cgc-eu

Documento técnico

SIPTRUNK

NUESTRA SOLUCIÓN

¿Desea trasladar su solución de telefonía tradicional hacia una solución de VoIP? ¿Usted posee ya una solución de telefonía IP?

La solución de Trunk SIP de CGC permite la recogida y la distribución de todas las llamadas salientes y entrantes. Esta oferta permite a las empresas que, como la suya, han elegido la centralización de sus infraestructuras de telefonía, armonizar los servicios propuestos en la totalidad del parque.

CGC les propone conectar directamente sus equipos en IP a través de la solución Trunk SIP, independientemente de la arquitectura ya instalada. Esta solución ofrece numerosas ventajas:

- Esta solución de Trunk SIP se adapta, cualesquiera que sean sus equipos de telecomunicaciones actuales: las funciones y servicios son homogéneas en todos los sitios clientes y, gracias a la portabilidad, el paso al Trunk SIP CGC es transparente;
- Gane tiempo con una solución rápida y simple de instalar: sin despliegue masivo en cada uno de sus sitios, solamente su sitio principal que alberga su PBX se ve afectado;
- Adapte sus usos gracias a la flexibilidad: ajuste su Trunk SIP al ritmo de su crecimiento o de sus actividades;
- Genere importantes ahorros en su servicio de telefonía: su gestión entre los sitios se simplifica, porque solamente los sitios principales están conectados. Además, ¡usted se beneficia de la gratuidad en las comunicaciones entre sus sitios!
- Usted se asegura una calidad telefónica de alta definición;
- Gestione los pedidos de sus servicios, el estado de su parque (números, portabilidades) y la facturación automática de sus sitios, centros o entidades;
- La solución Trunk SIP CGC es compatible con la mayoría de los IPBX del mercado.

» Lista de los IPBX aceptados e idóneos para la solución Trunk SIP CGC:

3CX, AASTRA, Alcatel·Lucent, Asterisk, AVAYA, cisco, FreeSWITCH, Gigaset, innovaphone PURE IP COMMUNICATIONS, SIEMENS, UNIFY, Yealink

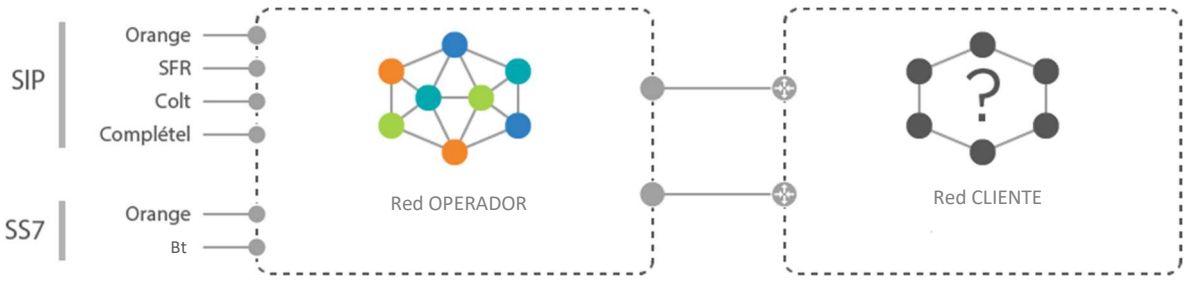
Nota:
Esta solución ha sido ensayada en los IPBX líderes en los mercados español. Si, por el contrario, el equipo elegido no está en la lista de los constructores/versión de software examinada, se deberán realizar pruebas de interoperabilidad.

La solución de Trunk SIP propuesta por CGC se basa en las características siguientes:

- Una conexión de acceso principal entre el/los equipos del cliente y las infraestructuras de CGC;
- Un dimensionamiento que se manifiesta en el «número máximo de comunicaciones simultáneas»;
- Unos números, geográficos o no de los sitios atribuidos o portados por CGC;

El dimensionamiento del Trunk SIP depende del volumen de tráfico telefónico entrante/saliente y del número de comunicaciones telefónicas simultáneas.

Estos elementos permiten establecer el dimensionamiento denominado «máximo» del Trunk SIP, así como las conexiones adecuadas que se instalarán entre la red del cliente y la infraestructura CGC.



Lo mejor de CGC:
Esta solución que se les ofrece está a la altura de la criticidad del servicio propuesto. Por esta razón, el servicio de Trunk SIP se asocia con una doble conexión del lado del operador sobre dos datacenters, así como una doble conexión, en la medida de lo posible, en combinación de tecnologías (Fibra o SDSL + ADSL de rescate).

1.2. RECOGIDAS Y DISTRIBUCIÓN DE LAS LLAMADAS

En el caso de subscribirse a una oferta Trunk SIP CGC, el tráfico entrante y saliente del conjunto de sus sitios es asumido por uno o dos puntos de recogida de su elección.

