UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TÍTULO DE LA TESIS:

"Fundamentación de factibilidad y conveniencia en el diseño de una propuesta de un Sistema de comunicación, basada en una solución tecnológica *Open Source* para la Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo**"**

Previa la obtención del Grado Académico de Magíster en Telecomunicaciones

ELABORADO POR:

JAVIER HERNÁN LÓPEZ ZAMBRANO

Guayaquil, Julio 2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Magíster Javier Hernán López Zambrano como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones.

Guayaquil, Julio 2014

DIRECTOR DE TESIS

_____
Ing. Juan García, MSc.

REVISORES:

_____ _____
Ing. Orlando Philco Ing. Luzmila Ruilova

DIRECTOR DEL PROGRAMA

_____
Ing. Manuel Romero Paz, MSc.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

DECLARACIÓN DE RESPONSABILIDAD

YO, JAVIER HERNÁN LÓPEZ ZAMBRANO

DECLARO QUE:

La tesis "**Fundamentación de factibilidad y conveniencia en el diseño de una propuesta de un Sistema de comunicación, basada en una solución tecnológica *Open Source* para la Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo**", previa a la obtención del grado Académico de Magíster, ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico de la tesis del Grado Académico en mención.

Guayaquil, Julio 2014

EL AUTOR

_____
JAVIER HERNÁN LÓPEZ ZAMBRANO

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

AUTORIZACIÓN

YO, JAVIER HERNÁN LÓPEZ ZAMBRANO

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución de la Tesis de Maestría titulada: "**Fundamentación de factibilidad y conveniencia en el diseño de una propuesta de un Sistema de comunicación, basada en una solución tecnológica Open Source para la Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo**", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, Julio 2014

EL AUTOR

_____

JAVIER HERNÁN LÓPEZ ZAMBRANO

DEDICATORIA

El presente trabajo, lo dedico a mi primogénito, donde mi mejor legado será de demostrarle que la realización de metas y sueños, son parte del crecimiento personal y profesional.

AGRADECIMIENTOS

Sobre todo, el agradecimiento a Dios, por permitirnos vivir y cumplir nuestras metas con su bendición, a mis Padres, por inculcar en mí, el sentido de crecimiento personal y profesional, a mi familia, por apoyarme es mis horas de realización de este trabajo, a Docentes, Tutor, Revisores, y Director de Programa, por el apoyo y aporte de nuevos conocimientos durante la Maestría y realización de mi Tesis.

RESUMEN

Hoy por hoy, las soluciones informáticas, se han constituido en herramientas de trabajo imprescindibles, las cuales permiten la eficiencia y eficacia en las labores diarias en cualquier empresa, es por ello que la presente tesis se centra en fundamentar la factibilidad y conveniencia de diseño de una propuesta de un sistema basado en solución Tecnológica Open Source para conseguir comunicación oportuna entre las distintas oficinas de la Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo ubicado en la provincia de Manabí, y brindar a su personal administrativo, la disponibilidad de un sistema de comunicación con un alto grado de prestaciones e independencia tecnológica a costes reducidos. Para el estudio y presentación de la propuesta, se realizó una investigación de tipo aplicada cuasi experimental, implementando laboratorios con servidores virtuales sobre la infraestructura real, analizando además factores cuantitativos, como tráfico, QoS, llamadas máximas (ERLANG) y factores cualitativos como adaptación y resistencia por parte del personal. La propuesta se basa en una ingeniería de implementación de dos servidores PBX (uno por edificio) con servicios VoIP (compartiendo salida a líneas de telefonía fija) e IM (como herramienta complementaria), aprovechando la infraestructura existente, para brindar interconexión entre los servidores y a la vez tengan independencia intra-edicio, lo cual garantiza una alta disponibilidad de estos servicios como medios de comunicación, disponibles para todo el personal.

PALABRAS CLAVES: Open Source, Elastix, PBX, VoIP, IM

ABSTRACT

Today, software solutions, have become essential tools work, which allow the efficiency and effectiveness in daily tasks in any business, which is why this thesis focuses on the feasibility and desirability base design a proposed solution based on Open Source Technology to get timely communication between the various offices of the Municipal Public Company for Water and Wastewater Portoviejo located in the province of Manabí, and provide administrative personnel system, the availability of a system communication with a high degree of independence and technological benefits to discounted costs. For the study and presentation of the proposal, such an investigation was conducted applied quasi-experimental, implementing laboratories with virtual servers on the real infrastructure, and analyzing quantitative factors such as traffic, QoS, called maximum (ERLANG) and qualitative factors such as adaptation and resistance from staff. The proposal is based on an engineering PBX implementation of two (one per block) with VoIP (output sharing fixed lines) and IM (as a complementary tool), leveraging existing infrastructure servers, to provide interconnection between servers and both intra-editions have independence, which ensures high availability of these services as a means of communication available to all staff.

KEY WORDS: Open Source, Elastix, PBX, VoIP, IM

Índice

Índice de Figuras

Índice de Tablas

1. Capítulo I: Introducción

1.1. Antecedentes

La tecnología ha tenido un despunte en la última década, y con ella las formas y medios de comunicación, convirtiéndose en una necesidad imprescindible para las personas y por consiguiente para las Empresas, el hecho de contar con algún medio de comunicación que sirva de herramienta en las labores diarias de su personal.

En la búsqueda por mejorar las formas de comunicarse, han aparecido soluciones tipo hardware y software las cuales en la actualidad son diversas y complementarias.

Dentro de los diversos medios de comunicación, cuya tendencia y evolución ha sido bastante considerable en la última década, encontramos dos tipos claramente posicionados en la actualidad: la telefonía IP y la mensajería instantánea.

Las soluciones tipo *Software Open Source* (SOS) han evolucionado significativamente a tal punto de competir con *software* propietarios en cuanto a funcionalidad, adaptabilidad, seguridad, fiabilidad y potencial de producción con el menor mantenimiento posible; y el hecho de ser redistribuible gratuitamente, su bajo costo de mantenimiento y la estabilidad operativa de estos sistemas, significan ventajas muy importantes al momento de comparar precios (de lo que cuesta un *software* propietario hoy en día).

Por la naturaleza de su código abierto, estas soluciones permiten ser integradas, personalizadas y ser utilizadas con otros tipos de sistemas más robustos, cuyos productos son complementarios, los cuales brindan respuestas integrales a las necesidades de las Empresas, y gracias a las mejoras constantes por parte de los desarrolladores, han convertido a los SOS en herramientas escalables, lo que mejora su competitividad con los modelos de *software* propietarios.

1.2. Justificación

La Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo (EPMAPAP), es una empresa dedicada a brindar servicios a la comunidad Portovejense, cuenta con algunas oficinas ubicadas en diferentes lugares geográficos, enlazadas por túneles de datos para la comunicación de sus equipos informáticos.

La EPMAPAP, tiene una infraestructura tecnológica que se encuentra acorde a las necesidades y exigencias de los objetivos de la Empresa, sin embargo, carece de suficientes medios para la comunicación de ámbito laboral entre el personal de las distintas oficinas, ya que sólo se dispone de unas cuantas líneas de telefonía convencional, lo cual provoca limitaciones e incide en la comunicación oportuna, provocando ineficiencia en la ejecución de los procesos administrativos.

En vista de la existencia de estas limitaciones a la hora de querer comunicarse el personal entre las distintas oficinas con que cuenta la EPMAPAP, y la presencia de una infraestructura tecnológica que se puede aprovechar, se considera factible la implementación del *SOS Elastix* como una solución *Open Source* adecuada y de bajo costes para PYMES y así contar con un Servidor *IM* y *PBX VoIP* para atender esta necesidad, poniendo a disposición estos medios de comunicaciones inmediatos a todos el personal de la Empresa.

1.2.1. Importancia y Pertinencia Social

- Brindar mayor número de medios de comunicación e integración de las líneas fijas, con la finalidad de contar con comunicación oportuna.
- Aprovechar estas herramientas para optimizar la eficiencia de los procesos administrativos de la empresa.
- Acortar la brecha tecnológica entre el personal y el uso de estas herramientas.

1.2.2. Importancia y Pertinencia Tecnológica

- Implementación de tecnología *Open Source*, para brindar servicios de comunicación *IM* y *VoIP*.

- Emplear esta tecnología para integrar las líneas telefónicas fijas, distribuidas de manera independiente en ambos edificios, para el uso común de todo el personal administrativo.

- Aprovechar infraestructura existente para brindar comunicación oportuna en base a la correlación del ancho de banda disponible versus protocolos y *QoS*, empleados para estos servicios.

1.3. Problema de Investigación

La carencia de suficientes medios de comunicación, incide en la comunicación oportuna entre el personal de las distintas oficinas y por ende provoca ineficiencia en la ejecución de los procesos administrativos.

1.4. Objetivos

1.4.1. General

Fundamentar la factibilidad y conveniencia de diseño de una propuesta de un sistema basado en solución Tecnológica *Open Source* para conseguir comunicación oportuna entre las distintas oficinas de la Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo.

1.4.2. Específicos

- Diagnosticar las afectaciones existentes a causa de problemas de comunicación

- Evaluar requerimientos de infraestructura y tecnología a usarse.
- Determinar el modelo de infraestructura para implementación de servidores *IM* y *PBX VoIP* aprovechando infraestructura existente.
- Diseñar la Propuesta de implementación.
- Determinar la factibilidad económica y tecnológica

1.5. Hipótesis

Una propuesta de servicio de *VoIP* e *IM* basado en una plataforma de *Software* Libre (*Elastix*) con disponibilidad para todo el personal administrativo de las distintas oficinas de la EPMAPAP, permitiría el despliegue de un sistema de comunicación con un alto grado de prestaciones e independencia tecnológica y de costes muy reducidos.

1.6. Variables

1.6.1. Independientes

- Infraestructura de comunicación existente
- Tecnologías de protocolos de comunicación

1.6.2. Dependientes

- Herramienta *Open Source*
- Tráfico de datos
- Factibilidad económica y tecnológica

1.7. Delimitación del Estudio

1.7.1. Clasificación

Campo : Sistemas

Área : Comunicaciones

Aspecto: Aplicaciones de Tecnología *Open Source* en sistemas de comunicación

1.7.2. Delimitación Espacial

El presente trabajo de propuesta de intervención, se lo realiza en el departamento de servicios informáticos de la Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo, en la provincia de Manabí.

1.7.3. Delimitación Temporal

El estudio de la presente propuesta de intervención se realiza desde junio a diciembre del 2013.

1.7.4. Software a utilizarse

El presente trabajo de tesis, tiene como alcance aprovechar la infraestructura de red de la EPMAPAP, para elaborar una propuesta de implementación de un sistema de comunicación, utilizando la distribución de Linux Elastix, considerado como un producto de comunicación unificada.

Elastix incluye los servicios de: Fax, Correo, Video Conferencia, VoIP y Mensajería Instantáneas, de los cuales se aprovecharan para la propuesta, los dos últimos servicios.

1.7.5. Infraestructura existente

La EPMAPAP, cuenta con dos edificios principales denominados edificio Central y edificio Matriz, aparte de las agencias y otras oficinas, estos dos edificios se interconectan por medio de un túnel de datos arrendado a un *ISP*.

Edificio Central, denominado así, porque en él se encuentra el centro de datos, cuenta con una red *LAN* de categoría 5A, que brinda servicio al personal de Recaudación, Atención al Cliente, Catastro e Informática.

Edificio Matriz, cuenta con una red *LAN* de categoría 6A, y en él se aloja personal de recaudación y todo el personal administrativo de la empresa.

1.7.6. Ancho de Banda

El análisis en cuento a ancho de banda que se define a continuación, es en base a la máxima capacidad de trasmitir datos por un medio, concepción por convención o tradicionalismo, y no por la definición propia o teórica de la terminología.

El ancho de banda de las redes *LAN* de ambos edificios, no es una limitante, ya que cuentan con equipos activos de red (*switch*) de 10/100/1000 *Mbps*, la única limitante que se tiene de ancho de banda, es en la interconexión entre los edificios, que cuenta con 1 *Mega CLEAR CHANNEL*, para el túnel de dato arrendado al *ISP*.

Edificio Central: Dispone de equipos activos tipo *Switch Cisco System* SRW2024 24-Port 10/100/1000 *Mbps*.

Edificio Matriz: Dispone de equipos activos tipo *Switch HP* (con tecnología *3com*) V1910-48G 48-Port 10/100/1000 Mbps.

Túnel de dato: *Router Cisco*, tecnología L3 *MPLS* (*Multiprotocol Label Switching*), latencia < 15ms**.**

1.7.7. Calidad de Servicios *QoS*

La EPMAPAP cuenta con equipos activos (*switch*) administrables, en las redes *LAN* de cada edificio, por lo que la calidad de servicio (*QoS*) se controlará desde los mismos equipos; a excepción del *QoS* en el túnel de datos que los interconecta, puesto que es el *ISP*, quien administra sus *routers*, es por ello que controlar el retardo, la variación de retardo y la pérdida de paquetes en el tunes de datos, será una limitante.

1.7.8. Seguridad

La seguridad en los sistemas de comunicación IP, es un tema muy complejo y amplio, puesto que la constante evolución de la tecnología, trae consigo nuevas brechas de vulnerabilidades, frente al hecho que los riegos actuales de las redes de datos, deben sumárseles los problemas de vulnerabilidad que trae consigo la tecnología *VoIP*; por tal motivo, para disminuir los riesgos de seguridad, se debe contemplar un sinnúmero de niveles de prevención, a nivel de infraestructura de red, de servidores, y de otros equipos y software adicionales que la integren.

Por tal motivo, el presente trabajo brindará ciertas recomendaciones, sin pretender cubrir este tema en su totalidad, ya que para eso se requeriría de un *PENTEST*.

Además, un punto a favor en cuanto a seguridad, es que al usar Software *Open Source*, este brindará mayor garantía, que un Software propietario, ya que al ser código abierto, se puede constatar que no incluya códigos que violen la seguridad y privacidad de los datos, como se ha escuchado casos recientes de software de algunas compañías, que recogen datos de los usuarios, sea para el análisis y beneficio particular de la Empresa, o para proporcionarlos a alguna red de espionaje como la conocida *ECHELON* considerada como base de la actual *PRISM* de la *NSA* de *EE.UU* (M. Á. M. Diariocrítico, 2013)

1.7.9. Economía

La implementación de un sistema de comunicación, empleando soluciones de tipo *Software Open Source*, versus soluciones de tipo *Software* propietario, de por si implican un ahorro en los costes, siempre y cuando se cuente con personal que tenga conocimientos en este tipo de tecnología, caso contrario, debería incluirse los costos de soporte en la configuración y capacitación de la administración del *Software Open Source (Elastix)*, sin embargo, el ahorro más significativo, está en que la EPMAPAP, ya cuenta con infraestructura de red *LAN* y túneles de datos (arrendados), los cuales serán aprovechados, quedando una inversión mínima, en equipos como teléfonos IP, tarjeta para troncales (ej: *Digium TDM410P*), entre otros equipos cuyos costos son mínimo, comparado con el valor total que podría tener, el despliegue integro de toda una infraestructura para estos sistemas de comunicación *VoIP*.

1.8. Diseño Metodológico

El presente trabajo contempla una investigación tipo aplicada cuasi experimental, puesto que se realizó laboratorios con servidores virtuales sobre la infraestructura real, para determinar los factores incidente y poder fundamentar acertadamente el diseño de propuesta; además tiene una connotación transeccional ya que la duración de estudio fue de aproximadamente 6 meses.

Además su alcance es correlacional con enfoque mixto, ya que se realizó un análisis comparativo entre las herramientas y los beneficios.

Los análisis que se realizaron son:

- Cuantitativo
    - Tráfico de datos de acuerdo al protocolo usado
    - Número máximo de llamadas establecidas por extensiones IP de forma paralela, respecto al ancho de banda disponible del enlace existente – *ERLANG*.

- Análisis de *QoS* respecto a problemas como: *jitter*, retardo, pérdida de paquetes.
- Número de llamadas realizada de manera convencional, para atender tareas y/o procesos administrativos

- Cualitativo
  - Grado de satisfacción de los usuarios

Los métodos que se utilizaron para la realización de la presente tesis, son: Encuesta, Medición y Experimento.

Universo - Muestra

Para el análisis cuantitativo y cualitativo se tomó como muestra representativa a todo el universo, comprendido por los 120 funcionarios administrativos de la EPMAPAP, distribuidos en ambos edificios.

2. Capítulo II: Generalidades de los sistemas telefónicos

2.1. Fundamentación Filosófica

La investigación se circunscribe dentro del paradigma crítico – propositivo, donde la finalidad es la identificación y comprensión, de los efectos de no contar con un sistema de comunicación apropiado; permitiendo el estudio para la presentación de una propuesta que mejore el alto grado de prestaciones a todo el personal administrativo de la EPMAPAP.

Incluye una visión de la realidad dentro de las comunicaciones internas, la cual generará interacción transformadora en el proceso, que permitan el progreso de la Institución, aprovechando los recursos tecnológicos existentes, representándole ahorros económicos.

2.2. Fundamentación Legal

El Estado Ecuatoriano con el avance de la tecnología y para el fortalecimiento del sector de las telecomunicaciones ha construido un marco legal que permita una adecuada regulación y expansión de los sistemas radioeléctricos y servicios de telecomunicaciones, además de promover actividades con criterios de gestión Institucional y beneficio social en un régimen de libre competencia.

Por lo que el presente punto trata de encontrar aspectos legales en los cuales la implementación de las comunicaciones y telefonía IP, sea posible en medio de un marco jurídico conforme a las leyes, reglamentos y normas vigentes en el sector de las telecomunicaciones en el Ecuador.

Acorde al Art. 1 (ámbito de la Ley), "…*Una red privada puede estar compuesta de uno o más circuitos arrendados, líneas privadas virtuales, infraestructura propia, o una combinación de éstos, conforme a los requisitos establecidos en los artículos siguientes. Dichas redes pueden abarcar puntos en el territorio nacional y en el extranjero. Una red privada puede ser utilizada para la transmisión de voz, datos, sonidos, imágenes o cualquier combinación de éstos.*", y el Art. 10 (Intercomunicaciones internas), "*No será necesaria autorización alguna*

para el establecimiento o utilización de instalaciones destinadas a intercomunicaciones dentro de residencias, edificaciones e inmuebles públicos o privados, siempre que para el efecto no se intercepten o interfieran los sistemas de telecomunicaciones públicos. Si lo hicieran, sus propietarios o usuarios estarán obligados a realizar, a su costo, las modificaciones necesarias para evitar dichas interferencias o intercepciones, sin perjuicio de la aplicación de las sanciones previstas en esta Ley. En todo caso, también estas instalaciones estarán sujetas a la regulación y control por parte del Estado.", del Capítulo I de la Ley Especial de Telecomunicaciones Reformada (Ley No. 184), considera que para la implementación de una red privada para transmitir voz, en este caso dentro de una institución pública, no se requiere de alguna autorización por parte del ente regulador, siempre y cuando no incurra en interferir o interceptar los sistemas de telecomunicaciones públicos. (Corporación Nacional de Telecomunicaciones, 1992) (Corporación Nacional de Telecomunicaciones, 2000)

2.3. Introducción

La comunicación tiene sus orígenes desde que la humanidad tuvo la necesidad de comunicarse y con el pasar de los años, proponerse la meta de romper las barreras del espacio, el medio y al hecho mismo de que tanto el emisor como el receptor estén obligatoriamente al mismo tiempo compartiendo la información o el mensaje.

Las telecomunicaciones tienen sus orígenes con la aparición del telégrafo en el siglo XVIII, y según (Cabezas, 2007), a mediados del siglo XIX ya conformaban sistema de comunicación de transmisión a larga distancias de mensajes codificados en morse, los mismos que se consideran como el verdadero precursor de las centrales telefónicas hoy en día.

Con la aparición de los teléfonos (1876), gracias a los aportes teóricos de Charles Bourseul, las pruebas iniciales de Johann Philipp Reis, los aportes contundentes de Antonio Meucci y la polémica sobre la patente atribuida a Alexander Grahamm Bell (según la historia), se comienza a transmitir la voz entre dos puntos distantes, y con esto comienza la evolución de esta tecnología, hasta

llegar hoy en día a los teléfonos digitales con tecnología IP, los cuales son capaces de transmitir no solamente voz, sino también imágenes y videos (Carballar, 2007) (Cabezas, 2007).

Con toda esta evolución tecnológica, los sistemas de comunicación, han conllevado a la creación de grandes redes telefónicas, las mismas que apoyadas por equipos de conmutación y de transmisión, han logrado que la voz viaje de un extremo a otro.

Estos sistemas o enlaces telefónicos, utilizan centrales, las cuales cumplen la función principal de conmutar los circuitos de una red pública y/o privada para establecer las llamadas telefónicas entre los usuarios, denominadas comúnmente centrales telefónicas, las mismas que también han ido evolucionando tecnológicamente a través de la historia:

- Centrales manuales, eran aquellas cuyas operadoras conectaban manualmente mediante un cable a los interlocutores que querían hablar.
- Centrales semiautomáticas y automáticas, cuya conmutación estaba basada en tecnología electromecánica, y se la realizaba mediante selectores mecánicos y relés.
- Centrales electrónicas, eran aquellas cuyos componentes mecánicos desaparecieron y la conmutación se realizaba mediante circuitos analógicos.
- Centrales digitales, en sus inicios consideradas así ya que sus componentes electrónicos de la central, incorporaban microprocesadores; posteriormente aparecieron las centrales que podían utilizar tanto líneas como extensiones analógicas y/o digitales, al igual que tecnología *RDSI*.
- Centrales IP, se trata de equipos con procesador y conexión Ethernet, que utilizan el protocolo IP para transmitir voz, datos y videos. Además se pueden equipar con interfaces para conectarlos con tecnologías analógicas o RDSI.

Todos estos tipos de centrales, han evolucionado principalmente en cuanto a la forma de conmutar y al tipo de señal que transportan, bien sean señales análogas o digitales.

Las señales análogas son ondas que varían de forma continua, por lo tanto pueden tomar cualquier valor, a diferencia de las señales digitales, las cuales sólo pueden tomar dos posibles valores (0 y 1), denominándose por lo tanto como señal digital binaria, como se observa en la figura 2.1. (Carballar, 2007) (Cabezas, 2007)

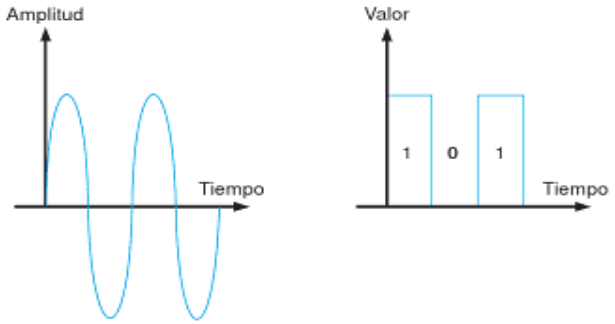


Figura 2.1 *– Señal analógica y señal digital (binaria)*
Fuente*: [Cabezas, 2007]*

Las señales generadas por la voz, son vibraciones sonoras captadas y transformadas por el micrófono del teléfono en señales eléctricas analógicas, las mismas que pueden ser afectadas fácilmente por ruidos introducidos por el entorno o los propios sistemas empleados en su transformación; mientras que las señales digitales son impulsos de tensión eléctricas, las mismas que son inmunes al ruido, ya que cualquier presencia de tensión será interpretado como un uno lógico y la ausencia de ésta como un cero lógico, quedándole la tarea a los equipos repetidores en determinar si los impulsos llegan atenuados, deformados o afectados por ruido. Por lo tanto la calidad de la transmisión digital no se ve afectada por la distancia, mientras que la analógica si, ya que existe mayor probabilidad de verse afectada por ruido, figura 2.2. (Carballar, 2007) (Cabezas, 2007)

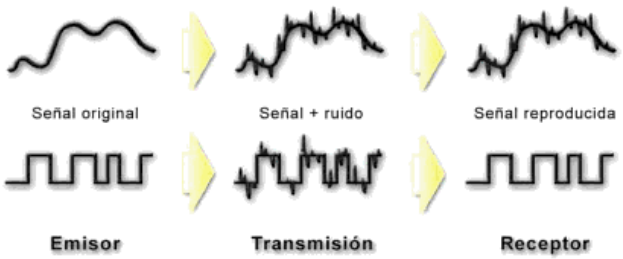


Figura 2.2 *– Principal ventaja de la tecnología digital*
Fuente*: [Carballar, 2007]*

Con la aparición de la red *Arpanet* a finales de los años sesenta, como una tecnología militar experimental, para garantizar que la información llegue a su destino aunque parte de la red estuviese destruida o interrumpida, comienza una nueva era, pasando de la conmutación por circuito a la nueva tecnología denominada conmutación por paquetes, la cual constituye la base fundamental de la telefonía *VoIP* de hoy en día. (Carballar, 2007)

En la actualidad, aún se cuenta con sistemas de comunicación híbridos, donde los puntos de distribución reciben y entregan señales análogas producto de la codificación de la voz, y los puntos de distribución se encargan de transmitir las señales convertidas a digital, como se observa en la figura 2.3, lo que puede llegar a considerarse como una desventajas en estos sistemas, ya que la conversión de señal análoga a digital, demanda de tiempo de procesamiento y por consiguiente mayor tiempo en la entrega y recepción de la señal entre el emisor y el receptor.

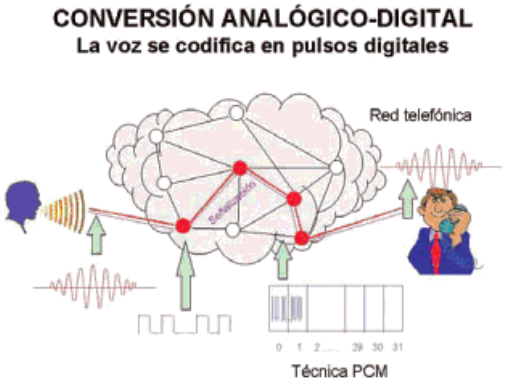


Figura 2.3 *– Sistemas analógico-Digital*
Fuente*: [Huidobro & Conesa, 2006]*

Con la aparición de los ordenadores digitales y desde hace uno años, la masificación de los dispositivos móviles, han conllevado a la tendencia actual de digitalizar los sistemas de comunicación. Entre los métodos más usados, se destaca la Modulación por Impulsos Codificados (*MIC*), la cual convierte la señal analógica en digital y la transmite por la misma línea junto al resto de señales, empleando multiplexación temporal.

