ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“DEMOSTRACIÓN DE LOS BENEFICIOS DE UN EQUIPO SESSION BORDER CONTROLLER EN LA INTEGRACIÓN DE TELEFONÍA CORPORATIVA CON REDES DE TELEFONÍA FIJA Y MÓVIL”

EXAMEN DE GRADO

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN TELECOMUNICACIONES

VÍCTOR HUGO PEZO ORTIZ

GUAYAQUIL – ECUADOR

AÑO: 2020

AGRADECIMIENTO

A Dios, por guiarme en cada paso de mi vida, y lograr alcanzar este objetivo propuesto que implica un mejoramiento profesional y a su vez el desarrollo de nuestra sociedad del conocimiento.

A la ESPOL, por ser centro de alto impacto a la sociedad por medio de la educación.

A los profesores, por brindarnos sus mejores conocimientos, capacidad y tiempo en este camino de aprendizaje

DEDICATORIA

A mi esposa, mi hija y a mi madre, por ser mi fortaleza en este camino de preparación profesional.

A mi hermana y a mis sobrinos, pues siento su cariño, a pesar de la distancia.

A mi padre, que me inspiró a iniciar este reto.

TRIBUNAL DE EVALUACIÓN

MSc. Jorge Brito

PROFESOR EVALUADOR

PhD. María Antonieta Álvarez

PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Ing. Víctor Hugo Pezo

RESUMEN

La presente propuesta busca demostrar como los equipos Session Border Controller, son cada vez más necesarios dentro de las implementaciones de servicio y de integración entre las redes de clientes corporativos y los proveedores de telefonía fija y móvil.

En el mercado de soluciones de telefonía existen un gran número de fabricantes de centrales y soluciones de call center, que concentran sus servicios en las capas de aplicación, brindando facilidades del negocio explícito, para lo cual fueron diseñadas y adquiridas por las empresas. Sin embargo, a nivel de capas de enlace, red, transporte y sesión, no manejan una gran cantidad de opciones que permitan interconectar diferentes tecnologías, manejar diferentes interfases, manipular mensajes de protocolos, así como atender problemas de seguridad, que no pueden de ninguna manera ser descuidados en la actualidad.

En este documento, analizaremos estos diferentes escenarios, en donde el Session Border Controller, se presenta como una necesidad que permite interconectar las redes de clientes y proveedores, brindando un mejor tiempo de implementación y una mejor experiencia de servicio a los clientes corporativos finales.

INDICE GENERAL

INDICE DE FIGURAS

CAPÍTULO 1

1. INTRODUCCION

1.1 Descripción de problema

Los clientes corporativos de telefonía presentan estructuras de red IP que necesitan tener conectividad a las Redes Públicas de Telefonía Conmutada (PSTN) y a los Sistemas de Telefonía Móvil Pública (PLMN), y así obtener los beneficios de los servicios ofertados por los proveedores fijos y móviles. Es aquí, en esta integración de diferentes tipos de interfase y en las capacidades limitadas de configuración del software del lado de los clientes, que se presenta la necesidad de implementar una solución que permita manejar la interoperabilidad de estas redes que integran cliente y proveedor.

Estos escenarios, como son el traslape de redes, manipulación de cabeceras, conversión de protocolos y soluciones de seguridad, conllevan a pérdidas de ingreso tanto para el proveedor como al propio cliente, que percibe principalmente altos tiempos de implementación como problemas en la calidad del servicio ofertado.

1.2 Propuesta

Debido al gran despliegue de las redes de telefonía SIP, los Session Border Controller, son equipos que han dejado de ser sólo utilizados en la interconexión de proveedores de telefonía tanto de sistemas de telefonía fijos como móviles. Estos ahora son colocados como punto de demarcación de redes de telefonía en la red de acceso del proveedor, atendiendo a clientes de forma segmentada, y a su vez, también en la premisa del cliente. Con esta propuesta queremos mostrar los diseños que permiten resolver los problemas más frecuentes en la interoperabilidad de troncales de telefonía IP, como son, el traslape de redes, manipulación de cabeceras de paquetes de telefonía SIP, traductor de interfases y soporte a la seguridad en el tráfico entre el cliente y los proveedores.

1.3 Objetivos

1.3.1 Objetivo general

Demostrar que un SBC se convierte en un aliado indispensable en la resolución de problemas de interoperabilidad de las redes de telefonía de clientes y proveedores.

1.3.2 Objetivo específico

- Revisar cómo los SBC permiten separar los segmentos de red de telefonía tanto del proveedor como del cliente.
- Analizar los escenarios en los que es necesario la manipulación de cabeceras.
- Mostrar cómo el SBC puede servir de traductor de interfases físicas, así como de protocolos de señalización.
- Enseñar cómo los SBC brinda servicios de seguridad a la red de telefonía.

1.4 Marco teórico

1.4.1 Telefonía IP

La telefonía IP consiste en transmitir voz sobre el protocolo IP. Este es el que se maneja regularmente en las redes que manejamos día a día, a través de los servicios de internet, y aplicaciones que usamos como usuarios residenciales, así como también a nivel de pequeñas, medianas y grandes empresas.

Este tipo de redes no fue diseñado inicialmente para la voz, por lo que la calidad, siempre fue un problema. Sin embargo, la evolución de la tecnología ha ayudado a que estos problemas se hayan podido manejar y superar satisfactoriamente [1].

La telefonía IP usa en su mayoría UDP para su tráfico de voz, por lo que no establece una conexión previamente ni un control de flujo, haciendo que su tráfico pueda ser asincrónico y sin confirmación de que haya llegado a su destino [2].

Los protocolos involucrados en la telefonía IP se pueden clasificar en tres grupos: señalización, transporte de media y plataforma de transporte e IP.

Los protocolos de señalización se manejan en la capa cinco del modelo OSI, es decir, en la capa de sesión. Entre los más conocidos, se encuentran: SIP, IAX, H.323, MGCP y SCCP.

Los protocolos de transporte de voz o media se manejan de igual forma en la capa cinco del modelo OSI y principalmente se utilizan para el inicio de sesión, control y terminación de sesiones.

Los protocolos que se manejan en plataforma de transporte e IP son los encargados de transportar a través de TCP, UDP e IP los paquetes SIP, RTP, SDP y RTCP utilizados en el transporte de la información. De estos protocolos se utiliza los servicios de multiplexación proporcionados por UDP. RTP no garantiza la fiabilidad del servicio, ni ayuda al control de congestión, sin embargo, sí permite que la información sea descifrada en el punto final [3].

En la figura 1.1 se observan los protocolos principales que intervienen en el tráfico de telefonía IP.

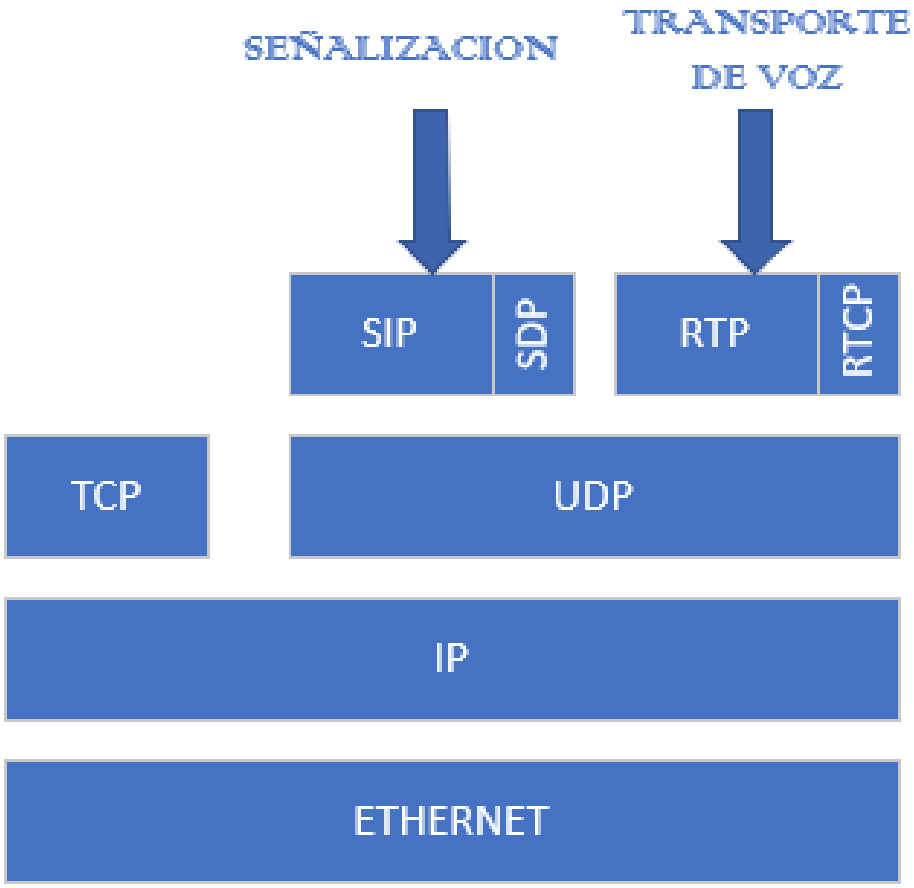


Figura 1.1 Protocolos telefonía IP

1.4.2 Protocolo SIP

El protocolo SIP usa métodos y respuestas para manejar las transacciones de una llamada. Los métodos son,

- INVITE, se genera la invitación a iniciar una transacción.
- ACK, permite manejar un reconocimiento de respuesta al anterior evento.
- BYE, termina una conexión establecida.
- CANCEL, finaliza un requerimiento.

- OPTIONS, maneja la información del servidor SIP.
- REGISTER, muestra la ubicación de un usuario.
- INFO, maneja información adicional de la transacción.

Las respuestas pueden ser,

- 1xx, con características de brindar información, como Trying, Ringing.
- 2xx, con información de éxito en la transacción, 202 Accepted.
- 3xx, maneja mensajes de redirección de requerimientos, 302 Moved Temporarily.
- 4xx, reporta problemas en la transacción, como 404 Not Found.
- 5xx, maneja errores de servidor, 501 Not Implemented.
- 6xx, errores globales como 603 Decline.

En la figura 1.2 se puede observar el registro, establecimiento y finalización de una llamada.