1.2.1. Recogida: Gestión del tráfico de llamadas entrantes

1.2.2. Recogida: Gestión del tráfico de llamadas entrantes

» Principio general de recogida de llamadas entrantes

Las comunicaciones establecidas con números de cliente; recogidas a partir de la red telefónica, son conducidas de forma global y no diferenciada, compartiendo la carga, hacia los softswitchs dedicados a la gestión de los Trunk SIP CGC.

Estas llamadas recogidas son enseguida conducidas de forma global y no diferenciada hacia el trunk SIP del cliente.

» Portabilidad de los números

Gracias a los mecanismos de portabilidad, usted conserva los números en la totalidad de sus sitios y ofrece a sus usuarios una solución completamente transparente.

El cliente podrá seguir en tiempo real, en cada sitio, el estado de las portabilidades en su interfaz de gestión de servicios. El cliente deberá previamente proporcionar a CGC:

- Los intervalos de geográficos a portar;
- El número de cabeza de línea de cada intervalo;
- El nombre del operador telefónico saliente de los números.

Cada solicitud de portabilidad será validada y firmada por el cliente para su validación ante el operador saliente.

El plazo de una portabilidad es:

- entre 3 y 5 días laborables.

El compromiso de servicio
CGC se compromete en todo el momento de la portabilidad a un plazo máximo de interrupción del servicio (en emisión y en recepción) de SEIS horas.
Según la experiencia y como información provisional, el tiempo de interrupción constatado generalmente es inferior a **dos minutos**.

» Funciones

CGC propone una gestión delicada de sus llamadas entrantes con la gestión de los reenvíos y de las restricciones. Usted puede definir de manera global todas sus llamadas entrantes por el sitio o bien por el SDA:

- Un reenvío inmediato;
- Un reenvío si no hay respuesta;
- Un reenvío si no hay conexión.

Por otro lado, usted tiene la posibilidad, de forma global o para cada usuario, de crear diferentes tipos de perfiles y de gestionar sus listas blancas y sus listas negras.

» Solicitar nuevos números

En complemento de la portabilidad de uno o varios números, CGC puede proporcionar tramos de número no geográficos extraídos de los intervalos que le son atribuidos por la CNMC. También es posible suministrar números geográficos.

En ese caso, la asignación de estos números se realiza respetando el plan de numeración. En todos los casos, el pilotaje se efectúa a través de la interfaz de gestión de los servicios suministrada por CGC.

1.2.1. Distribución: Gestión del tráfico de llamadas salientes

» Principio general de distribución de las llamadas salientes

El principio de enrutamiento de las llamadas salientes se aplica independientemente del tipo de llamada. Se aplica un tratamiento especial a las llamadas hacia los números de emergencia.

Según los mismos principios que para las llamadas entrantes, el SBC recoge las llamadas emitidas por el Trunk SIP del cliente y las distribuye de manera uniforme a los softswitchs dedicados a la oferta Trunk SIP CGC

» Interconexiones

CGC posee interconexiones multi-operadores. Esta redundancia permite asegurar en la salida una calidad óptima de las comunicaciones.

» Protección & medidas de seguridad

Con objeto de prevenir cualquier utilización fraudulenta del Trunk SIP CGC asignado al cliente (por ejemplo, en caso de intrusión o de error en los IPBX), un sistema de «*hack-limit*» permite vigilar el comportamiento del trunk y de activar las restricciones en los comportamientos anormales. Esta función se puede configurar a través de la herramienta de administración o por el Servicio Web.

1.2.2. Gestión de llamadas de emergencia

Los números de llamadas de emergencia son números de teléfono que permiten contactar con los servicios de emergencia a través de un número corto. CGC tiene la obligación de asegurar gratuitamente las llamadas de emergencia con destino al centro competente correspondiente a la localización del emisor de la llamada, así como la transmisión a los servicios de emergencia de las informaciones del emisor de la llamada (localización, número certificado, identidad). Los números de llamada de emergencia están adscritos a un centro de tratamiento definido de forma geográfica.

La gestión de la numeración de emergencia se gestiona por el operador con la oferta Trunk SIP CGC de manera totalmente transparente para el cliente.