El sistema digital en la telefonía, es una evolución más de los avances tecnológicos de este mundo globalizado y digitalizado, el cual, complementado con el internet, ha permitido un nuevo método de comunicación, denominado telefonía IP, o también llamada *VoIP* (Voz sobre IP), para trasmitir voz a bajo costo, aprovechando infraestructura ya existente por medio de protocolo de internet (IP), donde las *PYMES* la están incorporando en sus redes locales (*Ethernet* o *WiFi*) como sustituto del sistema tradicional de centralitas.

Este tipo de tecnología *VoIP*, cada día va ganando terreno al resto de tecnologías de comunicación, dado a que a su bajo coste y facilidad de adaptación a cualquier necesidad se va imponiendo frente a la aparente ventaja de confiabilidad ofrecida por las redes tradicionales.

Un hecho importante, que define a la tecnología *VoIP* como interesante para las *PYMES*, es que se puede aprovechar la infraestructura existente de una red *LAN MAN* o *WAN* para garantizar las *QoS* en la comunicación, y, que se puede incorporar con soluciones de tipo Software libre, las cuales disminuyen costes de implementación, y permiten la misma funcionalidad que equipos o software propietarios, garantizando así, la facilidad de adaptación, y la seguridad de la información, puesto que se conoce el código fuente de la solución.

Dentro de estas soluciones tipo Software libre, se encuentran algunas alternativas, las cuales complementadas con equipos telefónico y/o con software denominados *SoftPhone*, constituyen un conjunto de utilidades muy versátiles para ser usados por las *PYMES*.

2.4. Sistemas de Conmutación

En las redes telefónicas, unas de las principales funciones es la de conmutación, que no es más que la conexión que se realizan entre múltiples nodos existentes en diferentes puntos geográficos, para interconectar a usuarios de una red de telecomunicaciones.

A lo largo de la evolución de las redes telefónicas, encontramos tres tipos de conmutaciones: Por circuito, mensaje y por paquete.

2.4.1. Por circuito

La conmutación por circuito, según (Huidobro & Conesa, 2006), es la técnica donde el emisor y rector se comunican a través de un circuito único y especifico, el cual se establece al inicio de la misma, y liberado cuando culmina la comunicación, para quedar disponible nuevamente para otros usuarios. Este tipo de conmutación, es usada normalmente en las llamadas telefónicas, de una red telefónica pública, ilustración en la figura 2.4.

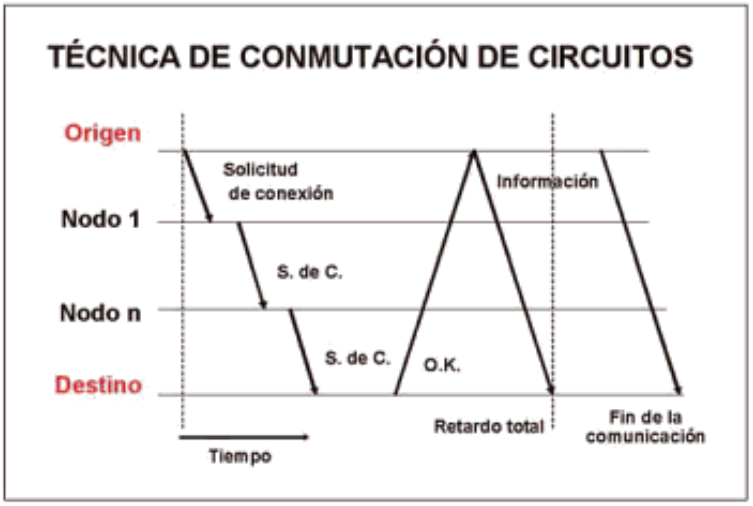


Figura 2.4 *– Conmutación por Circuito*
Fuente*: [Huidoro & Conesa, 2006]*

2.4.2. Por mensajes

Según (Tomasi, 2003), la conmutación por mensaje, es una forma de un sistema/red, donde los códigos de identificación del origen y destino, se transmiten a la red y se almacenan en una estación, estos datos no se trasfieren en tiempo real, ya que las estaciones lo harán cuando sea conveniente hacerlo, el tiempo que lleva a un mensaje pasar de una estación a otra puede ser variable, lo que implica un tiempo de retardo. Este tipo de conmutación es más eficiente que la de circuito, puesto que los mensajes que hayan llegado cuando se encuentren congestionada la red, se almacenan hasta poderlo transmitir cuando haya disminuido la carga.

2.4.3. Por paquetes

La conmutación por paquete, es un método que resuelve los inconvenientes de la conmutación por mensajes, en cuanto a la memoria necesaria para almacenar, y el tiempo de procesamiento dentro de los nodos, ya que, divide los mensajes en fragmentos pequeños denominados paquetes, con lo cual reduce significativamente el retardo acumulado dentro de la red.

Por otra parte, la conmutación por circuito sigue manteniendo una ventaja sobre la conmutación por paquete, la cual hace que sea ideal para aplicaciones en tiempo real, ya que no existen los retardos, productos del procesamiento efectuado dentro de los nodos en caso de la conmutación por mensaje o por paquete, sin embargo la conmutación por circuito tiene la desventaja, de que mientras dure la comunicación, debe bloquear todos los recursos necesarios para asegurar la transmisión. (Iñigo, Barceló, Cerdá, Peig, Abella, & Corral, 2008) .

Cuando un nodo debe enviar un paquete, debe decidir si para cada paquete escoge la ruta más adecuada, o antes de comenzar a trasmitir, define la ruta que todos los paquetes que constituyen a un mensaje, deben de seguir, de acuerdo a estas posibilidades, dan lugar a dos tipos de conmutación por paquete: Modo Datagrama, o modo Circuito Virtual.

2.4.3.1. Datagrama

La técnica del datagrama, consiste en que cada paquete que constituye un mensaje, se enrute por caminos diferentes, por consiguiente al tener tiempos de retardos variables, pueden llegar de forma desordenadas, lo que conlleva a que cada estación debe reordenarlos, empleando tiempo de procesamiento, propiciando al retardo. (Iñigo, Barceló, Cerdá, Peig, Abella, & Corral, 2008).

2.4.3.2. Circuito virtual

La técnica del Circuido virtual, consiste en decidir el camino por el cual se enrutarán todos los paquetes, antes de comenzar con la trasmisión, lo que conlleva a que la estación receptora, siempre los recibirá de forma ordenada, y los nodos no invertirán tiempo en decidir el camino que debe tomar cada paquete. En este modo, también se realizan las tres fases de la conmutación por circuitos: Establecimiento de circuito, transmisión de datos y liberación de circuito. (Iñigo, Barceló, Cerdá, Peig, Abella, & Corral, 2008).

2.4.4. Red Conmutada, punto a punto y multipunto

Una red de comunicación de acuerdo a su tamaño o complejidad, requerirá de un número determinado de nodos de conmutación y/o concentración, y de medios de trasmisión para la interconexión; cuando los equipos o terminales, se comunican siempre de la misma manera y de forma fija o permanente con otro punto, es necesario establecer un camino directo entre ellos, a esto se le denomina circuito punto a punto, pero si por lo contrario, la comunicación es esporádica, y con distintos puntos, lo que se requiere disponer son de nodos que a partir de la señalización recibida, establezca la ruta de interconexión para cada caso, entre los terminales a comunicarse. Si, una terminal requiere conectarse con múltiples puntos simultáneamente, para

compartir la misma información, se deberá establecer una conexión punto-multipunto. (Huidobro & Conesa, 2006).

2.4.5. Señalización

En las redes telefónicas, los equipos o terminales conectados, deben establecer, mantener y finalmente liberar un canal de comunicaciones, el cuales permiten a los usuarios intercambiar información, sea esta: voz, datos, textos o imágenes. Para que esto resulte, se precisa de una señalización, que no es más que el intercambio de información, relacionada con el establecimiento y control de las conexiones, la cual permite que la comunicación sea factible. (Castro & Fusario, 1999).

2.4.5.1. Funciones que cumple la Señalización

Entre las principales funciones se detallan las siguientes:

- Establecer y liberar el canal de comunicaciones
- Proporcionar información acerca del usuario final o destinatario de la llamada.
- Informar sobre el progreso de una llamada.
- Generar señales de alerta, tales como aviso de tener una llamada en espera, o de tener descolgado el microteléfono.
- Proporcionar información sobre la condición de una línea de abonado o de un circuito troncal.
- Envío de señales de congestión y ocupado.
- Asegurar la confiabilidad de las comunicaciones.
- Permitir la ejecución de funciones administrativas y de mantenimiento.

2.4.5.2. Señalización analógica

Es usada en las redes telefónicas analógicas, el objetivo de esta señalización es mantener lo más integra la señal de entrada en el receptor, su reproducción se realiza mediante una transmisión continua de estados de la señal útil. (Castro & Fusario, 1999).

2.4.5.3. Señalización digital

A diferencia de la señalización analógica, la forma de onda no desempeña un papel primordial, ya que los impulsos trasmitidos, se pueden construir a partir de la señal recibida, su reproducción se realiza mediante una trasmisión de cambios de estados discretos de la señal útil. Los distintos elementos (*hardware*) que intervienen en el establecimiento de un canal de comunicaciones, detectan estos estados significativos de corrientes. (Castro & Fusario, 1999).

2.4.5.4. Señalización CCITT 7

Con la aparición de las redes inteligentes, ha aparecido un complejo sistema de señalización por canal común, denominado CCITT7, por motivo que es el *CCITT* (*Consultative Committe International Telegraphy and Telephony*), quien definió la normativa, este tipo de señalización permite a los procesadores de control de dos centrales digitales o base de datos, comunicarse directamente e interactuar entre sí de forma óptima con medios de trasmisión digital. (Herrera, 2004).

2.4.5.5. Señalización Intercentral CCITT 7

Este sistema de canal común, optimizado para redes digitales, el cual se describe en la serie Q 700 de las recomendaciones del *CCITT*, está constituido por varias capas modulares, que cumplen funciones diferentes,

permitiendo así la transferencia de información de manera directa sobre las llamadas entre procesadores de central. (Herrera, 2004).

Soporta una amplia gama de aplicaciones y funciones administrativas, como:

- *RDSI*
- Redes inteligentes
- Servicios móviles
- Administración, operación y manejo de redes.

Entre las ventajas del *CCITT7*, se denota que cuenta con un canal común para el envío de mensaje de señalización, permitiendo ahorrar equipos en ambas centrales, dado que sólo se necesita de un emisor y un receptor en cada extremo del enlace, ésta combinación de un sólo emisor - receptor se le conoce como Terminal de señalización (TS), la cual cumple la función de logística en el procesador central del conmutador, de terminar la línea e iniciar la trasferencia de bits. (Herrera, 2004).

2.4.6. PSTN – RTC

La red telefónica, ha tomado algunos nombre en el transcurso de la evolución, inicialmente se le llamaba, red telefónica conmutada (*RTC*), luego red telefónica básica (*RTB*), red pública telefónica conmutada (*PSTN* por sus siglas en inglés *Public Switched Telephone Network*) o red telefónica conmutada general (*GSTB, General Switched Telephone Network*), y las redes que cuentan con sistemas digitales de transmisión entre centrales, se les llamó red digital integrada (*RDI*), ésta tendencia del uso de tecnología digital, llevó a la creación de la red digital de servicios integrados (*ISDN, Integrated Services Digital Network*), la cual no tan solo permite la transmisión digital entre centrales, sino que es de extremo a extremo entre las terminales, permitiendo la transmisión de

voz y datos, aprovechándosela por ejemplo en las videoconferencias. (Carballar, 2007).

2.4.7. PBX

Una *PBX* denominada inicialmente como *PABX* por sus siglas en Ingles, *Private Automatic Branch Exchange* o Central Privada Automática de Conmutación, no es más que un equipo para aplicaciones telefónicas que es controlado por un software para administrar las llamadas internas, sin necesidad de acceder a la red pública. Consta de dos unidades: La unidad de conmutación que se encarga de establecer el canal físico para la comunicación entre los usuarios, y la unidad de control que se encarga de atender la señalización entrante y saliente, procesar las señales recibidas e indicar a la unidad de conmutación qué circuitos de interconectar. (Huidobro & Conesa, 2006).

El objetivo principal de una *PBX*, es de interconectar las extensiones internas dentro de un Entidad, y a la vez permitir la interconexión con la red pública telefónica conocida como *PSTN*.

En la actualidad, la tendencia de la telefonía, es la de transmitir la voz por medio de la red internet, y en caso de la *PYMES* aprovechar sus redes *LAN, MAN o WAN*, a este tipo de tecnología se le denomina *VoIP PBX* ó *IP PBX*.

Dentro de las soluciones para *PBX*, encontramos algunas que son de tipo software, las cuales son instaladas en un computador, entre las cuales encontramos: *Software* propietario como *Axon Virtual PBX, 3CX Phone System*, etc, y *Software Open Source* como *Trixbox, Elastix*, entre otros.

2.5. Elastix

Elastix es una distribución *Open Source* basada en *Asterisk*, creada con la finalidad de establecer comunicaciones unificadas, incluye múltiples medios de

comunicación como: Servidor de Fax, Mensajería instantánea, Servidor de correos, Video Conferencia y Voz sobre IP, ilustración en la figura 2.5.

Figura 2.5 *– Servicios unificados en el Elastix*
Fuente*: [Elastix - ONLINE]*

Algunas de las características básicas de Elastix incluyen:

- Correo de Voz
- *Fax-a-email*
- Soporte para *softphones*
- Interfaz de configuración Web
- Sala de conferencias virtuales
- Grabación de llamadas
- *Least Cost Routing*
- *Roaming* de extensiones
- Interconexión entre *PBXs*
- Identificación del llamante
- *CRM*
- Reportación avanzada

Dentro de las características y funcionalidades específicas de los servicios *PBX* e *IM* tenemos:

PBX

- Grabación de llamadas
- Correo de voz
- Correo de *voz-a-Email*
- *IVR* configurable y flexible
- Soporte para sintetización de voz
- Herramienta para la creación de extensiones por lote
- Cancelador de eco integrado
- Provisionador de teléfonos vía web
- Soporte para videofonos
- Interfaz de detección de hardware
- Servidor *DHCP* para asignación dinámica de *Ips*
- Panel de operador basado en web
- Parqueo de llamadas
- Reporte de detalle de llamadas (*CDR*)
- Tarifación con reporte de consumo por destino
- Reportes de uso de canales
- Soporte para colas de llamadas
- Centro de conferencias con salas virtuales
- Soporte para protocolos *SIP* e *IAX*, entre otros
- Códecs soportados: ADPCM, G.711 (A-Law & μ-Law), G.722, G.723.1 (*pass through*), G.726, G.728, G.729, GSM, iLBC (opcional) entre otros.
- Soporte para interfaces análogas como *FXS/FXO* (*PSTN/POTS*)
- Soporte para interfaces digitales E1/T1/J1 a través de los protocolos PRI/BRI/R2
- Identificación de llamadas (*Caller ID*)
- Troncalización
- Rutas entrantes y salientes con configuración por coincidencia de patrones de marcado
- Soporte para *follow-me*
- Soporte para grupos de timbrado
- Soporte para *paging* e *intercom*

- Soporte para condiciones de tiempo
- Soporte para PINes de seguridad
- Soporte para *DISA* (Direct Inward System Access)
- Soporte para *Callback*
- Soporte para interfaces tipo *bluetooth* a través de teléfonos celulares (*chan_mobile*)

Mensajería Instantánea

- Servidor de mensajería instantánea basado en *OpenFire*
- Inicio de llamadas desde cliente de mensajería
- Servidor de mensajería es configurable desde web
- Soporta grupos de usuarios
- Soporta conexión a otras redes de mensajería como *MSN, Yahoo Messenger, GTalk, ICQ.*
- Reporte de sesiones de usuarios
- Soporte *Jabber*
- Soporte de *Plugins*
- Soporte *LDAP*
- Soporta conexiones *server-to-server* para compartir usuarios

(Elastix Freedom Communicate)

2.6. Telefonía IP

La telefonía IP, también llamada voz sobre banda ancha (*VoBB, voice over broad band*), voz sobre IP (*VoIP, voice over IP*), no es más que la tecnología de servicios que transmiten voz, aprovechando la red internet.

El término IP, hace referencia al protocolo de internet, el cual también es utilizado en las redes locales de datos, donde las PYMES están optando pasar voz sobre IP, aprovechando su infraestructura de red, como alternativa a las tradicionales centrales telefónicas.

La telefonía IP, en conjunto con las tecnologías inalámbricas, como *Wi-Fi*, están permitiendo la movilidad, característica que es propia de la telefonía móvil.

(Carballar, 2007)

2.6.1. Principales ventajas de la Telefonía IP

- Esta tecnología permite la trasmisión de voz, videos, datos, por el mismo medio.

- La telefonía IP, cuenta con equipos de inferior costes que los que se usan en la telefonía tradicional, ya que los equipos utilizados en esta tecnología, están completamente estandarizado, por lo que el reemplazo de un equipo es de mucha facilidad, dado que se puede usar de cualquier otro fabricante.

- Los precios del equipamiento de las redes IP, bajan a un ritmo acelerado, debido a que su uso es cada vez mayor, en comparación con la telefonía tradicional.

- Esta tecnología es muy flexible, puesto que se puede introducir una nueva funcionalidad en internet en cuestión de meses, lo que en el mundo de la telefonía tradicional llevaría algunos años.

- La telefonía IP, cuenta con una mejor utilización de los recursos, puesto que en las redes IP se liberan los recursos cuando no hay información transmitiéndose, a diferencia de la telefonía tradicional que en su técnica de conmutación por circuito, tiene un canal establecido durante todo el tiempo de la comunicación, sea que se transmita o no información.

- Entre las características principales que ofrece la telefonía IP, está la movilidad, la cual a diferencia de la telefonía tradicional, el usuario no está ligado a un punto físico, incluso, este tipo de movilidad tiene ventaja sobre la telefonía móvil, ya que si el teléfono celular se queda sin batería, no podrá establecer una comunicación, mientras que en la telefonía IP, puede desde

cualquier equipo (Portatil, *PDA*, *Tablet*, *Smart Phone*), conectarse a este servicio con su nombre de usuario y clave.

(Elastix Freedom Communicate)

2.6.2. Problemas en el desempeño en la Telefonía IP

Mal se podría llegar a pensar que la telefonía IP tiene todas las ventajas sobre las otras tecnologías de comunicación, sin embargo, existen problemas de rendimiento, principalmente sobre el internet, donde se derivan inconvenientes en la conmutación de paquetes, estos paquetes al compartir la cola de flujo de los *routers*, la interfaz de los *switch*, y el ancho de banda (que en muchos casos es limitada), resultan varios problemas técnicos de rendimientos como: Latencia, Pérdida de Paquetes, y *Jitter*. (Ganguly & Bhatnagarm, 2008).

2.6.2.1. Latencia

La latencia es el retardo total desde que un paquete sale del origen hasta que llega a su destino, uno de los factores con mayor incidencia es el del límite físico impuesto por la velocidad de la luz (o una onda electromagnética, en función de la portadora), otro factor incidente es el retardo de los flujos de cola en los *routers*, y por último, debido al limitado ancho de banda del enlace por donde se transmitirá el paquete. Es por esto que entre mayor sea el camino, el número de *routers* por donde pasa un paquete, y cuanto más tardía por la congestión del tráfico en el enlace, mayor será el valor total del retardo o latencia. (Ganguly & Bhatnagarm, 2008).

2.6.2.2. Pérdida de Paquetes

A diferencia de la conmutación de circuito, en la conmutación de paquete si existe la posibilidad de pérdida de paquetes, debido a que, si el *buffer* en la interfaz de salida de un *router* se llena, el próximo paquete que

llegue a la cola se perderá, por cuanto no existe más memoria para alojarlo, para evitar tal situación, se debe complementar con protocolos como el *TCP*, donde se hace verificación y se retrasmite en caso de que un paquete se pierda, lo cual puede significar mayor tiempo de latencia. (Ganguly & Bhatnagarm, 2008).

2.6.2.3. Jitter

El *Jiffer* es la variabilidad de tiempo (latencia), durante el envío de paquetes de un extremo a otro, esto se da, debido a la escasa probabilidad que todos los paquetes sigan la misma ruta, por lo que cada paquete llegará o muy pronto o muy tarde, dependiendo por lo *routers* que hayan pasado en el transcurso del camino. Este efecto puede reducirse con un *buffer* de *jitter*, pero eso acarrea mayor tiempo de ejecución y procesamiento. (Ganguly & Bhatnagarm, 2008).

2.7. VoIP

Voz sobre IP (*VoIP*), no es más que el estándar para transmitir voz sobre protocolo IP, dado al hecho que las redes IP fueron creadas inicialmente para transmitir datos, la tecnología ha tenido que evolucionar (sobre todo en la *QoS*) para lograr la transmisión de la voz por este mismo medio.

Para lograr la trasmisión de la voz sobre IP, se tuvo que lidiar primero con el mecanismo de la digitalización de la voz (la cual por naturaleza es analógica), mediante un proceso denominado muestreo (tomar muestra a intervalos de tiempo regulares de la amplitud de la señal analógica y transformarla en información digital 1s y 0s), gracias a Henry Nyquist en 1928 (ingeniero suizo que trabajaba en AT&T), se logró conocer cuál era el mínimo número de muestras para poder reconstruir una onda a su forma original, quien definió que la frecuencia de muestreo debe ser como mínimo el doble del ancho de banda ($f_m >= 2\ BW_s$), por lo tanto si el rango de frecuencia para una voz humana entendible es entre 400Hz a 4kHz, según el

teorema de Nyquist se debería muestrear a 8kHz (el doble de la frecuencia mayor). (Landivar, 2011).

2.7.1. Calidad de Servicio (QoS)

Cuando se habla de calidad de servicio (QoS), nos referimos a que el tiempo que le lleva a un paquete llegar a su destino, no se vea afectados por retrasos o perdidas.

Esta percepción que tiene el usuario final, en cuanto a la calidad de servicio, varía de acuerdo al tipo de aplicaciones, por ejemplo el correo electrónico, páginas web, o transferencia de archivos, no son sensibles al retardo o fluctuaciones de retardo, como lo son las aplicaciones que procesan voz y video, dentro de las causas más comunes que afectan a la calidad de la voz tenemos:

2.7.1.1. Eco

EL eco se produce cuando una parte de la señal de ida se refleja en la señal de vuelta, una de entre las causas comunes es cuando en la línea analógica se produce una combinación de señales, en el convertidor hibrido (de 24 hilos), más aun si la impedancia de la línea telefónica varía mucho. Otra causa de eco, es la naturaleza acústica, producido cuando la señal de sonido es retroalimentadas desde el micrófono al audífono. (Landivar, 2011).

2.7.1.2. Bajo nivel de volumen

Cuando la infraestructura de las redes telefónicas es de baja calidad, el volumen de la conversación se ve afectada, ya que las señales se atenúan significativamente, a tal punto que no se pueden detectar los tonos del *DTMFs*. (Landivar, 2011).

2.7.1.3. Retardo de voz

El retardo de la voz, es un problema inherente a la infraestructura de red, donde la voz experimenta retardos al pasar por la red y llegar al destino. Usualmente el retardo es menor a un segundo, si está por debajo de los 200 ms pasa desapercibido, pero si es mayor a 500 ms entonces la comunicación tiende a interrumpirse y la comunicación se traslape. (Landivar, 2011).

2.7.1.4. Distorsión de Voz

La distorsión de la voz se da usualmente cuando al usar un códec, para optimizar el uso del ancho de banda, se experimenta problemas de conectividad que generan perdida de información, y propician la distorsión, un ejemplo común es el de la voz robotizada. (Landivar, 2011).

2.7.1.5. Comunicación entrecortada

La comunicación entrecortada, se da principalmente por latencias elevadas, *jitter* elevados, o un ancho de banda limitado, dando lugar a la pérdida de paquetes, usualmente las causas se origina en la red y en último de los casos en el servidor *PBX* (cuando los recursos de memoria y/o *CPU* se encuentran muy elevados). (Landivar, 2011).

2.7.2. Protocolos VoIP

En la transmisión de *VoIP*, se involucran un sinnúmero de protocolos, clasificados en tres grupos: protocolos de señalización, de transporte de voz y de plataforma IP.

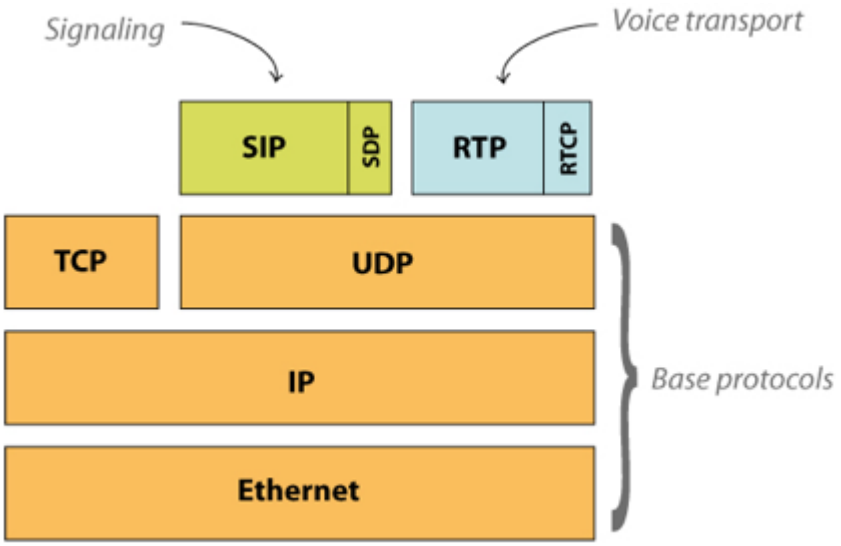


Figura 2.6 *– Protocolos usados en VoIP (con SIP o IAX)*
Fuente: *[Landivar, 2011]*

En la figura anterior se observa el esquema de protocolos utilizados por *VoIP*, y en el caso de *SIP* que soporta tanto *UDP* como *TCP* sólo lo vemos sobre *UDP*, debido a que en *Asterisk* la implementación de *SIP* solo está disponible para *UDP*. (Landivar, 2011).