- Se observa que los dos dispositivos se registran contra la central IP.
- Luego, reciben confirmación, OK.
- Uno de los dos dispositivos genera una llamada, por lo tanto, un INVITE, que es confirmado a través de un TRYING. De igual forma, del otro lado de la central, se manejan los mismos mensajes.
- Luego vemos un RINGING por parte del abonado B, y a su vez es comunicado al abonado A.
- Se genera un OK desde el abonado B, teniendo luego un ACK de regreso.
- Es aquí, donde comienza el tráfico de voz o media.
- Finalmente, uno de los dos abonados genera un BYE, y comienza el proceso de finalización de la llamada.
- Como último paso, se devuelve un ACK.

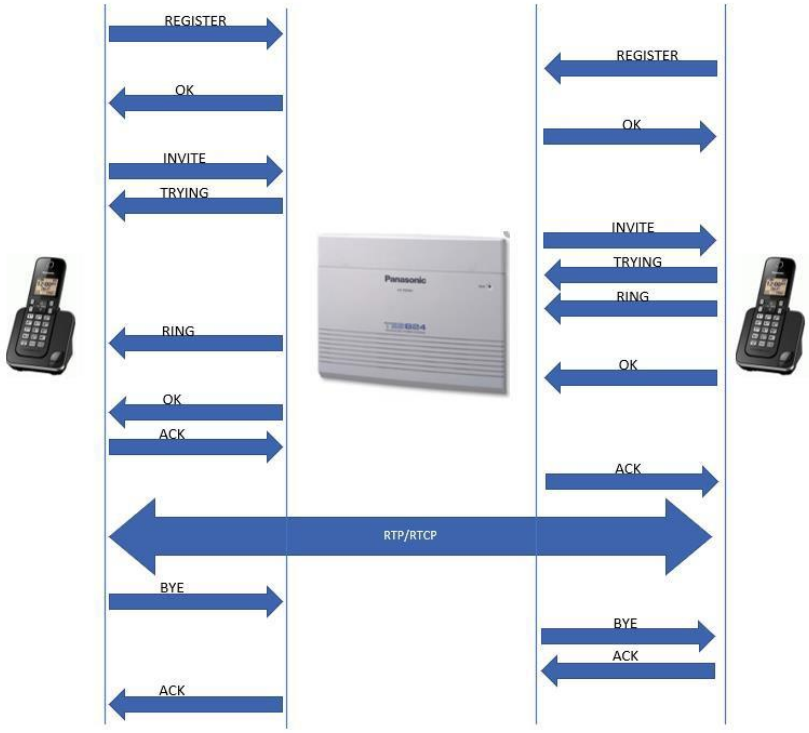


Figura 1.2 Registro, establecimiento y finalización de una llamada

1.4.3 NGN e IMS

NGN es una red de telefonía definida en los años 90 y que se desarrolló en una integración horizontal, de tal manera que el acceso, control y los servicios estén separados en capas de acuerdo con protocolos específicos o APIs.

NGN maneja una arquitectura flexible y permite al operador aumentar la productividad creando nuevos servicios multimedia basado en las preferencias de los usuarios.

En la figura 1.3 se puede observar el despliegue de una red NGN, en donde se tienen claramente definidas las capas de servicio, transporte y acceso.

En la capa de servicio, es donde se procesan los paquetes de acuerdo con el servicio solicitado. Aquí todos los paquetes llegan en un protocolo único, a diferencia de las redes de acceso y de transporte en donde convergen diferentes tipos de protocolos.

Es importante mencionar, que las conexiones apuntan a brindar servicios corporativos, vía SIP en redes de acceso IP, y en PRI, R2, cuando la red de acceso es TDM.

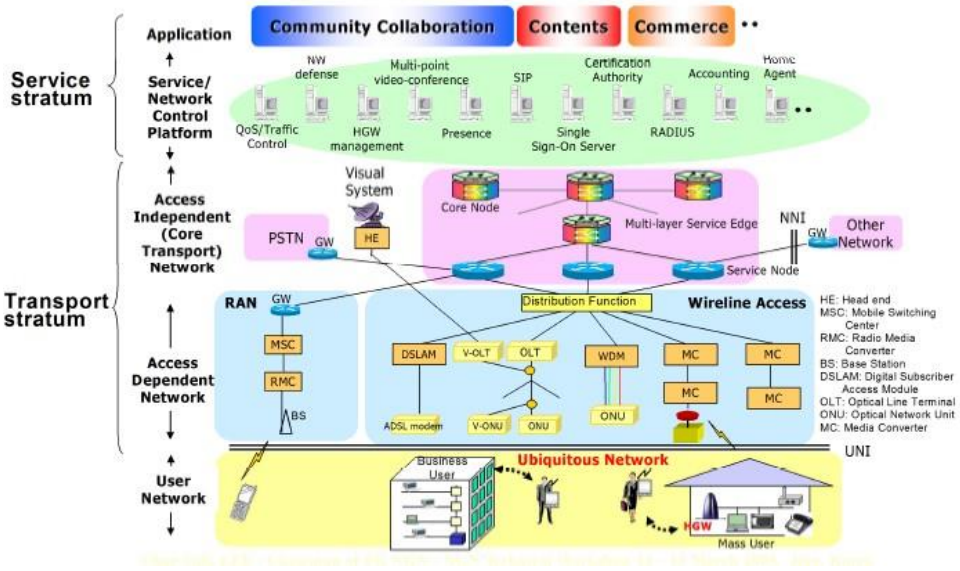


Figura 1.3 Redes de transporte y servicio NGN [3]

IMS, es una evolución de la red NGN, y que tiene su base en el protocolo SIP.

El IETF estandarizó SIP, mientras que el 3GPP estandarizó IMS como una arquitectura basada en SIP.

IMS, se definió para ubicarse como parte de la arquitectura UMTS, sin embargo, el 3GPP, ha definido interfases entre IMS y WLAN IEEE 802.11 a/b/g.

IMS ofrece la posibilidad a los operadores de manejar redes abiertas totalmente basadas en IP, con independencia de la red de acceso, pudiendo manejar desde una red de cobre en una operación fija, hasta una red móvil 3G o 4G.

En la figura 1.4 se observa la convergencia que se puede manejar entre redes fijas y móviles a través de IMS. Este es el elemento clave para

garantizar que las diferencias entre estas redes se puedan integrar y convertirse en una gran red multiacceso.

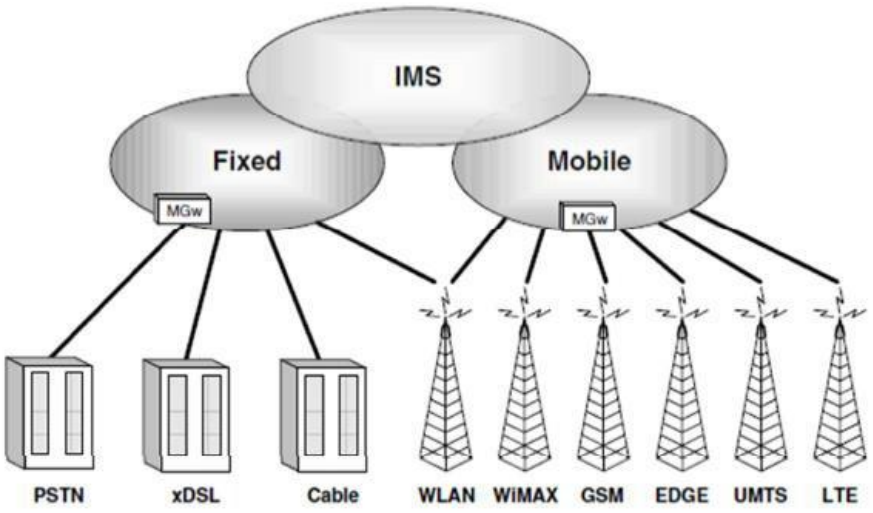


Figura 1.4 IMS como una red convergente Fijo-Móvil [3]

En la figura 1.5 podemos ver una estructura de una red IMS que principalmente se utiliza en el core de una red de telefonía móvil. Tradicionalmente, las redes móviles utilizaban SS7, para conectar sus servicios corporativos a la red, sin embargo, con IMS, ya sus servicios pueden ser manejado con SIP.

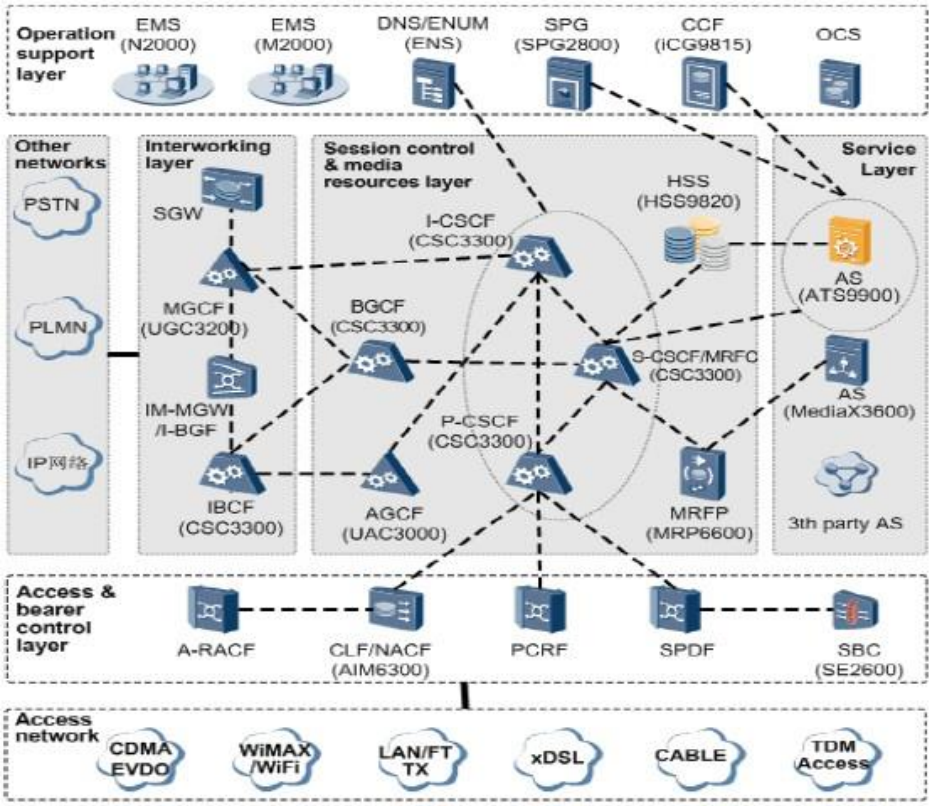


Figura 1.5 Arquitectura de una red IMS [4]

En la arquitectura, se puede apreciar las redes PSTN de operación fija, las PLMN de operación móvil y las redes adicionales que también pueden manejarse. El equipo que permite manejar conexiones SIP en este tipo de redes es el MGCF. En este caso el UGC3200, que hace de MGCF, maneja todos los protocolos de interconexión como son los protocolos de señalización, como los de media gateway. H.248 es el protocolo de señalización interno que permite manejar las instrucciones de control de recursos para crear y levantar los circuitos troncales TDM y sesiones RTCP en IP.