1.3. RENDIMIENTO Y CALIDAD DE LA SOLUCIÓN VOZ

CGC utiliza 4 indicadores de calidad para medir los resultados de sus comunicaciones VoIP:

Pérdidas paquetes	Plazo distribución	Jitter	Mos

1.3.1. Índice de pérdidas de paquetes

Los paquetes pueden perderse durante la transmisión, en tal caso puede haber pérdidas o malos funcionamientos en la audición de la señal de voz descodificada. Los códecs incorporan a menudo el encubrimiento de la pérdida de Paquetes, lo que contribuye a ocultar los efectos de los paquetes perdidos o descartados. Este índice de perdidas (Tp) se define como la adición a 1 del cociente entre el número de respuestas recibidas (Tr) por el equipo de medida y el número de solicitudes emitidas (Te).

$$Tp(\%) = 1 - \frac{Tr}{Te}$$

1.3.2. Plazo de distribución

El plazo de distribución, denominado a veces de tránsito, se define como el valor del intervalo de tiempo entre la emisión y la recepción de un «eco» ICMP (Internet Control Message Protocol) (Protocolo de mensajes de control Internet), llamado generalmente «Ping». Si el retraso en el tránsito de los paquetes excede los 100 milisegundos, los usuarios empiezan a percibir el retraso. Si el retraso excede los 200 milisegundos, los usuarios pueden enfrentarse a dificultades en la conversación, a causa de la interrupción del “protocolo” de conversación normal.

1.3.3. Jitter

El tiempo de tránsito de los paquetes puede variar considerablemente. A esta variación del retraso se la denomina Jitter o variación del retraso del paquete. Un teléfono IP o pasarela incorpora un amortiguador de Jitter que aplica una débil cantidad de retraso, con objeto de atenuar estas variaciones de sincronización. Si los paquetes llegan demasiado tarde, serán siempre descartados de ahí la conversión por un amortiguador de jitter en retraso adicional y en pérdida de paquetes.
El jitter medio es calculado en el conjunto de los paquetes IP recibidos en un intervalo de tiempo dado.

1.3.4. Calidad de llamada

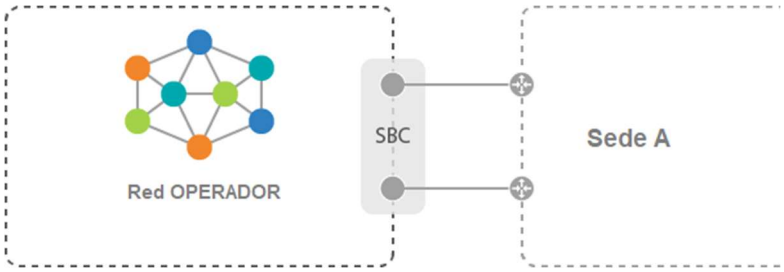
La calidad de una llamada se puede medir con pruebas subjetivas, pruebas intrusivas o monitorización no intrusiva. La calidad de la llamada se define generalmente conforme a los marcadores MOS. En el caso de CGC, las medidas se efectúan de un extremo a otro en la categoría «voz». Para efectuar las pruebas, une comunicación será utilizada por sitio «sondeado» y sitio «encuestador», y será reservada para las pruebas de forma permanente. CGC calcula la nota de MOS en base al códec «G.729», con objeto de limitar la banda ancha necesaria para la circulación de las pruebas.

ANEXO 1: ARCHITECTURA DEL TRUNK SIP

La solución Trunk SIP propuesta por CGC se adapta a la arquitectura existente y a sus prerrequisitos técnicos y geográficos, único o múltiples sitios.

Topología centralizada (un sitio principal)

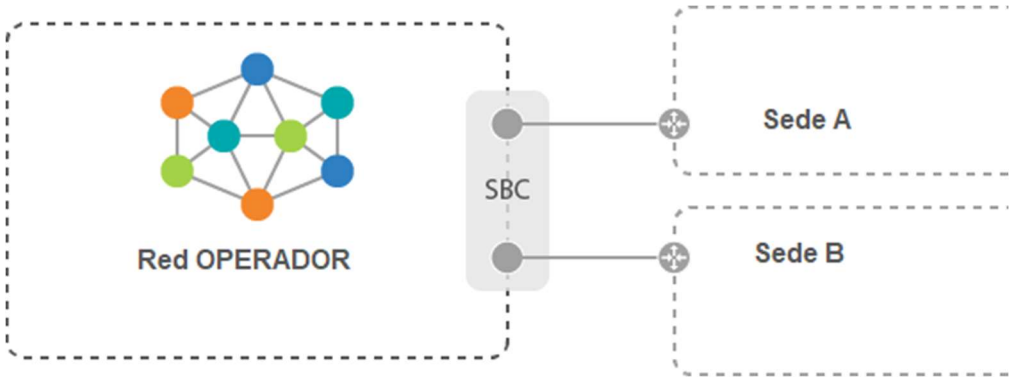
En el caso de que su Empresa posea un único sitio, o bien un sitio principal importante con pequeñas filiales o agencias, esta topología centralizada corresponde a sus necesidades.



La gran parte del tráfico llega al sitio principal. El o los equipos in situ se ocuparán de la distribución interna a la empresa, con destino a las agencias y filiales.

