Diseño e implementación de una solución de voz IP para la Registraduría de Antioquia

Viviana Andrea Rojas Giraldo

Ingeniería de Telecomunicaciones

Director(es) del trabajo de grado

Pedro Guerrero

INSTITUTO TECNOLÓGICO METROPOLITANO

15 de febrero de 2016

RESUMEN

Palabras clave: codecs, telefonía, GoS, VoIP, seguridad, Optimización tráfico, QoS, MPLS

Desde el invento del teléfono hasta la época actual, las comunicaciones telefónicas son indispensables en el desarrollo tecnológico, cultural y social de cada entorno a nivel mundial. En su desarrollo, los cambios de tecnología como pasar de un sistema análogo a uno digital y la utilización de nuevos protocolos han permitido la implementación y la oferta de nuevos y mejores servicios. Paralelamente se busca la optimización de recursos que conlleva a menores costos de implementación y sostenimiento para ofrecer precios y servicios competitivos a los usuarios.

Actualmente la plataforma de internet ha convergido servicios que permiten desarrollar nuevas estrategias de comunicación y el desarrollo de aplicaciones que se orientan a la utilización de todos los recursos disponibles a la vez que minimiza los costos de las nuevas implementaciones tecnológicas. La voz Ip se encuentra soportada por el conjunto de protocolos de comunicación TC/IP y es hoy uno de los servicios más utilizados para minimizar el impacto del consumo telefónico y lograr extender la comunicación a cualquier ámbito sin límites de tecnología ni distancia.

El presente proyecto tiene por objetivo diseñar e implementar una solución para el sistema de comunicaciones actual de la Registraduría Nacional del Estado Civil en Antioquia y que será soportado por una plataforma de voz sobre Ip proyectado a todo el Departamento a fin de mejorar las comunicaciones internas de los usuarios, facilitar la comunicación externa y minimizar el consumo de recursos. El diseño y la implementación se orientan, en lo posible, con el aprovechamiento de recursos disponibles, utilizando herramienta Open Source y dispositivos existentes. El análisis de la infraestructura de comunicaciones y los requerimientos establecidos para la implementación, tiene en cuenta aspectos importantes para la optimización del tráfico y establecer niveles adecuados de seguridad en el sistema de comunicaciones.

RECONOCIMIENTOS

Profesor Pedro Guerrero, por su asesoría y acompañamiento en la elaboración y desarrollo del trabajo.

A Nicolás Calle, coordinador del centro de sistemas de la Delegación de Antioquia por avalar el proyecto y a sus aportes al desarrollo del mismo.

Gabriel Darío Montoya, por su ayuda.

ACRÓNIMOS

VoIP	voz sobre IP
IP	protocolo de internet
VPN	red virtual privada
GoS	grado de servicio
PMT	proyecto de modernización tecnológica
WLAN	red de área local inalámbrica
SIP	protocolo de inicio de sección
CODEC	codificador – decodificador
NAT	traducción de direcciones de red
RTP	protocolo de transporte en tiempo real
WAN	red de área amplia
QoS	calidad de servicio
IAX	protocolo de intercambio entre asterisk
DoS	servicio de navegación
PBX	Central Secundaria Privada Automática
UDP	protocolo de datagrama de usuario
TCP	protocolo de control de transmisión
PPS	paquetes por segundo
DSP	procesador de señal digital
MPLS	Conmutación Multi-Protocolo mediante Etiquetas

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

El sistema de comunicaciones telefónico de la Registraduría Nacional del Estado Civil se encuentre operando en un 100% con los sistemas actuales que ofrecen los operadores de telefonía en cada una de sus sedes. Una comunicación con el ente del estado se origina tanto desde el usuario externo como de los funcionarios a nivel interior quienes a su vez se enlazan con sus sedes distribuidas en todo el territorio Nacional. La infraestructura actual presenta alta congestión por la demanda del servicio que se enfoca a todos los procesos de identificación de las personas y eventos democráticos como elecciones de representantes locales y nacionales.

En Antioquia, la Delegación Departamental soporta el sistema de comunicaciones que enlaza todos los municipios del departamento; para esta tarea cuenta con 20 líneas telefónicas y una en cada sede municipal. A la alta congestión del sistema se suma las políticas restrictivas de operación o gestión establecidas por oficinas centrales. En este panorama se atiende a una población de 2.464.322 Medellín y 3.821.797 para toda el área metropolitana, siendo en todo Antioquia un total de 6.456.207 personas distribuidas en los 125 municipios.

El desarrollo del proyecto cumple con dos objetivos generales: Por una parte, se elabora como requisito para optar al título de Ingeniera de Telecomunicaciones y por otra, se diseña e implementa una solución que garantice el adecuado manejo de los recursos existentes de los medios de comunicación que impacta el gasto público y repercute en un mejor desempeño de las funciones básicas de los usuarios y en general en beneficio de la sociedad. En la primera parte del documento se abordan las teorías generales que involucran el desarrollo del proyecto, de igual forma se contextualiza el área o el objeto de aplicación del trabajo realizando una breve descripción de la Registraduría Nacional del Estado Civil y de una de sus dependencias: la Delegación Departamental de Antioquia con sus 125 registradurías municipales. En la segunda parte se desarrolla paso a paso la metodología planteada realizando el análisis de la infraestructura actual, las políticas de administración y en general las condiciones de operación del sistema de comunicaciones actual. Posteriormente se analizan los elementos adicionales requeridos para ofrecer una solución a la problemática descrita y con el fin de dinamizar y agilizar los procesos que orientan a la obtención de mejores resultados en todos los campos de desempeño del que hacer de los usuarios de la Registraduría en Antioquia.

Finalmente se detalla el diseño del sistema y la arquitectura de comunicaciones a implementar con lo cual se logró mejorar el sistema de comunicaciones interno con la optimización de recursos técnicos del canal de comunicaciones existente. Esta solución impacta y enaltece el buen nombre de la Registraduría Nacional con una mejor calidad en la prestación de sus servicios en la Delegación Departamental de Antioquia y sus 131 Registradurías municipales, Auxiliares y Especiales. Así mismo, se describen las recomendaciones, conclusiones y trabajo futuro que se puede realizar derivados del presente proyecto.

Objetivos General

Diseñar e implementar un sistema de comunicaciones de voIp en la Delegación de Antioquia para comunicar las Registradurías del Departamento entre sí utilizando herramientas Open Source, aplicando métodos de optimización de tráfico y niveles adecuados de seguridad.

Objetivos Específicos

- Definir los mínimos requerimientos de tráfico para el soporte de una comunicación de voIP sobre los canales de acceso vigentes en la Delegación de Antioquia que soporte las 140 dependencias del Departamento.
- Diseñar la arquitectura de comunicaciones y servicios base de VozIP para la intercomunicación de las oficinas de Antioquia aplicando niveles mínimos de seguridad.
- Implementar el sistema de comunicaciones de Voz/IP entre la Delegación Departamental y dos sedes remotas de las Registradurías Municipales en Antioquia, proyectado a los 138 restantes del Departamento.

2. MARCO TEÓRICO

2.1 Antecedentes históricos

Para esta civilización que evoluciona vertiginosamente hacia la sociedad de la informática, los tiempos de respuesta y los sistemas de información son la clave del éxito de las empresas. La telefonía IP como herramienta para optimización de recursos en un sistema de comunicaciones.

La Registraduría Nacional del Estado Civil como entidad encargada de la identificación y la realización de los procesos electorales de los colombianos, ha requerido, requiere, y requerirá inversión permanente, progresiva y creciente en componentes tecnológicos y en la profesionalización del talento humano, unida a una política administrativa de proyección de la entidad como una empresa de Sistemas de Información fundamentada en su sistema de comunicaciones para la identificación y Procesos Electorales.

En su momento el proyecto de modernización tecnológica (PMT) de la Registraduría Nacional del Estado Civil, constituyo uno de los factores fundamentales para obtener eficiencia, efectividad, claridad y confianza en los procesos electorales y de identificación; pero este proyecto no abarco el sistema de comunicaciones en todas las fases del que hacer misional y aun se realizan procedimientos de administración de información manualmente con los correspondientes errores que ello conlleva. Se requiere soluciones, de manera urgente, que mejoren y complementen las funciones y la realización de las tareas.

El sistema de comunicaciones hace parte del engranaje fundamental de soluciones a los problemas de control de información en el procesamiento de cedulas de ciudadanía. Contribuye de manera óptima a la supervisión del flujo de documentos elaborados, pendientes, almacenados y entregados al ciudadano, con la generación de avisos y reportes dinámicos y estadísticos que facilitan al operador y a los administradores, conocer en cualquier punto del tiempo el comportamiento del sistema y del servicio.

Este sistema, cuya implementación se efectúa en primera instancia en la Delegación y Registraduría del Departamento de Antioquia, ha sido diseñada e implementada bajo los principios fundamentales de ingeniería de telecomunicaciones y de la tecnología de telefonía IP.

Se espera que dicha implementación no se muera tecnológicamente en el tiempo, por el contrario, su arquitectura abierta permite la integración con tecnologías y proyectos existentes y futuros

2.1.1 Registradurías Municipales

Están ubicadas en cada uno de los municipios del Departamento de Antioquia, las cuales fueron dotadas de un computador para el proceso de información. En ellas se captura los datos de la papelería que reciben, que les llegan y enviado a la Delegación Departamental de Antioquia (al igual que todos los departamentos en el país poseen la misma estructura y organización) o los Centros de acopio (CA) correspondientes donde es centralizada o consolidada toda la información.

Cuando el ciudadano requiere un servicio de la entidad se acerca a la respectiva oficina para la elaboración de su documento, y puede ser:

En primera instancia se elabora un registro civil de nacimiento, documento con el cual nace toda persona al mundo jurídico en el país. De este formato se generan Copias o certificados del registro y fotocopia del mismo. El documento se elabora una vez y su cancelación o modificación obedece a razones contempladas en ley, para tal evento. Otros trámites son el registro civil de matrimonio y el registro civil de defunción, de los cuales, también, se realizan certificados y fotocopias.

Seguidamente opera otro documento como es la tarjeta de identidad y la cual es vigente para la edad comprendida entre los 7 y 18 años de edad; en ella se consignan los datos básicos del registro civil del nacimiento y operan movimientos de primera vez, duplicado y rectificación, al igual que certificaciones de trámite.

Uno de los documentos más importantes, seguido del registro de nacimiento, es la elaboración de la cedula de ciudadanía, requerida cuando deja de ser vigente la tarjeta de identidad, es decir se tiene cumplido los 18 años. Este documento toma los datos base del registro civil de nacimiento y sobre el operan movimientos de duplicado, renovación (validad hasta el 2006) y rectificación, igualmente, se elaboran certificados de origen y autenticación cuando son requeridos por el usuario.

De todos los documentos anteriores se lleva un control del material utilizado y de los documentos que se elaboran, con el fin de desarrollar los respectivos resúmenes estadísticos y la sustentación del uso de los diferentes materiales.

2.1.2 Los centros de Acopio (CA)

Reciben cifras y los documentos de la Registraduría municipales, donde se procesa y se generan los respectivos informes para Oficinas Centrales, Delegación o cualquier otra entidad que requiera.

2.1.3 Delegación Departamental

Es el ente oficial administrativo, que funciona a nivel departamental y donde se consolida la información de todos los municipios pertenecientes a su Departamento.

Los cuadros resúmenes utilizados y enviados a esta dependencia, tiene en cuenta el tipo de documento utilizado, oficina y población, entre otros, así como los materiales dañados y empleados tienen su debido registro o control.

El proceso de solicitud y elaboración de registro civiles al ciudadano, en lo general no queda pendiente por proceso de realizarse a continuación de la solicitud, es decir, el documento es entregado al ciudadano e inmediatamente es ingresado a las bases de datos a nivel nacional.

Caso contrario ocurre con la solicitud de cedula: dicho trámite se realiza llenando la decadactilar la cual contiene un registro de control (número de preparación) y el número de cedula asignado al ciudadano. Una vez es diligenciado el formato, se envía a oficinas centrales donde es producida la cedula. En un tiempo aproximado de un año la cedula elaborada es enviada al municipio de trámite para ser entregada al usuario; este proceso genera movimiento de solicitud de cedula, llegada y entregada de cedula al ciudadano: tarea que se realiza manualmente en hojas o libros siendo dificultoso el control y su manejo. *(Giraldo Blandón, Pareja Bolívar, & Serna Guarín, 2004)*

2.2 Sistemas de comunicación de voz sobre IP

Este sistema de comunicaciones permite utilizar la plataforma de internet como un canal telefónico, permitiendo llevar la voz a cualquier destino sobre la red IP, proporcionando una base para agregar aplicaciones de comunicaciones unificadas más avanzadas, incluidas conferencias web y videoconferencias, que pueden transformar la forma en que se presta un servicio. De esta forma, detallamos algunas diferencias entre la telefonía tradicional y telefonía IP para que sea más fácil el reconocimiento de la opción que realmente traiga beneficios operativos y económicos al desempeño de las actividades de Empresariales.

características	Telefonía tradicional	Telefonía Ip
Ancho de banda	Menos ancho de banda	Mayor ancho de banda
Medio de transmisión	Cable de pares(línea telefónica)	Cable UTP(línea de internet)
Calidad de servicio	No hay que cumplir unos requisitos de calidad del servicio	La latencia tiene que estar entre 2000ms-3000ms
Servicios ofrecidos	Tarificación por tiempo Se establece llamada Ancho de banda fijo	Tarificación por ancho de banda No se establece llamada sino autenticación Ancho de banda variables
Tiempo de establecimiento	Aceptable para voz Muy largo para datos	No existe fase de establecimiento
Retardo de trasmisión	despreciables	Existe en toda comunicación Orden de mseg
Asignación de circuitos	Único y exclusivo para cada comunicación	Compartido por otra comunicaciones simultaneas
Identificación del destino	Solo en la fase de establecimiento	Se incluye un identificador en cada paquete
Necesidad de almacenar en la red	no	Si, en los nodos de la res
Flexibilidad de la red	Encaminamiento alternativo	Gran flexibilidad

Ilustración 1: Telefonía Tradicional Vs Telefonía Ip

Fuente: el autor

2.2.1 Arquitectura de VoIP

Terminales: teléfonos IP que pueden ser software o hardware.

- Hardware: terminales físicos con soporte VoIP nativo que pueden conectarse directamente a una red IP.
- Software: aplicaciones que simulan un teléfono con soporte VoIP. Pueden correr sobre cualquier dispositivo que disponga de conexión a la red (orde-nadores, móviles, etc.).

Servidor: provee el manejo y funciones administrativas para soportar el enrutamiento de llamadas a través de la red. Este elemento recibe distintos nombres en función del protocolo de señalización que se utilice. En un sistema basado en H.323, el servidor recibe el nombre de Gatekeeper. En cambio, en un sistema SIP, el servidor se conoce simplemente por Servidor SIP.

Gateway: dispositivo que hace de enlace con la telefonía fija tradicional. Actúa de forma transparente al usuario.

Red IP: provee conectividad entre todos los terminales. La red IP puede ser una red IP privada, na Intranet o Internet

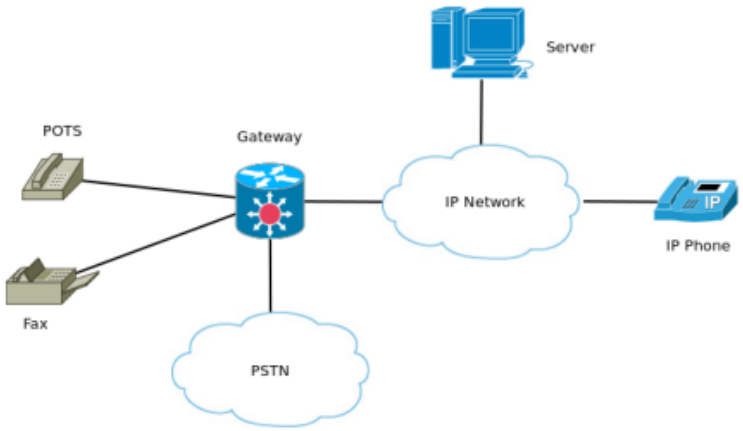


Ilustración 2: Arquitectura de VoIP

Fuente: (Domingo, *2014*)

Tipos de arquitectura de voz Ip

En el pasado, todas las redes de voz fueron construidas usando una arquitectura centralizada en la cual los Dumb Endpoints (teléfonos) fueron controlados por los conmutadores centralizados. Sin embargo, este modelo trabajo bien para los servicios de telefonía básica.

Uno de los beneficios de la tecnología VoIP, es que permite a las redes ser construidas usando una arquitectura centralizada o bien distribuida. Esta flexibilidad permite a las compañías construir redes caracterizadas por una administración simplificada e innovación de Endpoints (teléfonos), dependiendo del protocolo usado.

- **Arquitectura centralizada en VoIP**

En general, la arquitectura centralizada está asociada con los protocolos MGCP y MEGACO. Estos protocolos fueron diseñados para un dispositivo centralizado llamado Controlador Media Gateway o Call Agent, que maneja la lógica de conmutación y control de llamadas. El dispositivo centralizado comunica al Media Gateways, el cual enruta y transmite la porción audio/media de las llamadas (la información de voz actual).

En la arquitectura centralizada, la inteligencia de la red es centralizada y los dispositivos finales de usuario (endpoints) son relativamente mudos (con características limitadas). Sin embargo, muchas arquitecturas VoIP centralizadas usan protocolos MGCP o MEGACO.

Los defensores de la arquitectura VoIP centralizada, apoyan este modelo porque centraliza la administración, el provisionamiento y el control de llamadas. Simplifica el flujo de llamadas repitiendo las características de voz. Es fácil para los ingenieros de voz entenderlo. Los críticos de la arquitectura VoIP centralizada demandan que se suprimen las innovaciones de las características de los teléfonos (endponits) y que llegara a ser un problema cuando se construyan servicios VoIP que muevan más allá de características de voz.