1.4.4 Session Border Controller

Los clientes corporativos como por ejemplo los grandes call center buscan tener una integración de servicios entre las redes de servicio privadas que poseen con la red pública de telefonía fija y la red pública móvil.

Los Sesión Border Controller son equipos con la capacidad de poder integrar soluciones de telefonía, brindando como función principal la de implementar un punto de demarcación y seguridad para los servicios de misión crítica que manejan los clientes.

Algunos autores, califican a este equipo como un firewall de telefonía, por las características intrínsecas a este tipo de equipos.

Inicialmente, los Session Border Controller, eran equipos que solo estaban considerados para la frontera de comunicación entre proveedores de telefonía, principalmente proveyendo de interoperabilidad entre las diferentes troncales que se establecían entre redes que manejaban el protocolo SIP. Es decir, todo el tráfico que se manejaba de conexión entre dos grandes proveedores era manejado mediante un punto de interconexión que servía para poder delimitar a nivel de capa de sesión los millones de paquetes que circulaban a través de él.

Por citar un ejemplo, entre Ecuadortelecom S.A. y Conecel S.A, razones sociales de Claro fijo y móvil respectivamente, se tenía previo a la fusión de estas empresas un intercambio de tráfico de 20 E1s, lo cual representa 600 canales, en tráfico E1 TDM. Con el avance de integración de estas empresas, la señalización tuvo que pasar a SIP, ya que el servicio TDM no era escalable. Este involucraba la habilitación de un puerto físico por cada E1 que se habilitaba.

En este caso, se pasó de manejar 20 E1s o 600 conexiones TDM a un tráfico en la actualidad de casi 900 canales simultáneos de voz que pueden llegarse a consumirse sobre todo en horarios pico de tráfico.

Esto sumado a que Conecel, por ser un operador de servicios básicos, está en la obligación de interconectarse con todos los demás proveedores de

telefonía habilitados por el órgano regulador de telecomunicaciones, lo cual, conlleva a que intercambie tráfico con otros proveedores que también estén en la capacidad de manejen tráfico SIP, y es aquí, donde se utiliza a los Session Border Controller, como un punto de conexión entre proveedores.

Para un cálculo final, desde el punto de vista de Claro fijo, teniendo en cuenta a operadores como Telefónica, CNT fijo y móvil, CenturyLink, probablemente proyecte que su cantidad de sesiones simultaneas pase a 2000 en horario pico, cuando todos los proveedores manejen SIP en sus respectivos puntos de interconexión.

Entre los modelos de equipos que se usan para ese tipo de tráfico, están los Acme Packet SBCs, equipos carrier-class que permiten manejar ese volumen de tráfico con una alta disponibilidad, 99,999%. Esta tecnología se presenta como una de las tecnologías de gran crecimiento en la industria, a tal punto que ACME fue adquirida por Oracle hace 6 años.

Para el borde de la red de acceso o para la premisa del cliente, los fabricantes actualmente construyen soluciones más pequeñas y las suelen llamar tipo Enterprise. Con estos modelos, se sigue pensando en una alta disponibilidad, por la criticidad del tráfico que manejan, sin embargo, la cantidad de canales se maneja en base a licencias, con las cuales cada equipo tiene una capacidad máxima de sesiones.

En la figura 1.6 se puede observar una representación de una red IMS de telefonía fija/móvil, con conexión a la PSTN, con accesos residenciales a través de soluciones de telefonía para este tipo de clientes. Adicionalmente, vemos la representación de un Session Border Controller, que está delimitando la red de Acceso, para que así la señalización, no sea directamente con el UGC3200, sino que exista un firewall de telefonía que proteja internamente el tráfico.

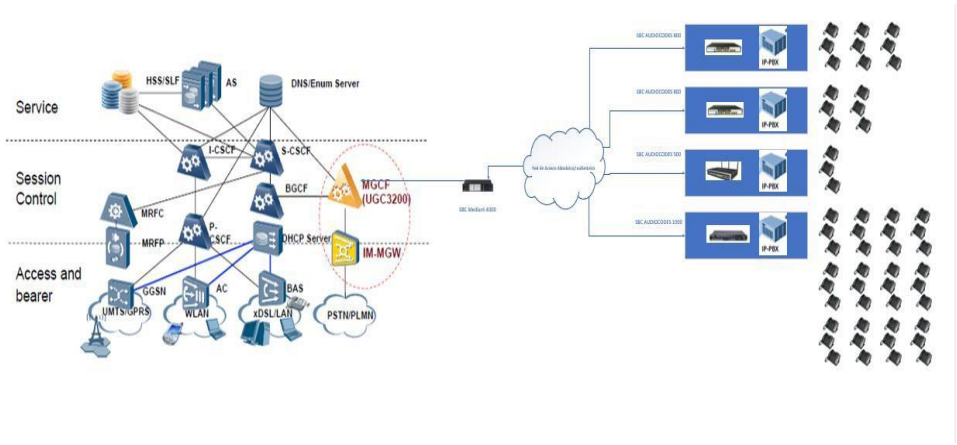


Figura 1.6 Representación de una red IMS con SBC de frontera en la red de acceso y en la premisa del cliente

También podemos observar que luego de la red de acceso, y en dirección hacia la premisa del cliente, existe otro dispositivo por cada cliente, que permite delimitar la red de telefonía interna del cliente con el ámbito que maneja el proveedor de telefonía. Aquí en esta representación se ha tomado como fabricante a los SBC Audiocodes y sus diferentes modelos de acuerdo con el tamaño de la red de telefonía.

Cada Session Border Controller realiza las funciones de router y de firewall, es por esto que funciona como un punto de demarcación, en capa 3 y en capa 5, (enrutamiento y sesión), evitando así que la red de telefonía del cliente sea extendida en capa 2. Esta característica mencionada evita también el traslape de redes.

Otra funcionalidad importante de un Session Border Controller es su capacidad de poder manipular las cabeceras de los mensajes en el protocolo SIP, tomando en cuenta que los proveedores definen políticas de interconexión que muchas veces no pueden ser completamente manejadas por las soluciones propias del cliente.

Los Session Border Controller, son equipos que también tienen la capacidad de manejarse como gateways que convierten la señalización y tráfico de voz, de acuerdo con los diferentes protocolos que se manejen entre el proveedor y el cliente.

Existen otras soluciones de SBC más orientadas a soluciones abiertas (OpenSource), sin embargo, los clientes corporativos y los proveedores, por el momento, prefieren soluciones con hardware dedicado a la función que deben cumplir estos equipos.

CAPÍTULO 2

2. DISEÑO DE INTERCONEXIÓN DE SOLUCIONES DE TELEFONÍA Y PROVEEDORES

2.1 Traslape de redes

En el proceso de implementación de servicios corporativos de telefonía, es común que existan clientes que ya tengan servicios con otros proveedores, así como redes de telefonía IP implementadas entre la matriz y sus sucursales.

En estos casos, existe todo un direccionamiento IP ya establecido y fijado tanto por los administradores de la red del cliente, si este cargo existe en la empresa, o por el proveedor inicial que implementó sus servicios anteriormente.

Un cliente puede tener la necesidad de tener varios proveedores con el fin de optimizar los costos relacionados a las llamadas telefónicas que va a realizar. Normalmente un proveedor de telefonía ya sea de PSTN o de PLMN, puede establecer precios preferenciales a sus clientes de acuerdo con el tipo de tráfico a realizar. Por ejemplo, un call center que desea tener llamadas a los celulares de sus clientes, debería preferir integrar su sistema de telefonía a la red de un operador celular, ya que los precios o planes ofrecidos por estos operadores son mejores por manejar tráfico ONNET.

Como se observa en la figura 2.1, el Reglamento para el Servicio de Telefonía Móvil Celular en su Artículo 2, Capítulo IX de Infracciones y Sanciones, determina como una infracción de segunda clase cobrar tarifas no autorizadas a los clientes y así controlar que exista una captación agresiva del mercado en base al tamaño dominante de su red.

2.- Infracciones de segunda clase:

- No proveer a los usuarios, que lo soliciten, cualquiera de los servicios autorizados.
- No cumplir con las especificaciones técnicas establecidas en el contrato de concesión o en el presente Reglamento.
- No acatar las disposiciones legales y reglamentarias vigentes, o las que dicte el CONATEL.
- Cobrar tarifas sobre las máximas permitidas, o tarifas no autorizadas.
- Conectar equipos terminales no homologados.
- Violación al derecho al secreto de las telecomunicaciones.
- No otorgar facilidades para que la Superintendencia de Telecomunicaciones revise e inspeccione las instalaciones de la operadora.
- La conducta culposa o negligente que ocasione daños, interferencias o perturbaciones en cualquier red de telecomunicaciones debidamente autorizada.
- Incumplir reiteradamente con requerimientos y con la presentación de información que debe proporcionar a la SNT o a la Superintendencia de Telecomunicaciones en los términos especificados en el presente Reglamento y en el contrato de concesión.

Figura 2.1 Artículo 42, Capítulo IX del Reglamento para el Servicio de Telefonía Móvil Celular

En la figura 2.2 podemos observar un caso, en donde el cliente ya tiene una red establecida con el direccionamiento privado 10.0.0.0/16. Es decir, una gran red privada que utiliza para comunicar sus dispositivos de red de servicios de internet, datos, telefonía y videoconferencia. Adicionalmente se tiene un proveedor actual de servicios de telefonía móvil que tiene otra gran red privada implementada, 172.16.32.0/19. Esta última no se cruza con la privada del cliente. El nuevo proveedor de telefonía quiere proporcionar direccionamiento 10.0.0.0/24, lo cual es un segmento relativamente pequeño, pero se cruza con las direcciones IPs de la matriz del cliente en Quito, donde están los servicios de comunicación SIP principales, y además a nivel de capa 3, el punto de enrutamiento principal se encuentra en este sitio.