2.7.2.1. De Señalización

Estos protocoles los encontramos en la capa de sesión (capa 5) del modelo *OSI*, y cumplen tareas de establecimiento de sesión, control del progreso de la llamada, entre otras cosas, entre esos protocolos encontramos:

- SIP
- IAX
- H.323
- MGCP
- SCCP

2.7.2.2. De transporte de voz

La función de este protocolo es de transportar la voz con el menor retraso posible (comúnmente denominados carga útil), luego que el protocolo de señalización haya establecido la llamada entre los usuarios, recibe el nombre de *RTP* (*Real-time Transport Protocol*).

2.7.2.3. De Plataforma IP

Estos protocolos son los usados básicamente en las redes *IP*, podemos mencionar entonces a *Ethernet*, *IP*, *TCP* y *UDP*.

2.7.3. Tipos de Protocolos de Señalización Digital

La información de estado del canal de transmisión (como desconectado, timbrando, respondido), información de control y otra información como *DTMFs*, *caller ID*, entre otros, son trasmitidos por medio de los protocolos de señalización, los cuales están clasificados en dos tipos, los llamados Señalización Asociada al Canal (*CAS*), y Señalización de Canal Común (*CCS*). (Landivar, 2011).

2.7.3.1. Señalización Asociada al Canal (CAS)

Estos tipos de protocolos *CAS*, trasmiten la señalización por el mismo canal en que viaja la información, el más conocido es el *robbed-bit*, usado en circuitos T1 y E1, el cual reemplaza el octavo bit de cada canal de comunicación cada seis *frames* y lo reemplaza por información de señalización. Otro protocolo *CAS* poco usado en nuestros días es el R2. (Landivar, 2011).

2.7.3.2. Señalización de Canal Común (CCS)

Estos tipos de protocolos *CCS*, transmiten la señalización y la información, por canales separados, un ejemplo de este protocolo es el *ISDN*, cuyo objetivo fue de facilitar las conexiones digitales para poder ofrecer una amplia gama de servicios integrados, por medio de dos tipos de interfaces denominados *BRI (Basic Rate Interface)* y *PRI (Primary Rate Interface)*, el primero usado popularmente en hogares, y el segundo para usuarios de mayor envergadura como negocios o empresas. (Landivar, 2011).

2.7.4. Protocolo SIP

SIP (Session Initiation Protocol), es un protocolo de señalización peer-to-peer que se encarga de establecer, modificar y finalizar una llamada mediante texto con mensajes de comunicación sencillos, creado con el objetivo de administrar sesiones multimedia entre dos o más partes, usando dos protocolos: *RTP* transmite la voz y el video y *SDP* negociar las capacidades de los *endpoints*, para cumplir con su función emplea métodos (mecanismo empleado para convenir una acción) y respuesta (contiene la respuestas de un método). (Landivar, 2011).

Métodos:

Método	Descripción
INVITE	Invita a un usuario a una llamada
ACK	Abreviación de *acknowledgement* (acuse de recibo) enviada para indicar que se ha recibido un mensaje
BYE	Termina una conexión entre usuarios o rechaza una llamada
CANCEL	Termina el requerimiento o búsqueda de un usuario
OPTIONS	Solicita información acerca de las capacidades del servidor *SIP*
REGISTER	Registra la ubicación de un usuario
INFO	Intercambia información de señalización en el transcurso de la sesión

Respuestas:

- *1xx Informational (e.g. 100 Trying, 180 Ringing)*
- *2xx Successful (e.g. 200 OK, 202 Accepted)*
- *3xx Redirection (e.g. 302 Moved Temporarily)*
- *4xx Request Failure (e.g. 401 Unauthorized, 404 Not Found, 482 Loop Detected)*
- *5xx Server Failure (e.g. 501 Not Implemented)*
- *6xx Global Failure (e.g. 603 Decline)*

Las fases para una llamada *SIP* son la registración y la sesión, la siguiente gráfica, ilustra de una forma simplificada la registración de un *endpoint SIP* en un servidor *SIP*.

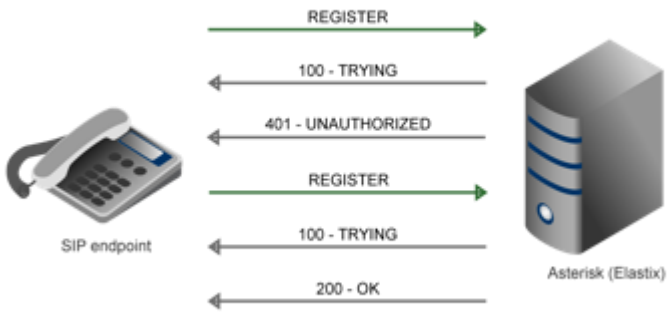


Figura 2.7 *– Registración SIP*
Fuente: *[Landivar, 2011]*

Posterior al registro, se inicia con la llamada telefónica, o comunicación entre *endpoints SIP*, la cual se ilustra en la siguiente gráfica, donde el autor de la fuente ha omitido los mensajes ACKs para mejorar la legibilidad.

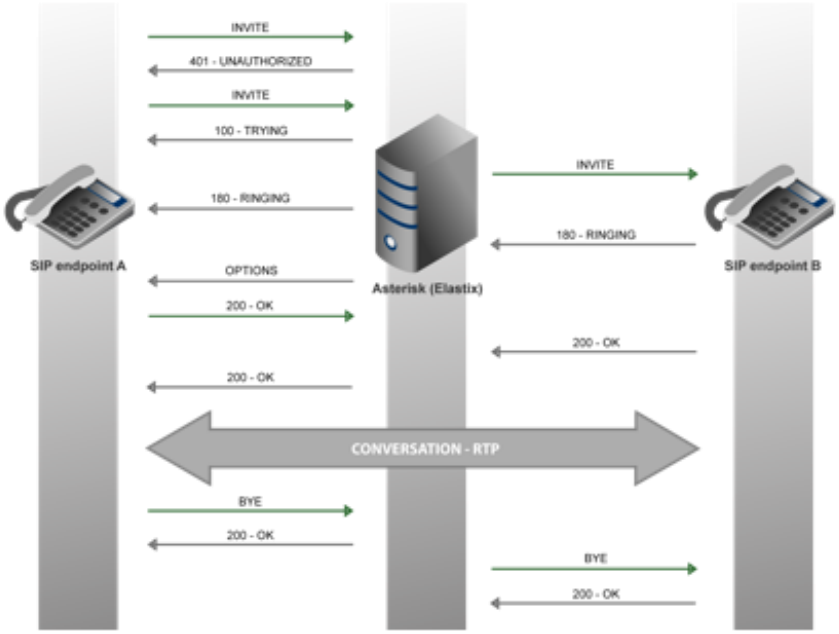


Figura 2.8 *– Sesión SIP entre dos teléfonos*
Fuente: *[Landivar, 2011]*

2.7.5. Protocolo IAX

IAX (*Inter-Asterisk eXchange*), es un protocolo de señalización que aún no está estandarizado por la IETF, pero se encuentra en proceso, creado por *Mark Spenser* (Creador de *Asterisk*), con el objetivo de solucionar los problemas existentes con los otros protocolos, dentro de las ventajas evidente frente al *SIP* tenemos que consume menos ancho de banda por cuanto es un protocolo binario a diferencia del *SIP* basado en texto, y soluciona mejor los problemas de *NAT* y *firewalls* ya que usa un solo puerto (4569) por donde transmite en *UDP* tanto la señalización como la voz, a diferencia del *SIP* que usa puertos separados (5060 para la señalización y pares de puertos entre el 10000 y 20000 para la voz). (Landivar, 2011).

IAX, emplea tres fases para una llamada, establecimiento de la llamada, llamada en curso, y colgado. La siguiente grafica ilustra el proceso de establecimiento entre dos equipos (A y B) los cuales representan a dos teléfonos o terminales.

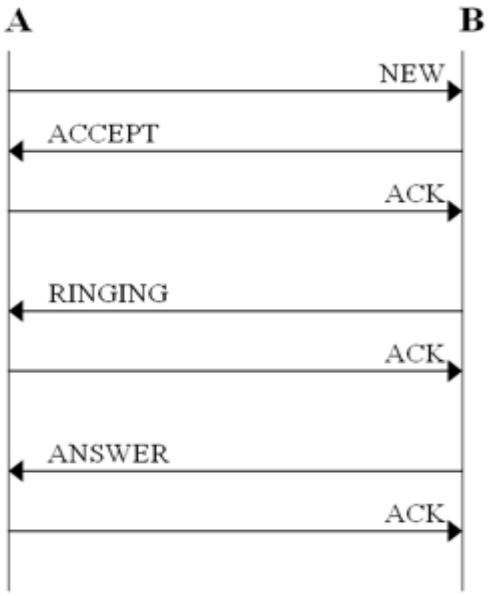


Figura 2.9 *– Establecimiento de una llamada IAX*
Fuente: *[Landivar, 2011]*

Una vez establecida la llamada, se inicia el intercambio de audio mediante unos paquetes llamada *frames*, enviados dentro del mismo flujo de comunicación que la señalización inicia.

Y por último el colgado, donde cualquier equipo puede enviar un mensaje *HANGUP* para finalizar la llamada.

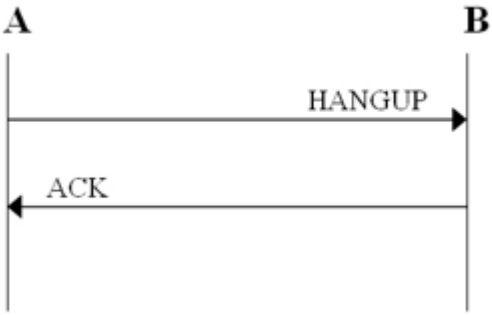


Figura 2.10 *– Colgado de una llamada IAX*
Fuente: *[Landivar, 2011]*

3. Capítulo III: Estudio de implementación de PBX VoIP y Servidor IM

3.1. Análisis de tráfico

Para el cálculo de tráfico, se tomó como muestra los registros de llamadas realizadas durante un mes en uno de los edificios (edificio matriz), de cuyos datos se distinguen, las llamadas establecidas con éxito y las que fueron negadas por encontrarse ocupada la única línea fija que dispone el edificio.

Como se observa en la gráfica 3.1, las horas pico en que se realizan mayor número de llamadas, son durante, las 8, seguido de las 10, 11 y 14 horas.

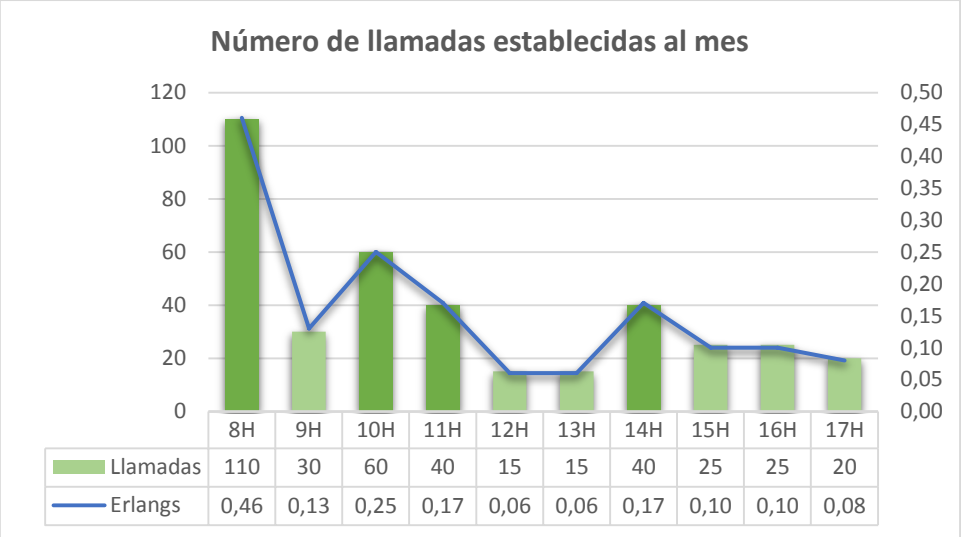


Figura 3.1 *– Estadística de llamadas establecidas*
Fuente: *[el Autor]*

Para determinar la intensidad de tráfico telefónico, generado en esta hora pico (8H), se debe emplear la siguiente fórmula: $it = vt / to$.

Donde ***vt*** corresponde al volumen de tráfico telefónico, en este caso 110 llamadas establecidas, por 5 min que es el promedio de tiempo empleado durante las llamadas, temporizador que está establecido en las centralillas telefónicas existente en la empresa.

Y, ***to*** representa al tiempo observado, para este caso los 20 días laborables del mes, por los 60 min comprendidos en la hora pico tomada como muestra.

Por lo tanto se tiene:

$$\boldsymbol{it = (110*5) / (20*60) = 550 /1200 = 0{,}46\ erlangs}.$$

Este resultado indica que la línea telefónica fija, se está utilizando por debajo del 50% de la disponibilidad, entre las 8:00 a las 8:59, lo cual conlleva a analizar por qué existe una considerable probabilidad de bloqueo, o negación de llamadas como se observa en la siguiente gráfica.

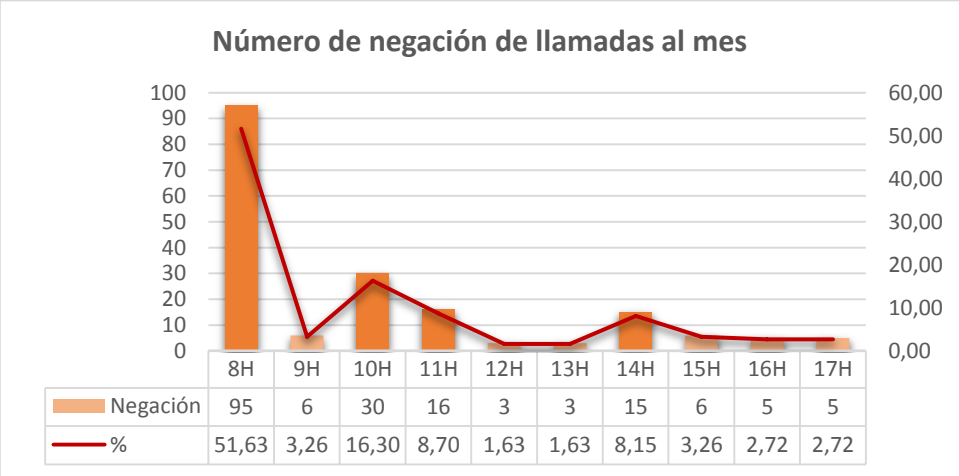


Figura 3.2 *– Estadística de llamadas negadas*
Fuente: *[el Autor]*

La probabilidad de bloqueo, está directamente relacionada con las horas picos, donde a mayor número de llamadas durante una hora, mayor es la probabilidad de bloqueo o negación del servicio, esto se debe a que el uso de la única línea fija en llamadas externas y/o internas, tiende a 1 Erlang.

Sin embardo, en el cálculo de la intensidad de tráfico, el resultado obtenido es un poco menor al 50%, lo que nos demuestra que la probabilidad de bloqueo considerable (figura 3.3), no se da porque la disponibilidad de la línea telefónica fija pasa ocupada casi toda la hora, sino que durante el tiempo de uso, mientras está establecida una llamada, existe entre un 80% a un 90% de probabilidad que otra llamada se trate de establecer, y al estar ocupado el circuito, ésta se niega.

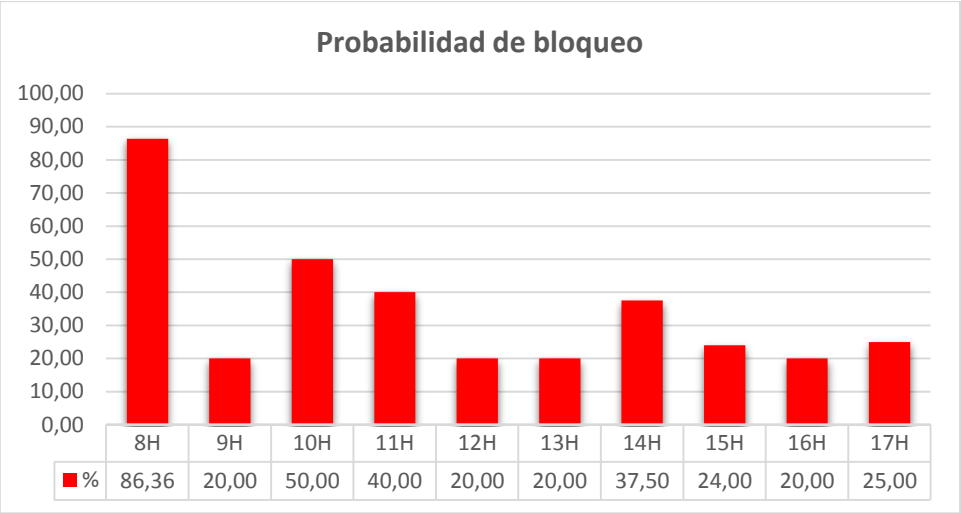


Figura 3.3 *– Estadística de probabilidad de bloqueo*
Fuente: *[el Autor]*

Por lo tanto, la disponibilidad de mayor grado de servicio (*GOS*) de la línea fija, se da durante las 9, 12, 13, 15, 16 y 17 horas, de las cuales, si descontamos una hora correspondiente a las del almuerzo, entonces, en un día laborable, tenemos un 50% de *GOS* versus a un 50% en que la probabilidad de bloqueo sea mayor, como se refleja en la figura 3.4.

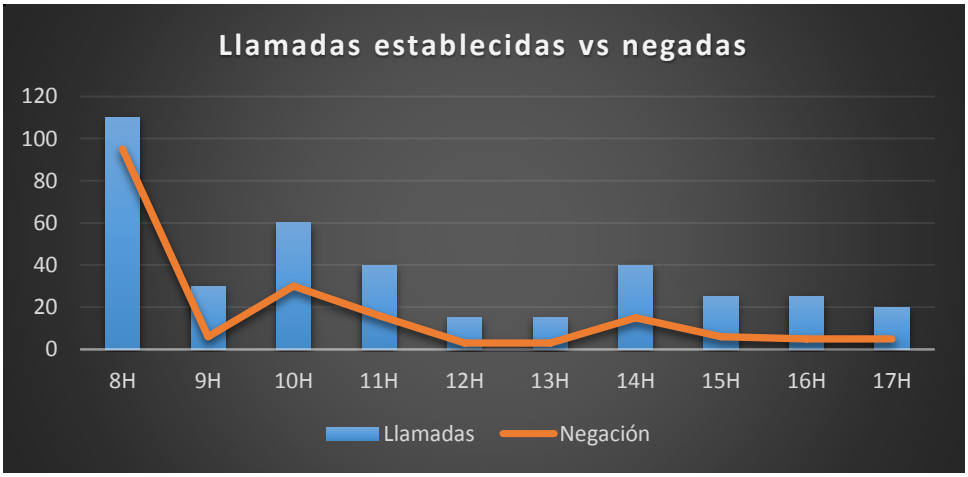


Figura 3.4 *– Comparativa, llamadas establecidas vs llamadas negadas*
Fuente: *[el Autor]*

LLAMADAS	TOTAL	%
Externas	150	39,47
Internas en mismo edificio	50	13,16
Internas entre edificios	180	47,37
	380	100,00

Tabla 3.1 *– Resumen de tipos de llamadas*
Fuente: *[el Autor]*

Como se observa en la Tablas 3.1, los porcentajes mayores, correspondiente al uso de recurso de la línea telefónica fija, está en las llamadas externas (siendo ésta la principal función y la razón de la existencia de una línea telefónica fija), y las locales entre edificios (matriz y central), lo cual denota que si el 47,37% de tráfico de llamadas, se la canaliza por la red interna (*VoIP*) al igual que el 13,16% de las llamadas internas propiamente (las cuales no utilizarían recurso de la línea fija), se tendría el 100% de *GOS* para las llamadas externas, lo cual conlleva a la disminución, de la probabilidad de bloqueo o negación del servicio para este tipo de llamadas.

3.2. Análisis de ancho de banda

Para determinar el ancho de banda necesario (refiriéndonos al máximo de tráfico que puede transitar por un medio de comunicación), de acuerdo al volumen de llamadas que se realizan, partimos del cálculo de Kbps que se requieren en el *Overhead* de cada empaquetado.

Dado que un paquete *VoIP*, incluye bytes para el encabezado Ethernet, *IP*, *UDP y RTP*, a parte del audio codificado, hay que determinar primero, cual es el consumo total del encabezado, para luego realizar un análisis, de acuerdo a los distintos códec de audio.

Para efectuar dicho cálculo y determinar la velocidad de transmisión por cada tamaño de paquetización (*head*), se debe emplear la siguiente fórmula:

$$Vtx = \left(\frac{Total\ Packet\ Size[Bytes] \times 8\ [Bits]}{1000}\right) \times Packet\ Rate[pps]$$

Dónde:

***Vtx*:** es la velocidad de transmisión

Total *Packet Size*: Corresponde al tamaño total del paquete en bytes, es decir la sumatoria del tamaño del paquete de voz (*VoipPacketSize*) con todas las cabeceras (*ETH*, *IP*, *UDP*, *RTP*).

***Packet Rate*:** Es la velocidad del paquete (se mide en pps, paquetes por segundo) y es derivada a partir del periodo de paquetización (puede calcularse también como la inversa del periodo de paquetización).

***Packetization Size*:** También conocido como *Payload Size*, depende del periodo de paquetización y del códec a utilizar.

En este caso se utilizará la fórmula, para el cálculo del *Vtx* por cada encabezado:

- Ethernet: 38 bytes Vtx = (38 x 8 /1000) x 50 = 15.2 Kbps
- IP: 20 bytes Vtx = (20 x 8 /1000) x 50 = 8 Kbps
- UDP: 8 bytes Vtx = (8 x 8 /1000) x 50 = 3.2 Kbps
- RTP: 12 bytes Vtx = (12 x 8 /1000) x 50 = 4.8 Kbps

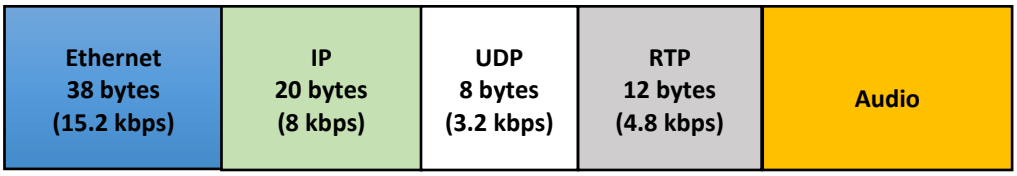


Figura 3.5 *– Esquema de un Overhead (31.2 kbps) sin incluir audio*
Fuente: *[el Autor]*

Una vez que se tiene determinado el total de paquetización (*Overhead*), figura 3.5, se debe sumar con el tamaño base del códec que se seleccione; para obtener el tamaño total del paquete *VoIP*, se realizará un análisis con 4 tipos de códec, cuya calidad va desde muy buena a una calidad promedio.

En el caso del G711 y G722, tienen un tamaño base de 64 Kbps, más, los 31.2 Kbps del *Overhead*, da un total de 95.2 Kbps, siendo el segundo un códec que da mejor calidad de audio y requiere de poco recurso de CPU a la hora de procesarse.

Para los casos en que se quiera compensar la disponibilidad de un limitado ancho de banda, con un buen performance de recursos de CPU, se puede usar los códec, GSM o G729, cuyos tamaños totales de los paquetes son de 44.2 y 39.2 Kbps

respectivamente (detallado en la tabla 3.2), siendo el segundo el ideal, para casos en que se dispone de un ancho de banda limitado.

Códec	Calidad Audio	Recursos CPU	Tamaño Base	Tamaño Total (Base + Carga)
G711	Buena	Muy pocos	64 kbps	95.2 kbps
G722	Muy Buena	Pocos	64 kbps	95.2 kbps
GSM	Aceptable	Promedio	13 kbps	44.2 kbps
G729	Promedio	Altos	8 kbps	39.2 kbps

Tabla 3.2 *– Listado de tamaño base y total por Códec*
Fuente: *[el Autor]*

Sin embargo, con la finalidad de determinar el verdadero ancho de banda requerido para las llamadas telefónicas generadas por una *PBX VoIP* de tipo *Software*, el *Overhead* (31.2 kbps) debe ser considerado como el doble, ya que estos utilizan doble canal de transmisión, por consiguiente los paquetes por segundos (PPS) no son 50 sino 100.

- Ethernet: 38 bytes Vtx = (38 x 8 /1000) x 100 = 30.4 Kbps
- IP: 20 bytes Vtx = (20 x 8 /1000) x 100 = 16 Kbps
- UDP: 8 bytes Vtx = (8 x 8 /1000) x 100 = 6.4 Kbps
- RTP: 12 bytes Vtx = (12 x 8 /1000) x 100 = 9.6 Kbps

Dando un total de 62.4 Kbps, al cual se le debe sumar el tamaño base del códec seleccionado tal y como se detalla en la tabla 3.3, para tener el valor real de carga que genera una llamada desde una *PBX* de tipo Software.

Códec	Calidad Audio	Recursos CPU	Tamaño Base a doble canal	Tamaño Total (Base + Carga)
G711	Buena	Muy pocos	128 kbps	190.4 kbps
G722	Muy Buena	Pocos	128 kbps	190.4 kbps
GSM	Aceptable	Promedio	26 kbps	88.4 kbps
G729	Promedio	Altos	16 kbps	78.4 kbps

Tabla 3.3 *– Listado de tamaño base y total por Códec para PBX de tipo Software*
Fuente: *[el Autor]*

Tomando de referencia el tamaño total de la *tabla 3.3*, se puede determinar, la equivalencia en cuanto a consumo de llamadas simultáneas, por cada tipo de códec (tabla 3.4), que podría efectuarse de acuerdo a la disponibilidad de ancho de banda.