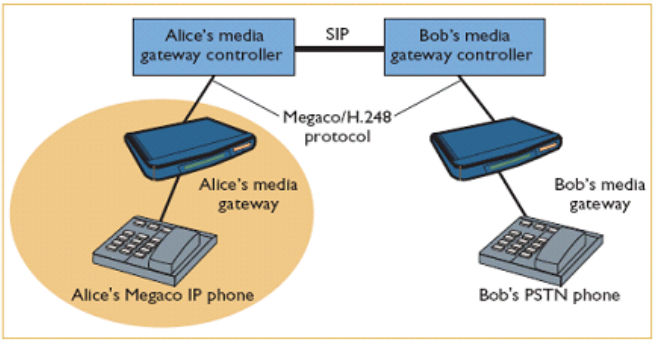


Ilustración 3: Arquitectura centralizada en VoIP

Fuente: ("Lección 19: Arquitecturas de VoIP," n.d.)

- **Arquitectura distribuida en VoIP**

La arquitectura distribuida está asociada con los protocolos H.323 y SIP. Estos protocolos permiten que la inteligencia de la red se distribuida entre dispositivos de control de llamadas y endpoints.

La inteligencia en esta instancia se refiere a establecer las llamadas, características de llamadas, enrutamiento de llamadas, provisionamiento, facturación o cualquier otro aspecto de manejo de llamadas. Los Endpoints pueden ser Gateways VoIP, teléfonos IP, servidores media, o cualquier dispositivo que pueda iniciar y terminar una llamada VoIP. Los dispositivos de control de llamadas son llamados Gatekeepers en una red H.323, y servidores Proxy o servidores Redirect en una red SIP.

Los defensores de la arquitectura VoIP distribuida apoyan este modelo por su flexibilidad. Permite que las aplicaciones VoIP sean tratadas como cualquier otra aplicación IP distribuida, y permite la flexibilidad para añadir inteligencia a cualquier dispositivo de control de llamadas o Endpoints, dependiendo de los requerimientos tecnológicos y comerciales de la red VoIP.

La arquitectura distribuida es usualmente bien entendida por los ingenieros que manejan redes de datos IP. Los críticos de la arquitectura distribuida comúnmente apuntan a la existencia de la Infraestructura PSTN como el único modelo de referencia que debiera ser usado cuando intentamos repetir los servicios de voz. Ellos también notan que las redes distribuidas tienden a ser más complejas. *("Lección 19: Arquitecturas de VoIP," n.d.)*

2.2.2 Seguridad en VoIP con plata formas abiertas

La seguridad en la telefonía IP consiste en proteger todos los componentes del sistema de telefonía IP, sobre una infraestructura de red de datos segura, para proporcionar tolerancia a fallos, estabilidad y escalabilidad, por eso se debe de pensar primero en proteger la red de datos y sus elementos más importantes como: *(Gil, 2012)*

- Protección en las redes Ethernet
- Protección en las redes WLAN
- Control de tráfico en diferentes zonas de seguridad
- Diferentes tipos de VPN

A medida que crece su implementación aumentan las preocupaciones por la seguridad de las comunicaciones y la telefonía IP (VoIP) es una tecnología que ha de apoyarse necesariamente en muchas otras capas y protocolos ya existentes de las redes de datos. Por eso en cierto modo la telefonía IP va a heredar ciertos problemas de las capas y protocolos ya existentes, siendo algunas de las amenazas más importantes de VoIP problemas comunes de seguridad que afectan de igual manera a las redes de datos. *(Campos Moreno & Guzman Munuera, 2008), (Alarcon Quigua, 2008)*

Seguridad en las aplicaciones y protocolos VoIp
Seguridad en el sistema operativo
Seguridad en los servicios
Seguridad de red
Seguridad fisica
Politica y Procedimiento

Aplicación	Elastix
Presentación	G.729/G.711
sesion	SIP
transporte	UDP/RTP/RTCP
Red	IP
Enlace	Ethernet
Fisica	Ethernet

Ilustración 4: Seguridad en VoIP

Fuente: el autor

2.2.3 VPN (red privada virtual)

Es una red privada construida dentro de una infraestructura de red pública, como por ejemplo Internet. Las empresas pueden usar una red VPN para conectar de manera segura oficinas y usuarios remotos por medio de un acceso a Internet económico suministrado por un tercero, en lugar de a través de enlaces WAN dedicados o enlaces de acceso telefónico de larga distancia.

Las organizaciones pueden usar una red VPN para reducir sus costes de ancho de banda de WAN, a la vez que aumentan las velocidades de conexión al usar la conectividad a Internet de ancho de banda elevado, tales como DSL, Ethernet o cable.

Una red VPN proporciona el máximo nivel de seguridad posible a través de Seguridad IP cifrada (IPsec) o túneles VPN Secure Sockets Layer (SSL) y tecnologías de autenticación. Estas redes protegen los datos que se transmiten por VPN de un acceso no autorizado. Las empresas pueden aprovechar la infraestructura de Internet fácil de aprovisionar de la VPN, para añadir rápidamente nuevos emplazamientos y usuarios. También pueden aumentar enormemente el alcance de la red VPN sin ampliar la infraestructura de forma significativa.

Una red VPN extiende la seguridad a los usuarios remotos.

Las redes VPN SSL y VPN IPsec se han convertido en soluciones de VPN principales para conectar oficinas remotas, usuarios remotos y partners comerciales, ya que:

- Proporcionan comunicaciones seguras con derechos de acceso específicos para los usuarios individuales, como por ejemplo empleados, contratistas o partners
- Mejoran la productividad al extender la red empresarial y sus aplicaciones
- Reducen los costes de las comunicaciones y aumentan la flexibilidad

Los dos tipos de VPN cifradas son:

- **VPN IPSec de sitio a sitio:** Esta alternativa a Frame Relay o a las redes WAN de línea alquilada permite a las empresas llevar los recursos de la red a las sucursales, las oficinas instaladas en casa y los sitios de partners comerciales.
- **VPN de acceso remoto:** Esta modalidad lleva prácticamente cualquier aplicación de datos, voz y vídeo al escritorio remoto, emulando el escritorio de la oficina principal. Una VPN de acceso remoto puede instalarse utilizando VPN SSL, IPsec o ambas, dependiendo de los requisitos de implementación. *(Cisco, 2010)*

Tunneling

El Tunneling, es un canal por el cual viajan los paquetes de datos, van cifrados; para posteriormente, ser descifrados por el usuario que esté autorizado para leer su contenido. El Tunneling, es uno de los métodos más utilizados para construir las VPN (Hamzeh, 1999).

Los mecanismos para realizar el tunneling más comunes:

- GRE (Generic Routing Encapsulation)
- Tunneling entre el origen y el router destino.
- Router a router
- L2PT
- PPTP

El Tunneling, abarca todo el proceso de encapsulación, enrutamiento y desencapsulación, en el cual envuelve, o encapsula, el paquete original dentro de un paquete nuevo, por lo que este paquete puede contener nueva información de direccionamiento y enrutamiento, que le permite viajar por una red. (Gutiérrez, 2015)

2.2.4 Optimización de tráfico de VoIP

La señal de telefonía IP y de videoconferencia IP puede verse afectada por diferentes factores*: (Ibarra Corretgé, 2008)*

La latencia o retardo de la señal: Las comunicaciones IP son servicios que no admiten latencia porque se trata de aplicaciones en tiempo real. Si la latencia de voz, en el caso de VoIP, sobrepasa los 250ms (milisegundos), la calidad de la llamada será pobre.

La pérdida de paquetes de datos (packet loss) a lo largo del viaje de la señal por una elevada tasa de error (no debe sobrepasar el 5%), o bien por la congestión del buffer de una interfaz, provocando el efecto de voces robóticas durante una llamada.

El jitter (audio de mala calidad): Al convertir la voz en paquetes de datos divididos que toman diferentes caminos entre emisor y receptor, pueden llegar a su destino de forma

desordenada produciéndose el efecto de jitter, imposibilitando la comunicación, debido a que las velocidades de llegada no son homogéneas.

Las claves que garantizan la calidad del servicio y controlar la pérdida de paquetes, la latencia y el jitter son: *(Landívar, 2008)*

Garantizar el ancho de banda

Para lograr calidad en la comunicación VoIP, se debe tener un canal dedicado o ancho de banda garantizado para dicha comunicación.

De esta forma se evitan las congestiones en la red y la pérdida de paquetes.

La correcta elección del códec facilita la optimización del ancho de banda.

Priorización de paquetes

Darles prioridad máxima a los paquetes de voz sobre el resto de los paquetes, harán que se disminuyan las demoras en la transmisión de los paquetes, garantizando que la latencia se encuentre dentro los parámetros recomendados.

La calidad de la red VoIP está 100% relacionada con la calidad que tendrán las comunicaciones del Contact Center.

2.2.5 MPLS (Multiprotocolo de Conmutación de Etiquetas)

Protocolo estandarizado por la IETF, tiene la característica de reenviar paquetes a través de una red usando información contenida en etiquetas añadidas a los paquetes IP; así mismo, utiliza RSVP (Resource Reservation Protocol) por sus siglas en inglés; (Protocolo para la Reservación de Recursos), como protocolo de señalización para la reserva de recursoS.

MPLS, reduce significativamente el procesamiento de paquetes que se requiere cada vez que un paquete ingresa a un router en la red, esto mejora el desempeño de dichos dispositivos y del desempeño de la red en general. Su principal objetivo es crear redes flexibles y escalables con un incremento en el desempeño y la escalabilidad. Esto lo logra mediante la ingeniería de tráfico, y su soporte de VPN, el cual ofrece calidad de servicio (QoS), con múltiples clases de servicio (CoS).

Las principales características de MPLS:

- Se configura a través de una red privada
- Permite garantizar latencias bajas y reducir la pérdida de paquetes

Integridad y confidencialidad de datos por VRF

- Permite implementar CoS y QoS
- Las VPN basadas en MPLS permiten compartir un único acceso a Internet entre todas las redes. No es necesario que las redes estén conectadas a Internet para acceder a la VPN
- No requiere por parte del cliente ningún software o hardware especifico.

Una red MPLS consiste de un conjunto de Routers de Conmutación de Etiquetas (LSR), los cuales tienen la capacidad de conmutar y rutear paquetes en base a la etiqueta que se ha añadido a cada paquete. Cada flujo es diferente y es llamado Clase de Equivalencia de Reenvío (FEC), así como también cada flujo tiene un camino específico a través de los LSR de la red, es por eso que se dice que la tecnología MPLS es "orientada a conexión".(Gutiérrez, 2*015*)

Ruteo basado en QoS. WSP y SWP

El ruteo basado en QoS ha sido un área de investigación muy activa por muchos años. Selecciona rutas en la red que satisfagan la QoS requerida para una conexión o grupo de conexiones. Además, el ruteo basado en QoS logra una eficiencia global en la utilización eficiente de los recursos. Un ejemplo de esto es al algoritmo Shortest-Widest-Path (WSP), el cual usa al ancho de banda como una métrica y selecciona los caminos que tienen un cuello de botella de ancho de banda mayor. El cuello de botella de ancho de banda representa la capacidad mínima no usada de todos los enlaces en el camino. En el caso de dos caminos con el mismo cuello de botella de ancho de banda, el camino con la mínima cantidad de saltos es seleccionado (Ver [4] por más información).

Los algoritmos de ruteo usados en CBR y la complejidad de los mismos, depende del tipo y del número de métricas que son incluídas en el cálculo de la ruta. Algunas de las restricciones pueden ser contradictorias (por ejemplo costo vs. ancho de banda, delay vs. throughput). Resulta que el ancho de banda y la cuenta de saltos son en general restricciones más útiles en comparación con el delay y jitter, ya que muy pocas aplicaciones no pueden tolerar una ocasional violación de dichas restricciones, y como el delay y jitter se pueden determinar por medio del ancho de banda alojado y número de saltos del camino donde va el flujo, éstas restricciones pueden ser mapeadas en restricciones de ancho de banda y número de saltos, en caso de ser necesario. Otro factor es que muchas aplicaciones en tiempo real requieren un determinado ancho de banda. El

número de saltos de una ruta también es una métrica importante, ya que cuantos más
Saltos atraviese un flujo, más recursos consumirá.

Con las implementaciones básicas del esquema de CBR, hay una especie de balance y equilibrio entre la conservación de recursos y el balance de carga. Un esquema de CBR puede seleccionar de las siguientes opciones para un camino viable para un flujo:

- **Shortest-Distance Path (SDP):** éste acercamiento es básicamente el mismo que el ruteo dinámico. Hace énfasis en preservar los recursos de la red por medio de la selección de los caminos más cortos.
- **Widest-Shortest Path (WSP):** éste acercamiento hace énfasis en balancear la carga por medio de la elección de caminos más "anchos" en cuanto al ancho de banda. Encuentra caminos con el mínimo número de saltos y, si encuentra múltiples caminos, se queda con el que tiene ancho de banda mayor.
- **Shortest-Widest Path (SWP):** éste acercamiento hace una especie de intercambio entre los dos extremos. Favorece a los caminos más cortos cuando la carga de la red es pesada y a los caminos más "anchos" cuando la carga de la red es moderada. Encuentra un camino con el ancho de banda más grande y, en caso de haber múltiples caminos, se queda con el que tiene la mínima cantidad de saltos.

En los últimos dos casos se consumen más recursos, lo cual no es eficiente cuando la utilización de la red es alta. Se debe hacer un balance o equilibrio entre la conservación de recursos y el balance de carga.

Vale hacer notar en este momento, que cualquiera de las 3 opciones superiores se pueden implementar en el software NET-TE, combinando correctamente la elección del tipo de pesos para los enlaces con la elección del criterio de TE. (Delfino, Rivero, & SanMartín, 2006)

2.2.6 Calculo de ancho de banda en Voip

Hay diferentes capas de empaquetamiento en la red (requeridos por el modelo OSI de 7 capas). El audio codificado necesita ser empaquetado dentro de paquetes RTP. A su vez, los paquetes RTP necesitan ser empaquetados dentro de paquetes UDP, que luego necesitan ser empaquetados dentro de paquetes IP. Ethernet es el tipo de red más común, y requiere otro empaquetamiento.

Para hablar de estos paquetes se referirán a estos colectivamente como **overhead**. Independientemente del codec utilizado, el overhead introducido en el paquete está fijo. Abajo se encuentra el overhead introducido por cada item:

RTP – 4.8 kbps

UDP – 3.2 kbps

IP – 8 kbps

Ethernet (sin utilizar QOS) – 15.2 kbps

El overhead total es de 31.2 kbps.

La Voz sobre IP (VoIP) requiere una cierta cantidad de ancho de banda para funcionar correctamente. Esta es la tasa de transferencia de datos y se mide en bits por segundo (bps). La fórmula utilizada para calcular el ancho de banda requerido por llamada es:

Ancho de banda = tamaño total de paquetes * PPS

donde PPS significa "paquetes por segundo" y se calcula de la siguiente manera:

PPS = (tasa de bits de códec) / (tamaño de la carga útil de voz).

El otro elemento del cálculo del ancho de banda, el tamaño total del paquete, se calcula:

Tamaño total del paquete = (cabecera de capa 2) + (cabecera IP/UDP/RTP) + (tamaño de la carga útil de voz).

Codec utilizado en la transmisión de VoIP. Un codec es un estándar de conversión del sonido a la señal digital y viceversa. Hay ocho diferentes codecs más utilizados, algunos de los cuales pueden tener más de una tasa de bits. La tasa de bits de codec se deriva del tamaño de muestreo de codec / intervalo muestreo de codec. El tamaño de muestreo de codec es el número de bytes capturados por el Procesador de Señal Digital (DSP) en cada intervalo de muestreo de codec.

A continuación, se observa una lista de codecs y su velocidad de bits*: ("Calcular Ancho de Banda en VoIP | ElastixTech - Aprende Telefonia IP Asterisk - Elastix," n.d.)*

Nombre	Estandar	Bit rate (kb/s)	Sampling rate (kHz)	Frame size (ms)	MOS (Mean Opinion Score)
G.711	ITU-T	64	8	Muestreada	4.1
G.723.1	ITU-T	5.6/6.3	8	30	3.8-3.9
G.726	ITU-T	16/24/32/40	8	Muestreada	3.85
G.729	ITU-T	8	8	10	3.92
GSM	ETSI	13	8	22.5	3.5-3.7
Speex	-	8, 16, 32	2.15-24.6 (NB) 4-44.2 (WB)	30 (NB) 34 (WB)	-
iLBC	-	15.2 / 13.3	8	20/30	4.1

Ilustración 5: Codecs

Fuente: *(Sierra Rodríguez & others, 2008)*

2.2.7 Protocolos utilizados en VoIp

2.2.8 SIP (Session Initiation Protocol)

Es un protocolo de señalización cuya función principal es crear, modificar y terminar sesiones a través de redes IP. Para ello permite localizar a los usuarios e intercambiar información de los medios implicados en la sesión. Es totalmente independiente del tipo de sesión a establecer, por lo que puede ser usado para iniciar conversaciones de voz, videoconferencias, aplicaciones compartidas, etc. También es independiente del protocolo de transporte (UDP, TCP, TLS/TCP) y del protocolo usado para negociar los parámetros de la sesión, que por defecto es SDP (Session Description Protocol). Al ser un protocolo muy genérico y versátil, se pueden implementar numerosas aplicaciones y funcionalidades.