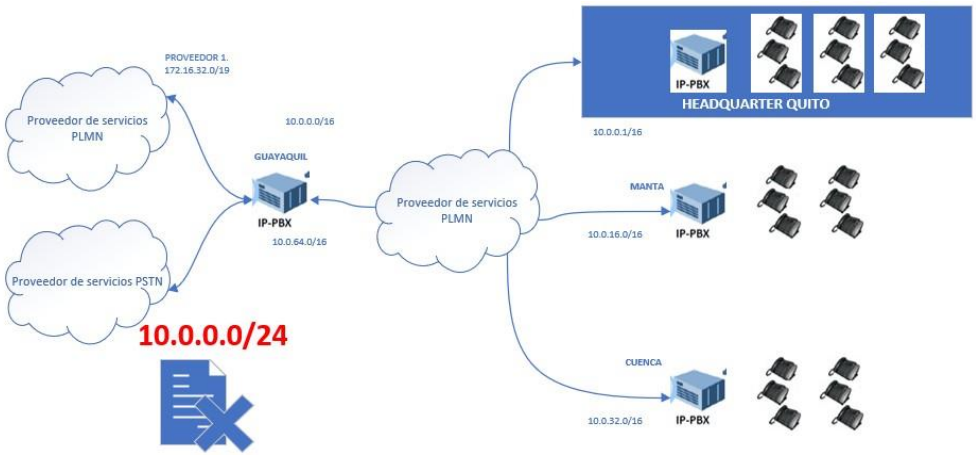


Figura 2.2 Traslape de redes privadas de proveedor y cliente

En este ejemplo, como lo muestra la figura 2.3, un Session Border Controller, sirve de frontera y aplicando un esquema de NAT TRAVERSAL, puede generar un intercambio de paquetes, en donde las redes privadas internas, son transformadas a una red privada global, no solo en CAPA 3, sino en CAPA 5.

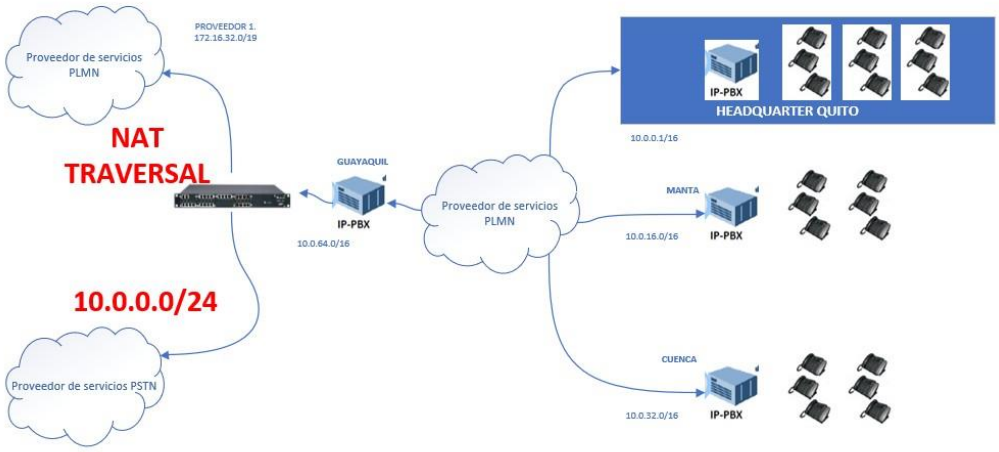
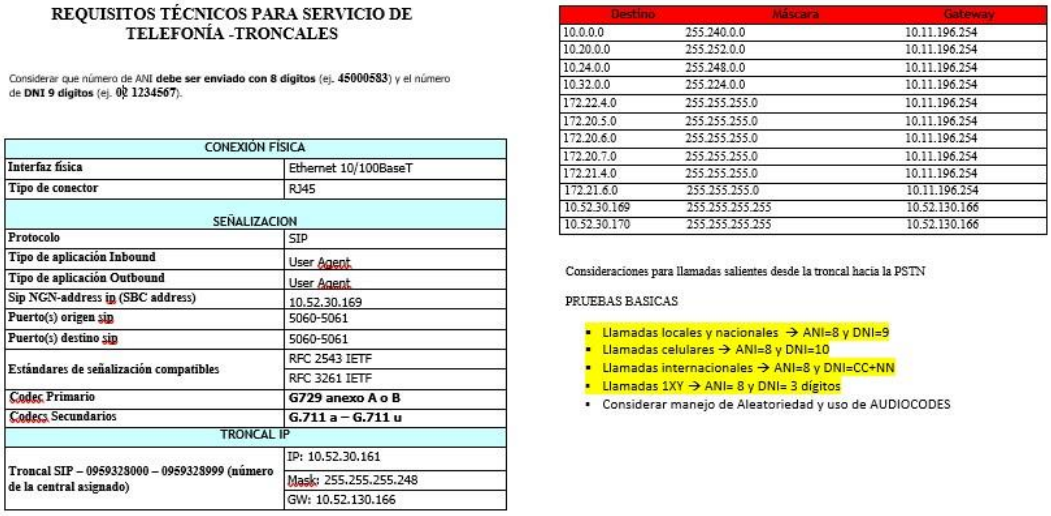


Figura 2.3 Implementación de un NAT TRAVERSAL por traslape de redes

2.2 Manipulación de cabeceras

Los proveedores de telefonía pública fija y móvil normalmente definen estándares de comunicación, que permiten implementaciones de servicios corporativos de telefonía de una forma ordenada. Estas reglas, permiten, definir las condiciones de configuración que deberán ser establecidas del lado del cliente para lograr un establecimiento de señalización y de voz.



REQUISITOS TÉCNICOS PARA SERVICIO DE TELEFONÍA -TRONCALES

Considerar que número de ANI **debe ser enviado con 8 dígitos** (ej. **45000583**) y el número de **DNI 9 dígitos** (ej. **0[illegible] 1234567**).

CONEXIÓN FÍSICA	
Interfaz física	Ethernet 10/100BaseT
Tipo de conector	RJ45
SEÑALIZACION	
Protocolo	SIP
Tipo de aplicación Inbound	User Agent
Tipo de aplicación Outbound	User Agent
Sip NGN-address ip (SBC address)	10.52.30.169
Puerto(s) origen sip	5060-5061
Puerto(s) destino sip	5060-5061
Estándares de señalización compatibles	RFC 2543 IETF
	RFC 3261 IETF
Codec Primario	**G729 anexo A o B**
Codecs Secundarios	**G.711 a – G.711 u**
TRONCAL IP	
Troncal SIP – 0959328000 – 0959328999 (número de la central asignado)	IP: 10.52.30.161
	Mask: 255.255.255.248
	GW: 10.52.130.166

Destino	Máscara	Gateway
10.0.0.0	255.240.0.0	10.11.196.254
10.20.0.0	255.252.0.0	10.11.196.254
10.24.0.0	255.248.0.0	10.11.196.254
10.32.0.0	255.224.0.0	10.11.196.254
172.22.4.0	255.255.255.0	10.11.196.254
172.20.5.0	255.255.255.0	10.11.196.254
172.20.6.0	255.255.255.0	10.11.196.254
172.20.7.0	255.255.255.0	10.11.196.254
172.21.4.0	255.255.255.0	10.11.196.254
172.21.6.0	255.255.255.0	10.11.196.254
10.52.30.169	255.255.255.255	10.52.130.166
10.52.30.170	255.255.255.255	10.52.130.166

Consideraciones para llamadas salientes desde la troncal hacia la PSTN

PRUEBAS BASICAS

- Llamadas locales y nacionales → ANI=8 y DNI=9
- Llamadas celulares → ANI=8 y DNI=10
- Llamadas internacionales → ANI=8 y DNI=CC+NN
- Llamadas 1XY → ANI= 8 y DNI= 3 dígitos
- Considerar manejo de Aleatoriedad y uso de AUDIOCODES

Figura 2.4 Requisitos técnicos para servicio de troncales de telefonía

Como se observa en la Figura 2.4, los proveedores determinan números de dígitos de las cabeceras de los números de A, así como los números de B, controlando el correcto establecimiento de las llamadas.

Por ejemplo, un administrador de una central telefónica IP, podría configurar en su central telefónica, que para llamar a números fijos de la ciudad donde se encuentra, de la misma forma que marcamos los números desde nuestra casa. Un usuario de CNT genera llamadas desde su casa marcando 7 números. Esta configuración de ser realizada en la central y bajo las condiciones de configuración del proveedor, simplemente no se completaría.

Figura 2.5 Ejemplo de manipulación de mensaje y número [5]

Como vemos en la figura 2.5, podemos observar, que existe una inicialización de una llamada, en la cual, se genera una cabecera INVITE, con sus parámetros, generados por el lado izquierdo de la comunicación. Luego al llegar al SBC, este comienza por transformar el formato del campo del Uniform Resource Identifier o URI, colocando un dominio en vez de la dirección IP que se observa en el campo de la izquierda. Es importante observar que no necesariamente es una transformación estrictamente pública, sin embargo, esta puede ser una definición interna realizada por el administrador de la red de telefonía.

Luego en la sentencia VIA, se puede observar cómo se cambia el formato de TCP a UDP, y también se modifica la localización a donde se debe dar respuesta, definiendo una dirección pública, como muestra en el ejemplo.

Max-forward, un parámetro, que también hace referencia a la cantidad de saltos que se puede manejar en dirección descendente, se modifica, para garantizar una conexión estricta conocida de n saltos.

En la sentencia FROM también se puede visualizar un cambio. Este va en relación de la definición de un prefijo, previo al número inicialmente generado.

El Call-ID también es manipulado por el SBC para tomar control total sobre la transacción a ser realizada, eliminando el ID que inicialmente se había generado.

El campo Contact, también sufre un cambio, que permite en este caso cambiar el puerto a utilizar en el proceso de intercambio de información.

En el ejemplo, también observamos el cambio de la opción de Privacy, de tal manera, que un usuario, pueda retener su identidad y a su vez mantenerse anónimo. Esta opción es útil cuando se desea compartir información sin querer estar asociado a la misma. Otros usuarios pueden pensar que su información puede ser utilizada para generarse propaganda no deseada, y por lo tanto, pueden manipular este campo.

P-Asserted-Identity es una opción que se utiliza en funciones de autenticación para hacer uso de un proxy saliente.

El campo manipulado Priority con el valor de Emergency, permite tener la percepción del cliente en cuanto a la importancia de la transacción.

Otra característica importante de la manipulación es la de poder manejar transcoding. Con esta opción se puede trabajar con las diferentes necesidades en relación con los códecs que se manejan en una llamada. Cuando el abonado A, no tiene un códec que el abonado B dispone, se presenta problemas en el establecimiento de las llamadas.