Códec	Número de llamadas Simultaneas							
	1	2	3	4	6	7	8	9
G711 (Kbps)	190,4	380,8	571,2	761,6				
G722 (Kbps)	190,4	380,8	571,2	761,6				
GSM (Kbps)	88,4	176,8	265,2	353,6	530,4	618,8	707,2	
G729 (Kbps)	78,4	156,8	235,2	313,6	470,4	548,8	627,2	705,6

Llamadas máxima simultaneas aceptable en horas pico

Llamadas simultaneas, con poca probabilidad de perdida de paquetes en horas pico

Llamadas simultaneas, con alta probabilidad de perdida de paquetes en horas pico

Tabla 3.4 *– Consumo en Kbps, dependiendo del número de llamadas simultaneas*
Fuente: *[el Autor]*

En la mayoría de las PBX existe la posibilidad de habilitar el método de supresión de silencios, el cual consiste en ahorrar transmisión de paquetes que no contengan sonidos, lo cuales se generan durante la ausencia de voz en una conversación. Esta habilitación de supresión de sonido puede ahorrar en un 50% el consumo de ancho de banda, dando la posibilidad de realizar más llamadas simultaneas, como se observa en el detalle de la tabla 3.5.

Códec	Número de llamadas Simultaneas							
	1	6	7	8	13	15	17	19
G711 (Kbps)	95,2	571,2	666,4	761,6				
G722 (Kbps)	95,2	571,2	666,4	761,6				
GSM (Kbps)	44,2	265,2	309,4	353,6	574,6	663,0	751,4	
G729 (Kbps)	39,2	235,2	274,4	313,6	509,6	588,0	666,4	744,8

Llamadas máxima simultaneas aceptable en horas pico

Llamadas simultaneas, con poca probabilidad de perdida de paquetes en horas pico

Llamadas simultaneas, con alta probabilidad de perdida de paquetes en horas pico

Tabla 3.5 *– Consumo en Kbps, de llamadas simultánea con supresión de silencios*
Fuente: *[el Autor]*

4. Capítulo IV: Aplicación de resultados

4.1. Análisis Cuantitativo

Para realizar el siguiente análisis de tráfico, se realizó muestreo del flujo de datos generado durante un día laborable tomado con *IPTraf*, transmitido por el túnel de datos que interconecta el edificio Central con el Matriz, el cual incluye paquetes de:

- Los 5 aplicativos de la empresa
- Correo corporativo (Zimbra)
- Navegación internet (limitada por usuario)
- Aplicativos de monitoreo y soporte implementado por el DSI (Dpto. Servicios Informáticos)

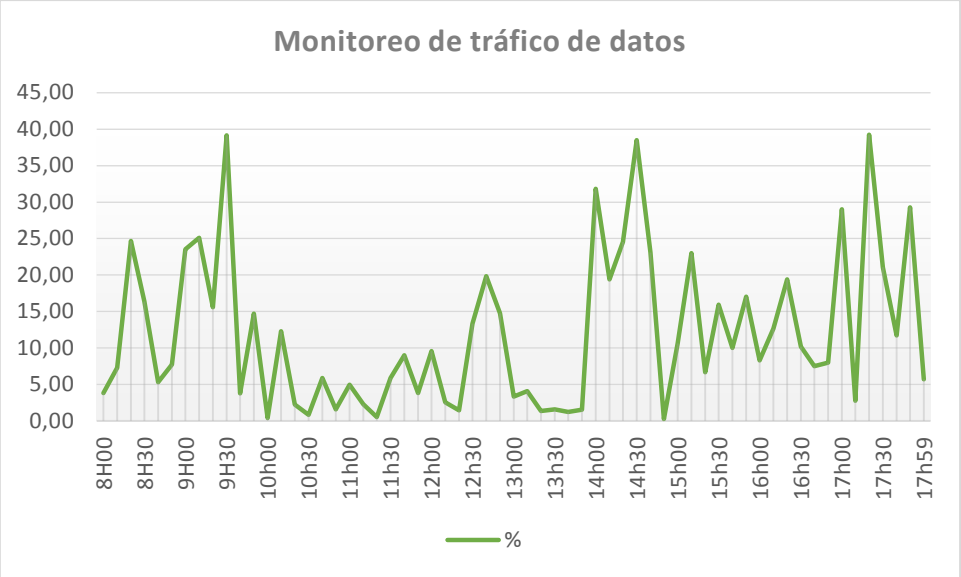


Figura 4.1 *– Monitoreo de tráfico de red, muestreo de un día laborable*
Fuente: *[el Autor]*

De acuerdo al análisis de tráfico generado en la red, se observa en la figura 4.1 que el consumo mayor del ancho de banda del túnel de datos está por debajo del 40%, lo cual deja una disponibilidad neta de trasmitir 600 Kbps, para usarlo con llamadas VoIP.

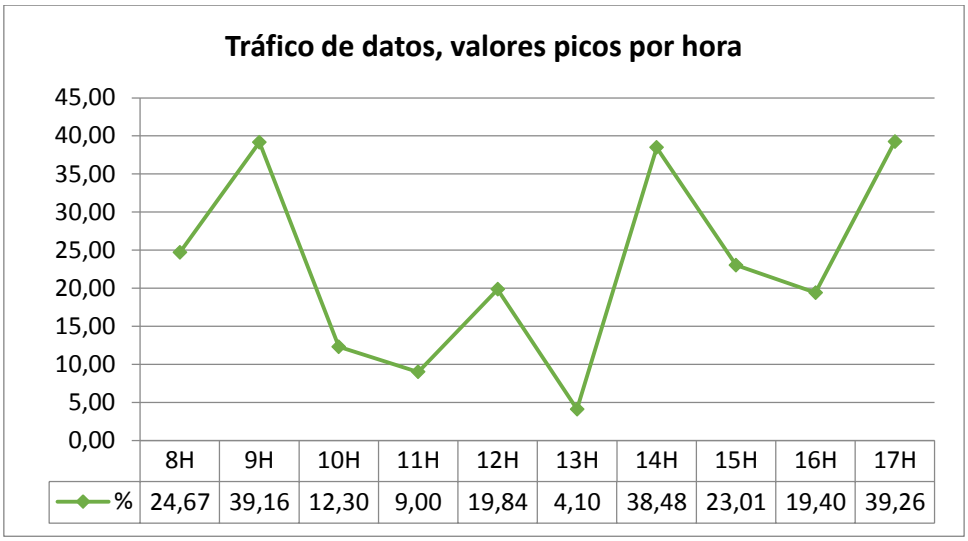


Figura 4.2 *– Gráfica de valores picos por hora, del tráfico de red*
Fuente: *[el Autor]*

Al graficar los picos más alto de consumos por hora, se observa que durante las 9, 14 y 17 horas, existe una demanda mayor en el ancho de banda, el cual tiende al 40%, si se promedia estos consumos picos (representados en porcentaje de acuerdo al ancho de banda máximo), se concluye que, el 22,92% de la disponibilidad del ancho de banda constituye el consumo promedio (cp), quedando la diferencia (77,08%) para poder ser aprovechado por *VoIP*.

Cálculo:

Cp = (24,67+39,16+12,30+9,00+19,84+4,10+38,48+23,01+19,40+39,26) / 10

Cp = 229,22 / 10 = 22,92%

Representado esto en Erlangs

it = 22,92% consumo promedio / 100% disponibilidad de enlace = 0,22 erlangs

Lo que demuestra, que se tiene una disponibilidad neta del 60% del ancho de banda del túnel de datos, y un 17,08% de holgura adicional, la cual se puede aprovechar en caso de horarios no pico.

Para las pruebas de laboratorio que se realizaron, se implementó dos máquinas virtuales (con *VirtualBox*), donde se instaló la versión de *Elastix* 2.4, seleccionando el códec G711 de los 4 analizados, por motivo que *Elastix*, utiliza por default el códec G711, de tipo U-Law, el cual emplea un sistema de cuantificación logarítmica que utiliza un método de compresión antes de codificar la señal, generando paquetes de 84 Kbps.

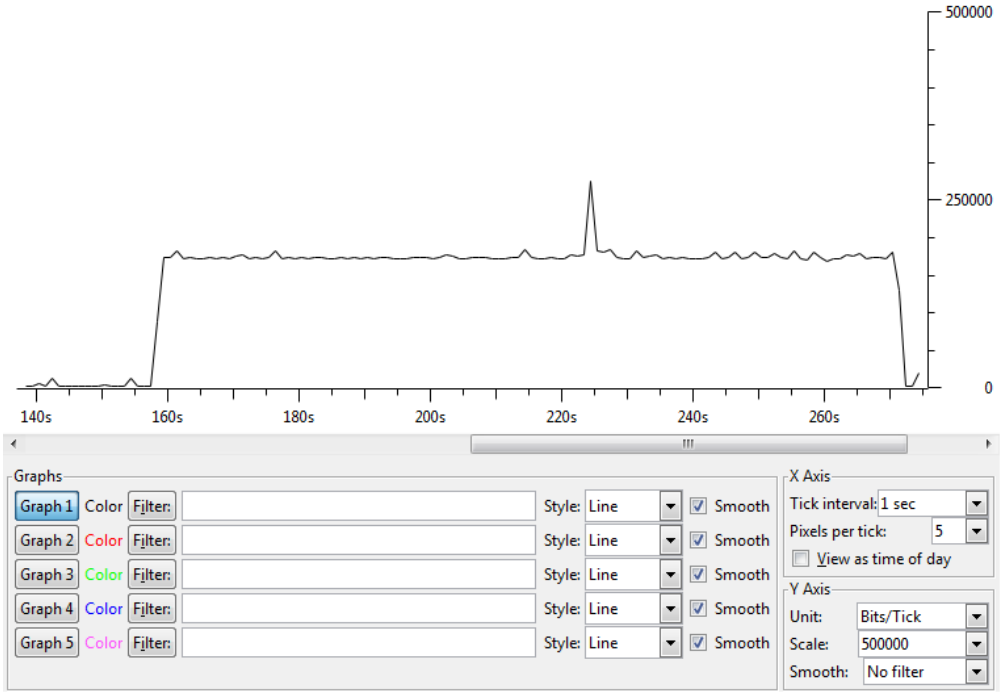


Figura 4.3 *– Gráfica de tráfico, generada por una llamada SIP - Wireshark*
Fuente: *[el Autor]*

Para la prueba de monitoreo del consumo de ancho de banda, generado por una llamada *SIP*, se empleó la herramienta *Wireshark*, dentro de un entorno mixto (infraestructura real con servidores virtualizados), tomando la muestra en horario no laborable para distinguir la gráfica correctamente; como se observa en la figura 4.3, al inicio se observa un consumo mínimo, que corresponde a datos (aproximadamente unos 10 Kbps), y durante la llamada, el consumo asciende a los 178000 bps o 178 Kbps, si se toma como referencia que un paquete *VoIP* con *códec* G711 u-law genera un consumo de 84 Kbps, y *Elastix* trabaja a doble canal, el consumo real es de 168 Kbps, lo cual concuerda con la gráfica, que muestra un consumo de 178 Kbps menos los 10 Kbps de datos que existió durante el tiempo de monitoreo.

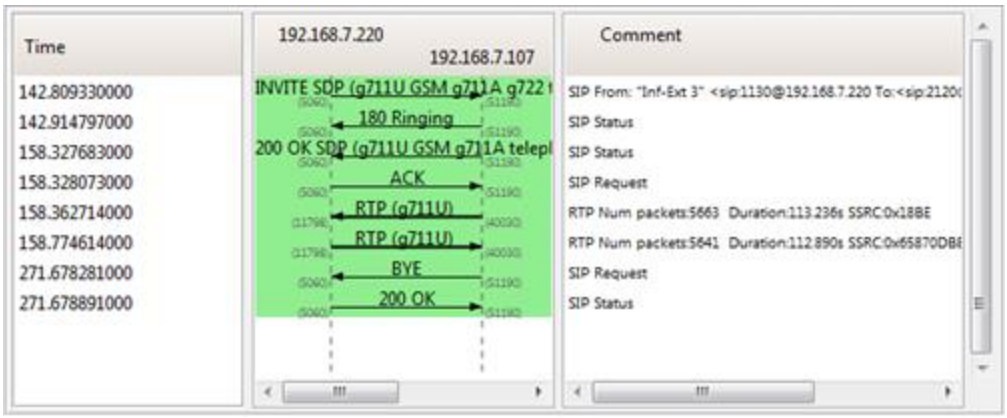


Figura 4.4 *– Gráfica de establecimiento de llamada SIP - Wireshark*
Fuente: *[el Autor]*

Con estos insumos, se puede determinar el número de llamadas *VoIP* simultáneas (verificado desde *Wireshark*, como lo demuestra la figura 4.4), que podrían generar un volumen tal, de intensidad de tráfico que pueda circular por el ancho de banda disponible del túnel de datos que enlaza el edificio Central con el Matriz.

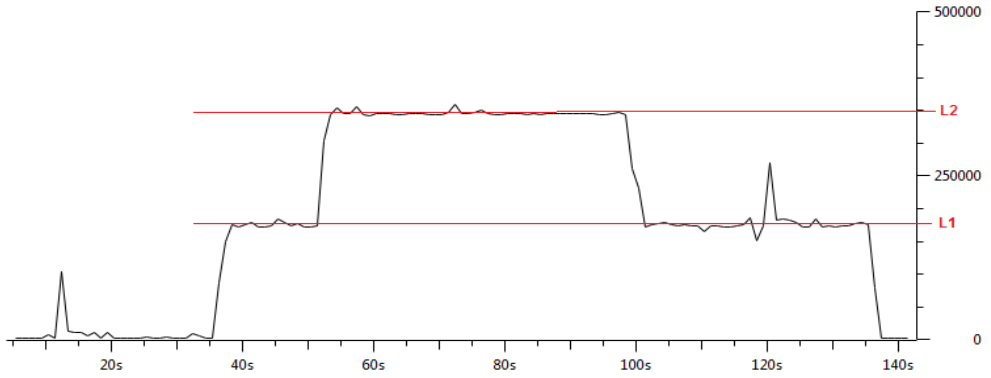


Figura 4.5 *– Gráfica de tráfico, generada por dos llamadas SIP - Wireshark*
Fuente: *[el Autor]*

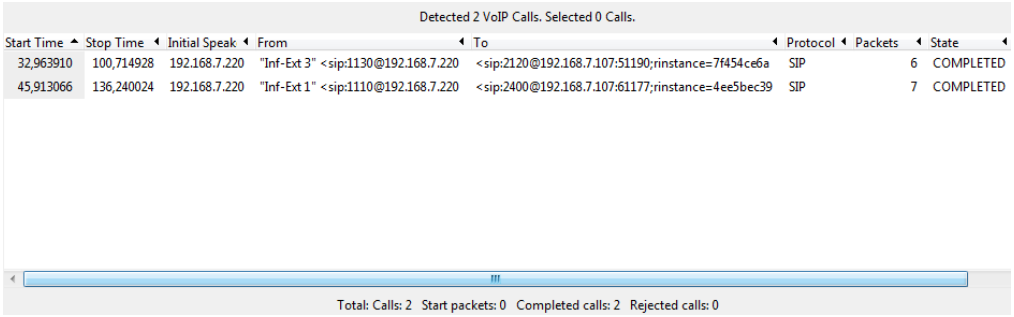


Figura 4.6 *– Registro de llamadas SIP completadas - Wireshark*
Fuente: *[el Autor]*

Como se observa en la figura 4.5, se tiene una primera llamada (L1), marcando un consumo aproximado de 178 Kbps, y una segunda llamada (L2), aumentando el consumo a 346 Kbps aproximadamente, descontando los 10 Kbps promediados de consumo de datos, durante la prueba de llamadas *VoIP*, se tiene un consumo de 336 Kbps, los cuales corresponden a las dos llamadas *SIP* de 168 Kbps, como ya se había determinado en la prueba anterior (figura 4.3).

Por lo tanto, de acuerdo a la conclusión obtenida en el análisis de la figura 4.2, se determina que la disponibilidad neta para usarlo en llamadas *VoIP* es del 60% del enlace, con una holgura adicional de un 17,08%, en horarios no pico, se puede determinar que es posible realizar entre 3 a 4 llamadas simultaneas con la disponibilidad de ancho de anda con que cuenta la Empresa.

Cálculo:

- Disponibilidad neta del 60% de ancho de banda

  it = (168 Kbps * 3 llamadas) / (600 Kbps disponibles)
  it = 504 / 600 = 0.84 erlangs

- Disponibilidad en horarios no pico del 77,08% de ancho de banda

  it = (168 Kbps * 4 llamadas) / (770,8 Kbps disponibles)
  it = 672 / 770,8 = 0.87 erlangs

Como se demuestra en el cálculo, de acuerdo a la disponibilidad del ancho de banda, se puede realizar entre 3 a 4 llamadas simultáneas, y si se activa la opción de supresión de silencio en al *Asterisk*, y en los equipos o *softphone*, se puede conseguir el doble de llamadas simultáneas.

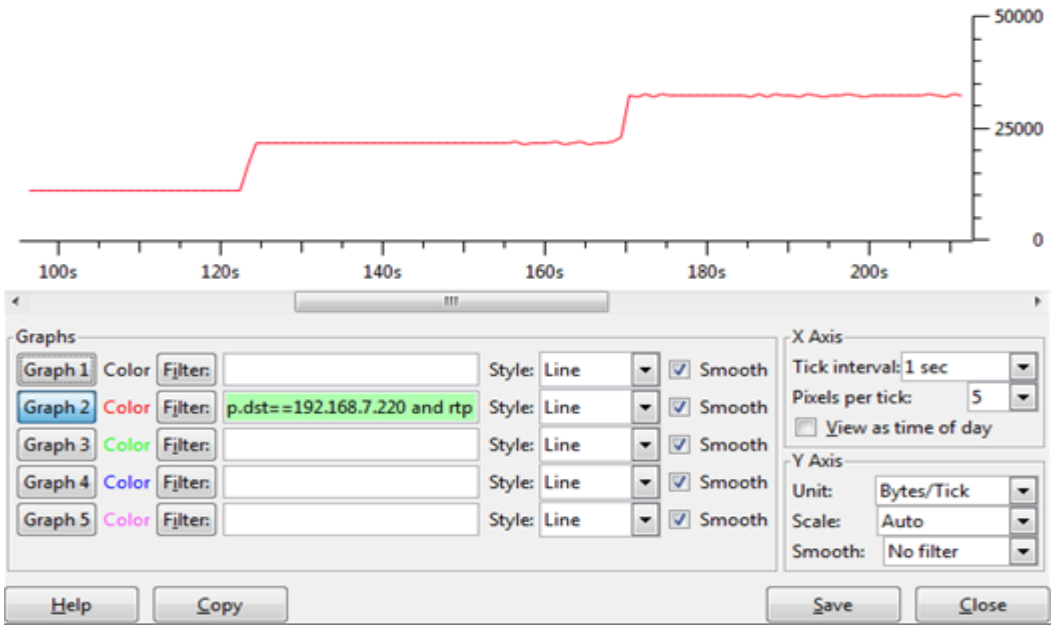


Figura 4.7 *– Gráfica de tráfico, filtro de paquetes a servidor PBX - Wireshark*
Fuente: *[el Autor]*

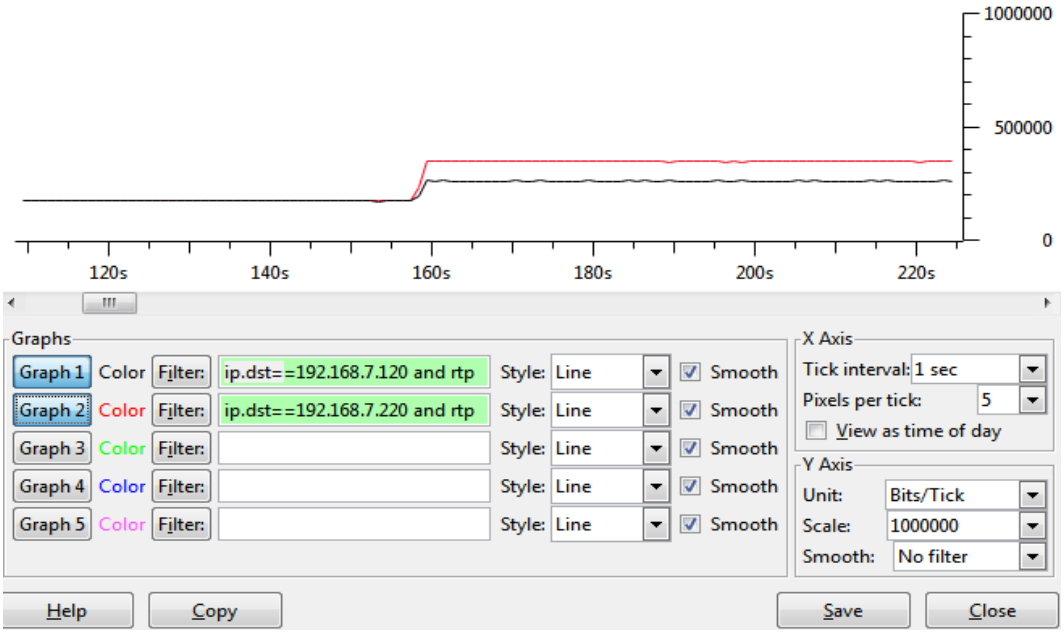


Figura 4.8 *– Gráfica de tráfico, filtro de paquetes a servidor PBX - Wireshark*
Fuente: *[el Autor]*

En las gráficas 4.7 y 4.8, se observa la aplicación de filtros en la representación del tráfico, para que sólo se visualice el consumo de los paquetes con destino a los servidores *PBX*, en el caso de la primera, todas las llamadas son con destino al servidor 192.168.7.220, y en la segunda gráfica, existen llamadas con destino a ambos servidores.

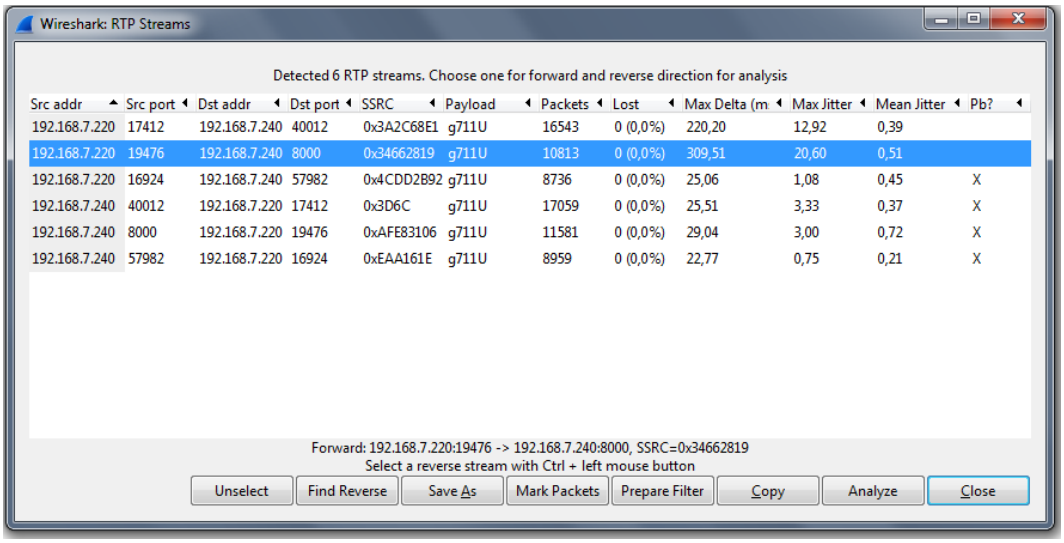


Figura 4.9 *– Estadísticas de capturas de paquetes RTP - Wireshark*
Fuente: *[el Autor]*

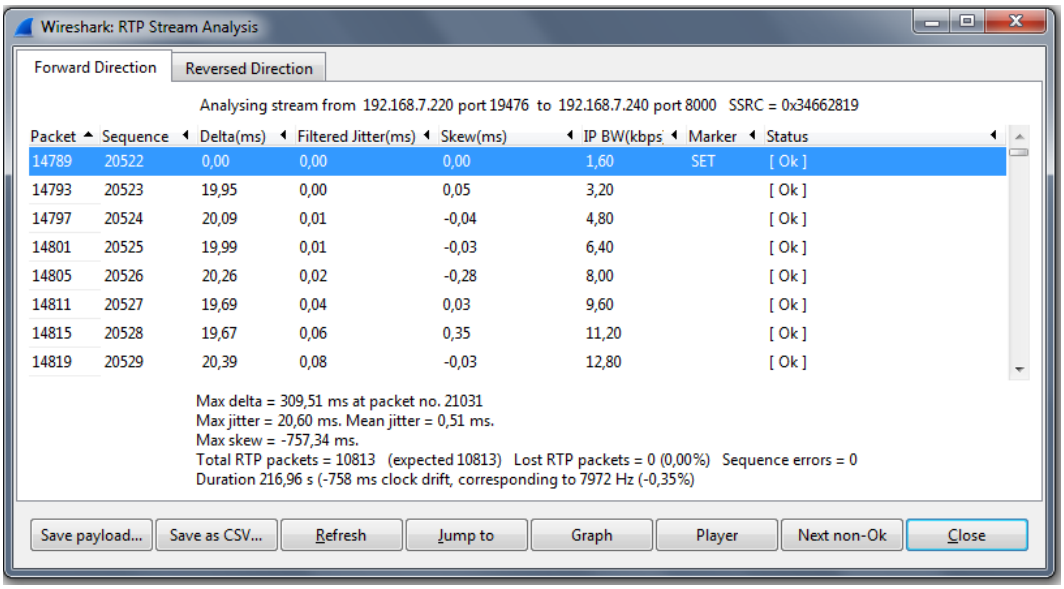


Figura 4.10 *– Estadísticas de los stream - Wireshark*
Fuente: *[el Autor]*

Las gráficas 4.9 y 4.10, detallan la estadística de paquetes *RTP*, donde se observa que no existe pérdida de paquetes (*Lost*), y que el valor máximo de *jitter* (*Max Jitter*) de una prueba de tres llamadas simultáneas, es de 20.60 ms.