Características Principales de SIP

SIP se describe como un protocolo de control para crear, modificar y terminar sesiones con uno o más participantes. Estas sesiones incluyen conferencias multimedia de Internet, o de cualquier red IP, llamadas telefónicas y la distribución multimedia. Los miembros en una sesión pueden comunicarse a través de multicast o por medio de una malla de relaciones unidifusión, o mediante una combinación de éstos. SIP soporta descripciones de la sesión que permitirá a los participantes a un acuerdo sobre un conjunto de tipos de medios compatibles. También es compatible con la movilidad del usuario, representando y redirigiendo las peticiones a la localización actual del usuario. SIP no está ligado a ningún protocolo de control de conferencia en particular.

Otra de las grandes tareas es garantizar que la llamada llegue a su destino. La realización de cualquier asignación de información descriptiva de la información de ubicación. Esto permite que el grupo involucrado en una llamada (puede ser una llamada en conferencia) se pone de acuerdo sobre las funciones admitidas, reconociendo que no todas las partes involucradas pueden soportar el mismo nivel de características. Por ejemplo, el vídeo puede ser o no ser compatible.

En una llamada un participante puede gestionar la misma, esto quiere decir que puede invitar a otros participantes en la llamada o puede cancelar las conexiones a otros usuarios, además de que los usuarios pueden ser transferidos o puestos en espera.

Un usuario tiene la posibilidad de cambiar las características de llamada durante el curso de la misma. Por ejemplo, una llamada puede haber sido creada con la característica de voz, pero en el transcurso de la llamada, los usuarios pueden necesitar para habilitar una función de vídeo. Un tercero puede unirse a una llamada puede y requerir diferentes características para estar habilitado y participar en la convocatoria.

Para no definir un nuevo sistema de direccionamiento, en algunos casos las direcciones de usuarios SIP están asociadas al correo electrónico. Cada usuario es identificado mediante una dirección URL jerárquica que se construye alrededor de elementos como el número de teléfono de un usuario, o el nombre del host por ejemplo, (sip:usario@compañia.com). Esto significa que es más sencillo para redirigir a alguien a otro teléfono, ya que es como redirigirse a una página web.

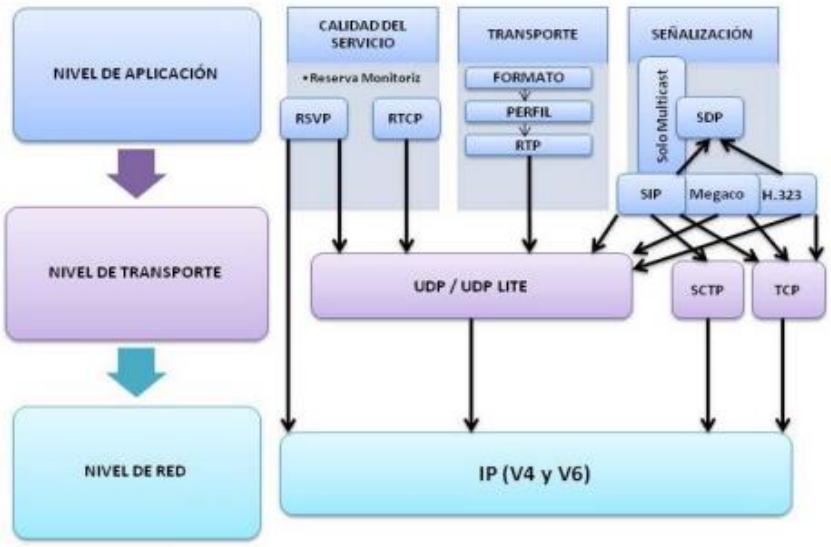


Ilustración 6: Protocolos sobre IP

Fuente:(Utilizados, Llamadas, & Troubleshooting, 2015)

Solicitudes SIP

Las solicitudes SIP tienen la característica de tener una línea de solicitudes para establecer la comunicación, SIP usa mensajes para la conexión y control de llamadas. Esta especificación define seis métodos básicos:

- **REGISTER:** El propósito es dejar un registro de acerca de la ubicación del usuario actual, información tal como lo es dirección IP y el puerto por el cual ha realizado el registro de mensajes.
- **INVITE:** Indica que un cliente está siendo invitado a participar en una llamada.
- **ACK:** Confirma la recepción del método Invite el cual es el que indica que se encuentra listo para establecer una comunicación.
- **BYE:** Este tipo de mensajes son utilizados para finalizar las sesiones multimedia, el que desee finalizar la conversación envía un Bye.
- **CANCEL:** Se utiliza para cancelar una sesión que no se ha establecido en su totalidad, es decir cuando el destinatario no ha confirmado una respuesta definitiva.
- **OPTIONS:** Consulta la información acerca de las capacidades de envío y recepción de teléfonos SIP.

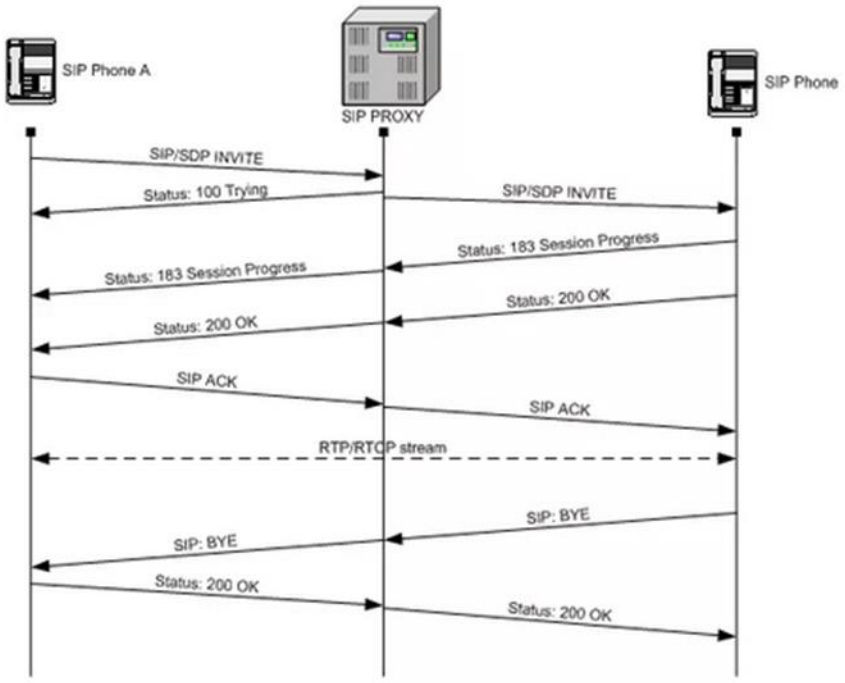


Ilustración 7: Solicitudes de SIP

Fuente: (Znaty, Dauphin, & Geldwerth, 2005)

Respuestas SIP

Cuando un agente de usuario o el servidor proxy reciben una solicitud, envía una respuesta. Cada solicitud debe ser respondida, excepto las solicitudes de ACK que no devuelven algún tipo de respuesta.

Las respuestas tienen un código de 3 dígitos, que coincide con los usados en HTTP, y que dependiendo del primer dígito del código tiene un significado distinto. Se pueden dividir en respuestas provisionales (1xx) y finales (2xx-6xx). Una transacción está formada por ninguna o varias respuestas provisionales y una sola respuesta final.
El código de respuesta es un número entero de 100 a 699 El cual indica el tipo de la respuesta. Hay seis clases de respuestas; Los tipos de respuesta en función del primer dígito son:

- 1xx: Respuestas provisionales, dan información, pero no finaliza una transacción.
- 2xx: Respuestas de éxito, indican que la petición ha tenido éxito.
- 3xx: Respuestas de redirección, la petición no ha tenido éxito, pero redirigen a otra dirección.

- 4xx: Respuestas de error del cliente que hizo la petición.
- 5xx: Respuestas de error del servidor que atiende la petición.
- 6xx: Respuestas de error globales a toda la red.

Problemas con SIP

NAT:

Puesto que el protocolo SIP fue creado pensando que no existiría el NAT y que todos los equipos IP tendrían asignada una IP pública (IPv6), con un NAT de por medio, SIP tiene dos problemas importantes:

- No es posible que dos teléfonos IP se envíen paquetes de voz entre sí través de la WAN utilizando las IP privadas de dichos teléfonos. Los paquetes RTP deben de ir dirigidos hacia las IP públicas del lado WAN de los respectivos routers.
- Aunque un paquete RTP se dirija correctamente hacia la IP pública de lado WAN de un router, no pasará a través del NAT y no llegará al teléfono SIP de destino si no existe en el NAT una asociación IP privada-puerto/IP pública-puerto. Es decir, si previamente no ha habido una conexión saliente a través de dicho NAT.

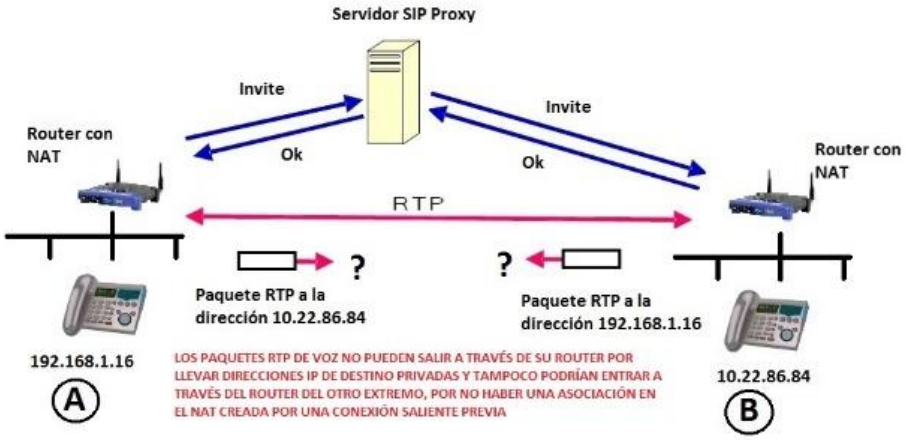


Ilustración 8: Conexión a través de NAT

Fuente: (Utilizados et al., 2015)

Dos graves problemas del protocolo SIP debidos al NAT

Se puede pensar a primera vista que el primero de los problemas tiene fácil solución si durante la fase de señalización SIP el SIP Proxy informa a cada teléfono SIP de la IP pública

y puerto a donde tiene que enviar los paquetes RTP de voz. Pero esta función exige modificar el contenido de los paquetes SIP ya que no es posible hacerlo mediante una simple modificación de direcciones IP en la cabecera de los paquetes SIP por parte del SIP Proxy.

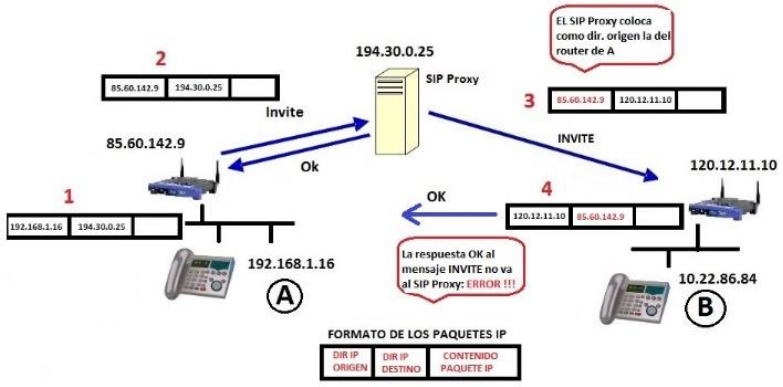


Ilustración 9: SIP Proxy

Fuente: (Znaty et al., 2005)

Un SIP Proxy retransmite mensajes SIP entre los extremos, pero no los modifica

En el diagrama anterior se observa que, si el SIP Proxy intenta informar al teléfono B de la IP pública del teléfono A colocando dicho valor en el campo DIR IP ORIGEN del paquete enviado, entonces la señalización SIP falla, ya que el mensaje de respuesta OK al mensaje INVITE no llega hacia quien envió dicho paquete, el SIP Proxy. Por lo tanto, la IP pública y puerto a donde se deben de dirigir los paquetes RTP de voz la deben de colocar en el interior de los mensajes SIP de INVITE los teléfonos SIP que quieren intervenir en la conversación. Pero para poder hacer esto es necesario que los teléfonos SIP conozcan los valores de IP pública y puerto con los que salen al lado WAN y para conseguir eso se utilizan los Servidores STUN (Session Traversal Utilities for NAT), cuyo funcionamiento se muestra en el siguiente diagrama:

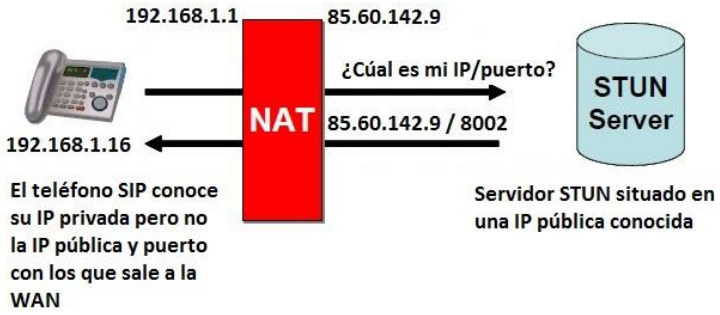


Ilustración 10: Funcionamiento Servidor STUN

Fuente: (Utilizados et al., 2015)

Cada uno de los teléfonos que participa en la conversación debe de acceder a un servidor STUN para conocer su IP y puerto con el que sale al exterior. Lógicamente los servidores STUN se encuentran siempre en direcciones IP públicas conocidas.

Utilizando este servidor STUN, o cualquier otro que esté configurado, el softphone es capaz de encontrar la IP pública con la que sale al exterior y utiliza esos valores para informar al teléfono SIP del otro extremo de la dirección y puerto donde debe de enviar los paquetes RTP de voz.

El protocolo STUN es simple y efectivo, y con él resolvemos el problema de como hace un teléfono IP para conocer la IP pública y puerto con los que sale hacia el lado WAN. Pero todavía tenemos el segundo problema: Debe de haber una asociación creada en el NAT para que entren paquetes de voz RTP desde el lado WAN hacia un teléfono SIP que está situado en el lado LAN. Y según el tipo de NAT utilizado, este problema tiene a su vez dos soluciones distintas:

- Si el NAT es de tipo Full Cone entonces la solución es inmediata. Cualquier paquete RTP de voz con destino a la IP pública-puerto utilizada para la comunicación con el SIP Proxy o con el servidor STUN será enviado por el NAT al teléfono SIP correspondiente. Y esto es así, aunque los paquetes RTP de voz provengan de una IP diferente, ya que en el NAT de tipo Full Cone no se examina ni la dirección IP de origen de los paquetes ni el puerto.

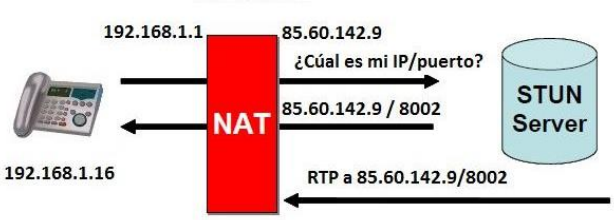


Ilustración 11: NAT de tipo Full Cone

Fuente: (Znaty et al., 2005)

- Si el NAT es de cualquiera de los otros tres tipos, Restricted Cone, Port Restricted Cone o Symmetric entonces es imprescindible además que los paquetes de voz RTP tengan como dirección de origen la propia del SIP Proxy o la del servidor STUN, ya que en estos tipos de NAT solo se dejan pasar paquetes hacia el lado LAN si provienen de la IP pública del lado WAN con la que se ha establecido la conexión de salida. Es decir, los paquetes de voz deben atravesar el SIP Proxy o el servidor STUN, lo cual es algo para lo que, en principio, no está pensado ninguno de los dos servidores.

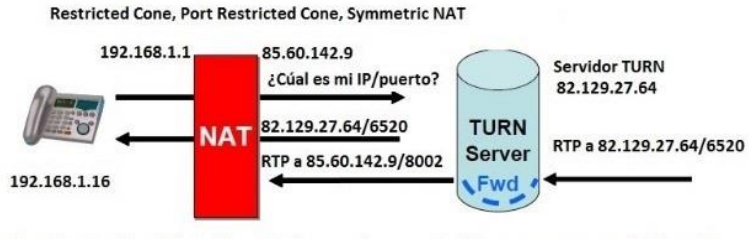


Ilustración 12: los otros tres tipos de NAT

Fuente: (Utilizados et al., 2015)

Los Firewalls:

Los cortafuegos a menudo impiden a dos equipos SIP la recepción de tráfico entrante o saliente RTP o incluso la propia señalización SIP. La única solución para que la VoIP mediante SIP funcione correctamente es identificar correctamente que puertos TCP/UDP deben ser abiertos. En cuanto a la señalización SIP no suele haber especiales problemas puesto que se utilizan puertos conocidos (5060 UDP). En el caso de los paquetes de voz el problema puede ser más complicado porque dependerá de la PBX IP que estemos utilizando para la

comunicación. En cualquier caso, hay que evitar en la medida de lo posible el abrir todos los puertos TCP y UDP.

Encriptación de las comunicaciones:

En una comunicación SIP es necesario proteger tanto la fase de señalización como la propia fase de transporte a través del protocolo RTP. La primera parte se garantiza mediante el denominado protocolo TLS (Transient Layer Security), que es justo el protocolo utilizado en las comunicaciones mediante https. La segunda parte obliga a utilizar el protocolo SRTP, que significa "secure RTP". Esto complica de nuevo las comunicaciones SIP ya que el protocolo es muy complejo y a menudo no hay compatibilidad entre diferentes fabricantes de equipos SIP. (Utilizados et al., 2015), (Znaty et al., 2005)

2.2.9 Estándar H.323

Define los requisitos para sistemas de comunicaciones multimedia en situaciones en donde el transporte de la información se realiza en una red basada en paquetes (Packet Based Network-PBN) que no puede proporcionar calidad de servicio (QoS) garantizada; los terminales H.323 pueden proporcionar servicios de audio y video (opcionalmente) en tiempo real y servicio de comunicación de datos.