Desde el punto de vista del proveedor, es importante tener el control sobre este tipo de parámetro, porque incluso está relacionado al ancho de banda utilizado en las transacciones.

Desde el punto de vista del cliente, es todo lo contrario, la calidad es lo más importante, sin importar el ancho de banda utilizado.

En la figura 2.6, se puede observar como un SBC ayuda a que exista más códecs soportados y mantenerlos disponibles para que el abonado B escoja, en el proceso de establecimiento de la llamada.

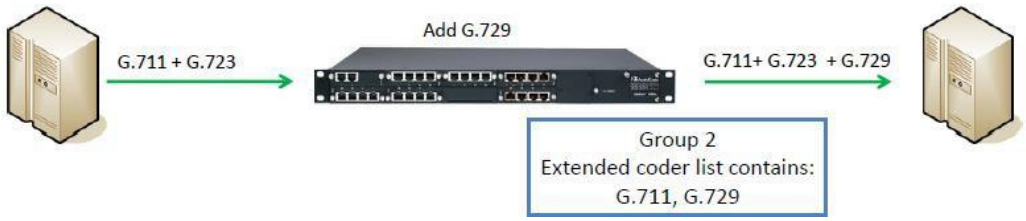


Figura 2.6 Extensión de códecs en una llamada [5]

Otra opción importante que permite los Session Border Controller, es restringir los códecs permitidos, en una de las dos fronteras, sea WAN o LAN, para así eliminar los códecs que no se quieren permitir en una transacción. En la figura 2.7, se puede observar, como el Session Border Control, realiza la función de prescindir del códec no deseado en el paquete SDP.

Figura 2.7 Eliminación de códecs en una transacción de telefonía. [5]

2.3 Conversión de protocolos

Una opción muy importante de los Session Border Controller, es que los fabricantes, están integrando la funcionabilidad de Gateway al equipo, para así resolver los problemas de integración entre los diferentes tipos de interfases físicas que se poseen. Este tipo de conversión a diferencia de manejarse como una transformación física implica adicionalmente, una serie de cambios, en los protocolos que se manejan.

Si por un lado se posee una interfase ethernet, y una señalización SIP, es posible que, por el otro lado, se posea una interfase TDM, de tal manera, que se maneje los protocolos E1 PRI y R2, y un mecanismo de conversión, sea el que permita recibir la llamada en un protocolo, realizar el cambio, y procesar las llamadas en el nuevo protocolo.

Figura 2.8 Esquemas de Session Border Controller como Gateway

En la figura 2.8, se puede observar distintos Session Border Controller, manejando su modalidad de Gateway, de tal manera, que en el primer caso de “PSTN Networks”, se puede observar que el proveedor de servicios de telefonía es el que posee la necesidad de conectarse a través de TDM, probablemente porque tenga E1s ya instalados en la premisa del cliente. Por otro lado, esto significa que en la parte LAN del Session Border Controller se maneja SIP, y el cliente mantiene una red de servicios IP.

Adicionalmente se puede observar que en la modalidad “Legacy TDM PBX”, una de las más frecuentes en la implementación de clientes corporativos, se tiene que la parte TDM se presenta hacia el lado del cliente. Probablemente en este caso, el cliente presente un sistema Legado, que no tiene interfases SIP disponibles, por lo tanto, requiere que el proveedor de servicios de telefonía haga entrega de su servicio en E1 PRI o R2.

Normalmente, cuando el cliente posee esta característica, el proveedor debe buscar una forma de entregar el servicio hacia su cliente, y debe decidir hasta donde extiende la señalización E1 en su red. El protocolo TDM ya no se está prefiriendo en la actualidad, debido a que las redes convergentes, MPLS, son en su mayoría IP. Es por esto, que es una mala idea para el proveedor, desplegar la red TDM desde un equipo de la plataforma IMS, pasar por un transporte en E1, luego a una red de acceso en TDM, y finalmente conectarse a una central telefónica en E1.

El manejo de problemas en esta solución es muy complicado. Normalmente se maneja en base a alarmas que pueden significar pérdidas de sincronización, y para esto se efectúa lazos, pero su análisis es complejo y no concluyente de donde puede estar el inconveniente.

Figura 2.9 Session Border Controller con interfases TDM. [5]

En la figura 2.9, se puede observar un equipo Session Border Controller, con interfases TDM, para el manejo de E1 TDM hacia la PSTN o hacia la PBX. De igual manera interfases IP, para el manejo de TRUNKs hacia la PBX o hacia el proveedor. Adicionalmente, estas mismas interfases, pueden manejar servicios SIP, pero en modalidad de cuentas de usuario FXS o FXO. Estos equipos también pueden tener interfases analógicas, que manejan líneas POTs, hacia el proveedor o hacia el cliente, de igual manera, FXS o FXO.

2.4 Soluciones de seguridad

Una de las principales razones por la cual un Session Border Controller es usado, es para dividir las redes del proveedor de servicios de telefonía y el cliente. De esta forma el cliente tiene oculta toda su red que incluso, por su diseño, puede tener fallas de seguridad, que pueden comprometer toda la red como tal.

Un diseño normal en los clientes corporativos es colocar una sola red LAN para todo el direccionamiento de los endpoints. Las redes privadas clase C y principalmente la clase B permite tener un gran espacio disponible y así dejar de preocuparse por una ordenada distribución de los segmentos de red.

Las centrales telefónicas o sistemas de telefonía de call center, enfocan más su arquitectura al servicio. Es por esto por lo que podemos encontrar infraestructura con una sola interfase de red, con la cual, el cliente corporativo, espera manejar tanto su tráfico privado de voz y datos, como su interacción con los diferentes proveedores de telefonía.

En el caso del proveedor Conecel, el servicio de telefonía se maneja, levantando el servicio del cliente, compartiendo tráfico en capa 2, con otros clientes. Es por esto, que el broadcast o los tráficos generados por los clientes, podrían recibirse sin mayor problema en otro cliente implementado con servicios similares.

Es por este diseño, que es importante habilitar servicios en Capa 3, y un Session Border Controller, permite hacerlo así, sin necesidad de generar muchos cambios dentro de la estructura de direccionamiento del proveedor.

Otro punto importante, que se ha encontrado, es que, por error, o por lo menos se piensa así; el cliente, coloca el direccionamiento de un equipo del proveedor, y así fácilmente el tráfico general de todos los servicios, en ese mismo broadcast, comienza a perderse. Todos los equipos, comienzan a enviar paquetes al equipo erróneo, y este no sabe qué hacer, porque no tiene las rutas adecuadas para tratar ese paquete. Por otro lado, el sistema, comienza a detectar duplicación de IP, empezando un grave problema en la red. Esto sumado a que, al tratar de resolver este problema, no es fácil, hacer seguimiento de tráfico en capa 2, por lo que rastrear de donde viene el tráfico erróneo, implica un análisis a nivel de switches y mac address, bastante complejo de manejar.

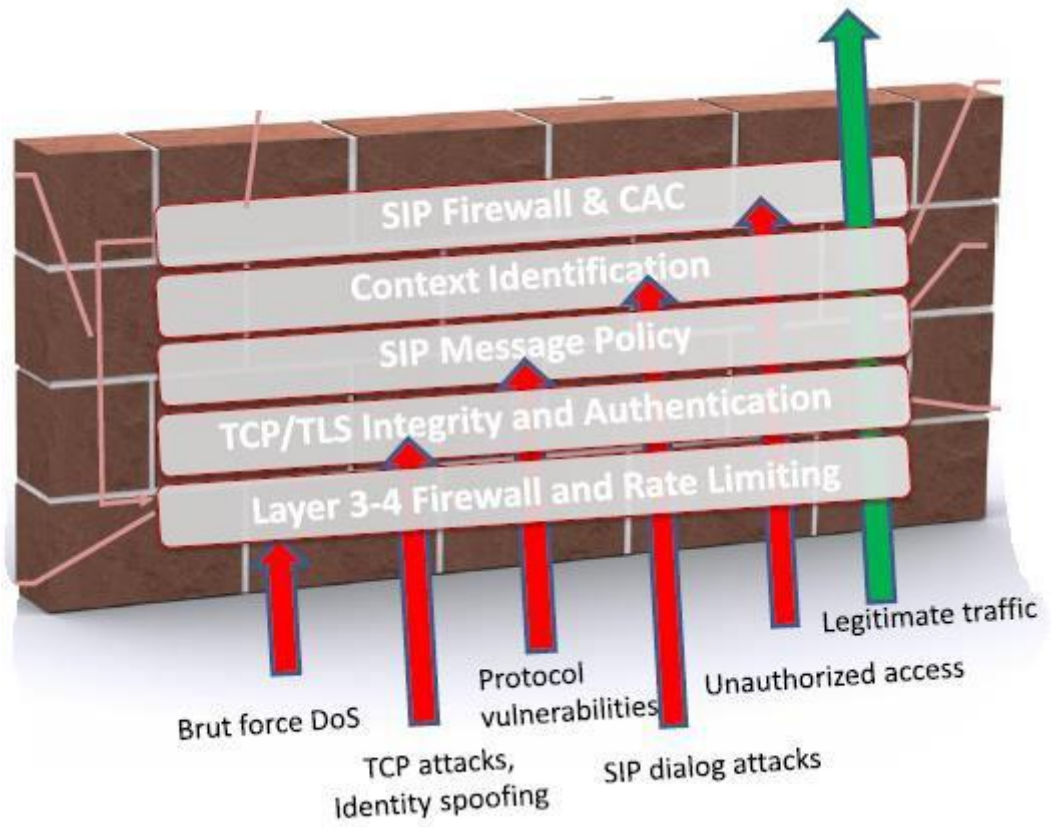


Figura 2.10 Fuertes estrategias de seguridad de un SBC

Como se observa en la figura 2.10, se observan los diferentes tipos de ataque que un Session Border Controller, puede manejar,

- En capa 3 y 4, un ataque de fuerza bruta puede ser manejado por una aplicación de una lista de acceso dinámica, que el Session Border Controller puede generar.
- En capa 4, de presentarse un ataque al protocolo TCP, con un intento de suplantación de identidad, el Session Border Controller, puede aplicarle protocolos de TCP/TLS con autenticación.
- Si el ataque, ya es manejado a través de vulnerabilidades del protocolo SIP, el Session Border Controller, puede descartar paquetes que tengan mal formaciones en su estructura.