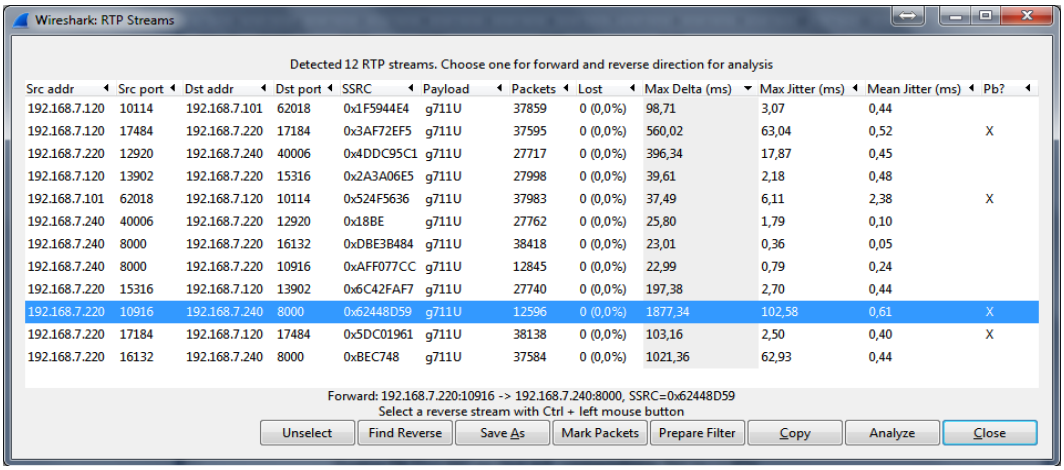


Figura 4.11 *– Estadísticas de capturas de paquetes RTP - Wireshark*
Fuente: *[el Autor]*

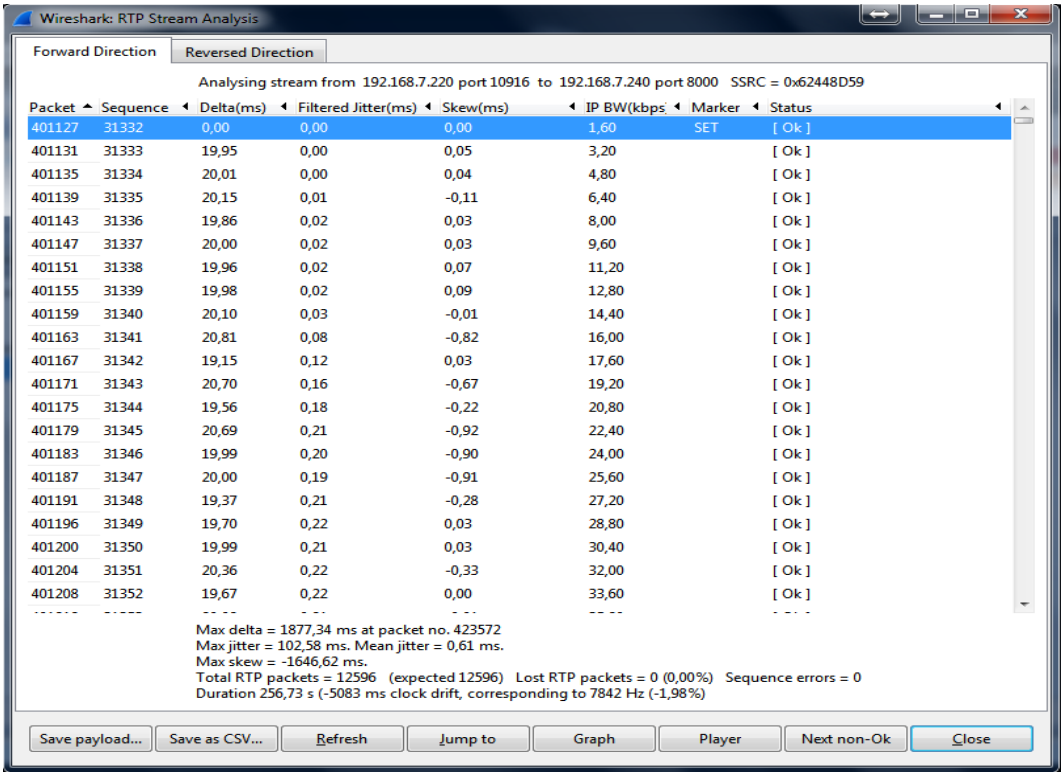


Figura 4.12 *– Estadísticas de los stream - Wireshark*
Fuente: *[el Autor]*

Las gráficas 4.11 y 4.12, detallan la estadística de paquetes *RTP*, donde se observa que tampoco existe pérdida de paquetes (*Lost*), y que el valor máximo de *jitter* (*Max Jitter*) de una prueba de cinco llamadas simultáneas (en un entorno sin consumo de red por otras aplicaciones), es de 102.73 ms.

Dentro del análisis de QoS, se determinó que en la mayoría de los casos, los problemas de, *jitter*, retardo y pérdida de paquetes, se da cuando un paquete pasa por varios ruteadores, o dominios de *broadcast* que puedan incidir en el retardo de los paquetes *VoIP*.

Cada edificio cuenta con su propia red local categoría (5e en uno y 6e en otro), administrados por *switchs* capa 3, donde en las pruebas locales que se realizaron, no se experimentaron ninguno de estos problemas.

Sin embargo, cuando se realizaron llamadas simultaneas inter-edificios, se pudo experimentar aumento de latencia, donde los tiempos de *jitter*, fueron incrementando a medida se incrementaban las llamadas simultaneas.

En las gráficas 4.9 y 410, se observa que en tres llamadas simultaneas, no existió perdida de paquetes, y el tiempo máximo de *jitter* fue de 20.60 ms, tiempo que está dentro de los parámetros normales y no causa ningún problema en la comunicación, mientras que en las pruebas de 5 llamadas simultaneas, gráficas 4.11 y 4.12, se observó un aumento del *jitter*, teniendo como resultado un valor máximo de 102.73 ms, el cual si bien es cierto es muy alto en comparación con el anterior, este no causo mayor molestia en la comunicación, y tampoco se observó perdida de paquete.

Este caso de aumento de latencia, se dio por la saturación en el ancho de banda, el cual lógicamente fue llevado al máximo de consumo con una prueba de 5 llamadas simultáneas, saliendo del máximo permitido, determinado en el la tabla 3.4 para atender este inconveniente, una solución, seria de separar el tráfico por *vlan*, y aumentar el *buffer Jitter* en los equipos (teléfonos IP, *SoftPhone*), para garantizar la *QoS* en la comunicación. Otra solución algo radical, sería la de implementar un enlace propio entre los edificio, cuyo proyecto fue propuesto por el DSI de la empresa y ha sido considerado su implementación a mediano plazo.

4.2. Análisis Cualitativo

Dentro del análisis cualitativo, se realizó una encuesta (empleando la herramienta *Google Drive*, formato incluido en el anexo), para determinar el grado de satisfacción de los usuarios, respecto a la prueba piloto de uso de esta tecnología.

Del total de encuestados (vía *Online*), se consiguió respuesta de 105 usuarios, correspondiente al 87,5% del universo, obteniendo los siguientes resultados, visualizados en la figura 4.13:

1. *Durante la prueba piloto con el sistema VoIP, Ud. logró establecer más llamadas que con el sistema de telefonía tradicional*: obtiene un 97% de aceptación.
2. *Usar un softphone es igual de sencillo que usar un teléfono físico*: obtiene un 97% de aceptación.
3. *La calidad de la voz, durante las llamadas telefónicas con el sistema propuesto fue*: obtiene un 100% de calidad buena hacia excelente.
4. *Disponer de su propia extensión telefónica instalada en su smartphone, le permitirá comunicación oportuna*: obtiene un 95% de aceptación.
5. *Preferiría al sistema telefónico tradicional por el sistema propuesto*: obtiene un 89% de no aceptación, lo cual valida y corrobora los resultados anteriores.
6. *Considera útil el servicio de IM para sus labores diarias*: obtiene un 90% de aceptación.
7. Disponer del servicio IM instalado en su smartphone, le permitirá comunicación oportuna: obtiene un 96% de aceptación.

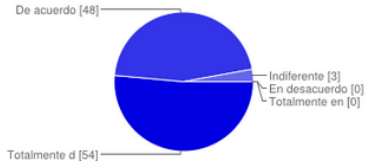
Con estos porcentajes de aceptación, se deja claro que, esta tecnología brinda el grado de satisfacción necesaria en los usuarios, como para ser considerada como una propuesta factible, y que brinda las prestaciones necesarias, para el aprovechamiento del personal administrativo de la empresa.

105 respuestas

Publicar datos de análisis

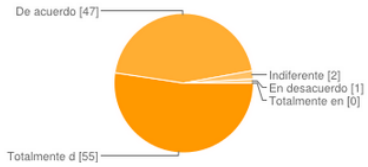
Resumen

Durante la prueba piloto con el sistema VoIP, Ud. logró establecer más llamadas que con el sistema de telefonía tradicional.



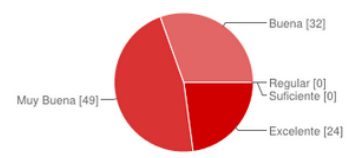
Totalmente de acuerdo	54	51%
De acuerdo	48	46%
Indiferente	3	3%
En desacuerdo	0	0%
Totalmente en desacuerdo	0	0%

Usar un softphone es igual de sencillo que usar un teléfono físico



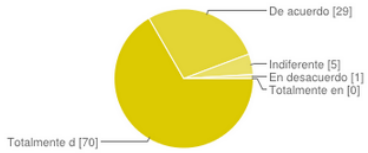
Totalmente de acuerdo	55	52%
De acuerdo	47	45%
Indiferente	2	2%
En desacuerdo	1	1%
Totalmente en desacuerdo	0	0%

La calidad de la voz, durante las llamadas telefónicas con el sistema propuesto fue:



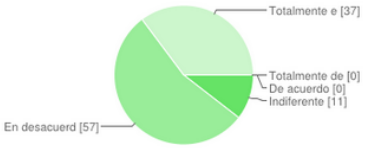
Excelente	24	23%
Muy Buena	49	47%
Buena	32	30%
Regular	0	0%
Suficiente	0	0%

Disponer de su propia extensión telefónica instalada en su smartphone, le permitirá comunicación oportuna.



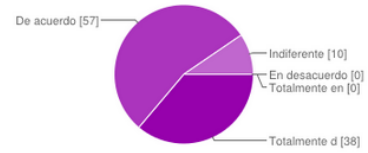
Totalmente de acuerdo	70	67%
De acuerdo	29	28%
Indiferente	5	5%
En desacuerdo	1	1%
Totalmente en desacuerdo	0	0%

Preferiría al sistema telefónico tradicional por el sistema propuesto



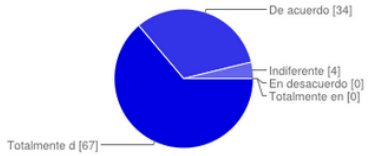
Totalmente de acuerdo	0	0%
De acuerdo	0	0%
Indiferente	11	10%
En desacuerdo	57	54%
Totalmente en desacuerdo	37	35%

Considera útil el servicio de IM para sus labores diarias



Totalmente de acuerdo	38	36%
De acuerdo	57	54%
Indiferente	10	10%
En desacuerdo	0	0%
Totalmente en desacuerdo	0	0%

Disponer del servicio IM instalado en su smartphone, le permitirá comunicación oportuna.



Totalmente de acuerdo	67	64%
De acuerdo	34	32%
Indiferente	4	4%
En desacuerdo	0	0%
Totalmente en desacuerdo	0	0%

Figura 4.13 *– Resumen de respuesta de la encuesta*
Fuente: *[google drive]*

5. Capítulo V: Propuesta

5.1. Esquema de propuesta

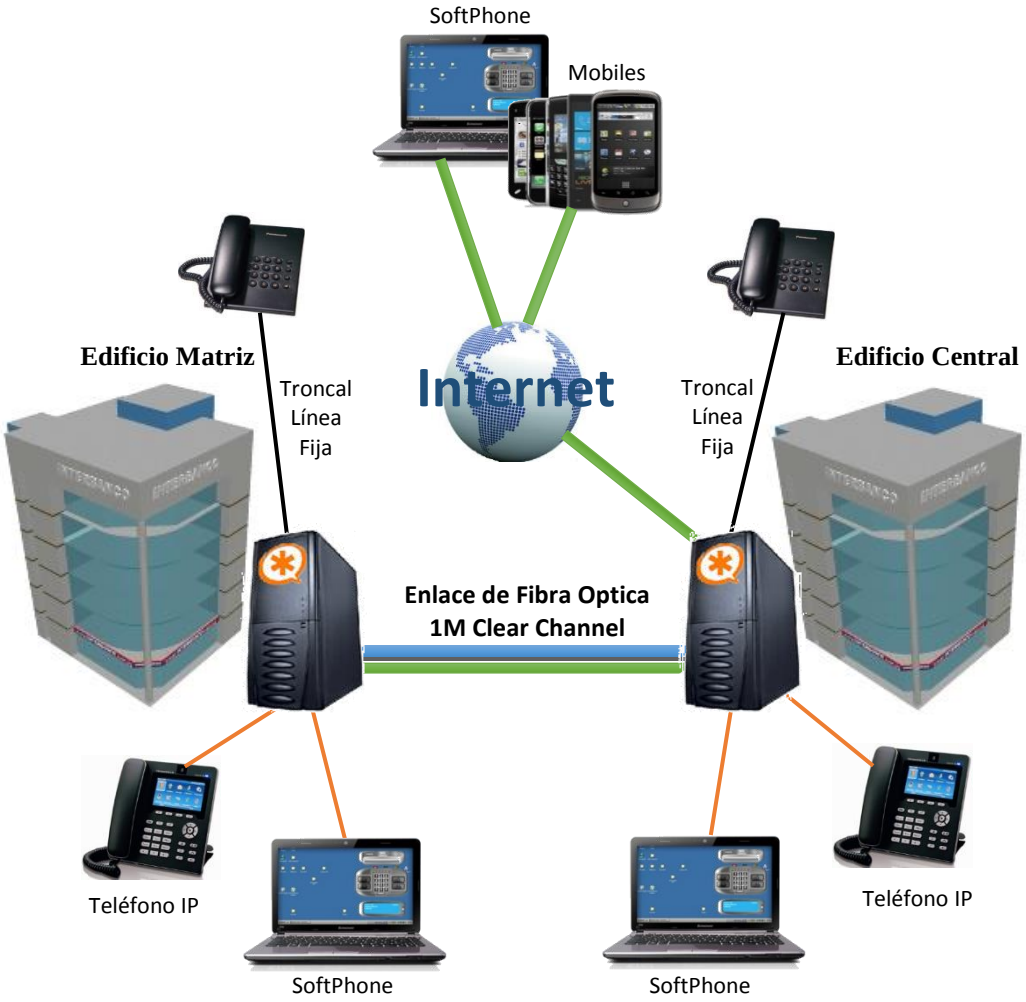


Figura 5.1 *– Esquema de propuesta de implementación*
Fuente: *[el Autor]*

Según el esquema de la figura 5.1, la propuesta, contempla el uso de dos servidores Elastix para llamadas *VoIP* aprovechando el módulo *Asterisk*, y de mensajería instantánea (*IM*) usando el módulo de *OpenFire*, cuyos servidores serán de características básicas en cuanto a *hardware* ya que sus prestaciones o performance no deben ser altos, para administrará un máximo de 60 a 70 usuarios

aproximadamente, con una proyección de crecimiento de hasta 100 usuarios máximo por edificio.

Con la dotación de un servidor por edificio, se garantizará la disponibilidad del servicio para cada grupo de usuarios locales, y en el caso que se interrumpa el enlace interno que une a los edificios, existirá la opción de seguir comunicados, interconectándose por la línea fija, a un costo de aumento de la probabilidad de bloqueo o negación de servicios, mientras dure la interrupción.

Y, si uno de los servidores se interrumpe su operatividad, aún existirá un grupo de usuarios que podrá tener el servicio de comunicación disponible.

Dentro de cada edificio, la *PBX (Elastix),* administrará las llamadas locales, las interconexiones entre usuarios de cada edificio por medio del enlace de fibra óptica, y las llamadas externas por medio de la trocal de la línea telefónica fija.

Por medio del internet, administrado desde el servidor *proxy* en el edificio central, existirá la posibilidad que usuarios se conecten a las *PBX's* de cualquiera de los dos edificios, considerando, que si se conectan a la *PBX* del edificio matriz desde el internet, la *QoS* podría verse afectado por el aumento de latencia, dado que los paquetes deben viajar de ida y vuelta por el túnel de datos (enlace de fibra), para poder entrar y salir por el servidor *proxy*.

Cada edifico cuenta con su propia red local, dotada de equipos activos administrables (*switch* 10/100/1000 Mbps), en los cuales se implementaran *VLan*, para separar el tráfico y por ende mejorar la *QoS* de las llamadas *VoIP* como se observa en la figura 5.2, dando prioridad a estos paquetes, y para las llamadas entre edificio, se debe solicitar al *ISP*, se implemente *QoS* en sus *routers*, o implementar el proyecto de enlace propio por fibra óptica, presentado por DSI (Departamento de Servicios Informáticos), donde se tendrá el control de realizar las configuraciones necesarias, y mejor aún, no se tendrá problema de limitación de ancho de banda, y por ende de llamadas telefónicas *VoIP*.

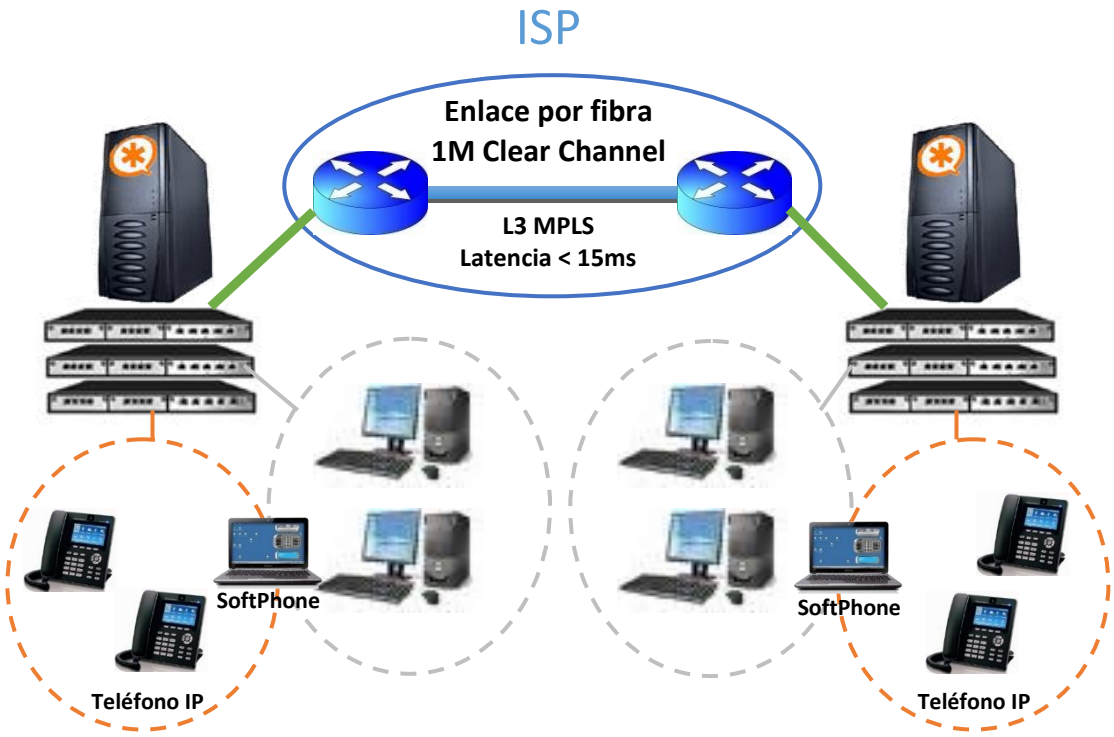


Figura 5.2 *– Esquema sobre implementación de vlan para QoS*
Fuente: *[el Autor]*

Además se propondrá configuraciones, para la integración de la pequeña centralilla telefónica analógica (Panasonic TDA-100) que dispone la Empresa, con el sistema de telefonía VoIP, por si el DSI (Departamento de Servicios Informático), quiere tener un sistema hibrido entre telefonía *VoIP* y telefonía analógica.

Figura 5.3 *– Integración entre PBX Elastix y Central Panasonic TDA-100*
Fuente: *[el Autor]*

5.2. Configuraciones iniciales

El proceso de Instalación de la distribución Elastix se explica en el tutorial que se encuentra en los anexos de la presente Tesis, donde lo importante es que desde el proceso de instalación o posterior al mismo, se establezca los parámetros necesarios para que estos servidores sean parte de la red, en este caso: Nombre del Servidor, *IP*, y *DNS*.

Elastix es una distribución sobre *Linux Centos*, por lo tanto para realizar la configuración de estos datos, posterior a la instalación si no se lo hizo, se debe escribir el comando *setup*, y luego seleccionar *Configuración de red*, luego se deberá registrar los datos en las opciones que aparecen: *Editar dispositivo* y *Editar la configuración DNS*.

- **Editar dispositivo**

Si dispone de dos tarjetas de red, y se pretende acceder desde el internet, se deberá configurar una IP local y una IP pública, en este caso seleccionaremos la eth0 para realizar las configuraciones de la IP local.

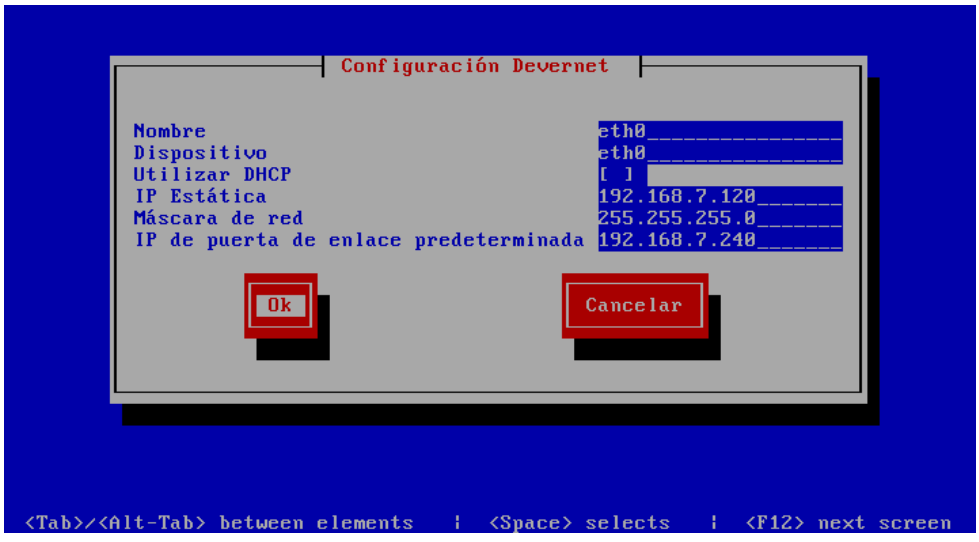


Figura 5.4 *– Configuración de IP y Gatawey - Elastix*
Fuente: *[el Autor]*

Tal y como se muestra en la figura 5.4, se debe ingresar los parámetros: Ip, mascara de red y puerta de enlace, y luego dar click en Ok y finalmente en Guardar.

- **Editar la configuración DNS**

Para el caso de la configuración DNS, lo que se requiere es dar un nombre al servidor *Elastix*, con el cual puede ser accedido dependiendo de las configuraciones que se haga en el servidor proxy para resolver el nombre, y además ingresar la IP del servidor DNS que en este caso es el del servidor proxy, como se observa en la figura 5.5.

Figura 5.5 *– Configuración de Nombre de equipos y DNS - Elastix*
Fuente: *[el Autor]*

Luego que se registran los valores, se da click en Ok, y finalmente Guardar y cerrar; para que estas configuraciones se actualicen en el servidor, se debe cerrar las opciones del comando *setup*, y ejecutar el comando *service network restart*.

Realizada estas configuraciones, se puede acceder al panel de administración del *Elastix* desde cualquier navegador, tan sólo escribiendo en el url la Ip o nombre del servidor *Elastix* que se ha configurado.