El H.323 especifica que los paquetes de voz sean encapsulados en el protocolo RTP (Real-Time Transport Protocol) y transportados en UDP (User Datagram Protocol). Para gestionar la calidad de la comunicación de vos en la red, se utiliza el protocolo RTCP (Real-Time Control Protocol).

REAL-TIME TRANSPORT PROTOCOL (RTP Y RTCP)

El Real-Time Transport Protocol (RTP) es un protocolo de transporte en tiempo real que tiene como objetivo proporcionar un servicio de entrega extremo que transmite datos en tiempo real, tales como audio y video. (Tanenbaum & Romero Elizondo, 2009)

El Real-Time Control Protocol (RTCP) se basa en la transmisión periódica de paquees de control para todos los participantes de una sesión, utilizando los mismos mecanismos de distribución de los paquetes de datos. El paquete RTCP contiene información importante para la monitorización de la entrega de los dos paquetes de audio, tales como: jitter entre llegada de paquetes, numero de paquetes perdidos, número total de paquetes y octetos transmitidos, y otros datos útiles para el diagnóstico, seguimiento y corrección de algunos tipos de condiciones de error en la red.

La Calidad de Servicio (QoS) en H3.23

La calidad del servicio puede ser definida como la "capacidad de la red para garantizar y mantener ciertos niveles de rendimiento para cada aplicación de acuerdo con las necesidades específicas de cada usuario".

Aunque el concepto de calidad (QoS) usualmente se refiere a la fidelidad de la señal de voz recibida, también puede aplicarse a otros aspectos, tales como: disponibilidad de la red, la probabilidad de bloqueo, la existencia de los servicios especiales (conferencias, la identificación del usuario que llama, etc,), la escalabilidad y la penetración.

La Calidad de la Señal de Voz en H.323

La calidad de reproducción de voz en la red telefónica es fundamentalmente subjetiva, aunque las medidas estándar hayan sido desarrolladas por la ITU. Para la transmisión de voz sobre redes de paquetes hay cuatro factores principales que influyen en la calidad del servicio: ancho de banda, retardo (de extremo a extremo) del paquete, demora jitter y pérdida de paquetes.

Ancho de Banda en H.323

El ancho de banda mínimo necesario para la transmisión de la señal de voz es una función de la técnica de codificación utilizada. El ancho de banda disponible en la red y el mecanismo de compartimiento de este ancho de banda entre varias aplicaciones tienen influencia directa en el retraso por el paquete y consecuentemente en la calidad del servicio resultante.

Retraso de Paquete en H.323

El retraso del paquete se define formalmente como la diferencia de tiempo, en segundos entre el instante en que el terminal que llama envía el primer bit del paquete en el instante que el terminal llamado recibe este bit. Su comportamiento es aleatorio dependiendo de la carga en la red.

Pérdida de Paquetes en H.323

Las redes P no garantizan la entrega de los paquetes. Debido a los fuertes requisitos de retardo impuestos por las aplicaciones interactivas en tiempo real, no se pueden utilizar protocolos de transporte fiables tales como TCP. La pérdida de paquetes es, por tanto, inevitable, y puede influir significativamente en la calidad de servicio de voz sobre P.

Mejorar la Calidad de Servicio de Voz IP

Para alcanzar un nivel de QoS adecuado para el tráfico de voz sobre una red P se pueden adoptar una serie de medidas para: garantizar el ancho de banda requerido para la transmisión de paquetes de voz (por ejemplo: Protocolo de reserva de recursos), minimizar los retrasos sufridos por los paquetes en la red y que sean lo más constantes posible (por ejemplo: utilización de mecanismos de priorización de paquetes de voz, utilizar técnicas de enrutamiento que favorezcan a las rutas con menos retardo, utilizar los mecanismos más eficientes para el enrutamiento de paquetes en los routers) y eliminar o minimizar la fluctuación (jitter) de retardo sufrido por los paquetes (por ejemplo: usar dejitter buffer).

Clasificación o Identificación del Tráfico en H.323

La clasificación del tráfico se puede hacer paquete a paquete (analizando las características del tráfico de cada paquete) o sesión a sesión (cuando el transmisor negocia una clasificación extremo a extremo antes de la transmisión). La política de clasificación de paquetes es fijada por el operador de red y puede basarse en varios criterios, tales como: tipo de tráfico contenido en el paquete, la dirección de la puerta física, dirección MAC, dirección IP de la fuente o destino, puerta de aplicación, etc.

La Disciplina de Despacho en H.323

Almacenamiento temporal de paquetes, llamados colas, la disciplina de despacho define como el nodo de red servirá los paquetes almacenados en las colas. Cuando la red transporta simultáneamente tráfico de voz y datos, debe asociarse niveles de prioridad diferentes para ambos tipos de tráfico, con la disciplina de despacho priorizando el tráfico de voz para minimizar el retraso que estos paquetes sufren en cada nodo de la red.

Las Técnicas de Control de Congestión de Tráfico en H.323

Técnicas de control de la congestión supervisan el tráfico en la red para anticipar y prevenir la ocurrencia de congestión, generalmente a través del descarte de paquetes. Las dos técnicas principales que operan con este objetivo son la Random Early Detection (RED) Y su versión con ponderación, Weight Random Early Detention (WRED).

Random Early Detection (RED)

Cuando sucede un timeoyt en el transmisor TCP, el protocolo reduce el tamaño de la ventana de transmisión e inicia el proceso de inicio lento (slow start), donde el tamaño de la ventana se aumenta gradualmente a medida que el transmisor va recibiendo acuses de recibo positivos desde el receptor.

Weigth Random Early Detention (WRED)

En el algoritmo WRED la probabilidad de un paquete entrante para ser desechado se define por la tasa de ocupación de la cola y una pesa asociado al flujo (o clase de flujo) a la que pertenece el paquete. Lo que se busca con el WRED es que los paquetes de mayor prioridad tengan menos probabilidades de descartarse.

Se debe de recordar que el descarte de un paquete de voz no reducirá el flujo que, llegada de este tipo de paquete, una vez que el UDP no responde a la perdida d paquetes. Por lo tanto, un gran flujo de tráfico de voz puede causar desbordamiento en una cola WRED y, en consecuencia, una alta tasa de pérdida de paquetes.

Las Arquitecturas para la calidad de Servicio en H.323

El modelo de servicios integrados propone dos clases de servicios, más allá del servicio habitual de mejor esfuerzo, que son:

- servicio garantizado: para aplicaciones en tiempo real, como voz IP, que requieren un ancho de banda límite garantizado para el retraso.
- Servicio de carga controlada: para aplicaciones que requieren servicio de “mejor que mejor esfuerzo “, pero sin garantía de ancho de banda o límite de demora.

Otros Requisitos para la Voz IP en H.323

El uso de la Voz IP constituye una buena alternativa para la implantación de redes multimedia corporativas o incluso para la implementación de backbones, con capacidad para la integración de tráfico de las empresas proveedores de servicios de telecomunicaciones.

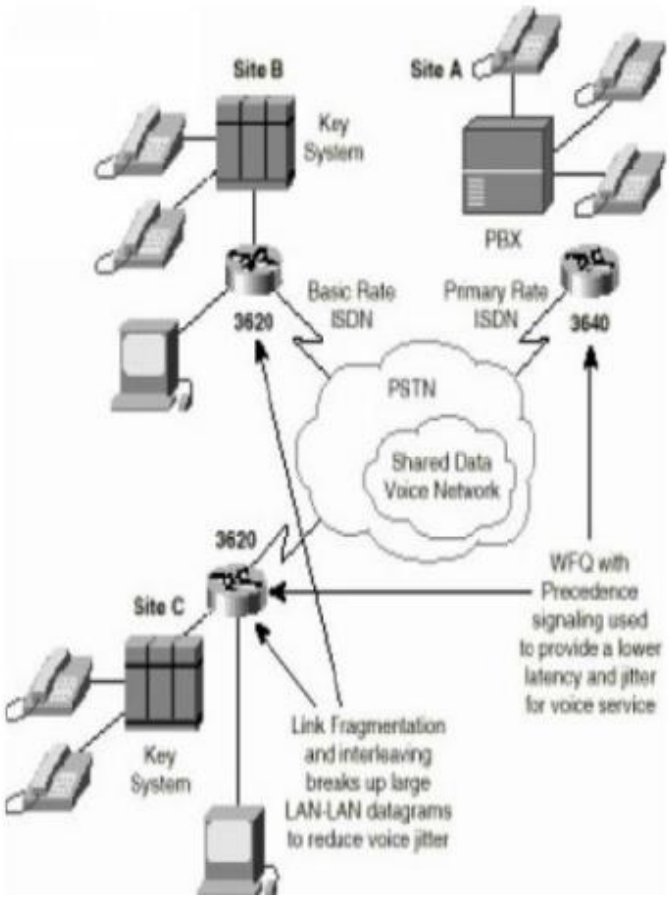


Ilustración 13: VoIP en H.323

Fuente:(Sosa, 2015)

H.323 VS. SIP

Tanto H.323 como SIP para el establecimiento y señalización de llamadas, así como intercambio de capacidades, control de medios y servicios adicionales sobre redes IP. A continuación, se establecen comparaciones entre ambas tecnologías, identificando diferencias, similitudes, ventajas, etc.

- **teleconferencia o videoconferencia**

Sobre redes IP, H.323 ha sido la referencia durante más o menos los últimos cinco años. Sin embargo, desde la aparición de SIP, se comienza a poner en entredicho esta supremacía. Este hecho está fundamentado en la naturaleza propia de H.323 que expone una serie de

factores que lo limitan como un protocolo para las grandes masas. Inicialmente H.323 se creó con la idea de extender SS7 hacia estas redes, y siempre con la premisa de la total compatibilidad con los estándares anteriores, ya sean para conmutación de circuitos o de paquetes. En cierto modo, la idea era llevar la telefonía convencional hacia redes IP. Ahora bien, la integración de H.323 con Internet se ve obstaculizada por características propias de ésta tecnología. Por ejemplo, H.323 no usa ninguno de los estándares aprobados por el IETF para Internet: no proporciona servicios complementarios ni se aprovecha del trabajo que ya está hecho y que funciona correctamente.

- **Seguridad**

H.323 define mecanismos de seguridad y facilidades de negociación vía H.235, también puede utilizar SSL la capa de transporte. Por su parte SIP soporta mecanismos de autenticación vía HTTP.

- **Arquitectura**

H.323 cubre servicios como capacidad de intercambio, control de conferencia, señalización básica, QoS, registro, etc. A diferencia de SIP, que, por ser modular, cubre servicios de señalización de llamadas, localización y registro de usuarios. Otras características son manejadas por protocolos ortogonales.

Las entidades que sostienen una red H.323 incluyen gateways, terminales, puentes de comunicación junto a un Gatekeeper. La arquitectura para este protocolo es par a par (peer-to-peer) soportando comunicación de usuario-por-usuario sin necesidad de una entidad de control centralizado.

SIP como se explicó inicialmente, incluye los user agents, análogos a los terminales de H.323 pero que pueden operar como cliente o servidor, dependiendo del rol que tome en una llamada particular, si es solicitando o respondiendo una petición de sesión. La arquitectura SIP requiere un servidor Proxy para enrutar las llamadas a otras entidades y un servidor de registro, los demás componentes de la red no están definidos y no son obligatorios para establecer una llamada.

- **Video y Data Conferencia**

H.323 soporta tanto la conferencia de datos como la de video. Tienen lugar procesos para el control de la conferencia y la sincronización de los streams de audio y video. SIP no soporta protocolos como el T.120 para la conferencia de datos. No posee mecanismos de sincronización ni de control para la conferencia.

- **Codificación de mensajes**

En H.323 los mensajes son codificados en un formato binario compacto que es apropiado para conexiones de banda ancha y banda angosta. Este tipo de codificación se emplea para reducir el tamaño de la transmisión y resguardar el ancho de banda. SIP sólo entiende mensajes estilo direcciones URL y los mensajes son codificados en textos, en lugar de binario. Esto facilita su entendimiento, pero aumenta el tamaño del mensaje que será enviado.

- **Estabilidad**

Inicialmente H.323 no contempló el aspecto de direccionamiento, ya que nace en el entorno de las redes LAN. Posteriormente se trató de subsanar este problema introduciendo el concepto de "zona H.323", que sin embargo sigue teniendo problemas de escalabilidad, y otros como el direccionamiento entre zonas. Con respecto a los componentes de red y el soporte de múltiples conversaciones, se dificulta para zonas H.323 muy grandes, ya que el Gatekeeper tiene que conocer el estado de cada llamada que maneja. En SIP cuando la carga de llamadas en la red es elevada, se pueden usar los servidores de redirección, que no mantienen ningún tipo de estado. Es más, aun manteniendo los servidores como proxies, podemos usarlos con ó sin estado ('stateful' ó 'stateless'), beneficiándose del hecho de que, por defecto, SIP funciona sobre UDP.

- **Funcionabilidad**

Cada protocolo maneja la configuración llamadas, el control de las llamadas, y medios de diversas maneras. H.323 contiene la definición de cada uno de ellos. Mientras que SIP define configuración de llamadas y uso de protocolos para control de llamadas, siendo manejado cada uno por separado. Por otro lado, está la capacidad de intercambio. Después de configurar la llamada en H.323, los terminales anuncian la capacidad que ellos tienen para variables como compresión y video, ya que dichas variables pueden cambiar durante la llamada, la configuración de la llamada puede ser cambiada a mitad de llamada (mid-call). Para el caso de SIP estos parámetros sólo pueden ser cambiados a la inicial una nueva llamada. Para la comunicación multimedia, el hecho de que SIP no permita “mid-call” podría ser relevante. *(Sosa, 2015)*

2.2.10 Protocolo IAX

IAX (Inter-Asterisk Exchange) es un protocolo desarrollado por la firma Digium con la finalidad de comunicar servidores VoIP; soporta una gran variedad de codecs y un gran número de canales (streams), con lo que se puede utilizar para transportar señalización y cualquier tipo de datos entre puntos finales (terminales VoIP) a través del puerto UDP 4569. IAX es un protocolo binario, diseñado y organizado para reducir la carga en flujos de datos de voz.

IAX soporta el envío de señalización y datos por múltiples canales, con lo cual los datos de varias llamadas se encapsulan en un conjunto de paquetes y se añaden a un datagrama IP, reduciendo el retardo y el overhead asociado a los canales individuales, lo anterior se conoce como trunking y ayuda a mejorar la utilización del ancho de banda y reducir los tiempos de procesamiento.

IAX proporciona control y transmisión de flujos de datos multimedia sobre redes IP, cuyas principales aplicaciones son videoconferencias y presentaciones remotas. Por otro lado, IAX es un protocolo transparente a los cortafuegos y eficaz para trabajar en redes internas debido a que el tráfico de voz se transmite en banda (in-band).

El protocolo IAX establece sesiones internas que pueden utilizar cualquier codec para transmisión de voz o video, y está basado en los estándares SIP, MGCP y RTP (Real-Time Transfer Proto- col).

El protocolo IAX fue diseñado para transmitir voz, pero puede transportar cualquier media stream, incluyendo video. Actualmente IAX es un protocolo abierto y la comunidad de desarrolladores de tecnología IAX están incorporando diversos tipos de media.

Descripción del protocolo IAX

IAX es un protocolo par a par orientado a VoIP que incluye funciones de control y de media, diseñado para describir y transportar llamadas multimedia mediante el IP. El diseño de IAX permite la multiplexación de señales y llamadas multimedia sobre un mismo puerto UDP asociado entre dos pares. La señalización unificada de IAX y la trayectoria de medias logran transparencia sobre NAT, la cual es una ventaja de IAX sobre otros protocolos similares.

IAX es un protocolo binario cuyos principales beneficios son la eficiencia en la asignación del ancho de banda, robustez contra ataques y facilidad de implementación. La unidad

elemental de comunicación entre dos pares IAX es una trama (frame); IAX define varias clases de tramas.

Arquitectura IAX

Como indica su nombre **fue diseñado como un protocolo de conexiones VoIP entre servidores Asterisk,** aunque hoy en día también sirve para conexiones entre clientes y servidores que soporten el protocolo.

Los objetivos de IAX son:

- Minimizar el ancho de banda usado en las transmisiones de control y multimedia de VoIP
- Evitar problemas de NAT (Network Address Translation)
- Soporte para transmitir planes de marcación

Entre las medidas para reducir el ancho de banda cabe destacar que IAX o IAX2 es un protocolo binario en lugar de ser un protocolo de texto como SIP y que hace que los mensajes usen menos ancho de banda.

Para evitar los problemas de NAT el protocolo IAX o IAX2 usa como protocolo de transporte UDP, normalmente sobre el puerto 4569, (el IAX1 usaba el puerto 5036), y tanto la información de señalización como los datos viajan conjuntamente (a diferencia de SIP) y por tanto lo hace menos proclive a problemas de NAT y le permite pasar los routers y firewalls de manera más sencilla.