CAPÍTULO 3

3. ANÁLISIS DE RESULTADOS

3.1 Esquema de red

A continuación, vamos a analizar una solución implementada para un Banco, en la cual se necesitó la colocación de varios equipos Session Border Controller, para brindar el servicio de telefonía fija hacia un sistema Genesys de Call Center, con el cual los departamentos de atención al cliente atienden solicitudes y generan oportunidades comerciales.

Adicionalmente, los servicios eran requeridos a nivel nacional, es decir, se recibe tráfico con los códigos 04, 02, 03, 05 y 07. Adicionalmente, el banco requería concentrar todo su tráfico en una sola ubicación en la ciudad de Guayaquil.

Desde el punto de vista regulatorio, el órgano regulador de este tipo de servicio define en el reglamento del servicio de telefonía fija local, capítulo 3 artículo 8, que no se pueden modificar los números de origen ni destino de las llamadas, según lo establecido en los planes técnicos fundamentales de numeración y de señalización.

Es por esta razón, que se necesita, un Session Border Controller, para que así se reciba la señalización y la media, en una ciudad autorizada con el respectivo código de área, y luego reenviar el tráfico hacia la ciudad que va a centralizar el servicio.

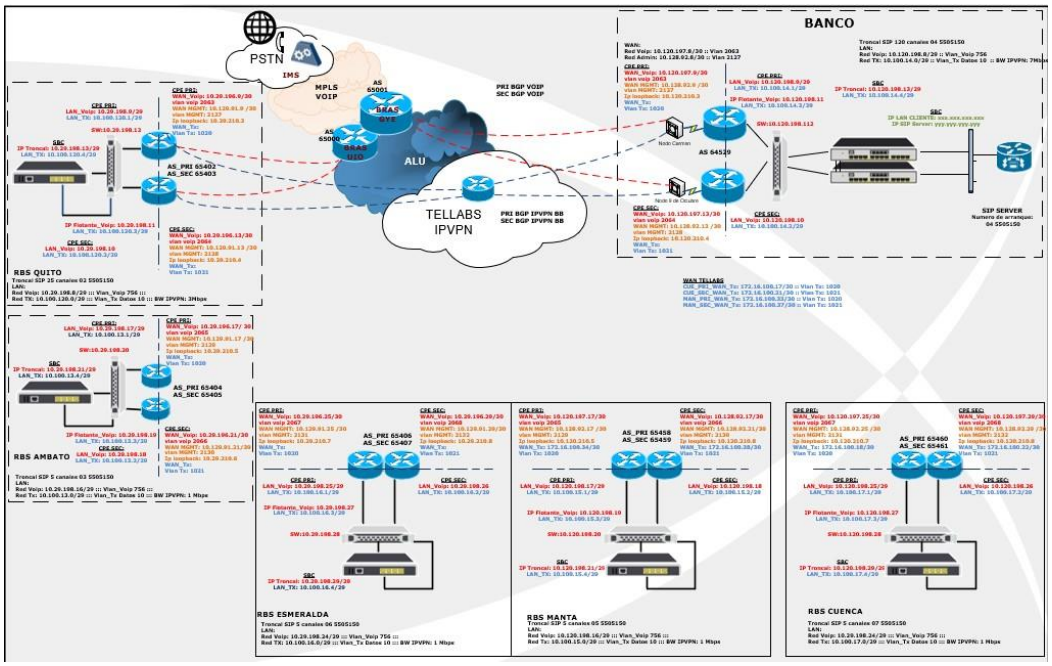


Figura 3.1. Esquema de red de una solución con Session Border Controller

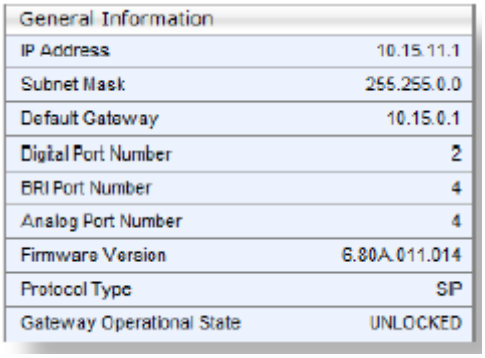
En la figura 3.1. se puede observar 5 localidades diferentes y que pertenecen a los códigos 02, 03, 05, 06 y 07. En cada una de estas ciudades, se implementa un Session Border Controller. Todos estos equipos manejan señalización contra el proveedor de telefonía y así en cada ciudad se recibe la señalización y la media necesaria para cumplir con los lineamientos determinados por el órgano regulador. Luego a través de circuitos de datos se transporta el tráfico hacia la ciudad de Guayaquil, para que entre los equipos de los nodos y los que se encuentran en la premisa del cliente, se maneje la señalización y media de una troncal privada, que reciba en un arreglo de equipos redundantes, la señalización de la ciudad y a su vez la de los otros 5 nodos.

La importancia de este caso es que todas las características de seguridad y de tratamiento de paquetes SIP puede ser manejado a través de estos equipos, brindando mucha seguridad en el servicio entregado al cliente.

Para el cliente tuvo una importancia alta, ya que la solución, permitió brindarle un producto que optimizó costos de personal en todas las ciudades, y a su vez, el proveedor, tiene una infraestructura, que permite brindar este servicio a más clientes, porque se crea un ámbito independiente para cada troncal.

3.2 Configuración de un equipo Audiocodes

Los pasos para poder configurar un equipo Session Border Controller, comienzan con los pasos tradicionales de un equipo de telecomunicaciones, a nivel físico, para luego subir a la configuración de IP, y finalmente las características que nos permiten manejar el tratamiento de la sesión SIP establecida. En la figura 3.2, podemos observar los parámetros básicos de IP que se configuran y un estatus de los puertos físicos presentes en el equipo.



General Information	
IP Address	10.15.11.1
Subnet Mask	255.255.0.0
Default Gateway	10.15.0.1
Digital Port Number	2
BRI Port Number	4
Analog Port Number	4
Firmware Version	6.80A.011.014
Protocol Type	SIP
Gateway Operational State	UNLOCKED

Figura 3.2. Configuración de IP en un Session Border Controller

En la figura 3.3, vemos una vista de la interfase global de administración de un Session Border Controller.

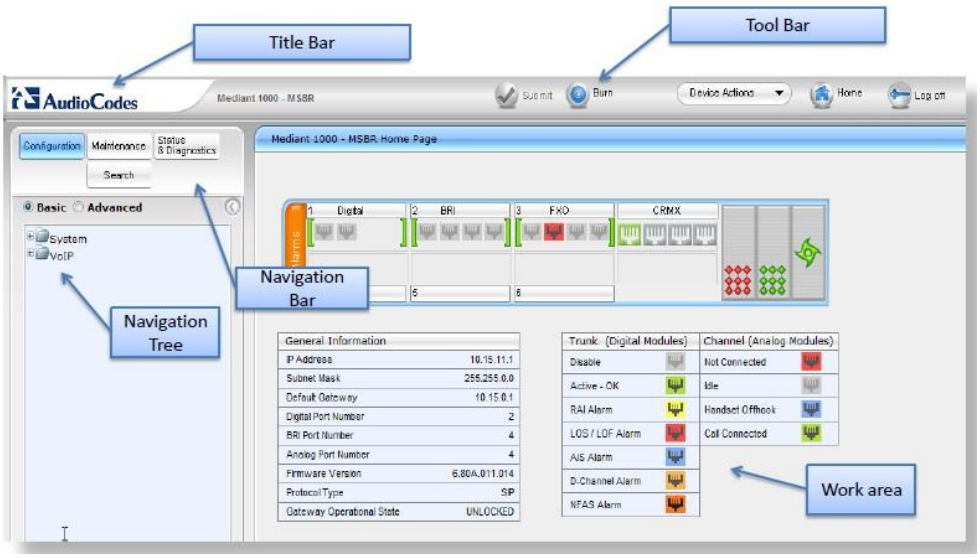


Figura 3.3. Panel de navegación de un Session Border Controller Mediant 1000

Para realizar una configuración básica, se deben de manejar dos instancias, que estén representadas por dos redes que permitan manejar una relación básica de IP PBX y otra de proveedor de servicios de telefonía o ITSP.

En la figura 3.4. observamos el esquema de conexión mencionado anteriormente.

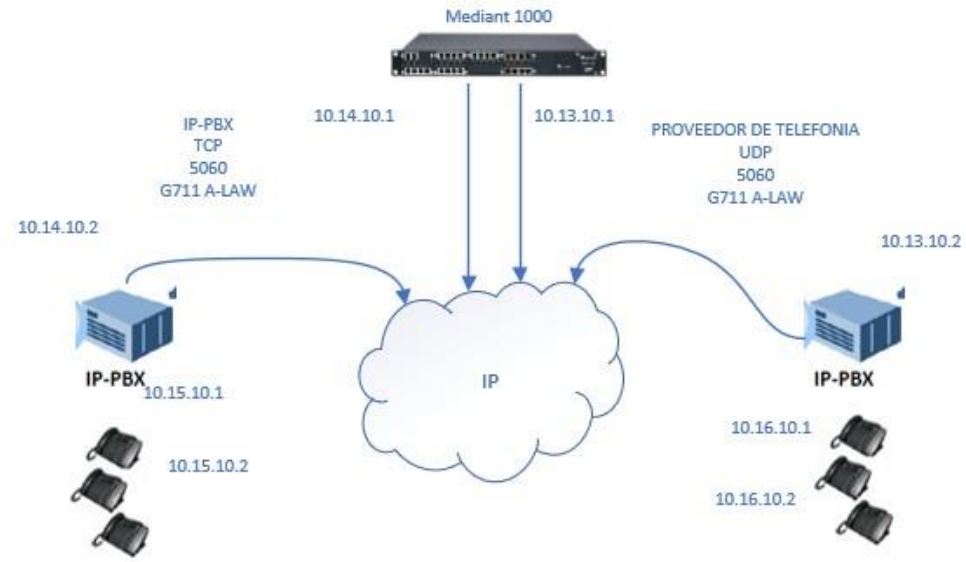


Figura 3.4. Esquema de conexión básico a través de un Session Border Controller

La figura 3.5, describe la primera instancia de configuración de los equipos. El Realm, define los puertos de media que van a ser utilizados.