Topología distribuida (dos sitios)

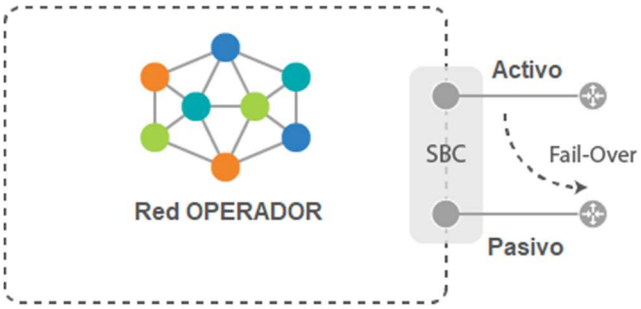
En el caso de que su Empresa no esté muy fragmentada y comporte varios sitios importantes, es también posible conectar las conexiones de recogida en dos sitios, independientemente del modo de utilización de sus conexiones (en modo «Global & Auxilio» o bien en «Reparto de carga»)



ANEXO 2: REDUNDANCIA DEL TRUNK SIP

Modo «Global & Help»

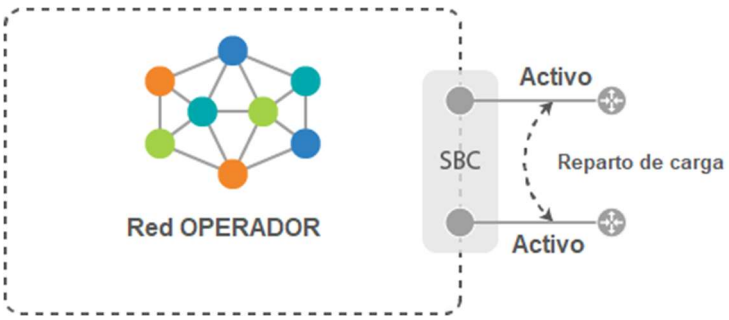
El sitio cliente se conecta mediante dos conexiones en tecnología mixta: una conexión «activa», utilizada en función global y una conexión «pasiva» utilizada en rescate, para asegurar un funcionamiento óptimo, incluso en modo degradado.



La transición– o «Fail-Over» de una conexión hacia la otra se efectúa en menos de 90 segundos. En caso de cambio de conexión, se interrumpen las conversaciones con el exterior. Las conversaciones internas al sitio pueden continuar.

Modo «Reparto de Carga»

El sitio cliente está también conectado con dos conexiones de tecnología mixta, pero las dos conexiones están «activas». CGC preconiza este tipo de seguridad para los sitios que deben estar en todo momento operativos, y gestionar la distribución y la gestión del tráfico.



El tráfico se reparte entre las conexiones de acceso. En caso de fallo de una conexión o de un equipo distante, el SBC CGC detecta el error y dirige la totalidad del tráfico hacia la conexión que permanece operativa.

ANEXO 3: DISPOSITIVOS DE SEGURIDAD

Confidencialidad

Los flujos entre nuestras infraestructuras y nuestros transportistas utilizan interconexiones físicas directas, sin pasar por la Internet pública. Por otro lado, nuestras propias infraestructuras, como se indica en el párrafo precedente, responden a criterios de seguridad de muy alto nivel, y están en conformidad con las certificaciones y particularmente con el RGS.

Desde un punto de vista legal, nosotros garantizamos en toda la cadena de las comunicaciones la conservación de las identidades reales de todas las llamadas que pasan por nuestra red, incluidas las llamadas anónimas y las que presentan identidades falsas.

Autentificación de las comunicaciones

Desde un punto de vista protocolario SIP ofrecemos dos soluciones de autentificación:

- Nuestros sistemas conocen las direcciones IP de los equipos de interconexión de los clientes (los dos pares de SBC ACME) y rechazan las llamadas procedentes de una fuente desconocida mediante el posicionamiento de normas de firewall (IP ACL).
- Además, los intercambios pueden ser igualmente autentificados por parejas usuario/contraseña, que permiten verificar los intercambios SIP. Este método está a menudo reservado para los equipos móviles, que deben poder unirse a nuestras infraestructuras, desde cualquier dirección originaria.

Perfiles de consumo & protección

Proponemos la posibilidad de definir unos perfiles de consumo "normal" en los trunks, que permita así reaccionar en directo si las infraestructuras del centro de trabajo llegaran a verse comprometidas. En ese caso, en caso de pirataje de los centros de telefonía del cliente (Alcatel OXE, o cualquier equipo vinculado), estamos en condiciones de detectar los usos telefónicos anormales y restringir dinámicamente las llamadas autorizadas, con objeto de evitar los fraudes telefónicos, y, en consecuencia, las facturas elevadas para el cliente.

Por otro lado, el uso de los equipos de tipo SBC garantiza una protección total y un bloqueo automático contra los ataques de fuerza bruta/de diccionario, ataque por paquetes mal formateados, etc.