Funcionamiento de IAX

Para poder entender el protocolo IAX vamos a ver un ejemplo del flujo de datos de una comunicación IAX2:

Una llamada IAX o IAX2 tiene tres fases:

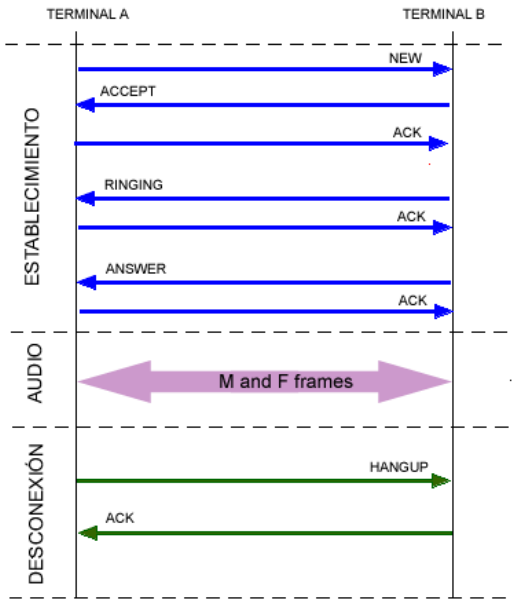


Ilustración 14: llamada IAX o IAX2

Fuente:(“Protocolo IAX | ElastixTech - Aprende Telefonia IP Asterisk - Elastix,” n.d.)

Establecimiento de la llamada

El terminal A inicia una conexión y manda un mensaje “new”. El terminal llamado responde con un “accept” y el llamante le responde con un “Ack”. A continuación, el terminal llamado da las señales de “ringing” y el llamante contesta con un “ack” para confirmar la recepción del mensaje. Por último, el llamado acepta la llamada con un “answer” y el llamante confirma ese mensaje.

Flujo de datos o flujo de audio

Se mandan los frames M y F en ambos sentidos con la información vocal. Los frames M son mini-frames que contienen solo una cabecera de 4 bytes para reducir el uso en el ancho de banda. Los frames F son frames completos que incluyen información de sincronización. Es importante volver a resaltar que en IAX este flujo utiliza el mismo protocolo UDP que usan los mensajes de señalización evitando problemas de NAT.

Liberación de la llamada o desconexión
La liberación de la conexión es tan sencillo como enviar un mensaje de "hangup" y confirmar dicho mensaje.

Consideraciones de seguridad en AIX

IAX soporta tres procesos de autentificación: texto plano (plaintext), hash MD5 (Message-Digest algorithm 5), y contraseña RSA de intercambio. Dichos procesos no consideran el cifrado de medias (media path) ni de las cabeceras entre puntos finales, para ello existen soluciones que incluyen el uso de un artefacto de red privada virtual (VPN, Virtual Private Network) o de software para encriptar el canal en cualquier otra capa que establezca un método entre los puntos finales con túneles configurados y operacionales.

Existen dos formas de negación de servicio (DoS, Denial of Service):

- Sobrecargando a los pares con peticiones falsas: Se evita identificando sobrecargas, y emitiendo una alarma o una acción de protección.
- Ataque ingenioso: Se puede realizar mediante la inyección de medias con la finalidad de ocasionar un exceso de procesamiento al insertar paquetes fuera de orden y enviando órdenes como hangup o transfer. Estos ataques requieren desactivar la supervisión del canal binario ya que el número de secuencia de los mensajes necesita sincronizarse con el inter- cambio del protocolo.

Actualmente, se encuentra en investigación el hecho de que IAX pueda cifrar los canales entre los puntos finales mediante el intercambio de llaves RSA o de una llave dinámica en el establecimiento de la llamada, cuya aplicación representa una solución para acoplamiento seguro entre instituciones bancarias, por ejemplo.

IAX y NAT

El protocolo IAX2 fue diseñado para trabajar en dispositivos NAT. El uso de un puerto normal UDP para señalización y transmisión de comunicación mantiene los requisitos mínimos que exigen los cortafuegos, lo cual facilita la implementación de IAX en redes seguras.

IAX vs SIP – comparación entre IAX y SIP

IAX fue creado por Mark Spencer (también creador de AsterisK) para paliar una serie de problemas o inconvenientes que se encontró al utilizar SIP en VoIP y que pensó que debía ser mejorado.

Las principales diferencias ente IAX y SIP son las siguientes:

- **Ancho de banda**

  IAX utiliza un menor ancho de banda que SIP ya que los mensajes son codificados de forma binaria mientras que en SIP son mensajes de texto. Asimismo, IAX intenta reducir al máximo la información de las cabeceras de los mensajes reduciendo también el ancho de banda.

- **NAT**
  En IAX la señalización y los datos viajan conjuntamente con lo cual se evitan los problemas de NAT que frecuentemente aparecen en SIP. En SIP la señalización y los datos viajan de manera separada y por eso aparecen problemas de NAT en el flujo de audio cuando este flujo debe superar los routers y firewalls. SIP suele necesitar un servidor STUN para estos problemas.

- **Estandarización y uso**

  SIP es un protocolo estandarizado por la IETF hace bastante tiempo y que es ampliamente implementado por todos los fabricantes de equipos y software. IAX está aún siendo estandarizado y es por ello que no se encuentra en muchos dispositivos existentes en el mercado.

- **Utilización de puertos**

  IAX utiliza un solo puerto (4569) para mandar la información de señalización y los datos de todas sus llamadas. Para ello utiliza un mecanismo de multiplexión o "trunking". SIP, sin embargo, utiliza un puerto (5060) para señalización y 2 puertos RTP por cada conexión de audio (como mínimo 3 puertos). Por ejemplo, para 100 llamadas simultáneas con SIP se usarían 200 puertos (RTP) más el puerto 5060 de señalización. IAX utilizaría sólo un puerto para todo (4569).

- **Flujo de audio al utilizar un servidor**

En SIP si utilizamos un servidor la señalización de control pasa siempre por el servidor, pero la información de audio (flujo RTP) puede viajar extremo a extremo sin tener que pasar necesariamente por el servidor SIP. En IAX al viajar la señalización y los datos de forma conjunta todo el tráfico de audio debe pasar obligatoriamente por el servidor IAX. Esto produce un aumento en el uso del ancho de banda que deben soportar los servidores IAX sobre todo cuando hay muchas llamadas simultáneas.

Otras funcionalidades

IAX es un protocolo pensado para VoIP y transmisión de video y presenta funcionalidades interesantes como la posibilidad de enviar o recibir planes de marcado (dialplans) que resultan muy interesante al usarlo conjuntamente con servidores Asterisk. SIP es un protocolo de proposito general y podría transmitir sin dificultad cualquier información y no sólo audio o video. *(lavariega arista, 2007), ("Protocolo IAX | ElastixTech - Aprende Telefonia IP Asterisk - Elastix," n.d.)*

2.2.11 Asterisk vs FreePBX

Asterisk es software open source, hecho en lenguaje C y creado originalmente por Mark pencer (actual CTO de Digium, empresa que patrocina la mayor parte del desarrollo de Asterisk). Este software, por sí solo, no es una herramienta plug-and-play que venga lista para hacer llamadas, sino que es necesario atravesar por numerosos pasos (descarga, compilación, instalación y configuración) para que pueda realizar labores útiles. Sin embargo, es un elemento base (una plataforma para crear cosas más grandes) para que de allí podamos construir un sin fin de aplicaciones basadas no solamente en voz, sino en la unión con datos y/o cualquier otro sistema de cómputo que necesitamos que interactúe con un teléfono.

ventajas:

- Tienes total control: puedes hacer lo que quieras y actualizar en cualquier momento.
- Al compilar, tu conmutador se ajustará a la arquitectura de tu PC.
- Puedes elegir que módulos quieres compilar y cuáles no.

Desventajas:

- Tienes que hacer todo a mano.
- Programar por línea de comandos puede no ser tan natural para algunas personas.
- Toma un mayor tiempo de implementación.

FreePBX

Como tal, FreePBX no es una distribución (aunque hay un ISO que se puede descargar que instala CentOS + FreePBX + Asterisk en un solo paso). FreePBX es una interfaz gráfica web que nos permite simplificar el trabajo de configuración básica de Asterisk. Utiliza PHP y MySQL, y lo que hace es crear una representación más sencilla de comprender para facilitar la creación de usuarios, troncales, extensiones y otros puntos fundamentales de la configuración de Asterisk.

FreePBX es un apoyo importante para la administración de Asterisk por personal no técnico, y es la interfaz web de-facto para configurar Asterisk. Es desarrollado y mantenido por Schmooze Com Inc.

Ventajas:

- Te ayuda a configurar Asterisk más rápidamente.
- Prácticamente todas las distribuciones open source disponibles hacen uso de esta interfaz.

Desventajas:

- No todos los módulos están soportados.
- *Para mayor control tienes que recurrir a la línea de comandos a final de cuentas.*

(“Asterisk vs Elastix vs Trixbox vs AsteriskNow vs FreePBX,” 2013)

2.2.12 Plataformas propietarias y abiertas de voz Ip

2.2.13 Plataformas propietarias

Avaya

Colaboración sin problemas para el mercado mediano, movilidad en video y voz, usando cualquier dispositivo, Cambiando la manera en la que su fuerza de trabajo móvil y distribuido colabora. Proporcione una experiencia atractiva para voz, video y movilidad

sobre prácticamente cualquier dispositivo. Lo suficientemente simple para funcionar en cualquier dispositivo y lo suficientemente potente para soportar 2.000 usuarios con software virtualizado. Fácil de usar. Fácil de gestionar. Valor excepcional.

Panasonic

La tendencia mundial en el área de comunicaciones es unificar todos los medios de comunicación para que interactúen entre sí de forma fluida y transparente. El servidor de Voz por IP Panasonic le brinda un conjunto completo de funciones de comunicaciones y telefonía en red, para pequeñas y mediana empresa, con una amplia selección de terminales fijos e inalámbricos, auriculares y softphones. Los recursos del sistema se pueden mejorar y ampliar fácilmente a través de aplicaciones de software y licencias para responder a las necesidades de organizaciones con una o varias sedes.

2.2.14 Plataformas abiertas

Asterisk

Es una PBX IP de código abierto que posee diversos módulos con los cuales es posible operar como una simple centralita IP, como Gateway, como MediaServer, etc. Asterisk tiene licencia GPL (General Public License) y si bien originalmente fue desarrollado para el sistema operativo Linux, en la actualidad también funciona en BSD, MacOSX, Solaris y Microsoft Windows, aunque en su plataforma nativa Linux es la mejor soportada de todos. *(Gomez Lopez & Gil Montoya, 2008)*

SER

Es un servidor de VoIP basado en el protocolo SIP a través del cual es posible construir una infraestructura de telefonía IP a gran escala. En un esquema SIP, puede operar como registrar, Servidor Proxy, Servidor Redirect, etc. La ventaja principal es que al ser código abierto mantiene un espacio para nuevos plug-in para nuevas aplicaciones. Al operar con el estándar SIP, hace fácil su interoperabilidad con otros fabricantes de sistemas y equipos SIP. Posee en la actualidad módulos con soporte de presencia, autenticación mediante un servidor AAA (ej. RADIUS), llamadas remotas XML-RPC, etc. SER también ofrece una interfaz aplicación/servidor basado en Web donde se puede monitorizar el estado del servidor y gestionar todas sus prestaciones. SER es públicamente disponible bajo licencia GPL.

RTP Proxy

Es un servidor que permite operar en conjunto con el SER y cualquier servidor Proxy, resolviendo el tema del NAT Transversal con el manejo adecuado de puertos. Uno de los más utilizados es el RTP Proxy de Portaone. *(Blanquicet & Rodriguez, 2014)*

3. METODOLOGÍA

El sistema de comunicaciones empleado en la Delegación de Antioquia está constituido por una conexión dedicada a internet para (trámites) operaciones generales de correo el cual se enlaza al ISP a través de Oficinas Centrales y una línea telefónica en cada sede para la comunicación entre sí de las mismas y desde cada una con la delegación. Este acceso a internet no pudo ser utilizado por las restricciones establecidas desde Oficinas Centrales. Para la solución de dicho inconveniente fue necesario un acceso independiente y un pleno acceso a los dispositivos de borde en los cuales se establecieron las configuraciones para garantizar políticas de optimización del canal y la seguridad mínima requerida, por lo que se calcula el servidor a partir de un nuevo enlace.

Los costos actuales por consumo telefónico en todo el departamento ascienden a 40.000.000, con los cálculos realizados se pudo establecer que el consumo puede bajar a más del 45%, lo que implicaría un ahorro de 18.000.000 utilizando un recurso que ya se tiene instalado como son los accesos a internet para cada dependencia. Lo anterior se deriva de estadísticas tomadas donde se obtiene que alrededor del 30% de las llamadas se realizan a nivel interno de la entidad.

La Registraduría municipal requiere un ancho de banda (Bw) de 500k, tal como se pudo evidenciar en el consumo generado por una llamada de VoIP (ver gráfico) y un punto configurado en el router para garantizar el Bw y las políticas administrativas de seguridad necesarias. El códec utilizado es el G.726.

En la sede central se considera todo el tráfico demandado por la entidad. En total son 132 extensiones municipales incluyendo sedes auxiliares. Se calcula una demanda de tráfico partiendo de un total de 20 líneas. El códec G.726 consume 32 Kbps y ethernet (32 Kbps) para un total de 64 *Kbps* sobre la red de datos. Para determinar el tráfico ofrecido con 132 usuarios y considerando que en la hora cargada se realizan 3 llamadas de 4 minutos cada una, entonces el volumen de tráfico sería:

V = 132 (usuarios)* 3 llamada / usuario * 4 minutos / llamada
V = 1584 minutos

$$\therefore \boldsymbol{v} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{10}} \boldsymbol{ti} = \boldsymbol{c} * \boldsymbol{dm}$$

C: cantidad de solicitudes de servicio

Dm: duración media de cada llamada

Con un GoS de 0.05

Ahora la intensidad de tráfico: **A =** $\frac{V}{T} = \frac{1}{T}\sum_{i=1}^{n} ti = \frac{V}{T}$

$A = \frac{C.dm}{T}$ **[Erlang]**

A = 1584/60 = 25.56 Erlang

De la tabla de Erlang B, para un tráfico de 25.56 Erlang con una probabilidad de bloqueo del 5%, se obtiene el número de líneas necesarias que en este caso son 31 líneas o canales.

El ancho de banda requerido será de 19 canales por el códec utilizado;

Bw (sede central) = códec * Bw llamada
Bw (sede central) = 64 Kbps*31= 1984 Kbps ≈ 2 Mbps

Partiendo que se tienen 20 líneas actualmente, y como la intensidad de tráfico requerido es de 25.6 *Erlang*, entonces el GoS actual es del 30 *%* lo que indica que con la nueva implementación se está mejorando en un 25 *%* al sistema de comunicaciones actual, el cual se libera de toda la demanda interna de llamadas.

En la ilustración 15 se detalla el esquema de la arquitectura mínima para el servicio de voz IP.

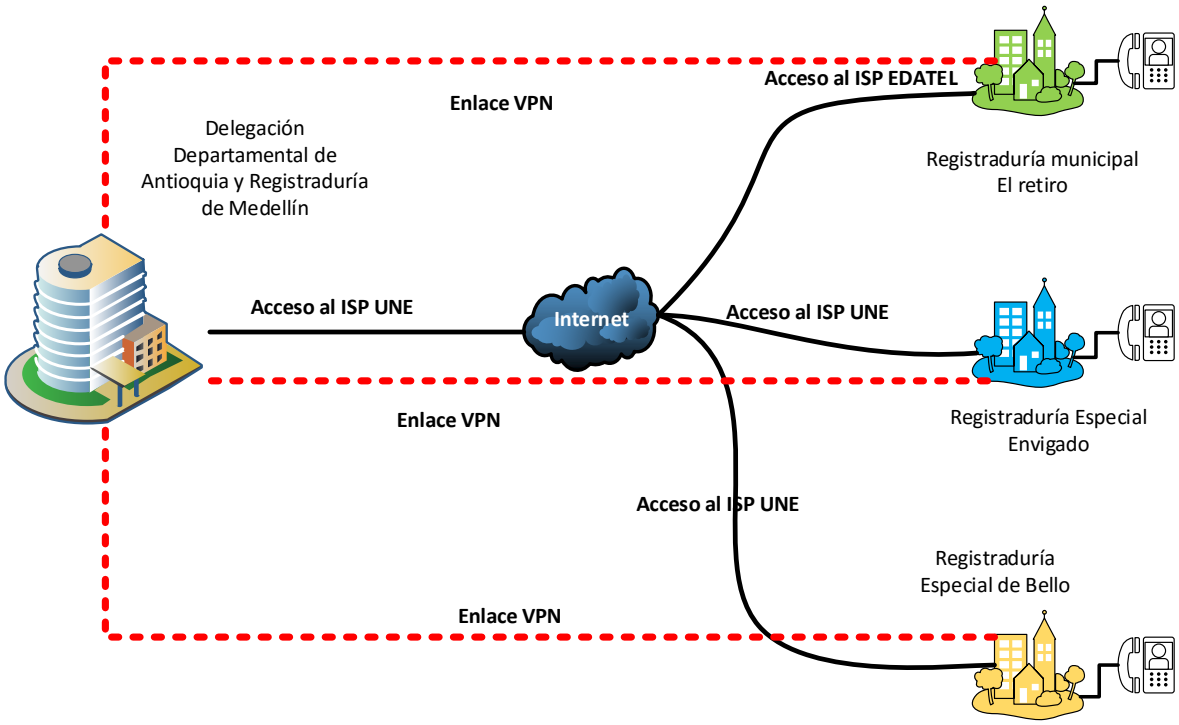


Ilustración 15: Arquitectura base de VoIP

Fuente: el autor

El diseño anterior parte de la infraestructura actual de comunicaciones, la cual se muestra en la ilustración 16.