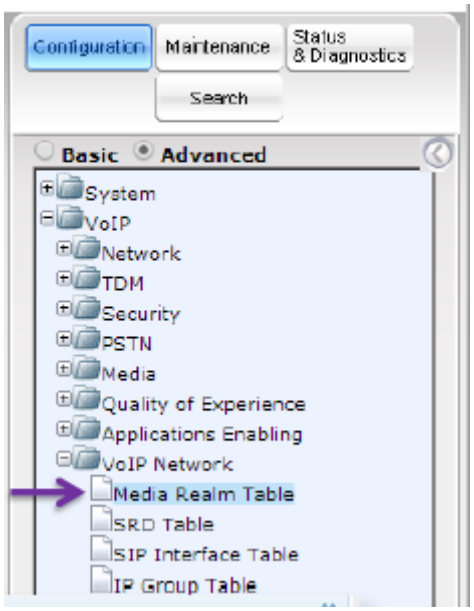


Figura 3.5. Tabla de Media Realm

La tabla SIP define los puertos de conexión a nivel de señalización. La figura 3.6, muestra la configuración de la tabla SIP.

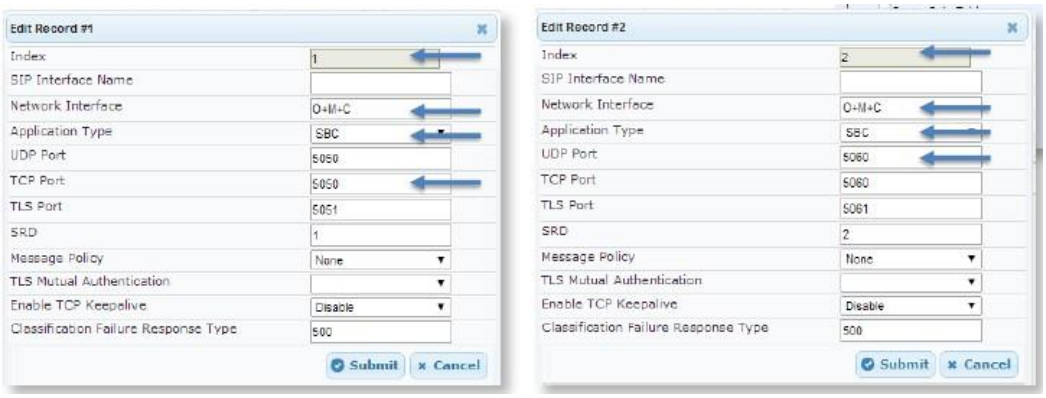


Figura 3.6 Tabla SIP

La siguiente es la configuración del Source Routing Domain (SRD), que es una entidad global de un contenedor de las configuraciones relacionadas a un ámbito. Normalmente se realiza una por cliente, por lo que si la solución es para varios clientes, este parámetro permite manejar multitenants. La figura 3.7 nos muestra la configuración de SRD.

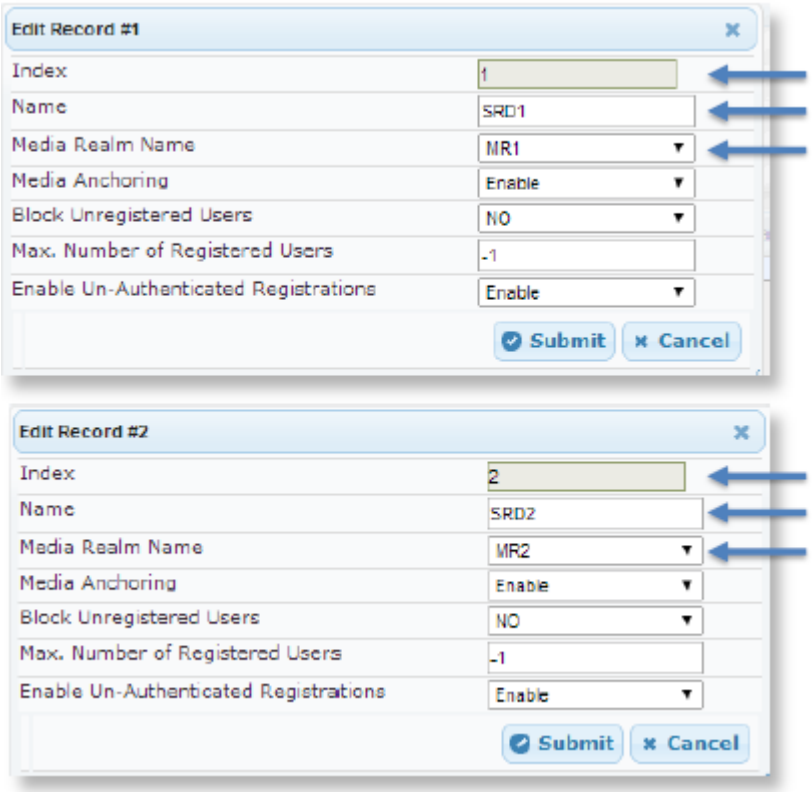


Figura 3.7. Descripción de parámetros SRD

La figura 3.8 muestra la configuración de los Proxy-Sets, que indica los puntos con los cuales va a señalizar el Session Border Controller, tanto del lado del proveedor como de la central telefónica.

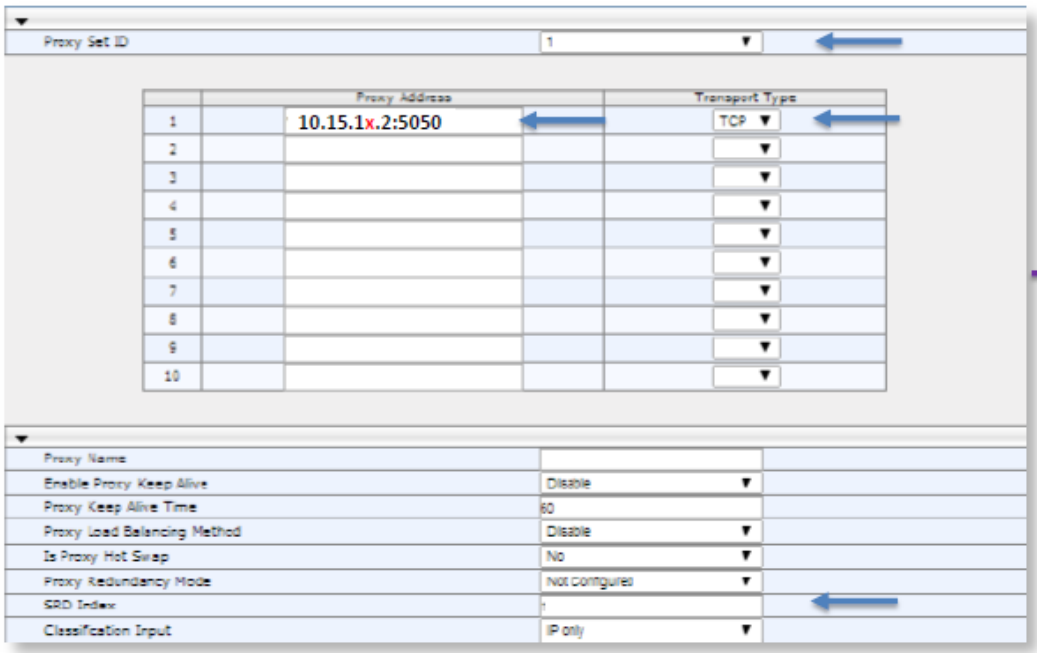


Figura 3.8. Proxy set del lado de la IP-PBX

La siguiente configuración importante como se observa en la Figura 3.9, es la de IP Profile, con la cual se definen la forma en la que las interfases van a ser llamadas para realizarse la manipulación de los mensajes.

Figura 3.9 IP Profile de interfases para manipulación de headers

Finalmente, en la figura 3.10, se puede observar la configuración de los códecs que van a ser permitidos, agregados o eliminados dentro de la transacción de telefonía.

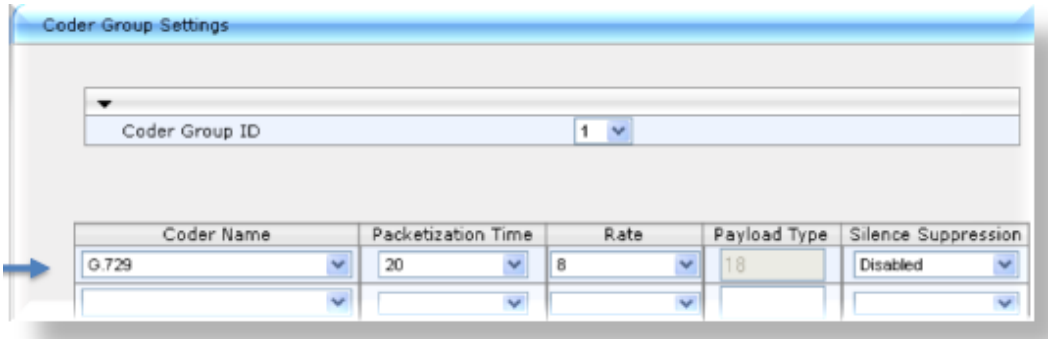


Figura 3.10. Configuración de códecs en un Session Border Controller

3.3 Cabeceras de señalización SIP

A continuación, vamos a revisar el siguiente caso, en donde un cliente se quejaba de que no podía realizar algunas llamadas dentro de su call center, y la llamada era rechazada. Al revisar, dentro del syslog que nos brinda el Session Border Controller, se verificó que el mensaje de error era un “488 Not Acceptable Here” y que su causa de desconexión era “Release_Because_Media_Mismatch”.

Como se observa en la figura 3.11, se puede observar que la señalización muestra un rechazo con un mensaje 400.