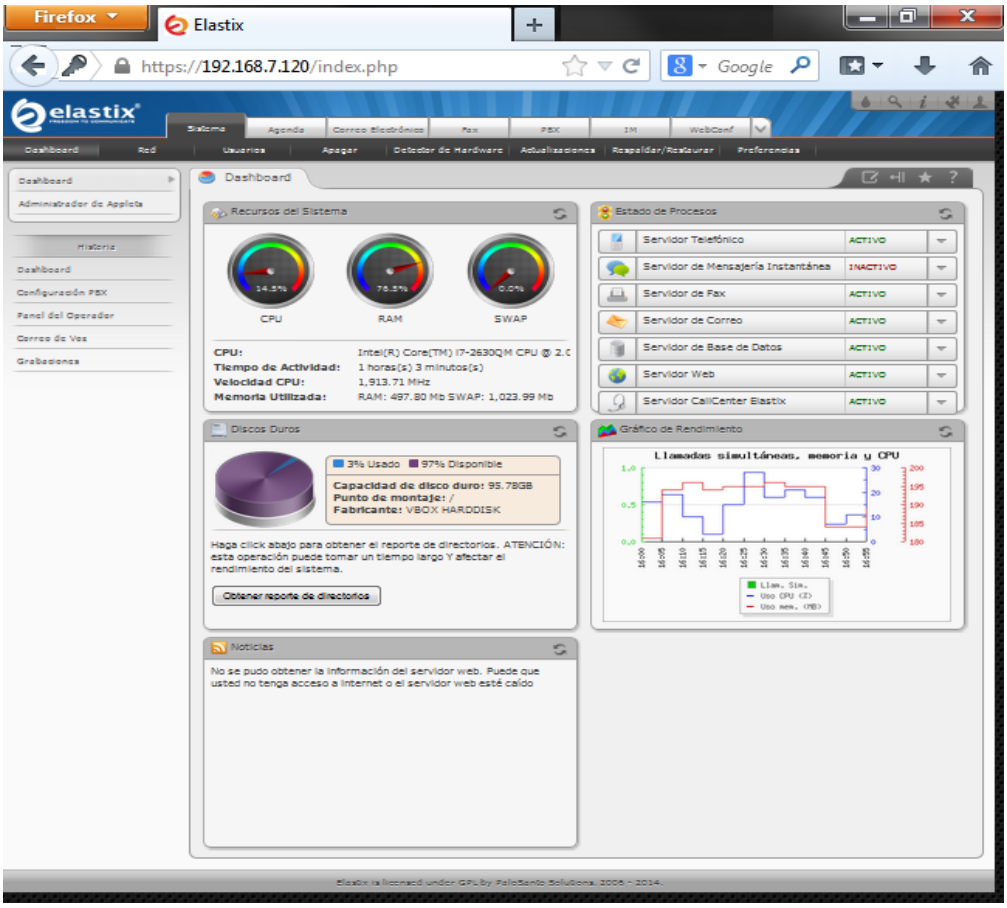


Figura 5.6 *– Panel de Administración de Elastix*
Fuente: *[el Autor]*

Para ingresar al panel de *Elastix*, pedirá el nombre de usuario y clave que se registraron durante la instalación, una vez dentro del panel, la primer pantalla que se carga, es donde se muestran los recursos principales del servidor *Elastix (Figura 5.6)*, como: Recursos del Sistema, Estado de Procesos (muy importante verificar que el Servidor Telefónico, y el Servidor de Mensajería Instantánea, estén siempre activo para mantener la disponibilidad de estos servicios), Discos Duros, Gráfico de Rendimiento (esta parte también es muy importante ya que grafica el uso de CPU y Memoria durante las llamadas simultaneas), y Noticias referente a los componentes de la distribución Elastix.

5.3. Creación de extensiones

Para iniciar con las configuraciones, se debe dar click en la pestaña *PBX*, mostrando las opciones para añadir extensiones. En *Device* tenemos la posibilidad de seleccionar entre diferentes tipos de extensiones, sin embargo en esta propuesta se trabajó con extensiones de tipo SIP.

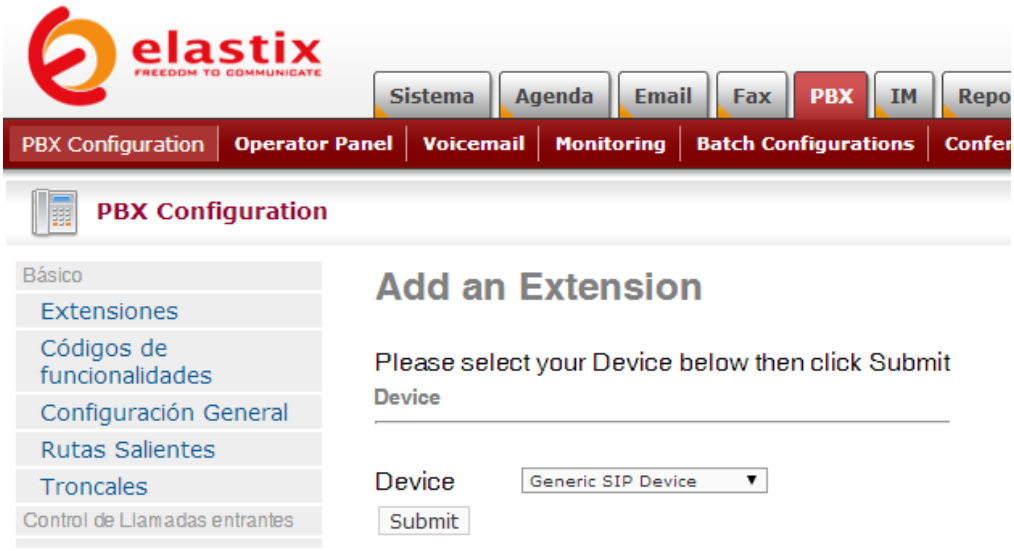


Figura 5.7 *– Panel de inicial de PBX Configuration*
Fuente: *[el Autor]*

Como se observa en la figura 5.7, la opción por default que se muestra en *Device*, es la de *Generic SIP Device*, y para iniciar con el proceso de configuración se debe dar click en el botón *Submit*.

Para la creación de una extensión SIP, los campos principales que se requieren son los siguientes:

- **User Extension**: el número de la extensión que se le asignará a una persona o departamento.
- **Display name**: el nombre que se mostrará en el listado de extensiones configuradas, para distinguir la relación respecto a, la persona o departamento a quien se asignará.
- **Secret**: palabra secreta que sirve para permitir vincular en la PBX, al dispositivo que se le configure dicha extensión telefónica.

La presente propuesta, no pretende cumplir la función de un tutorial, por lo tanto no se explicaran más que los campos que se requerirán, de tal formar que, para crear una extensión *SIP* se consideraran los tres campos descritos, y expuesto en la siguiente figura:

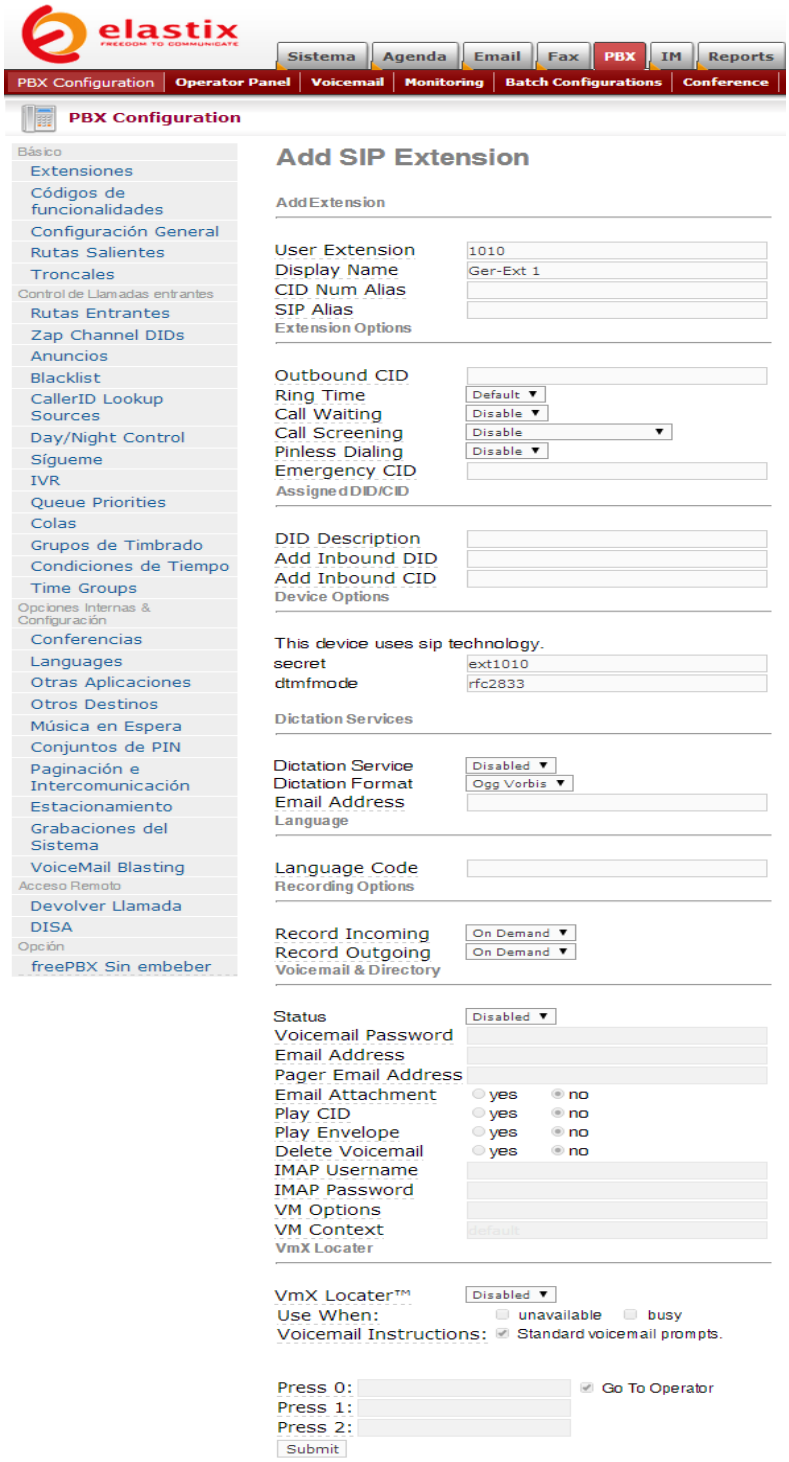


Figura 5.8 *– Ficha para creación de extensión SIP*
Fuente: *[el Autor]*

5.4. Configuración de extensiones en teléfonos IP, Softphone y Smartphone

Para las pruebas de conexión, se emplearon teléfonos IP, los cuales por su mediano/alto costo de inversión, deben ser implementado por lo menos uno por oficina y vinculado con el número de la extensión principal asignado a la misma; los *SoftPhone* que en su gran mayoría son para cada funcionario y serán instalados en sus PC; y los *SmarPhone*, que serán instalado en los móviles de los funcionarios que pertenecen a la parte directiva de la empresa, quienes por sus funciones, requieren de movilidad por sus actividades laborales.

- **Teléfonos IP – Cisco SPA525G**

Dentro de las pruebas que se realizaron, se escogió el modelo SPA525G de la marca Cisco, al cual se le debe asignar una dirección IP para que forme parte de la red y pueda ser encontrado por la PBX, como se observa en la figura 5.9.

Figura 5.9 *– Configuración de IP al equipo – CISCO SPA525G*
Fuente: *[el Autor]*

Luego se debe proceder con la configuración de la extensión que se va a asignar al teléfono IP, para este caso, se hará referencia a los tres campos principales que se deben de registrar, los cuales se distinguen en la figura 5.10:

- ***User Id:*** El número de la extensión asignado
- ***Password:*** La palabra clave que se le asignó en el campo *secret* cuando se creó la extensión.
- ***Proxy:*** La dirección IP del servidor *PBX* a donde se está vinculando el equipo.

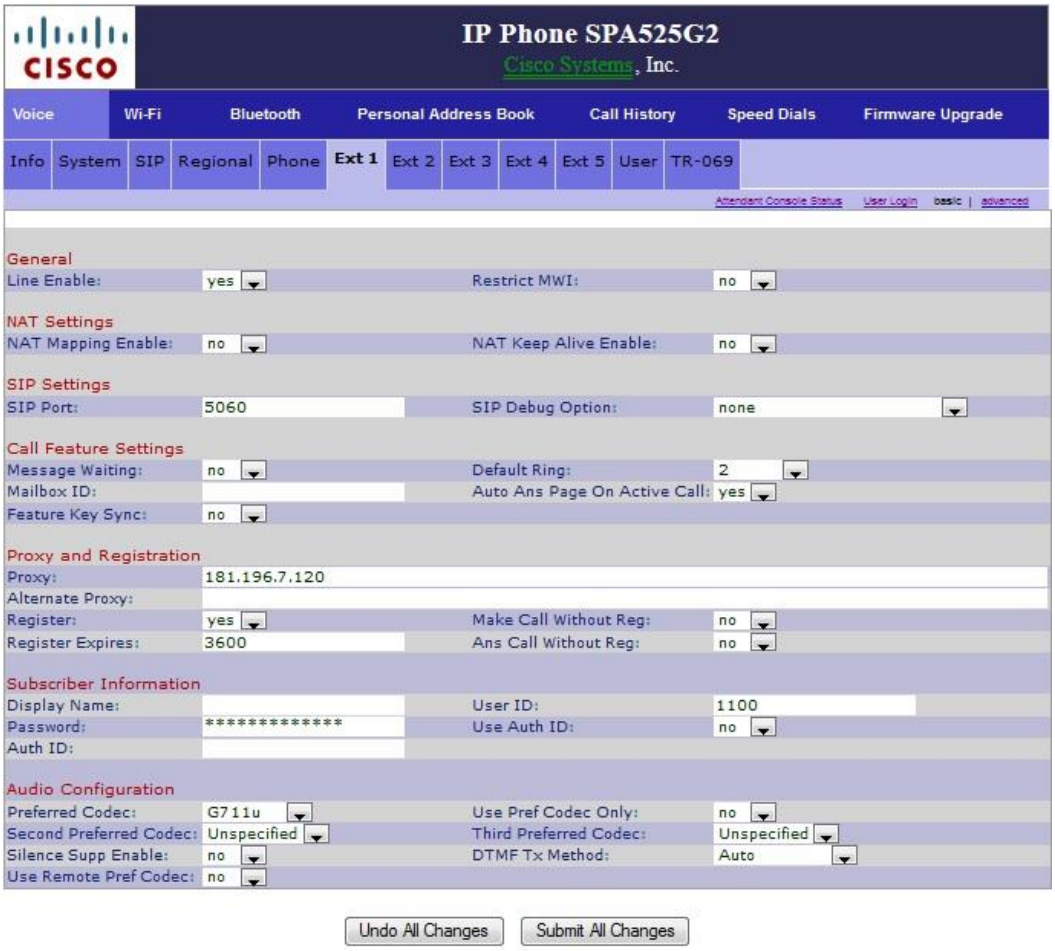


Figura 5.10 *– Configuración de extensión SIP - CISCO SPA525G*
Fuente: *[el Autor]*

- **SoftPhone 3CXPhone**

Uno de los *SoftPhone* que se utilizó para las pruebas, fue el *3CXPhone*, el cual se instala en la PC, y se realiza la configuración respectiva, previo a su uso, en este caso no se debe realizar una configuración de IP al equipo, puesto que éste usa y se identifica por medio de la IP de la PC, los campos a configurarse se detallan a continuación, los mismo que se observan en la figura 5.11:

- ***Extension - ID:*** El número de la extensión asignado
- ***Password:*** La palabra clave que se le asignó en el campo *secret* cuando se creó la extensión.
- ***I am in the office – local IP:*** La dirección IP del servidor *PBX* a donde se está vinculando el equipo.

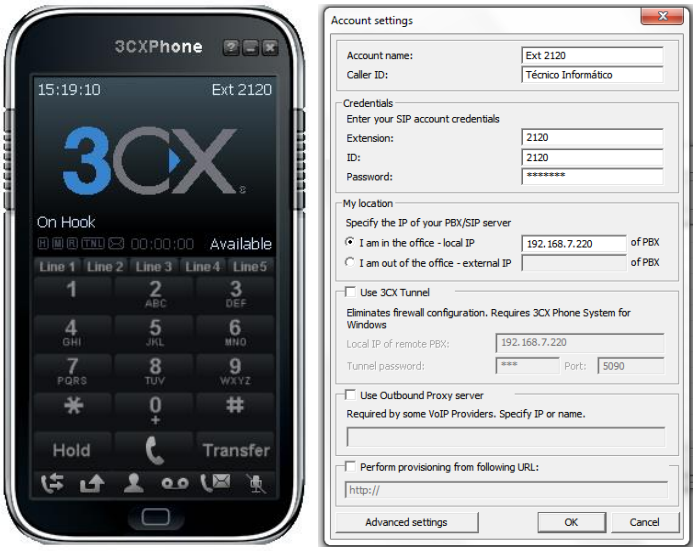


Figura 5.11 *– Configuración de extensión SIP - 3CXPhone*
Fuente: *[el Autor]*

- **SoftPhone Zoiper**

Otro SoftPhone que se usó en las pruebas, fue el Zoiper, el cual también debe ser instalado en la PC, y debe ser configurado previo a su uso, de igual forma, no se asigna IP al SoftPhone, puesto que éste usa para identificarse la IP de la PC, los campos a configurarse se detallan a continuación, los mismo que se observan en la figura 5.12:

- ***Nombre de usuario:*** El número de la extensión asignado
- ***Contraseña:*** La palabra clave que se le asignó en el campo *secret* cuando se creó la extensión.
- ***Dominio:*** La dirección IP del servidor *PBX* a donde se está vinculando el equipo.

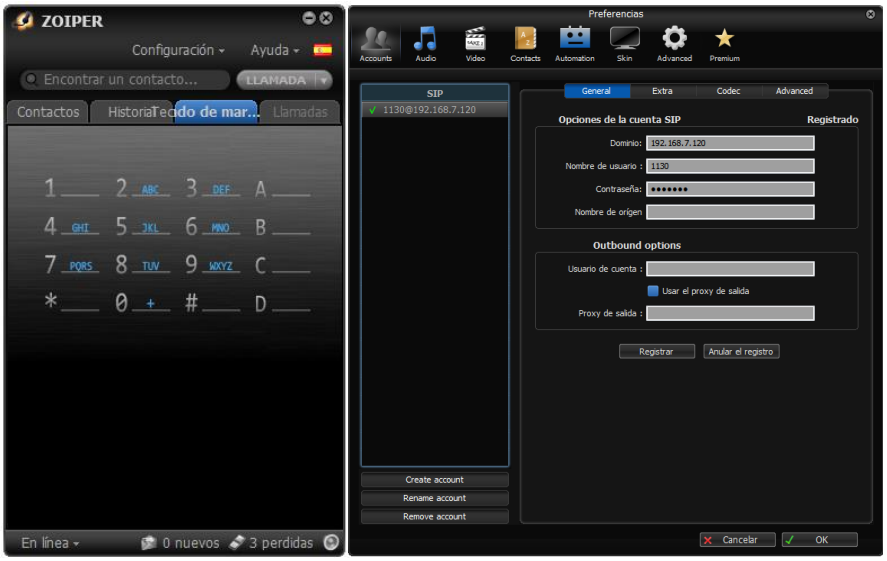


Figura 5.12 *– Configuración de extensión SIP - Zoiper*
Fuente: *[el Autor]*

- **SmartPhone Zoiper**

Muchos *SoftPhone*, o programas para PC, tienen su versión para dispositivos móviles, denominados *SmartPhone*; para la prueba de este tipo de opción, se utilizó el *Zoiper*, el cual también debe ser instalado en el dispositivo móvil, y puede ser usado por medio de la *WIFi* o conexión de datos del dispositivo, dependiendo si en el servidor proxy existe la redirección de puertos de una llamada *VoIP*.

Para configurar, se procede, ingresando a *Add account*, donde se debe seleccionar entre una extensión *SIP* o *IAX*, para este caso la primera, luego los campos que se detallan a continuación, los mismos que se observan en la figura 5.13:

- ***Username:*** El número de la extensión asignado
- ***Password:*** La palabra clave que se le asignó en el campo secret cuando se creó la extensión.
- ***Host:*** La dirección IP del servidor PBX a donde se está vinculando el equipo.

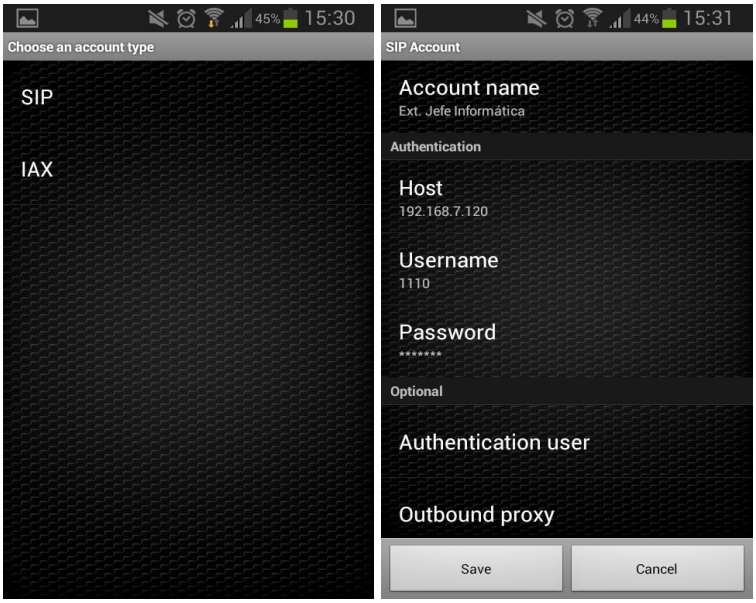


Figura 5.13 *– Configuración de extensión SIP – Zoiper App*
Fuente: *[el Autor]*

Luego para verificar, que la extensión se configuró correctamente, y/o que el servidor *PBX* tiene conectividad con el dispositivo móvil, en el listado de

extensiones debe aparecer ya configurada con el nombre (*account name*) que se le asignó, y un visto y punto en color verde, caso contrario, será de color rojo, el cual indica que ha tenido problema con la conexión, tal y como se observa en la figura 5.14.

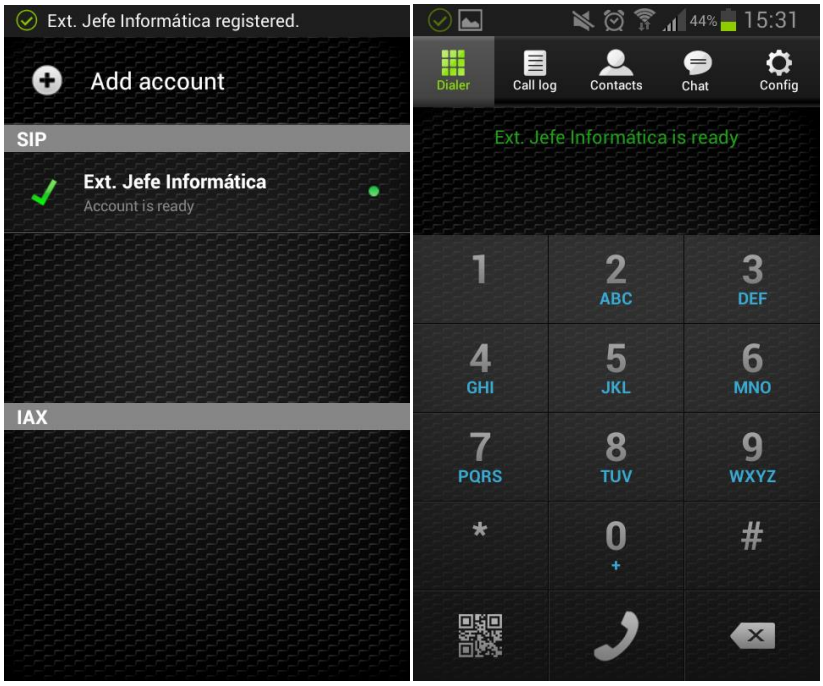


Figura 5.14 *–Extensión configuración correctamente - Zoiper App*
Fuente: *[el Autor]*

5.5. Definición del DataPlan

Para la definición del *DataPlan*, hay que primero analizar, cual es la forma en que se organiza el personal de la Empresa, y como están distribuidos entre los Edificios, a continuación se presenta en la figura 5.15 el organigrama a nivel de directores y área de asesoría a la gerencia.

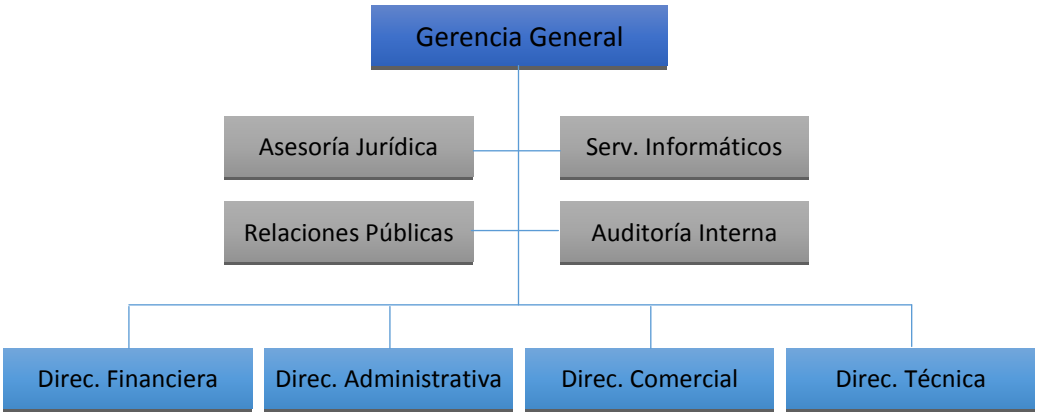


Figura 5.15 *– Organigrama General de la EPMAPAP*
Fuente: *[datos proporcionados por la Empresa]*

La EPMAPAP, cuanta con dos edificios, donde en el denominado Matriz, se encuentra en su gran mayoría la parte directiva, comprendida por la Gerencia con sus Directores de Áreas y Jefes de unidades de Asesoramiento, y su personal operativo correspondiente, sin embargo, en el edificio denominado Central, por encontrarse el *DataCenter*, cuenta también con una oficina para el Jefe de la unidad de Servicios Informáticos con su personal, y para la responsable de Auditoría Interna, además de personal de la Dirección Comercial.

En el caso de las extensiones vinculadas al personal que labora en el edificio Central, y por su definición de personal administrativo, tendrían que estar en el edificio Matriz, se les creará extensiones en los dos edificios, y se enrutará de un número a otro entre edificios, para que siempre se los localice en la extensión principal, sin que quien los llame, tenga que estar probando entre una y otra extensión.

La lógica implícita, en la definición de la numeración (la cual consta de 4 dígitos) para las extensiones telefónicas es la siguiente:

Primer dígito: éste define el número del edificio al que corresponde la extensión, 1 para el edificio Matriz, y 2 para el edifico Central.

Segundo dígito: define al área administrativa a la que pertenece la extensión, y en el caso de la 9 que representa a las extensiones de Call Center. Éste dígito, también representará al número que se asignará al grupo de timbrado para englobar al personal que corresponda.