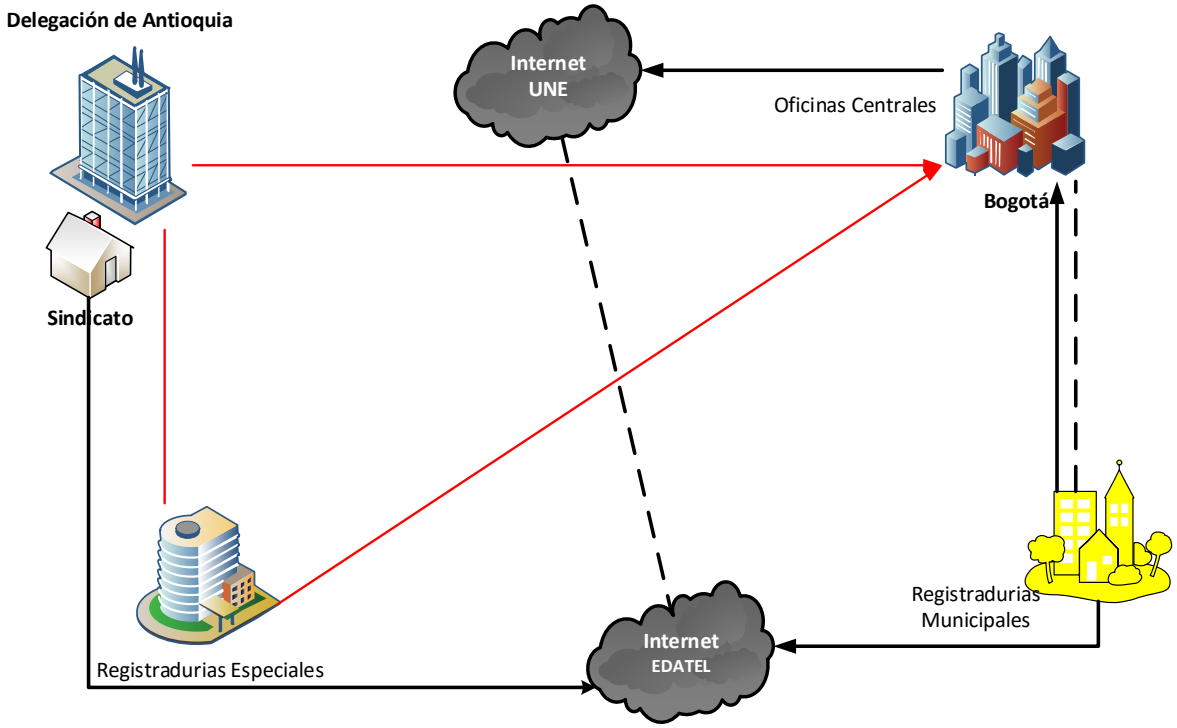


Ilustración 16: Estado actual de la conexión

Fuente: el autor

Con lo anterior se determina entonces, la configuración lógica y apropiada para la implementación de cada una de las sedes tal como se observa en la ilustración 17.

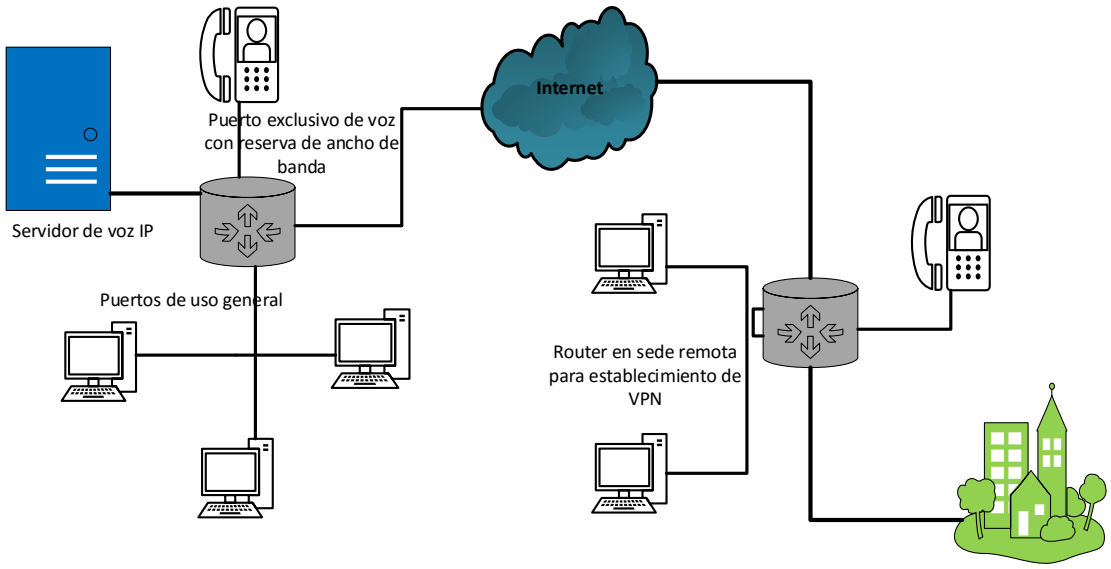
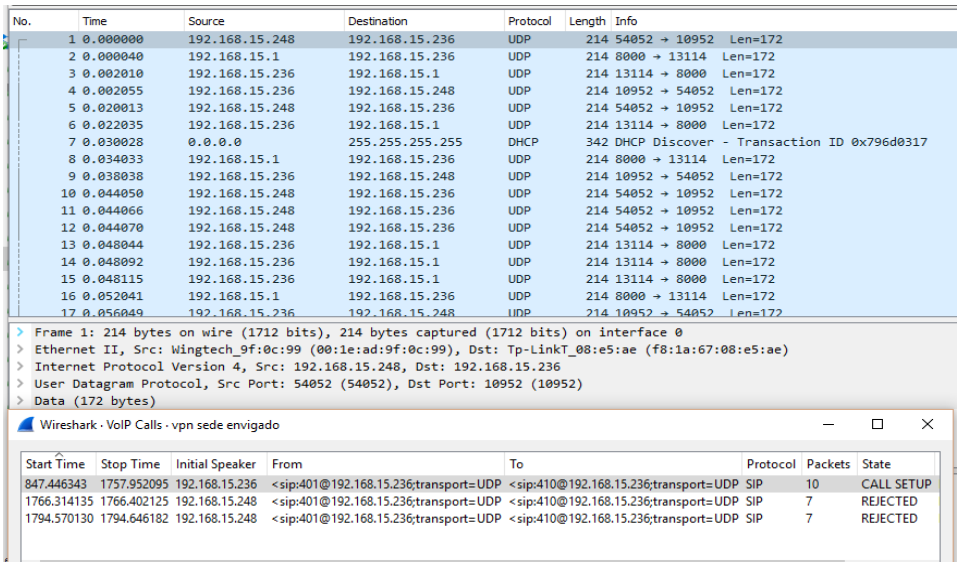


Ilustración 17: Optimización del sistema de comunicaciones

Fuente: el autor

En la ilustración 18 se detalla el tipo de tráfico que circula a través de la sede de Envigado



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.15.248	192.168.15.236	UDP	214	54052 → 10952 Len=172
2	0.000040	192.168.15.1	192.168.15.236	UDP	214	8000 → 13114 Len=172
3	0.002010	192.168.15.236	192.168.15.1	UDP	214	13114 → 8000 Len=172
4	0.002055	192.168.15.236	192.168.15.248	UDP	214	10952 → 54052 Len=172
5	0.020013	192.168.15.248	192.168.15.236	UDP	214	54052 → 10952 Len=172
6	0.022035	192.168.15.236	192.168.15.1	UDP	214	13114 → 8000 Len=172
7	0.030028	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x796d0317
8	0.034033	192.168.15.1	192.168.15.236	UDP	214	8000 → 13114 Len=172
9	0.038038	192.168.15.236	192.168.15.248	UDP	214	10952 → 54052 Len=172
10	0.044050	192.168.15.248	192.168.15.236	UDP	214	54052 → 10952 Len=172
11	0.044066	192.168.15.248	192.168.15.236	UDP	214	54052 → 10952 Len=172
12	0.044070	192.168.15.248	192.168.15.236	UDP	214	54052 → 10952 Len=172
13	0.048044	192.168.15.236	192.168.15.1	UDP	214	13114 → 8000 Len=172
14	0.048092	192.168.15.236	192.168.15.1	UDP	214	13114 → 8000 Len=172
15	0.048115	192.168.15.236	192.168.15.1	UDP	214	13114 → 8000 Len=172
16	0.052041	192.168.15.1	192.168.15.236	UDP	214	8000 → 13114 Len=172
17	0.056049	192.168.15.236	192.168.15.248	UDP	214	10952 → 54052 Len=172

```
> Frame 1: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0
> Ethernet II, Src: Wingtech_9f:0c:99 (00:1e:ad:9f:0c:99), Dst: Tp-LinkT_08:e5:ae (f8:1a:67:08:e5:ae)
> Internet Protocol Version 4, Src: 192.168.15.248, Dst: 192.168.15.236
> User Datagram Protocol, Src Port: 54052 (54052), Dst Port: 10952 (10952)
> Data (172 bytes)
```

Wireshark · VoIP Calls · vpn sede envigado

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State
847.446343	1757.952095	192.168.15.236	<sip:401@192.168.15.236;transport=UDP	<sip:410@192.168.15.236;transport=UDP	SIP	10	CALL SETUP
1766.314135	1766.402125	192.168.15.248	<sip:401@192.168.15.236;transport=UDP	<sip:410@192.168.15.236;transport=UDP	SIP	7	REJECTED
1794.570130	1794.646182	192.168.15.248	<sip:401@192.168.15.236;transport=UDP	<sip:410@192.168.15.236;transport=UDP	SIP	7	REJECTED

Ilustración 18: VPN sede Envigado

Fuente: el autor

En el proceso de monitoreo se revisa las condiciones de funcionamiento del canal donde se detalla la no congestión del canal. En la ilustración19 re realizan algunas muestras del estado.

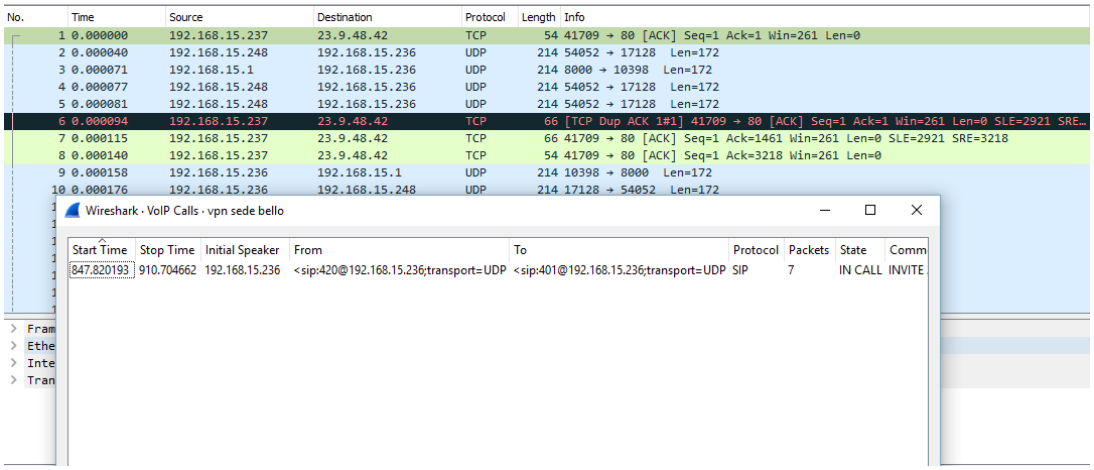


Ilustración 19: VPN sede Bello

Fuente: el autor

Se realiza una prueba del canal con solo voz ip en una hora diferente a laboral para determinar el consumo de canal

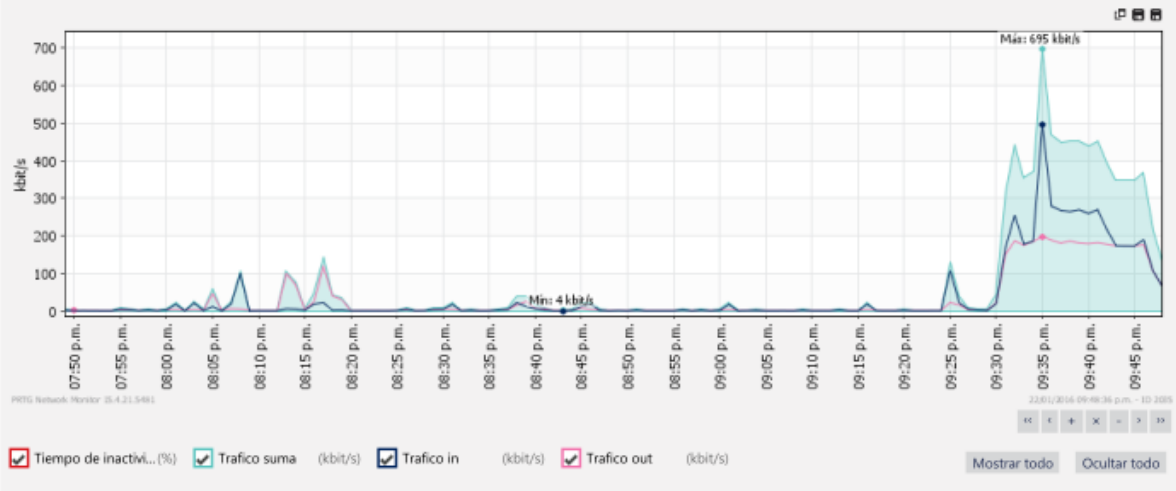


Ilustración 20: Monitoreo de llamada

Fuente: el autor

En las ilustraciones 21, 22 y 23 se analiza el tráfico a fin de obtener características de seguridad en las cuales el tráfico de voz no pueda ser interceptado por cualquier otro usuario ajeno al sistema de comunicaciones. De la misma forma se obtiene el funcionamiento del canal de manera normal acorde a los parámetros y requisitos establecidos en la parte inicial del diseño.

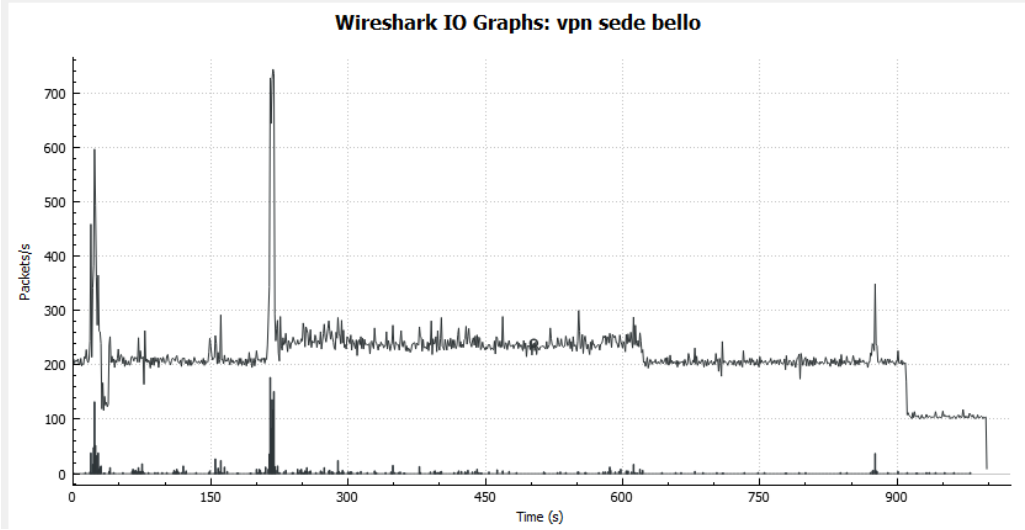


Ilustración 21: Estadística de llamada VPN sede Bello

Fuente: el autor

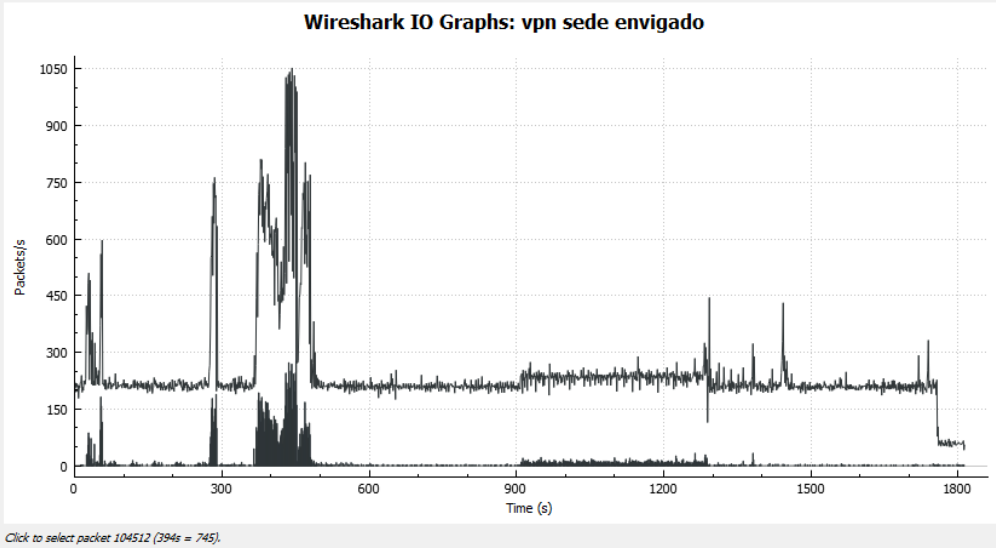


Ilustración 22: Estadística de llamada VPN sede Envigado

Fuente: el autor

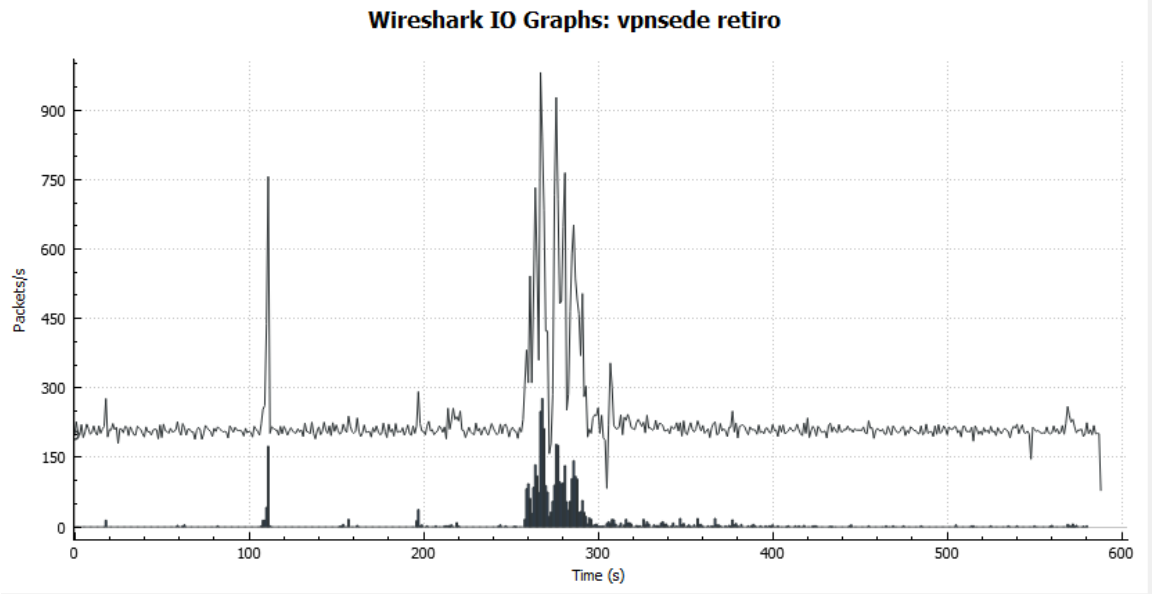


Ilustración 23: Estadística de llamada VPN sede Retiro

Fuente: el auto

4. RESULTADOS Y DISCUSIÓN

La realización del presente proyecto pudo determinar las condiciones de operación del sistema de comunicaciones actual en la Registraduría Nacional del Estado Civil, no sólo en el departamento de Antioquia sino, en todo el territorio nacional. El primer aspecto, es el consumo de recursos existentes que conlleva un gasto público considerable, y en lo cual se ha demostrado, puede mejorar en gran medida; el segundo aspecto es la mejora en las condiciones de operación interna lo cual repercute en la prestación del servicio al usuario externo.