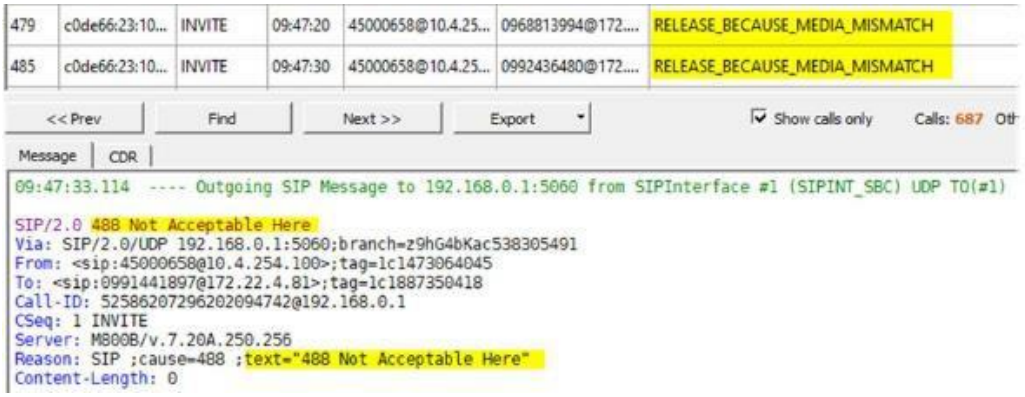


Figura 3.11. Mensaje SIP con error y causa de rechazo

En la figura 3.12 se observa una cabecera con oferta de códec G729, G711A y G711U que si es transaccionada correctamente con G711.

```
INVITE sip:0980457850@172.17.33.232:5060 SIP/2.0
From: sip:3418@172.16.35.32;tag=42EF00AE-9999-4A45-941B-B8B2F97FE605-1482856
To: <sip:0980457850@172.16.35.32:5060>
Call-ID: FDFD50AE-61C3-46CF-814A-A4AE84EADE3B-1167952@172.16.35.32
CSeq: 1 INVITE
Content-Length: 297
Content-Type: application/sdp
Via: SIP/2.0/UDP 172.16.35.32:5060;branch=z9hG4bKC13D721D-9D9D-4705-8097-9A96E74FE0D1-6665553
Contact: <sip:3418@172.16.35.32:5060>
Allow: ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, REFER, UPDATE
User-Agent: M800B/v.7.20A.250.256
Max-Forwards: 68
X-Genesys-CallUUID: VRKIES5ABD1CJFU92H8L75ODA000GVVC
X-ISCC-CofId: location=SIP_Server_Switch;cofid=17999425
Session-Expires: 1800;refresher=uac
Min-SE: 90
Supported: uui,100rel,timer

v=0
o=- 1606665125 1 IN IP4 172.17.33.231
s=Bria 5 release 5.5.0 stamp 97575
c=IN IP4 172.17.33.231
t=0 0
m=audio 9810 RTP/AVP 18 8 0 101
a=sendrecv
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=yes
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
```

Figura 3.12. Llamada con oferta de códecs G729, G711A y G711U

En la figura 3.13, se puede observar una llamada con oferta de códecs G729 y OPUS.

```
09:42:22.488  ---- Incoming SIP Message from 172.16.35.32:5060 to SIPInterface #1 (SIPINT_PBX2) UDP TO(#1

INVITE sip:6011103@172.17.33.231:5060 SIP/2.0
From: sip:3364@172.16.35.32;tag=42EF00AE-9999-4A45-941B-B8B2F97FE605-1477774
To: <sip:6011103@172.16.35.32:5060>
Call-ID: FDFD50AE-61C3-46CF-814A-A4AE84EADE3B-1163904@172.16.35.32
CSeq: 1 INVITE
Content-Length: 349
Content-Type: application/sdp
Via: SIP/2.0/UDP 172.16.35.32:5060;branch=z9hG4bKC13D721D-9D9D-4705-8097-9A96E74FE0D1-6642402
Contact: <sip:3364@172.16.35.32:5060>
Allow: ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, REFER, UPDATE
User-Agent: Bria 5 release 5.5.0 stamp 97575
Max-Forwards: 69
X-Genesys-CallUUID: VRKIES5ABD1CJFU92H8L75ODA000GUBJ
X-ISCC-CofId: location=SIP_Server_Switch;cofid=17996128
Session-Expires: 1800;refresher=uac
Min-SE: 90
Supported: uui,100rel,timer

v=0
o=- 1606612089 1 IN IP4 172.17.33.122
s=Bria 5 release 5.5.0 stamp 97575
c=IN IP4 172.17.33.122
t=0 0
m=audio 60374 RTP/AVP 9 8 18 120 0 101
a=sendrecv
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=yes
a=rtpmap:120 opus/48000/2
a=fmtp:120 useinbandfec=1; usedtx=1; maxaveragebitrate=64000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

Figura 3.13. Llamada con oferta de códecs G729 y Opus

En la figura 3.14, se puede observar una llamada con sólo el códec G729 y que es rechazada porque en el Session Border Controller, no se encuentra habilitado este códec.

```
09:47:33.881  ---- Incoming SIP Message from 172.16.35.32:5060 to SIPInterface #0 (SIPIN

INVITE sip:0991441897@172.17.33.232:5060 SIP/2.0
From: sip:3359@172.16.35.32;tag=42EF00AE-9999-4A45-941B-B8B2F97FE605-1479732
To: <sip:0991441897@172.16.35.32:5060>
Call-ID: FDFD50AE-61C3-46CF-814A-A4AE84EADE3B-1165489@172.16.35.32
CSeq: 1 INVITE
Content-Length: 248
Content-Type: application/sdp
Via: SIP/2.0/UDP 172.16.35.32:5060;branch=z9hG4bKC13D721D-9D9D-4705-8097-9A96E74FE0D1-6E
Contact: <sip:3359@172.16.35.32:5060>
Allow: ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, REFER, UPDATE
User-Agent: Bria 5 release 5.5.0 stamp 97575
Max-Forwards: 69
X-Genesys-CallUUID: VRKIES5ABD1CJFU92H8L750DA000GUU5
X-ISCC-CofId: location=SIP_Server_Switch;cofid=17997335
Session-Expires: 1800;refresher=uac
Min-SE: 90
Supported: uui,100rel,timer

v=0
o=- 1606632656 1 IN IP4 172.17.33.88
s=Bria 5 release 5.5.0 stamp 97575
c=IN IP4 172.17.33.88
t=0 0
m=audio 63102 RTP/AVP 18 101
a=sendrecv
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=yes
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

Figura 3.14. Llamada con oferta de sólo códec G729.

Luego del cambio efectuado, se observa cómo se ve en la figura 3.15, que la llamada se logra establecer correctamente.

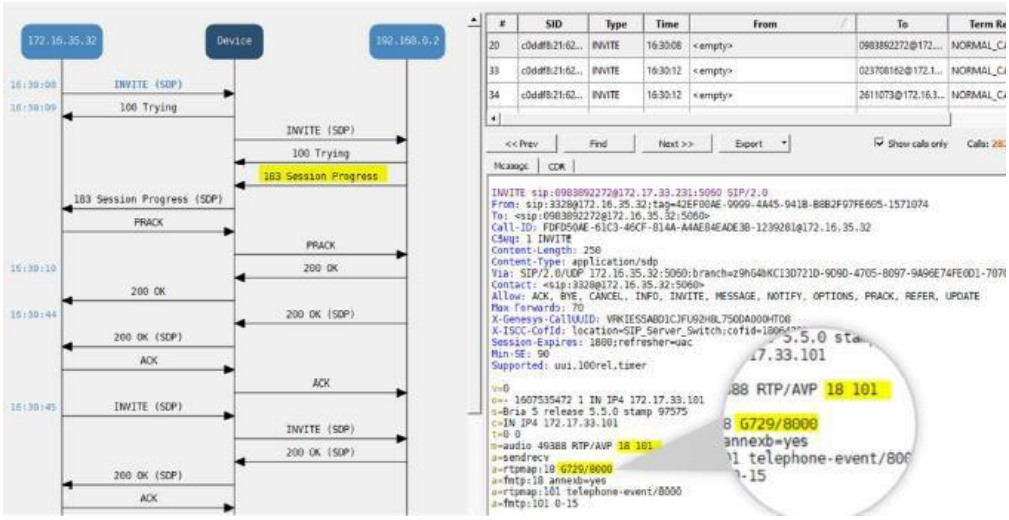


Figura 3.15. Llamada con códec G729 y transacción exitosa.

CAPÍTULO 4

4. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

En este trabajo de titulación, se ha podido demostrar la necesidad de un Session Border Controller, dentro de la estructura de servicio que brindan los proveedores de telefonía hacia los clientes corporativos de telefonía fija y móvil.

Los proveedores de telefonía están en la actualidad observando y agregando esta solución a los análisis financieros que comparan los costos de implementación versus ingresos y así incluirlo en la mayoría de las implementaciones, en donde la rentabilidad lo permita, consiguiendo una frontera, que tiene grandes ventajas hacia la integración exitosa de clientes y proveedores.

Por el lado del cliente, al poder manejar este tipo de equipos, brindan un mayor nivel de seguridad a su tráfico, y concentran sus soluciones de telefonía a generar la mayor cantidad de servicios orientado a la operación entre agentes, supervisores y clientes finales.

Finalmente, el tiempo de implementación de un proyecto se ve optimizado, ya que del lado del proveedor se define un estándar de implementación, que crea servicios muy rápidamente en las plataformas del core de telefonía, sin tener que hacer cambios que podrían afectar globalmente a todos los clientes.

Los operadores de telefonía pueden tener talento humano que vea directamente estas implementaciones y se encarguen de que el Session Border Controller solucione la mayoría de los problemas de integración de este tipo de servicios.

4.2 Recomendaciones

Los servicios de telefonía en especial los de telefonía fija, son soluciones tradicionales, que deben converger para no ser desplazados por la tecnología. Un equipo Session Border Controller, aparte de brindar todas las características analizadas en este documento, puede brindar, una integración, a soluciones

modernas de tecnología, como las que estamos manejando actualmente a nivel mundial, por COVID19.

La pandemia, que tiene una afectación mundial, ha acelerado una transformación digital, y una de ellas, es el teletrabajo y la educación. Con estas necesidades, aplicaciones como Zoom y Teams, han venido para quedarse. Aquí la telefonía, puede servir de servicio complementario, para integrar, a usuarios que hayan tenido problemas de conectividad.

Las soluciones brindadas por Session Border Controller, deben de seguir integrando más soluciones de comunicación. Un servicio que actualmente no se está requiriendo es endpoints de videoconferencia, ya que las reuniones por distanciamiento social están en algunos casos restringidas.

Una buena recomendación, es integrar estas soluciones con Teams y a su vez con troncales telefónicas. Estos conectores, actualmente no funcionan para todos los fabricantes y es un desarrollo tecnológico que debe impulsarse.

BIBLIOGRAFÍA

[1] E. Landívar, de *Comunicaciones Unificadas con Elastix Volumen 1*, 2011, p. 268.

[2] A. G. PhD, «Sistemas de VOIP,» Guayaquil, 2015.

[3] D. Marcano, «NGN e IMS,» Guayaquil, 2015.

[4] H. T. C. Ltd, «UGC3200 Product Introduction,» Guayaquil, 2015.

[5] U. Marrochi, «Audiocodes SBC Essentials & Configuration v. 6.8,» Guayaquil, 2015.