0. Gerencia General
1. Servicios Informáticos
2. Asesoría Jurídica
3. Relaciones Públicas
4. Auditoría Interna
5. Dirección Financiera
6. Dirección Administrativa
7. Dirección Comercial
8. Dirección Técnica
9. Call Center

Tercer dígito: para el caso de las Direcciones de áreas, el tercer dígito representa a las sub-áreas, y en el caso de la Gerencia y unidades de asesoramiento, este dígito representa al secuencial dependiente del personal.

Cuarto dígito: representa al secuencial correspondiente al personal de una sub-área, cabe indicar que en el caso de las extensiones cuyo cuarto dígito es un 0, y corresponde a la extensión inicial que define una Dirección de área, Unidad de Asesoramiento o Departamento de una sub-área, éste corresponderá al número vinculado con dicha oficina, el cuál debería ser un teléfono IP.

En el caso de los números establecidos a los *IVR* (*Interactive Voice Response*) de cada edificio, corresponderá al 000, distinguiéndose por el primer dígito asignado, en este caso el 1000 y 2000 correspondientemente a cada edificio.

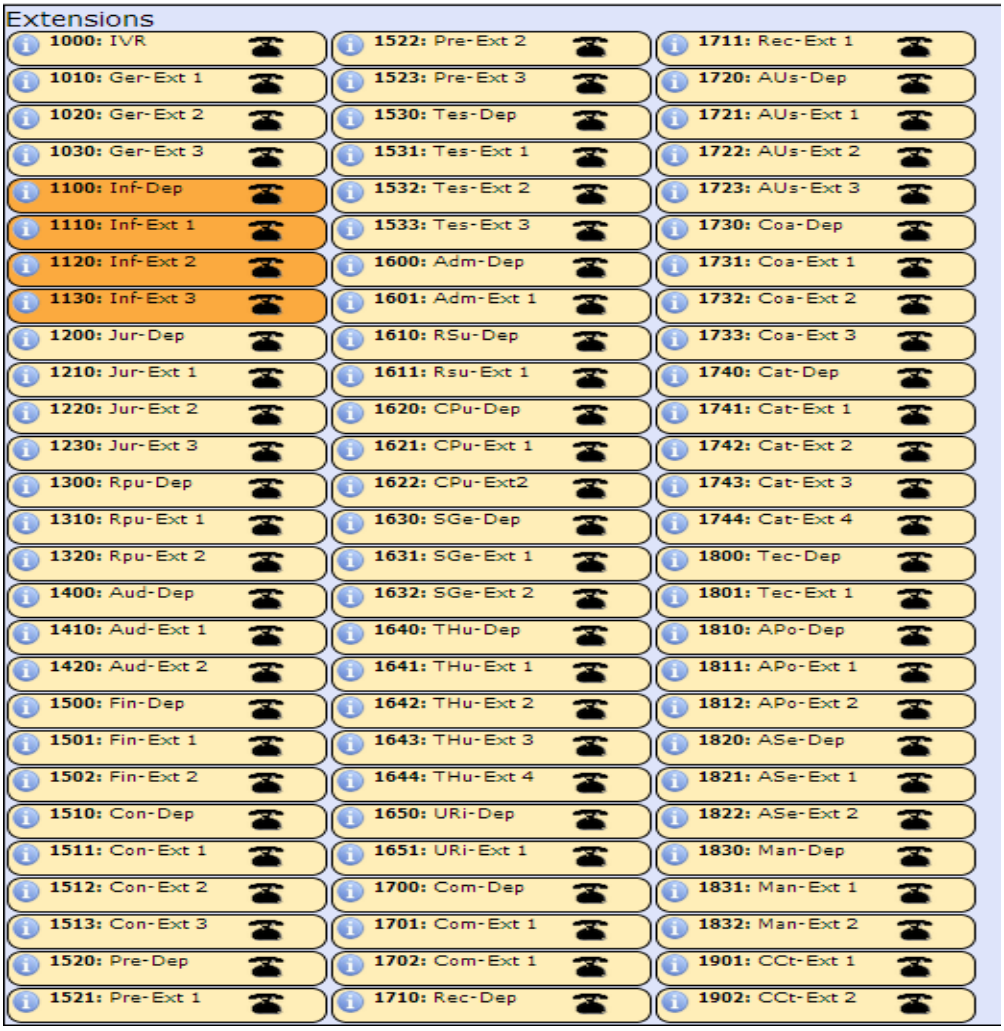


Figura 5.16 *– Listado de Extensiones – Edificio Matriz*

Fuente: *[el Autor]*

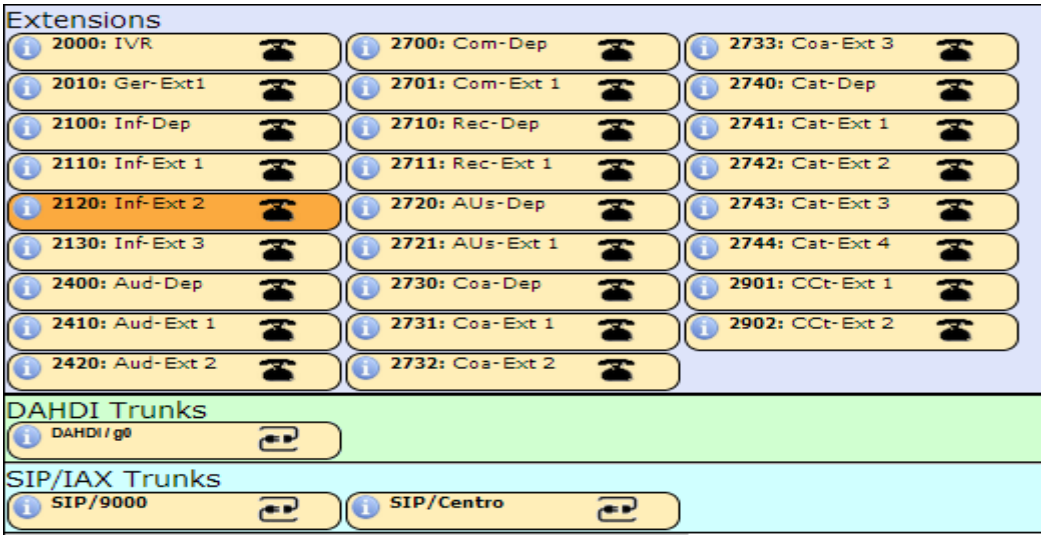


Figura 5.17 *– Listado de Extensiones – Edificio Central*

Fuente: *[el Autor]*

Configuración IVR:

Para poder implementar una *IVR* (*Interactive Voice Response*), se debe realizar configuraciones previas, como, seleccionar o vincular grabaciones de acuerdo a las opciones que se implementaran, para ello se debe seleccionar la opción ***Grabaciones del Sistema***, y realizar lo correspondiente, entre ello, seleccionar del listado de grabaciones que vienen con *Elastix*, o realizar sus propias grabaciones y cargarlas dentro del *Elastix*, tal y como se muestra en la figura 5.18.

Figura 5.18 *– Grabaciones de Sistema, para sonidos de IVR*
Fuente: *[el Autor]*

Una vez, que se disponga de todas las grabaciones que se vayan a usar, de debe seleccionar ***IVR*** (Recepcionista digital en español), y registrar las opciones correspondientes, el nombre para este caso es ***Contestadora***, donde cada opción (0-8), vincula con el número principal de cada departamento (Grupo de extensiones, figura 5.19), el cual es un número de grupo, donde al comunicarse alguien, timbraran todas las extensiones vinculadas a ese grupo, y el primero que conteste tomará la llamada.

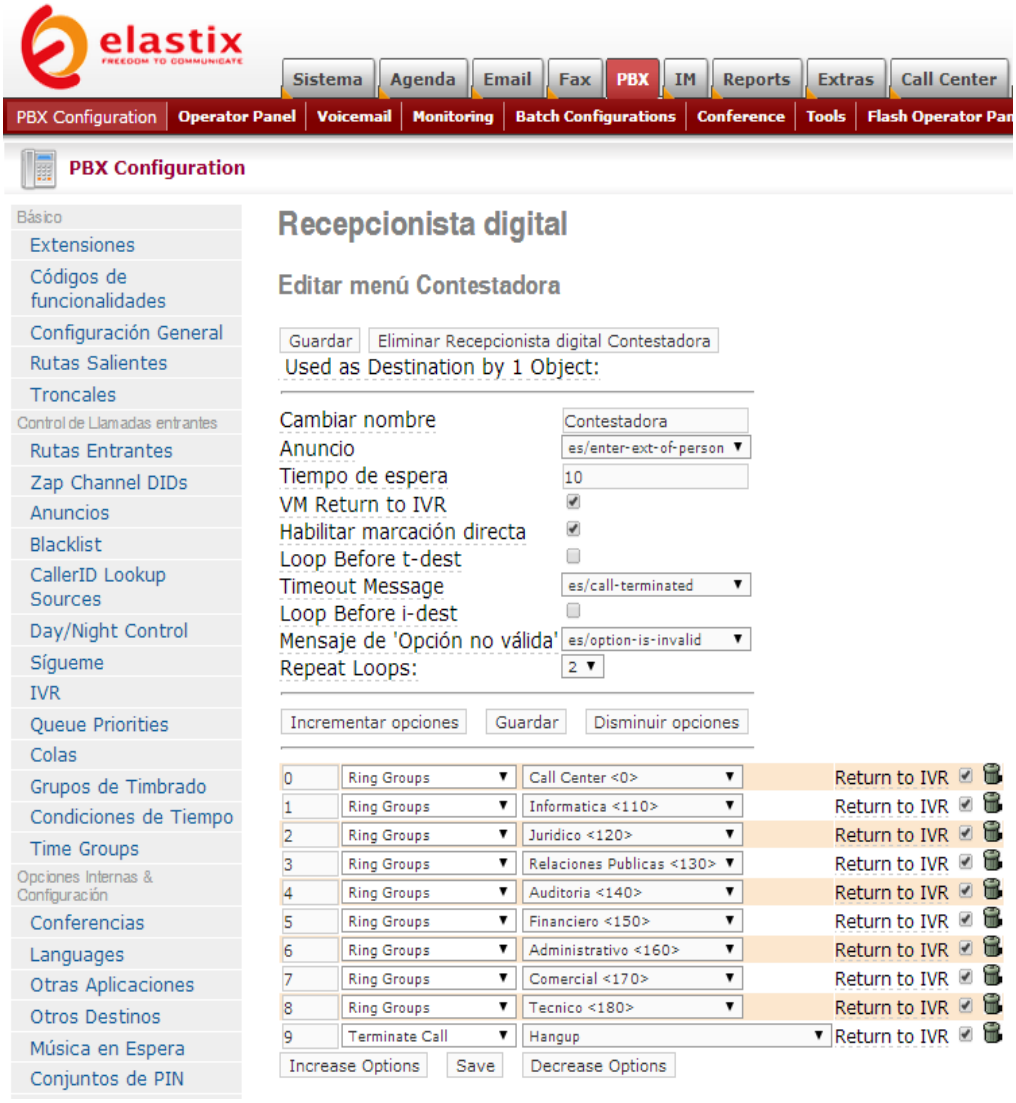


Figura 5.19 *– Configuración de opciones de una IVR*
Fuente: *[el Autor]*

Por último se debe vincular el número de la extensión definida (en este caso 1000), para que responda a las opciones de llamado a una *IVR*, para ello se debe ingresar a la opción ***Follow Me*** (Sígueme en español), y registrar el 1000 en el casillero ***Follow-Me List***, y seleccionar IVR (nombre que se le haya dado) en ***Destination if no answer***. En ***Anuncio***, ***Timeout Message***, y ***Mensaje de 'Opción no válida'***, se debe seleccionar la grabación o sonido que se haya configurado previamente, figura 5.20.

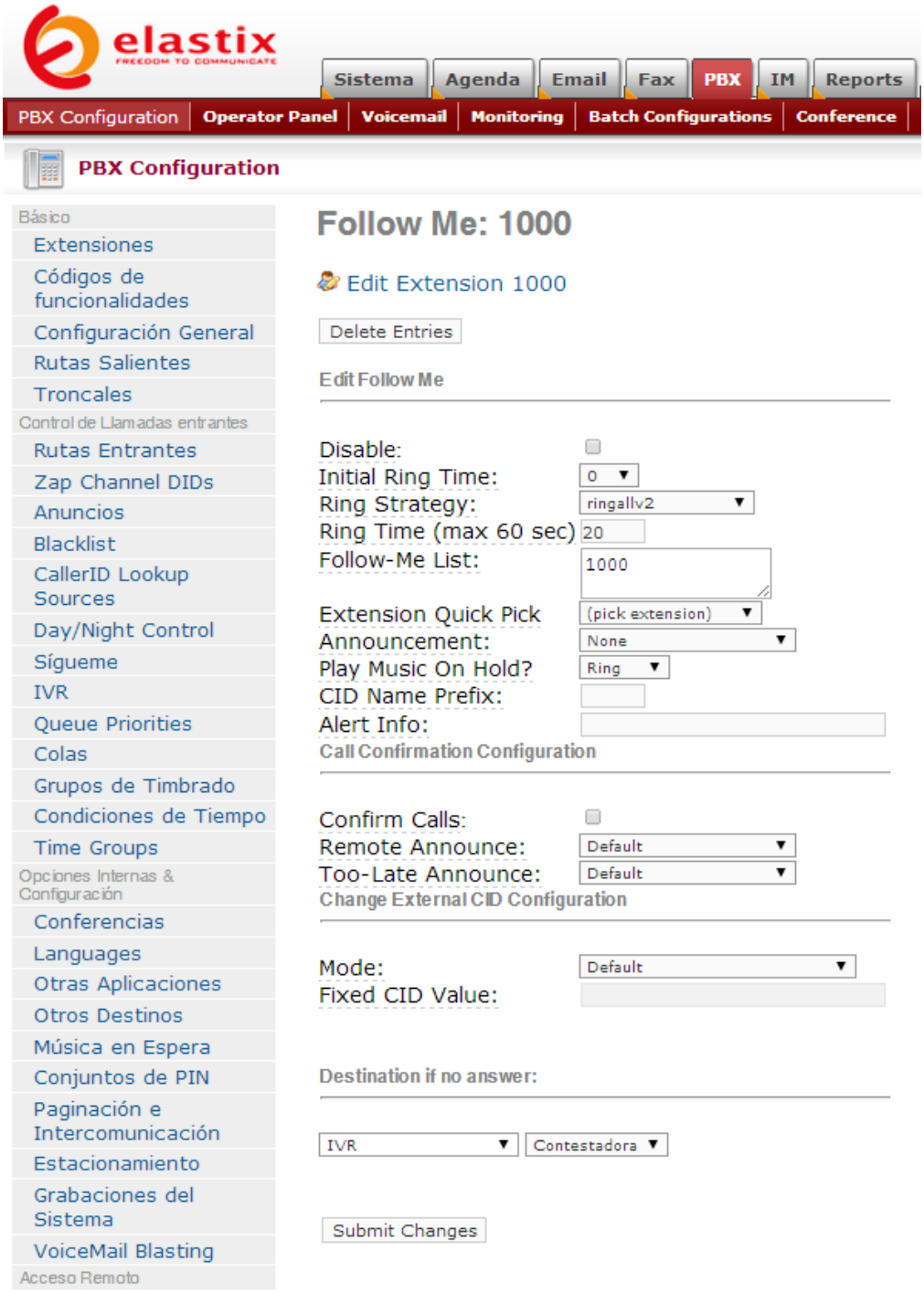


Figura 5.20 *– Vinculación de IVR con número de extensión*

Fuente: *[el Autor]*

Configuración Grupo de Extensiones:

Complementando la configuración de la *IVR*, donde cada opción se vinculaba con un número de grupo, se explica a continuación el procedimiento, el cual también se refleja en la figura 5.21.

Se debe seleccionar la opción de ***Grupo de timbrado***, donde en ***Número de grupo de extensiones*** se debe dar el ingresar el número que comprende a todo un grupo de extensiones, las mismas que son registradas en el cuadro de texto ***Lista de extensiones***.

En el caso del primer digito define el edificio, 1 para la matriz y 2 para el central, el segundo digito define el departamento, terminado en un 0 como tercer digito para todos.

Figura 5.21 *– Configuración de Grupo de timbrados*
Fuente: *[el Autor]*

Configuración Follow Me:

Tal y como está descrito en el *DataPlan*, cada departamento tiene un dígito que lo identifica (segundo dígito), y los funcionario (Jefe Departamental), que tiene asignado el mismo número, en ambos edificio (distinguiéndose por el primer dígito), cuando alguien lo llame a un edificio distinto a donde está su oficina principal, la *PBX* de ese edificio, le redireccionará automáticamente la llamada a su extensión principal, es así que:

En el caso de la extensión de la oficina de Auditoría Interna, cuyo Jefe departamental, hace oficina en el edificio central (2), cuando le llamen al número de la oficina del edifico matriz (1), ésta llamada será redireccionada de la extensión 1400 a la 2400. Para ello entremos a la opción ***Follow Me***, y seleccionamos la extensión en este caso del edificio de donde se redireccionará la llamada (1400), y en ***Follow-Me List*** se especifica la extensión de la otra *PBX* (2400), terminado en #, lo cual le indica a la *PBX* que debe redireccionar a una extensión externa, saliendo por la troncal (previamente configurada), especificada en ***Destination if no answer***, dichas configuraciones se muestran en la siguiente figura:

Figura 5.22 *– Configuración de redirección de llamada del edifico 1 al 2*
Fuente: *[el Autor]*

En este segundo caso, la extensión es la asignada específicamente al Jefe Departamental de Informática, quien hace oficina en el edificio matriz (1), cuando le llamen al número de la oficina del edifico central (2), esta llamada será redireccionada de la extensión 2110 a la 1110. Para ello entremos a la opción ***Follow Me***, y seleccionamos la extensión en este caso del edificio de donde se redireccionará la llamada (2110), y en ***Follow-Me List*** se especifica la extensión de la otra *PBX* (1110), terminado en #, lo cual le indica a la *PBX* que debe redireccionar a una extensión externa, saliendo por la troncal (previamente configurada), especificada en ***Destination if no answer***, para que los cambios tenga efecto, se debe dar click siempre en el botón ***Submit Changes***, en la figura 5.23, se visualiza dichos campos a configurar.

Figura 5.23 *– Configuración de redirección de llamada del edifico 2 al 1*
Fuente: *[el Autor]*

5.6. Configuración de trocal

Como ya se había indicado, cada edifico tiene su propia línea fija para tener acceso a llamadas externas, para aprovecharlas, se debe configurar como trancoles, empleando una tarjeta *Digium TDM410* (figura 5.24), la cual permite conectar líneas análogas y administrarlas desde la central PBX.

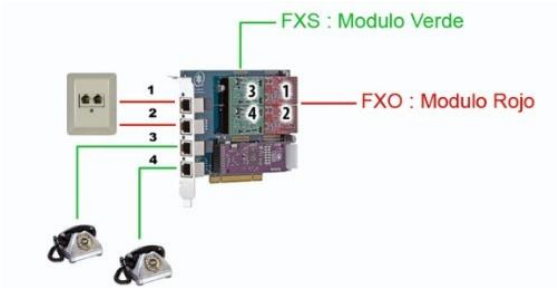


Figura 5.24 *– Tarjeta PCI, Digium TDM410 (FXS/FXO)*
Fuente: *[internet]*

Esta tarjeta es de fácil acceso y de bajo coste, la cual dispone de 2 módulos *FXS* (*Foreign eXchange Station*, estación exterior de intercambio) y *FXO* (*Foreign eXchange Office*, oficina exterior de intercambio), además de un módulo de cancelación de eco.

Para este caso, se usaran los módulos *FXO*, los cuales permitirán conectar hasta 2 líneas fijas análogas, y el archivo de configuración en la *PBX* debe contener los datos correspondiente (figura 5.25). Accedemos al archivo /etc/dahdi/system.conf, donde la última línea, hace referencia a la activación, de la cancelación de eco durante las llamadas.

```
loadzone=es
defaultzone=es
fxoks=1-2
fxsks=3-4
echocanceller&#61mg2,1-4
```

Figura 5.25 *– Configuración del archivo system.conf*
Fuente: *[el Autor]*

Al finalizar, se debe cargar estas configuraciones en la consola de administración con el comando ***dahdi_cfg –vvvv***, la cual muestra un resumen de los 4 canales cargados correctamente. Aunque este proceso solo se lo debe realizar como verificación o en caso que no se haya detectado la tarjeta, sin embargo este modelo y marca de tarjeta, tienen compatibilidad con elastix y generalmente son autodetectadas.

Una vez que se haya configurado la tarjeta Digium, de debe proceder con la configuración de la troncal, para lo cual se debe seleccionar la opción **Troncales,** y seleccionar el tipo de troncal que se va a configurar, para este caso es una ***DAHDI***. Luego, se debe asignar un nombre ("LineaFija"), y constatar el identificador ("g0"), a continuación se muestra una captura de estas configuraciones en la figura 5.26.

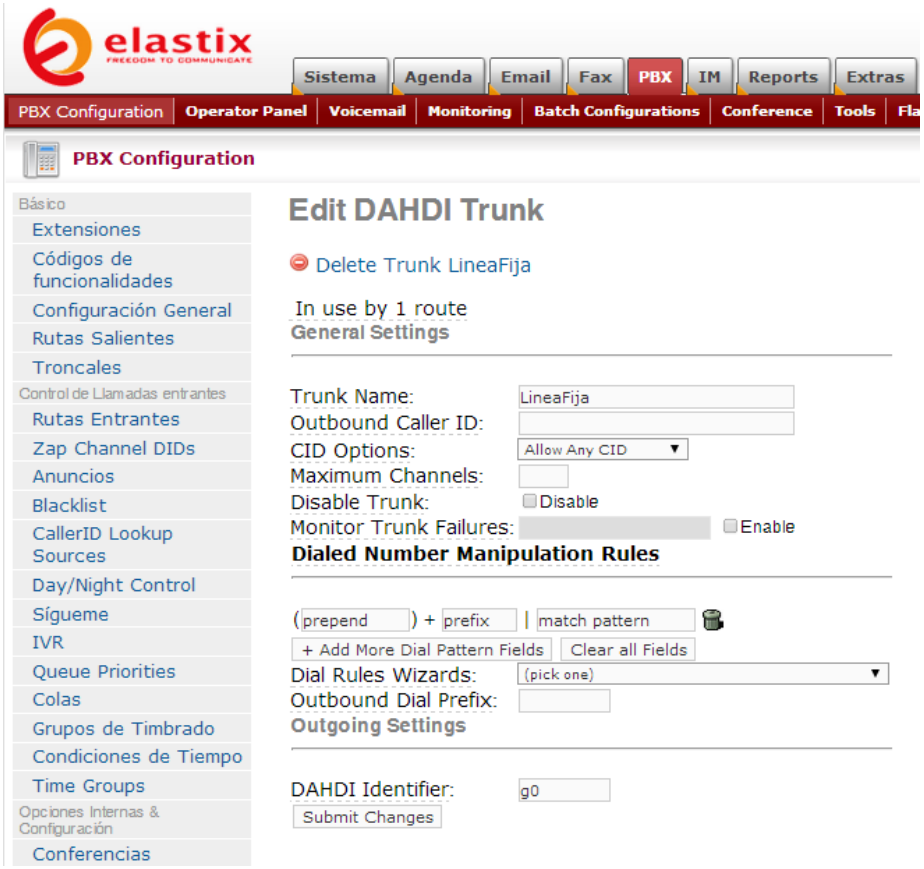


Figura 5.26 *– Configuración de troncal DAHDI, para línea fija telefónica*
Fuente: *[el Autor]*

Una vez que se tiene configurado la troncal, se debe proceder a realizar las configuraciones necesarias, para que toda llamada que se requiere salir por la línea fija, se enrute desde la *PBX* a la troncal y tenga así acceso a una llamada externa, para ello, se debe entrar a la opción de ***Rutas Salientes***, y realizar las configuraciones pertinentes, como consta en la figura 5.27:

- ***Route Name:*** Se le asigna un nombre a la ruta.
- ***Dial Patterns that will use this Route:*** Se especifican las condiciones de marcado, en este caso todo número con prefijo 05 (llamada dentro de la

provincia), y 09 (llamada a línea celular), se enrutará por la o las troncales que se hayan definido.

- ***Trunck Sequence for Matched Routes:*** Aqui se especifica, la secuencia de trolcales por la que debe enrutarse la llamada en cado de que cumpla una condición de marcado, en este caso primero se intentará salir por la propia línea fija local (LineaFija), y en caso que se encuentre ocupada, tratará de salir por la línea fija del otro edificio, para lo cual tendrá que pasar por una troncal definida como InterEdicio (Interconexión entre edificios), la cual usa el enlace de fibra para realizar dicha interconexión.

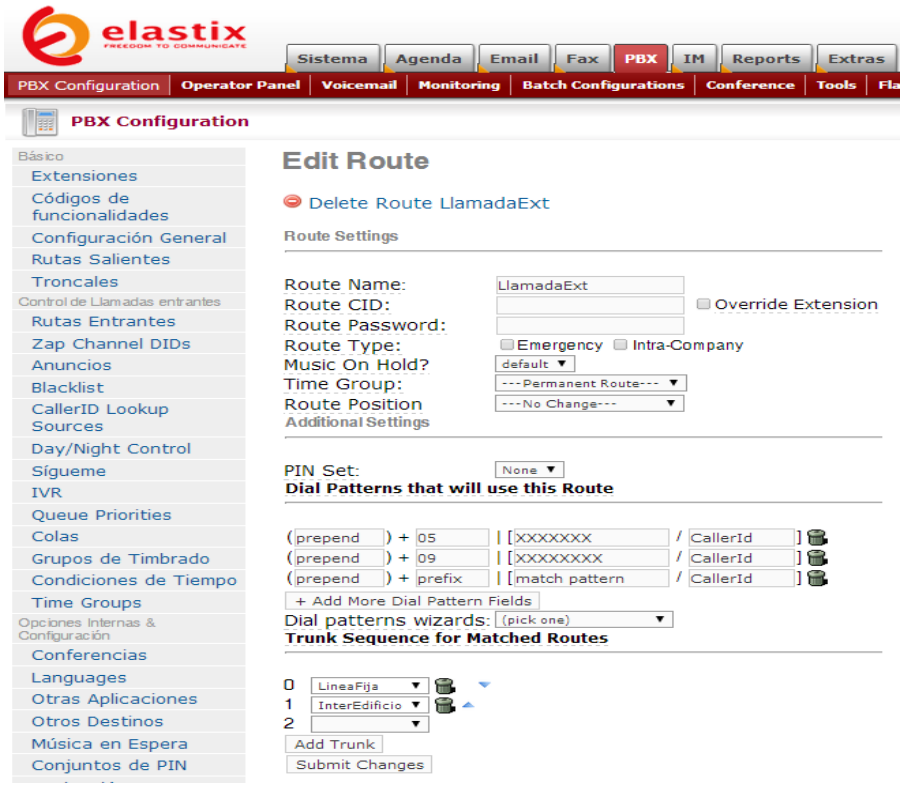


Figura 5.27 *– Configuración de Rutas Salientes de llamadas por las troncales*
Fuente: *[el Autor]*

Para que exista esta dualidad en las llamadas externa por cada edificio, y en caso de que se encuentre ocupada, usar como salida, la línea fija del otro edificio, por medio de la interconexión de las *PBX*, se debe realizar las mismas configuraciones en ambas *PBX* de cada edifico.