El canal de comunicaciones telefónico en la Delegación de Antioquia, se encuentra operando totalmente independiente del canal de datos que es administrado por Oficinas Centrales, y en ese sentido se tienen implementadas las políticas establecidas por el ente para el desarrollo de las funciones de identificación que se desarrollan dentro de la entidad. Debido a esta situación, para la implementación del sistema se necesitó de un canal independiente, que al momento sólo opera en las registradurías municipales y de esto se excluye las registradurías especiales, auxiliares y algunas de alta densidad de población. Aunque cabe anotar que con la debida autorización, se puede utilizar el canal existente, toda vez que el consumo actual permite el espacio para la nueva implementación del servicio propuesto.

A pesar de la carencia de recursos especiales, se pudo demostrar desde una implementación sencilla la utilización de recursos acorde a los nuevos desarrollos tecnológicos que apuntan a un mejor aprovechamiento de recursos y a un ofrecimiento o disponibilidad de nuevos servicios. En esta implementación, a pesar que se utilizan los elementos mínimos necesarios, debido a las condiciones de presupuesto de la entidad, se pudo aprovechar también recursos existentes y demostrar las mejoras que implicó en diferentes aspectos.

5. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

Para el logro de los objetivos se realiza un levantamiento y análisis de la información del estado actual de las comunicaciones, abordando los aspectos fundamentales de la teoría que involucra el desarrollo del proyecto. De todo esto, se encontró que las políticas administrativas del canal actual no permitieron implementar sobre el mismo sistema el desarrollo del proyecto por lo que se requirió un canal independiente.

Seguido a lo anterior, se realiza el análisis de la arquitectura mínima necesaria a implementar y se hacen las instalaciones y medidas pertinentes para la evaluación y análisis de resultados. Con la implementación del modelo de comunicación, se llega a determinar la funcionalidad del proyecto y las implicaciones económicas y funcionales para su implementación al 100%.

El proyecto no sólo puede extenderse a todo el departamento si no que posteriormente se podría implementar a nivel nacional, lo que implicaría para la Registraduría y el estado, una mejora en el sostenimiento de las comunicaciones internas, mejora en la atención ciudadana y un significativo ahorro en costos de operación. Aunque la implementación se realiza en tres sedes, queda el sistema habilitado para escalarse y soportar las demás dependencias del departamento y de la misma forma se podrían establecer troncales para la operación de extensiones adicionales en las sedes más grandes.

Las comunicaciones de la plataforma sólo se realizan a nivel interno pero es posible escalar el proyecto a un sistema que permita la comunicación fuera de la entidad y para usuarios externos, además, como se ha mencionado anteriormente, la solución realizada en Antioquia es posible extenderla a todo el país. Se propone un trabajo de investigación a nivel estadístico para determinar la representación económica real a nivel de todo el departamento, el país y lo que representa para la entidad y el estado los consumos actuales de telefonía. La troncalización no fue necesaria porque cada sede solo funciona con una extensión, por lo que no se requiere hacer control o enrutamiento de tráfico. La troncalización será pertinente cuando cada sede crezca en número de extensiones.

Con la adquisición de nuevos recursos, se puede extender la plataforma para implementar un sistema de comunicaciones que permita salir de la entidad a usuarios externos. Otro aspecto a implementar es la QoS a nivel WAN que se puede obtener implementando una red MPLS. Finalmente, se propone realizar una auditoría en seguridad para determinar si el aseguramiento del sistema está pertinente o se pueden implementar mejores políticas de funcionamiento, al igual que se recomienda la ubicación de otro servidor funcionando en forma paralela a través de tecnología Mirroring.

REFERENCIAS

Alarcon Quigua, A. (2008). Estudio, implementacion y análisis de tráfico de una red bajo protocolo SIP. *Journal of Chemical Information and Modeling*. http://doi.org/10.1017/CBO9781107415324.004

Asterisk vs Elastix vs Trixbox vs AsteriskNow vs FreePBX: Explicando la diferencia. (2013, July). Retrieved from http://asteriskmx.org/asterisk-vs-elastix-vs-trixbox-vs-asterisknow-vs-freepbx-explicando-la-diferencia/

Blanquicet, I., & Rodriguez, L. (2014). *Estudio de aplicaciones para la propuesta de implementacion de voz sobre IP en pymes agencias de viajes en Cartagena*. Retrieved from http://190.25.234.130:8080/jspui/handle/11227/745

Calcular Ancho de Banda en VoIP | ElastixTech - Aprende Telefonia IP Asterisk - Elastix. (n.d.). Retrieved February 8, 2016, from http://elastixtech.com/calcular-ancho-de-banda-en-voip/

Campos Moreno, J. M., & Guzman Munuera, M. J. (2008). Instalacion y configuracion de centralita VoIP basada en Asterisk.

Cisco. (2010). Red privada virtual - Virtual Private Network (VPN). Retrieved February 9, 2016, from http://www.cisco.com/web/LA/soluciones/la/vpn/index.html

Delfino, a, Rivero, S., & SanMartín, M. (2006). Ingeniería de tráfico en Redes MPLS. Retrieved from http://iie.fing.edu.uy/investigacion/grupos/artes/fce/net-te/Ingenieria_de_Trafico_en_Redes_MPLS-Paper.pdf

Domingo, L. D. (2014). Diseño de aplicaciones sobre VoIP con mecanismos de geoposicionamiento.

Gil, R. G. (2012). Seguridad en VoIP: Ataques, amenazas y riesgos. *Universitat de Valencia. Fecha de última Visita*, *2*. Retrieved from http://www.it-docs.net/ddata/896.pdf

Giraldo Blandón, J., Pareja Bolívar, M., & Serna Guarín, L. (2004). *sistema para administracion y control de la informacion en las registradurias del departamento de antioquia.*

Gomez Lopez, J., & Gil Montoya, F. (2008). *VoIp y Asterisk Redescubriendo la telefonía*. *Journal of Chemical Information and Modeling* (Vol. 53). http://doi.org/10.1017/CBO9781107415324.004

Gutiérrez, M. S. (2015). MPLS como tecnología para optimizar el ancho de banda de las

redes privadas virtuales, 1–18.

Ibarra Corretgé, S. (2008). Seguridad en VoIP, 17.

Landívar, E. (2008). Comunicaciones Unificadas con Elastix, 220.

lavariega arista, A. (2007). *Diseño y desarrollo de un softphone para telefonia IP utilizando el protocolo IAX*.

Lección 19: Arquitecturas de VoIP. (n.d.). Retrieved February 8, 2016, from http://datateca.unad.edu.co/contenidos/2150509/Contenido_en_linea/leccin_19_arquitecturas_de_voip.html

Protocolo IAX | ElastixTech - Aprende Telefonia IP Asterisk - Elastix. (n.d.). Retrieved February 8, 2016, from http://elastixtech.com/protocolo-iax/

Sierra Rodríguez, A., & others. (2008). Instalación de un sistema VoIP corporativo basado en Asterik. Retrieved from http://repositorio.upct.es/handle/10317/737

Sosa, F. (2015). Estandares de VoIP SIP vs H323.

Tanenbaum, A. S., & Romero Elizondo, A. V. (2009). *Sistemas operativos modernos*. México: Pearson Education.

Utilizados, C., Llamadas, T. De, & Troubleshooting, R. De. (2015). Ejemplo expreso de la configuración de conexión de troncal del SORBO del Cisco CallManager (CME).

Znaty, S., Dauphin, J., & Geldwerth, R. (2005). SIP : Session Initiation Protocol, 1–14.

APÉNDICE

Codec utilizado en la implementación

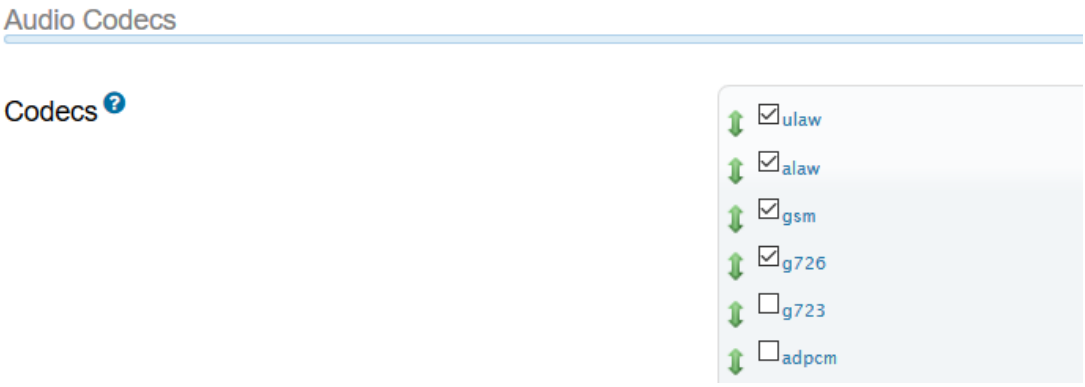


Ilustración 24: Configuración de códec en FreePBX

Fuente: el autor

Seguridad establecida en la comunicación de cada una de las sedes

5 items

		Name	Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged Out
- D		carlosa	**********	any		default	192.168.103.13	192.168.103.14	Feb/09/2016 19:06:46
- D		jhonp	**********	any		default	192.168.103.3	192.168.103.4	Jan/20/2016 17:39:30
- D		leo	********	any		default	192.168.103.7	192.168.103.8	Jan/01/1970 00:00:00
- D		peter	********	any		default	192.168.103.1	192.168.103.2	Feb/05/2016 06:17:26
- D		peter2	********	any		default	192.168.103.11	192.168.103.12	Jan/01/1970 00:00:00

Ilustración 25: Configuración de usuarios VPN en Mikrotik

Fuente: el autor

8 items

		Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
- D	R	LAN	Bridge	1598	2.1 Mbps	183.0 kbps	233	176
D	RS	MikroTik	Wireless (Atheros AR9	1600	2.1 Mbps	183.0 kbps	233	176
D	R	ether1	Ethernet	1598	32.9 kbps	195.6 kbps	20	22
D	S	ether2	Ethernet	1598	0 bps	0 bps	0	0
D	S	ether3	Ethernet	1598	0 bps	0 bps	0	0
D	S	ether4	Ethernet	1598	0 bps	0 bps	0	0
D	S	ether5	Ethernet	1598	0 bps	0 bps	0	0
- D	R	pptp-out1	PPTP Client		0 bps	0 bps	0	0

Ilustración 26: Configuración de interfaces en Mikrotik

Fuente: el autor

Características de la utilización de una red MPLS

Protocolo	Cuándo se utiliza	Nivel de seguridad	Comentarios
IPSec	• Conexión a un servidor VPN de terceros	Alto	• Permite conectar a un servidor VPN que no sea de Microsoft.
MPLS	• Conexión a un servidor VPN de terceros	Alto	• Permite compartir un único acceso a Internet entre todas las redes. No es necesario que las redes estén conectadas a Internet para acceder a la VPN. • Otorga mayor control a los administradores sobre sus redes. • Mejora la interacción del usuario con el sistema y reduce costos al asignar recursos con mayor eficiencia al ancho de banda
L2TP	• Internet Security and Acceleration (ISA) Server 2004 • ISA Server 2000 • Servidor VPN de Windows	Alto	• Usa enrutamiento y acceso remoto. • Menos complicada que la solución de túnel IPSec, pero requiere que el servidor VPN remoto sea un equipo servidor ISA o un servidor VPN de Windows.
PPTP	• ISA Server 2004 • ISA Server 2000 • Servidor VPN de Windows	Moderado	• Usa enrutamiento y acceso remoto. • Las mismas restricciones que L2PT, aunque algo más fácil de configurar. • Se considera que L2TP es más seguro, ya que utiliza cifrado IPSec.

Ilustración 27: Comparación entre las tecnologías utilizadas para la optimización del ancho de banda en las VPN

Fuente: (Gutiérrez, 2015)

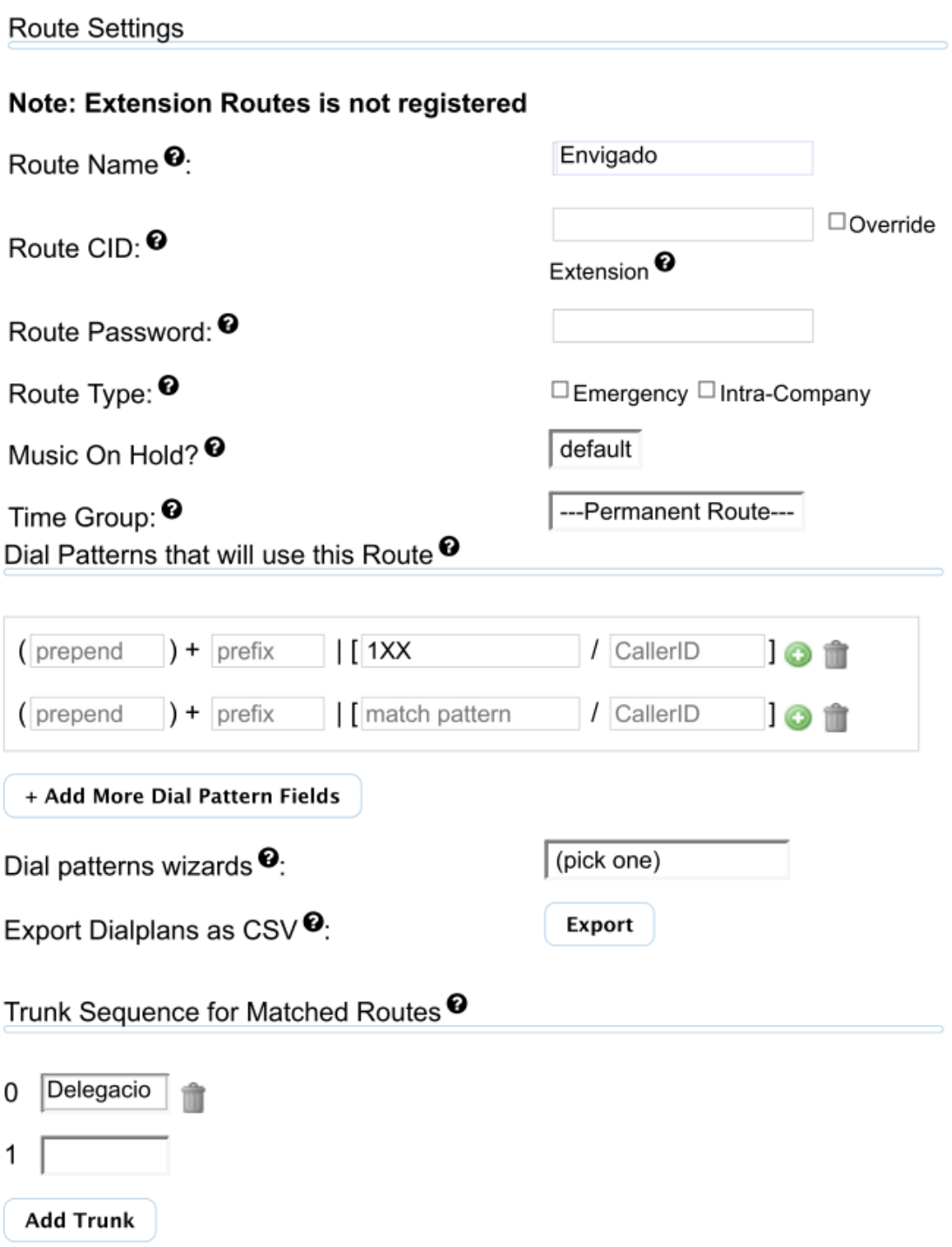


Ilustración 28: Configuración de troncal en FreePBX

Fuente: el autor

Tabla de los municipios lejanos cuyo prestador del servicio de internet es Edatel.

