Interworking base protocol; QoS and accounting feature groups	\$0	1	\$0												
NN3820-PWR-DC	-48 volt DC power option (single supply)	\$0	1	\$0												
NN3820-O-PS-DC	300 watt DC power supply	\$1.058	1	\$1.058												
NN3800-SD-R-25	Routing license - 250 session system	\$1.210	1	\$1.210												
NN3800-SD-LB-25	Load balancing license - 250 session system	\$1.210	1	\$1.210												
NN3800-SD-BP-SIP-C	Slp Base protocol	\$0	1	\$0												
NN3800-SD-UP-S-.25-.35	Session license upgrade from 250 to 350 sessions	\$3.910			1	\$3.910										
NN3800-SD-UP-R-.25-.35	Routing license upgrade from 250 to 350 sessions	\$108			1	\$108										
NN3800-SD-UP-LB-.25-.35	Load balancing license upgrade from 250 to 350 sessions	\$108			1	\$108										
NN3800-SD-UP-S-.35-.5	Session license upgrade from 350 to 500 sessions	\$2.700					1	\$2.700								
NN3800-SD-UP-R-.35-.5	Routing license upgrade from 350 to 500 sessions	\$194					1	\$194								
NN3800-SD-UP-LB-.35-.5	Load balancing license upgrade from 350 to 500 sessions	\$194					1	\$194								
NN3800-SD-UP-S-.5-1	Session license upgrade from 500 to 1000 sessions	\$14.569							1	\$14.569						
NN3800-SD-UP-R-.5-1	Routing license upgrade from 500 to 1000 sessions	\$1.890							1	\$1.890						
NN3800-SD-UP-LB-.5-1	Load balancing license upgrade from 500 to 1000 sessions	\$1.890							1	\$1.890						
NN3800-SD-UP-S-1-2	Session license upgrade from 1000 to 2000 sessions	\$25.326									1	\$25.326				
NN3800-SD-UP-R-1-2	Routing license upgrade from 1000 to 2000 sessions	\$648									1	\$648				
NN3800-SD-UP-LB-1-2	Load balancing license upgrade from 1000 to 2000 sessions	\$648									1	\$648				
NN3800-SD-UP-S-2-4	Session license upgrade from 2000 to 4000 sessions	\$27.702											1	\$27.702		
NN3800-SD-UP-R-2-4	Routing license upgrade from 2000 to 4000 sessions	\$648											1	\$648		
NN3800-SD-UP-LB-2-4	Load balancing license upgrade from 2000 to 4000 sessions	\$648											1	\$648		
NN3800-SD-UP-S-4-8-HA	Session license upgrade from 4000 to 8000 sessions	\$15.417													1	\$15.417
NN3800-SD-UP-R-4-8-HA	Routing license upgrade from 4000 to 8000 sessions	\$648													1	\$648
NN3800-SD-UP-LB-4-8	Load balancing license upgrade from 4000 to 8000 sessions	\$648													1	\$648
	Subtotal system Net Price			\$35.208		\$4.126		\$3.089		\$18.349		\$26.622		\$28.998		\$16.713
SER-STD	Standard service support plan - 1 Year		1	\$6.760	1	\$842	1	\$630	1	\$3.743	1	\$5.430,89	1	\$5.916	1	\$3.409
	Subtotal Support Year 1			\$6.760		\$842		\$630		\$3.743		\$5.431		\$5.916		\$3.409
SER-INST-D	Installation - 8 hours - during business day (including T&E)	\$2.934	3	\$7.922												
	Subtotal Installation			\$7.922												
GRAN TOTAL				\$49.890		\$4.967		\$3.719		\$22.092		\$32.053		\$34.914		\$20.122

Monseñor Solero Sanz #100 Of. 501
 Providencia - Santiago, Chile
 Teléfono: (56-2) 5958700
 Fax: (56-2) 5958713
<http://www.itelecom.cl>

PROPUESTA COMERCIAL - SBC ACME PACKET

ANEXO B