IDENTIFICADOR DEL SERVICIO	LOCALIDAD	TECNOLOGÍA
REGISTRADURIAABRIAQUI	ABRIAQUI	3 Mbps Internet Edatel
REGISTRADURIAAMAGA	AMAGA	4 Mbps Internet Edatel
REGISTRADURIAAMALFI	AMALFI	3 Mbps Internet Edatel
REGISTRADURIAANDES	ANDES	8 Mbps Internet Banda Ancha
REGISTRADURIAANGOSTURA	ANGOSTURA	4 Mbps Internet Edatel
REGISTRADURIAANORI	ANORI	3 Mbps Internet Edatel
REGISTRADURIAAPARTADO	APARTADO	8 Mbps Internet Banda Ancha
REGISTRADURIAARBOLETES	ARBOLETES	4 Mbps Internet Edatel
REGISTRADURIAARGELIA	ARGELIA	3 Mbps Internet Edatel
REGISTRADURIAANTIOQUIA	SANTAFE DE ANTIOQUIA	8 Mbps Internet Banda Ancha
REGISTRADURIABRICENO	BRICEÑO	3 Mbps Internet Edatel
REGISTRADURIABURITICA	BURITICA	3 Mbps Internet Edatel
REGISTRADURIACACERES	CACERES	4 Mbps Internet Edatel
REGISTRADURIACAMPAMENTO	CAMPAMENTO	3 Mbps Internet Edatel
REGISTRADURIACANASGORDAS	CANASGORDAS	4 Mbps Internet Edatel
REGISTRADURIACAREPA	CAREPA	8 Mbps Internet Banda Ancha
REGISTRADURIACAROLINA	CAROLINA	4 Mbps Internet Edatel
REGISTRADURIACISNEROS	CISNEROS	4 Mbps Internet Edatel
REGISTRADURIACOCORNA	COCORNA	3 Mbps Internet Edatel
REGISTRADURIABELMIRA	BELMIRA	3 Mbps Internet Edatel
REGISTRADURIABETANIA	BETANIA	4 Mbps Internet Edatel
REGISTRADURIACONCORDIA	CONCORDIA	4 Mbps Internet Edatel
REGISTRADURIAABEJORRAL	ABEJORRAL	3 Mbps Internet Edatel
REGISTRADURIAALEJANDRIA	ALEJANDRIA	4 Mbps Internet Edatel
REGISTRADURIAANGELOPOLIS	ANGELOPOLIS	4 Mbps Internet Edatel
REGISTRADURIAANZA	ANZA	3 Mbps Internet Edatel
REGISTRADURIAARMENIA	ARMENIA	3 Mbps Internet Edatel
REGISTRADURIABOLIVAR	CIUDAD BOLIVAR	4 Mbps Internet Edatel
REGISTRADURIACAICEDO	CAICEDO	3 Mbps Internet Edatel
REGISTRADURIACARAMANTA	CARAMANTA	3 Mbps Internet Edatel
REGISTRADURIACAUCASIA	CAUCASIA	8 Mbps Internet Banda Ancha

REGISTRADURIACONCEPCION	CONCEPCION	3 Mbps Internet Edatel
REGISTRADURIADABEIBA	DABEIBA	4 Mbps Internet Edatel
REGISTRADURIADONMATIAS	DON MATIAS	4 Mbps Internet Edatel
REGISTRADURIAEBEJICO	EBEJICO	3 Mbps Internet Edatel
REGISTRADURIAELBAGRE	EL BAGRE	4 Mbps Internet Edatel
REGISTRADURIAENTRERRIOS	ENTRERRIOS	4 Mbps Internet Edatel
REGISTRADURIAFREDONIA	FREDONIA	4 Mbps Internet Edatel
REGISTRADURIAFRONTINO	FRONTINO	4 Mbps Internet Edatel
REGISTRADURIAGIRALDO	GIRALDO	4 Mbps Internet Edatel
REGISTRADURIAGUADALUPE	GUADALUPE	4 Mbps Internet Edatel
REGISTRADURIAGUATAPE	GUATAPE	4 Mbps Internet Edatel
REGISTRADURIAGRANADA	GRANADA	3 Mbps Internet Edatel
REGISTRADURIAGOMEZPLATA	GOMEZ PLATA	4 Mbps Internet Edatel
REGISTRADURIAHELICONIA	HELICONIA	3 Mbps Internet Edatel
REGISTRADURIAITUANGO	ITUANGO	3 Mbps Internet Edatel
REGISTRADURIAHISPANIA	HISPANIA	4 Mbps Internet Edatel
REGISTRADURIAJARDIN	JARDIN	4 Mbps Internet Edatel
REGISTRADURIAJERICO	JERICO	4 Mbps Internet Edatel
REGISTRADURIALAPINTADA	LA PINTADA	4 Mbps Internet Edatel
REGISTRADURIALIBORINA	LIBORINA	4 Mbps Internet Edatel
REGISTRADURIAMACEO	MACEO	4 Mbps Internet Edatel
REGISTRADURIAMONTEBELLO	MONTEBELLO	3 Mbps Internet Edatel
REGISTRADURIANARINO	NARINO	3 Mbps Internet Edatel
REGISTRADURIANECHI	NECHI	3 Mbps Internet Edatel
REGISTRADURIANECOCLI	NECOCLI	4 Mbps Internet Edatel
REGISTRADURIAPENOL	PE?OL	4 Mbps Internet Edatel
REGISTRADURIAPEQUE	PEQUE	3 Mbps Internet Edatel
REGISTRADURIAPUEBLORRICO	PUEBLORRICO	4 Mbps Internet Edatel
REGISTRADURIAPTOBERRIO	PUERTO BERRIO	8 Mbps Internet Banda Ancha
REGISTRADURIAPUERTONARE	PUERTO NARE	3 Mbps Internet Edatel
REGISTRADURIASABANALARGA	SABANALARGA	3 Mbps Internet Edatel
REGISTRADURIASALGAR	SALGAR	4 Mbps Internet Edatel
REGISTRADURIASANANDRES	SAN ANDRES DE C.	3 Mbps Internet Edatel
REGISTRADURIASANCARLOS	SAN CARLOS	3 Mbps Internet Edatel
REGISTRADURIASANFRANCISCO	SAN FRANCISCO	3 Mbps Internet Edatel

REGISTRADURIASANJERONIMO	SAN JERONIMO	4 Mbps Internet Edatel
REGISTRADURIASJOSEDELAMONTANA	SAN JOSE DE LA MONTA?A	3 Mbps Internet Edatel
REGISTRADURIASJUANURABA	SAN JUAN DE URABA	4 Mbps Internet Edatel
REGISTRADURIASANLUIS	SAN LUIS	3 Mbps Internet Edatel
REGISTRADURIASANPEDRO	SAN PEDRO DE LOS MILAGROS	4 Mbps Internet Edatel
REGISTRADURIASPEDROURABA	SAN PEDRO DE URABA	4 Mbps Internet Edatel
REGISTRADURIASANRAFAEL	SAN RAFAEL	4 Mbps Internet Edatel
REGISTRADURIASANVICENTE	SAN VICENTE	3 Mbps Internet Edatel
REGISTRADURIASTABARBARA	SANTA BARBARA	4 Mbps Internet Edatel
REGISTRADURIASTAROSAOSOS	SANTA ROSA DE OSOS	8 Mbps Internet Banda Ancha
REGISTRADURIASTODOMINGO	SANTO DOMINGO	4 Mbps Internet Edatel
REGISTRADURIASEGOVIA	SEGOVIA	4 Mbps Internet Edatel
REGISTRADURIASONSON	SONSON	3 Mbps Internet Edatel
REGISTRADURIASOPETRAN	SOPETRAN	4 Mbps Internet Edatel
REGISTRADURIATAMESIS	TAMESIS	4 Mbps Internet Edatel
REGISTRADURIATARAZA	TARAZA	4 Mbps Internet Edatel
REGISTRADURIATARSO	TARSO	4 Mbps Internet Edatel
REGISTRADURIATOLEDO	TOLEDO	3 Mbps Internet Edatel
REGISTRADURIATURBO	TURBO	8 Mbps Internet Banda Ancha
REGISTRADURIAURRAO	URRAO	4 Mbps Internet Edatel
REGISTRADURIAVALDIVIA	VALDIVIA	4 Mbps Internet Edatel
REGISTRADURIAVALPARAISO	VALPARAISO	4 Mbps Internet Edatel
REGISTRADURIAVEGACHI	VEGACHI	4 Mbps Internet Edatel
REGISTRADURIAVENECIA	VENECIA	4 Mbps Internet Edatel
REGISTRADURIAVIGIADELFTE	VIGIA DEL FUERTE	3 Mbps Internet Edatel
REGISTRADURIAYALI	YALI	4 Mbps Internet Edatel
REGISTRADURIAYARUMAL	YARUMAL	8 Mbps Internet Banda Ancha
REGISTRADURIAYONDO	YONDO	3 Mbps Internet Edatel
REGISTRADURIAZARAGOZA	ZARAGOZA	4 Mbps Internet Edatel
REGISTRADURIAREMEDIOS	REMEDIOS	4 Mbps Internet Edatel

REGISTRADURIAURAMITA	URAMITA	4 Mbps Internet Edatel
REGISTRADURIAPTOTRIUNFO	PUERTO TRIUNFO	3 Mbps Internet Edatel
REGISTRADURIASANROQUE	SAN ROQUE	4 Mbps Internet Edatel
REGISTRADURIAMURINDO	MURINDO	3 Mbps Internet Edatel
REGISTRADURIAOLAYA1	SUCRE	4 Mbps Internet Edatel
REGISTRADURIABETULIA	BETULIA	4 Mbps Internet Edatel
REGISTRADURIAMUTATA	MUTATA	4 Mbps Internet Edatel
REGISTRADURIACARACOLI	CARACOLI	4 Mbps Internet Edatel
REGISTRADURIACHIGORODO	CHIGORODO	8 Mbps Internet Banda Ancha
REGISTRADURIATITIRIBI	TITIRIBI	3 Mbps Internet Edatel
REGISTRADURIAYOLOMBO	YOLOMBO	4 Mbps Internet Edatel

Ilustración 29: Estado actual del ancho de banda de los municipios

Fuente: Registraduria de Antioquia

Tabla de códigos de los municipios de Antioquia, base de referencia para la creación de extensiones IP en cada sede

Código Deapartamento	**Nombre Departamento**	**Código Municipio**	**Nombre Municipio**
05	ANTIOQUIA	001	MEDELLIN
05	ANTIOQUIA	002	ABEJORRAL
05	ANTIOQUIA	004	ABRIAQUI
05	ANTIOQUIA	021	ALEJANDRIA
05	ANTIOQUIA	030	AMAGA
05	ANTIOQUIA	031	AMALFI
05	ANTIOQUIA	034	ANDES
05	ANTIOQUIA	036	ANGELOPOLIS
05	ANTIOQUIA	038	ANGOSTURA

05	ANTIOQUIA	040	ANORI
05	ANTIOQUIA	042	SANTAFE DE ANTIOQUIA
05	ANTIOQUIA	044	ANZA
05	ANTIOQUIA	045	APARTADO
05	ANTIOQUIA	051	ARBOLETES
05	ANTIOQUIA	055	ARGELIA
05	ANTIOQUIA	059	ARMENIA
05	ANTIOQUIA	079	BARBOSA
05	ANTIOQUIA	086	BELMIRA
05	ANTIOQUIA	088	BELLO
05	ANTIOQUIA	091	BETANIA
05	ANTIOQUIA	093	BETULIA
05	ANTIOQUIA	101	CIUDAD BOLIVAR
05	ANTIOQUIA	107	BRICEÑO
05	ANTIOQUIA	113	BURITICA
05	ANTIOQUIA	120	CACERES
05	ANTIOQUIA	125	CAICEDO
05	ANTIOQUIA	129	CALDAS
05	ANTIOQUIA	134	CAMPAMENTO
05	ANTIOQUIA	138	CAÑASGORDAS
05	ANTIOQUIA	142	CARACOLI
05	ANTIOQUIA	145	CARAMANTA

05	ANTIOQUIA	147	CAREPA
05	ANTIOQUIA	148	EL CARMEN DE VIBORAL
05	ANTIOQUIA	150	CAROLINA
05	ANTIOQUIA	154	CAUCASIA
05	ANTIOQUIA	172	CHIGORODO
05	ANTIOQUIA	190	CISNEROS
05	ANTIOQUIA	197	COCORNA
05	ANTIOQUIA	206	CONCEPCION
05	ANTIOQUIA	209	CONCORDIA
05	ANTIOQUIA	212	COPACABANA
05	ANTIOQUIA	234	DABEIBA
05	ANTIOQUIA	237	DON MATIAS
05	ANTIOQUIA	240	EBEJICO
05	ANTIOQUIA	250	EL BAGRE
05	ANTIOQUIA	264	ENTRERRIOS
05	ANTIOQUIA	266	ENVIGADO
05	ANTIOQUIA	282	FREDONIA
05	ANTIOQUIA	284	FRONTINO
05	ANTIOQUIA	306	GIRALDO
05	ANTIOQUIA	308	GIRARDOTA
05	ANTIOQUIA	310	GOMEZ PLATA
05	ANTIOQUIA	313	GRANADA

05	ANTIOQUIA	315	GUADALUPE
05	ANTIOQUIA	318	GUARNE
05	ANTIOQUIA	321	GUATAPE
05	ANTIOQUIA	347	HELICONIA
05	ANTIOQUIA	353	HISPANIA
05	ANTIOQUIA	360	ITAGUI
05	ANTIOQUIA	361	ITUANGO
05	ANTIOQUIA	364	JARDIN
05	ANTIOQUIA	368	JERICO
05	ANTIOQUIA	376	LA CEJA
05	ANTIOQUIA	380	LA ESTRELLA
05	ANTIOQUIA	390	LA PINTADA
05	ANTIOQUIA	400	LA UNION
05	ANTIOQUIA	411	LIBORINA
05	ANTIOQUIA	425	MACEO
05	ANTIOQUIA	440	MARINILLA
05	ANTIOQUIA	467	MONTEBELLO
05	ANTIOQUIA	475	MURINDO
05	ANTIOQUIA	480	MUTATA
05	ANTIOQUIA	483	NARIÑO
05	ANTIOQUIA	490	NECOCLI
05	ANTIOQUIA	495	NECHI

05	ANTIOQUIA	501	OLAYA
05	ANTIOQUIA	541	PEÐOL
05	ANTIOQUIA	543	PEQUE
05	ANTIOQUIA	576	PUEBLORRICO
05	ANTIOQUIA	579	PUERTO BERRIO
05	ANTIOQUIA	585	PUERTO NARE
05	ANTIOQUIA	591	PUERTO TRIUNFO
05	ANTIOQUIA	604	REMEDIOS
05	ANTIOQUIA	607	RETIRO
05	ANTIOQUIA	615	RIONEGRO
05	ANTIOQUIA	628	SABANALARGA
05	ANTIOQUIA	631	SABANETA
05	ANTIOQUIA	642	SALGAR
05	ANTIOQUIA	647	SAN ANDRES DE CUERQUIA
05	ANTIOQUIA	649	SAN CARLOS
05	ANTIOQUIA	652	SAN FRANCISCO
05	ANTIOQUIA	656	SAN JERONIMO
05	ANTIOQUIA	658	SAN JOSE DE LA MONTAÑA
05	ANTIOQUIA	659	SAN JUAN DE URABA
05	ANTIOQUIA	660	SAN LUIS
05	ANTIOQUIA	664	SAN PEDRO
05	ANTIOQUIA	665	SAN PEDRO DE URABA

05	ANTIOQUIA	667	SAN RAFAEL
05	ANTIOQUIA	670	SAN ROQUE
05	ANTIOQUIA	674	SAN VICENTE
05	ANTIOQUIA	679	SANTA BARBARA
05	ANTIOQUIA	686	SANTA ROSA DE OSOS
05	ANTIOQUIA	690	SANTO DOMINGO
05	ANTIOQUIA	697	EL SANTUARIO
05	ANTIOQUIA	736	SEGOVIA
05	ANTIOQUIA	756	SONSON
05	ANTIOQUIA	761	SOPETRAN
05	ANTIOQUIA	789	TAMESIS
05	ANTIOQUIA	790	TARAZA
05	ANTIOQUIA	792	TARSO
05	ANTIOQUIA	809	TITIRIBI
05	ANTIOQUIA	819	TOLEDO
05	ANTIOQUIA	837	TURBO
05	ANTIOQUIA	842	URAMITA
05	ANTIOQUIA	847	URRAO
05	ANTIOQUIA	854	VALDIVIA
05	ANTIOQUIA	856	VALPARAISO
05	ANTIOQUIA	858	VEGACHI
05	ANTIOQUIA	861	VENECIA

05	ANTIOQUIA	873	VIGIA DEL FUERTE
05	ANTIOQUIA	885	YALI
05	ANTIOQUIA	887	YARUMAL
05	ANTIOQUIA	890	YOLOMBO
05	ANTIOQUIA	893	YONDO
05	ANTIOQUIA	895	ZARAGOZA

Ilustración 30: Códigos de los municipios para el diseño del plan de marcación

Fuente: Registraduria de Antioquia

FIRMA ESTUDIANTES Viviana A Rojas G

FIRMA ASESOR 

FECHA ENTREGA: __15-02-2016___

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO___ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA: _____