5.7. Integración con otra PBX Elastix

La integración de las *PBX* (ubicada una en el edificio Central y la otra en la Matriz), tienen como objetivo interconectar las llamadas entres funcionarios de un edificio con los del otro edificio, por medio del enlace de datos (Tunel por fibra óptica arrendado a un *ISP*), de una forma transparente, y además gestionar llamadas entrantes y salientes por las líneas telefónica fija de cada edificio, como si fuera una misma central telefónica.

Para conseguir esta integración, se debe proceder con la configuración de la trocal y luego la creación de rutas salientes en cada una de las PBX, haciéndose referencia a los datos de conexión una de la otra.

Para configurar la troncal, se debe seleccionar la opción **Troncales,** y luego el tipo, para este caso ***SIP***, el nombre de la Troncal que se usa en ambas *PBX* es "InterEdificio", donde se debe configurar los datos del *PEER* (datos local del server) y *USER* (datos del server remoto a cual se interconecta), además de la cadena de conexión en el campo *Register String*, para poder interconectarse ambas *PBX*, tal y como se observa en la figura 5.28 correspondiente a la configuración de la *PBX* del edificio Matriz, y la figura 5.29 correspondiente a la configuración de la *PBX* del edificio Central.

Una vez que se tiene configurado la troncal *SIP*, se debe proceder a realizar las configuraciones necesarias, para que toda llamada local se enrute a la PBX correspondiente, y además enrute por esta misma troncal *SIP* (InterEdificio) las llamadas externas; para ello, se debe entrar a la opción de ***Rutas Salientes***, y realizar las configuraciones pertinentes: en nombre de la ruta se le registra como "Inter-Edif", y la condición de marcado depende de la *PBX*, si se está en la *PBX* de la Matriz, toda llamada local que se haga a una extensión que comienza por el digito 2, se enrutará a la *PBX* del Centro, y en caso que se está en la *PBX* del Centro y se realiza una llamada a una extensión que comienza por 1, se enrutará a la PBX de la Matriz, tal y como se observa en la figura 5.30, y 5.31, referente a las configuraciones de la Matriz y del Centro respectivamente.

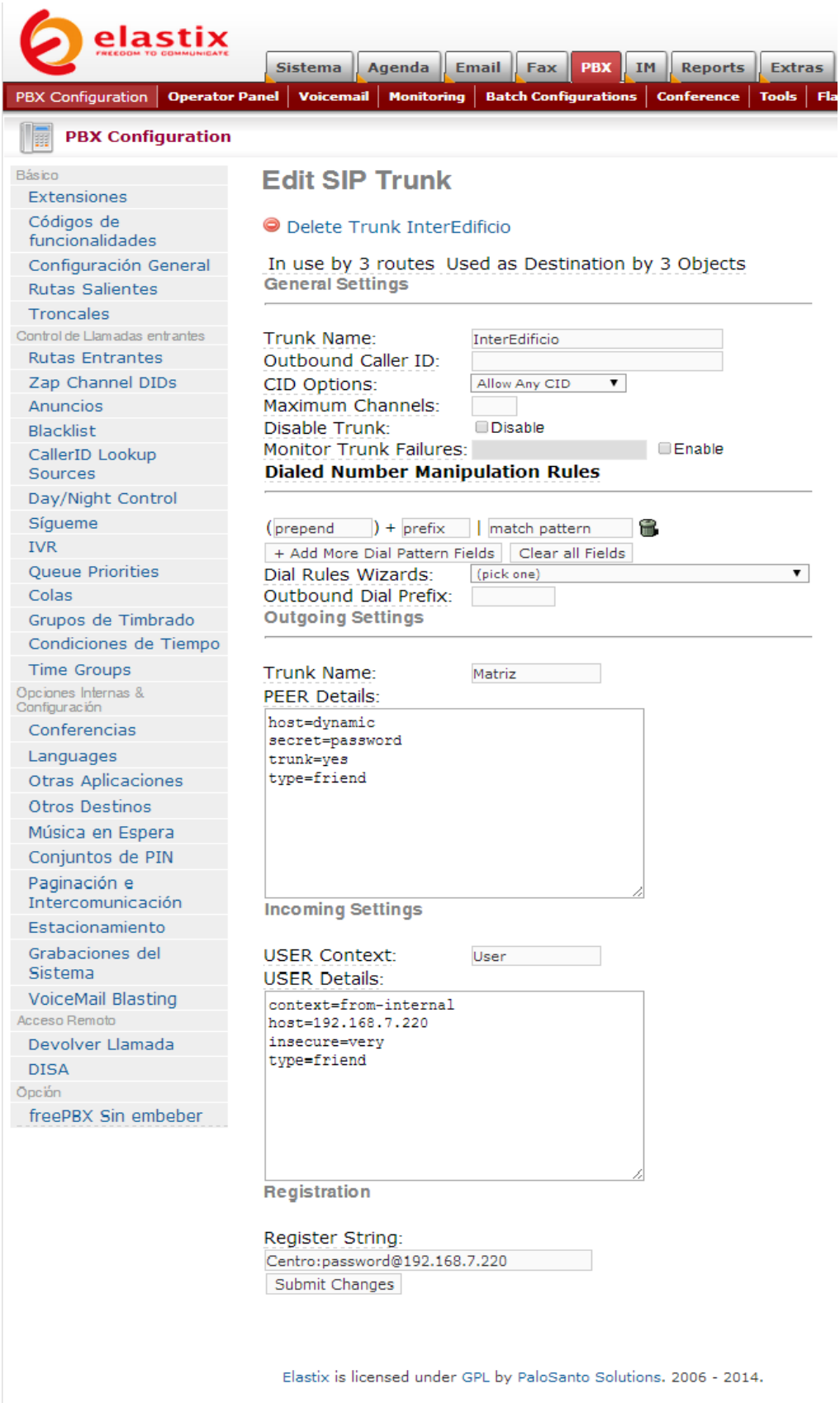


Figura 5.28 *– Trocal para interconectarse con la otra PBX – Config. Matriz*
Fuente: *[el Autor]*

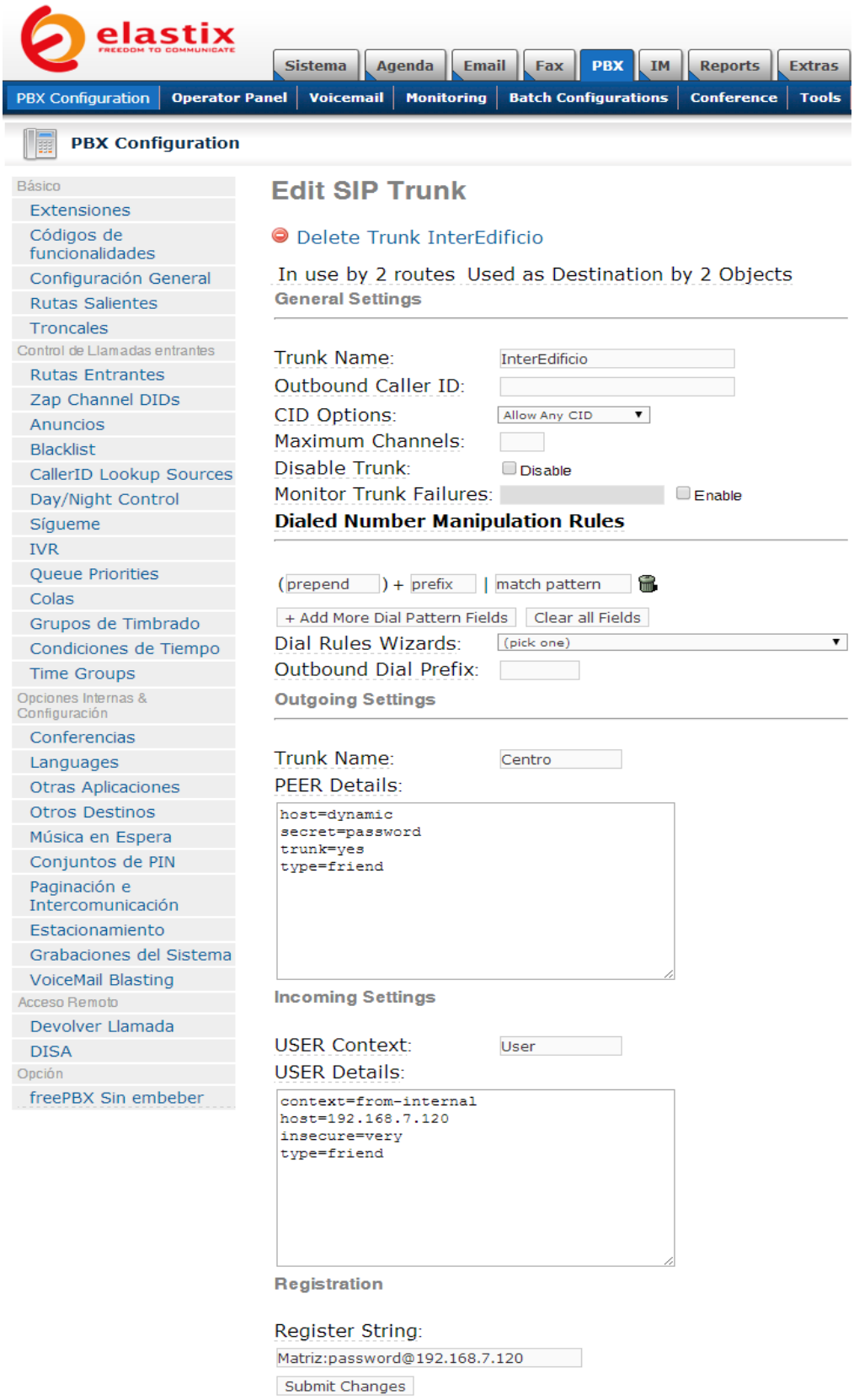


Figura 5.29 *– Trocal para interconectarse con la otra PBX – Config. Centro*
Fuente: *[el Autor]*

Figura 5.30 *– Configuración de ruta para interconexión entre PBX – Matriz*
Fuente: *[el Autor]*

Figura 5.31 *– Configuración de ruta para interconexión entre PBX – Centro*
Fuente: *[el Autor]*

Para verificar la interconexión entre las PBX, podemos entrar a la consola del servidor y escribir el comando ***asterisk –vvvvvr***, para entrar a la administración de *asterisk*, y con el comando especifico ***sip show registry***, se mostrará las conexiones entre los servidores, tal y como se muestra en las figuras 5.32 y 5.33 correspondiente a la consola de la matriz y del centro respectivamente.

```
ElastixMatriz*CLI> sip show registry
Host                                    dnsmgr Username       Refresh State
          Reg.Time
192.168.7.220:5060                      N      Centro             105 Registered
          Sun, 30 Mar 2014 10:31:48
1 SIP registrations.
ElastixMatriz*CLI>
```

Figura 5.32 *– Registro de conexión a la PBX remota – PBX Matriz*
Fuente: *[el Autor]*

```
ElastixCentro*CLI> sip show registry
Host                                    dnsmgr Username       Refresh State
          Reg.Time
192.168.7.120:5060                      N      Matriz             105 Registered
          Sun, 30 Mar 2014 10:32:14
[redacted]:5060                         N      9000               105 Registered
          Sun, 30 Mar 2014 10:32:50
2 SIP registrations.
ElastixCentro*CLI>
```

Figura 5.33 *– Registro de conexión a la PBX remota – PBX Centro*
Fuente: *[el Autor]*

En la segunda figura, se visualiza dos conexiones, las cuales se encuentran establecidas, lo cual se puede corroborar en la columna de estado donde se muestra la palabra “Registered”; una corresponde a la *PBX* remota (del otro edificio), y la otra a una extensión *SIP*, que el Gobierno Autónomo Descentralizado de Portoviejo, tiene con la Empresa (por medio de un enlace privado), con la intensión de comunicarse con los funcionarios de la parte Directiva, ya que tiene inherencia por ser una Empresa Municipal.

Para configurar este conexión con el GAD, se procede de la misma forma que las anteriores, se configura la troncal *SIP*, y luego la ruta saliente (se debe crear en ambas *PBX*), tal y como se muestra en las figuras 5.34, 5.35 y 5.36

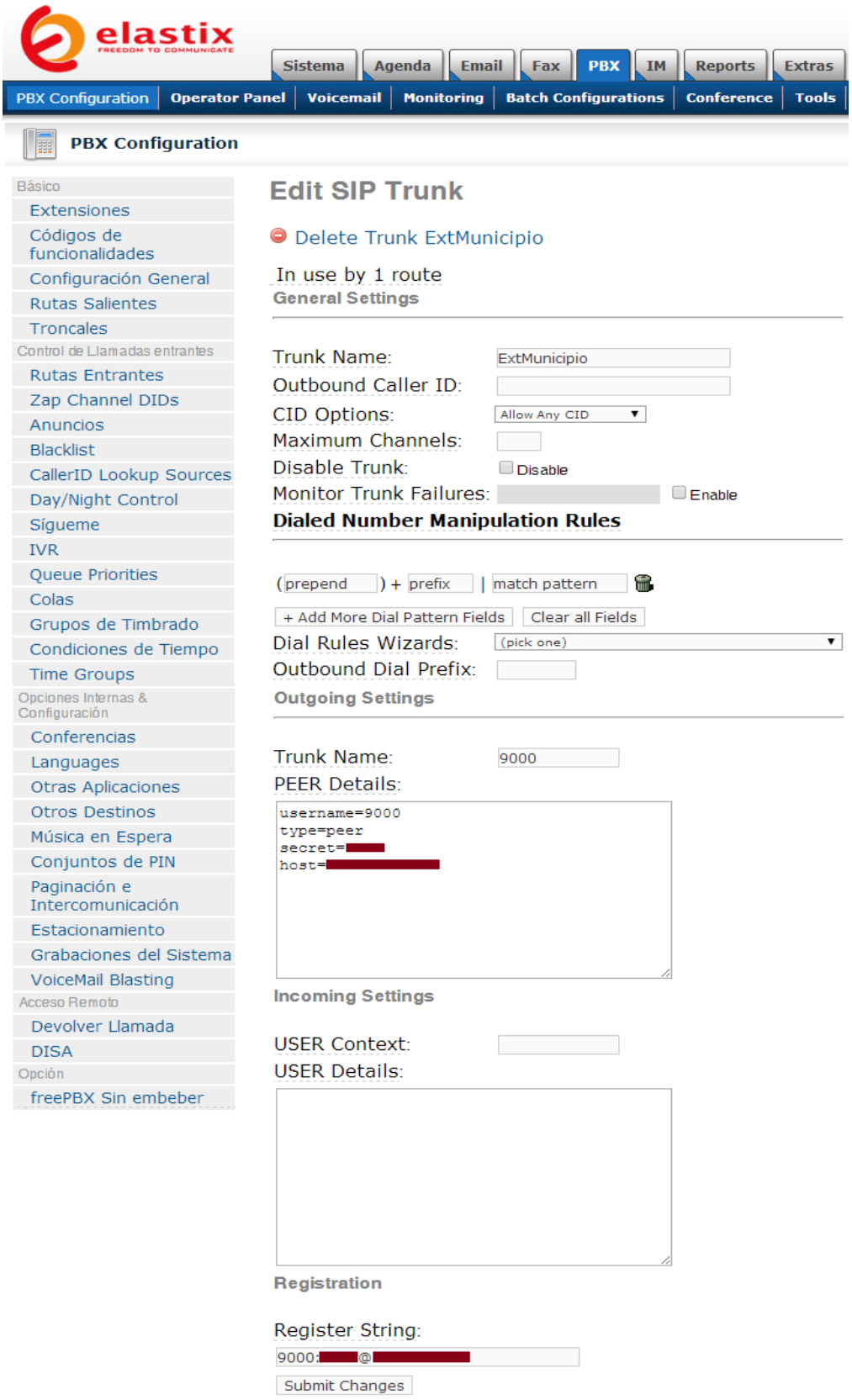


Figura 5.34 *– Trocal para interconectarse con PBX GAD – Config. Centro*
Fuente: *[el Autor]*

Figura 5.35 *– Configuración de ruta saliente a PBX GAD – Matriz*
Fuente: *[el Autor]*

Esta ruta saliente configurada del lado del edificio matriz, indica en la condición de marcado, que si se realiza una llamada a una extensión que comience con 9 (extensiones SIP del GAD), ésta saldrá por la troncal “InterEdificio”, la cual corresponde a la interconexión entre las dos PBX, ya que la llamada debe enrutarse por el enlace de fibra a la PBX del Centro y esta dirigirá a la trocal del GAD como destino final.

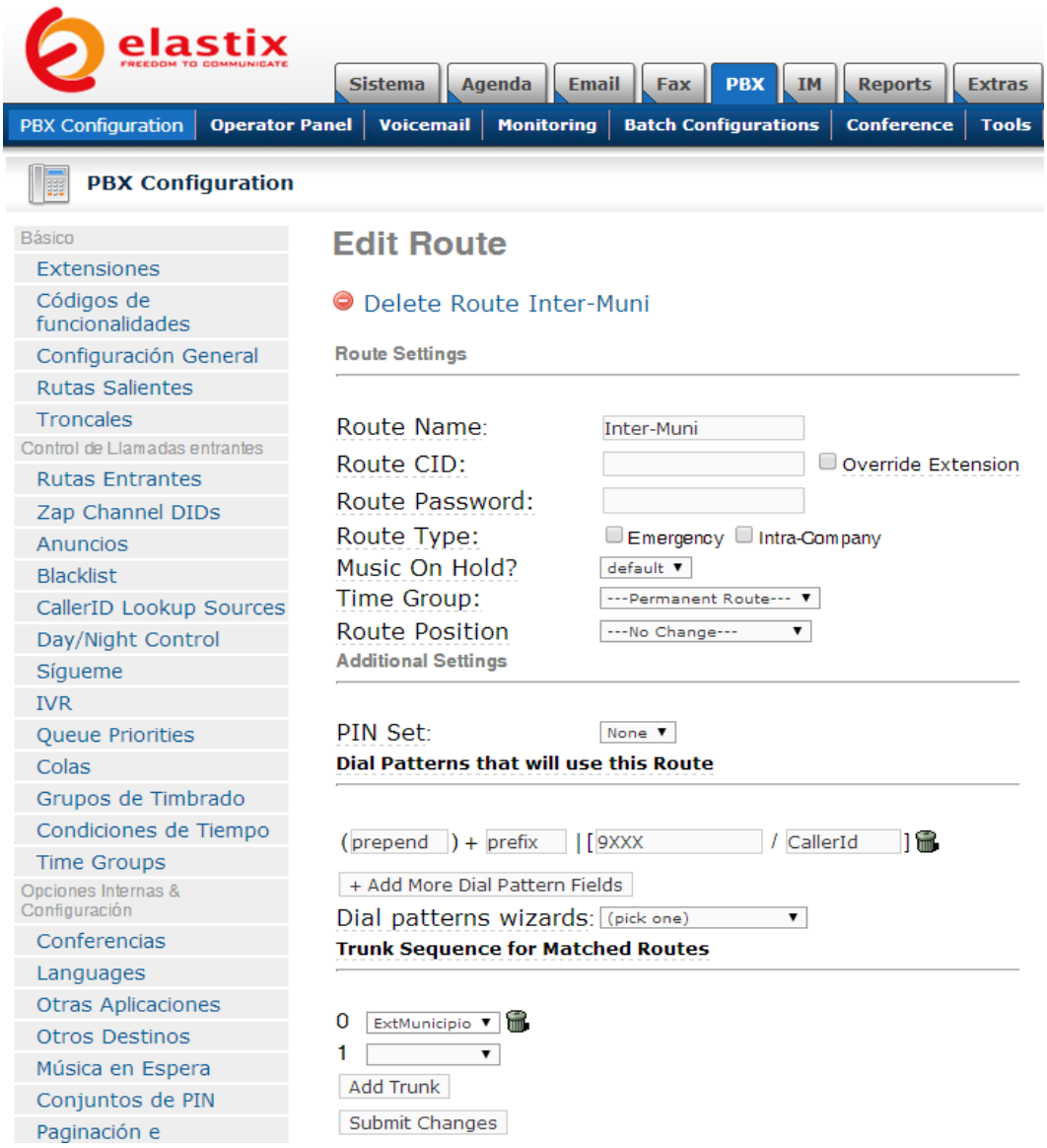


Figura 5.36 *– Configuración de ruta saliente a PBX GAD – Centro*
Fuente: *[el Autor]*

Esta ruta saliente configurada del lado del edificio central, indica en la condición de marcado, que si se realiza una llamada a una extensión que comience con 9 (extensiones *SIP* del GAD), ésta saldrá por la troncal "ExtMunicipio", la cual interconecta entre *PBX* Centra y la del GAD, dando posibilidad a comunicarse con funcionarios del Municipio.

5.8. Configuración de servicio IM

El servicio *IM* (Mensajería Instantánea), es un servicio que complementaria al objetivo principal, de brindar medios de comunicación oportuna, aunque una llamada es una forma de comunicación directa, la mensajería instantánea, es un opción ventajosa en el caso que un funcionario no pueda recibir una llamada y no se establezca la comunicación, mientras que un mensaje puede ser revisado en el momento que el funcionario se ponga operativo nuevamente y responder para completar la comunicación.

El *Elastix*, brinda este servicio por medio del *OpenFire*, el cual viene preconfigurado, requiriendo la configuración del usuario administrador, y determinando si se conecta a una base de datos propia, o externa, para este caso se trabaja con una base de datos local (propia), y luego proceder con el registro de los usuarios y sus grupos respectivo.

Dentro del servicio ***IM***, luego de haber realizado las configuraciones preliminares, y haber logueado (figura 5.37) con el usuario administrador, se debe seleccionar el menú ***Usuarios/Grupos***, y escoger la opción ***Crear Nuevo Usuario***, y proceder al registro de cada uno de los usuarios, como se visualiza en la figura 5.38.

Este procedimiento se lo debe realizar en cada uno de los servidores, con el conjunto de usuarios que le pertenece a cada edificio, el cual se podrá interconectar luego que se realice las configuraciones de integración en los servidores, para el servicio IM.

Figura 5.37 *– Inicio de sesión del servicio IM*
Fuente: *[el Autor]*

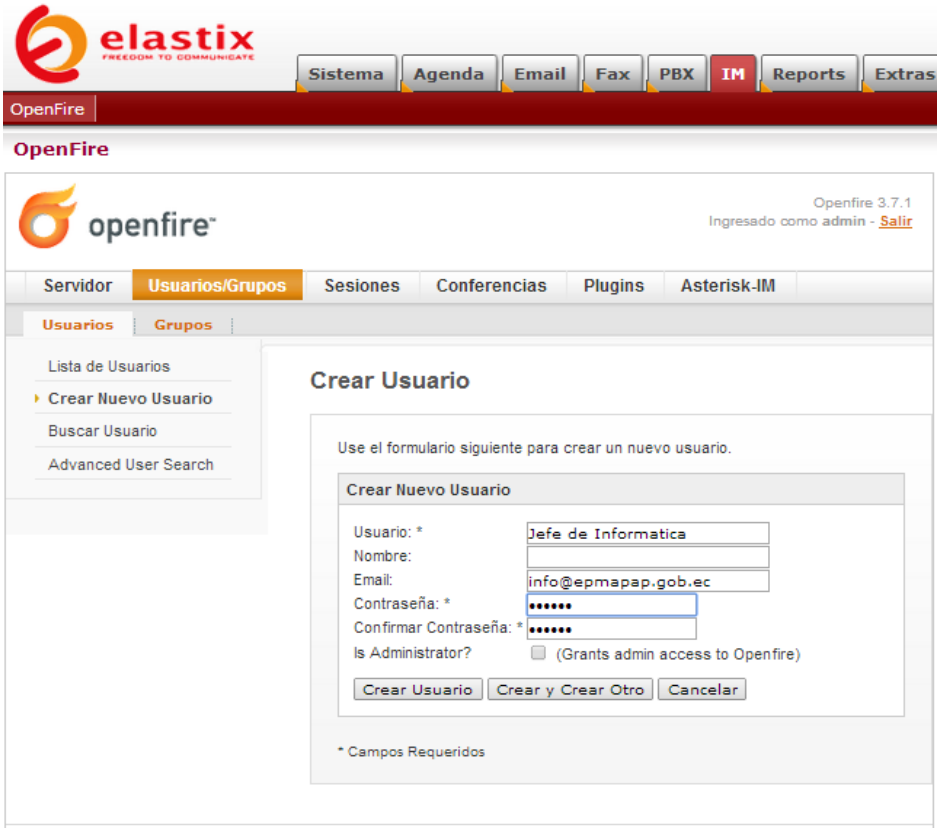


Figura 5.38 *–Registro de usuario en servicio IM*
Fuente: *[el Autor]*

Figura 5.39 *– Registro de etiqueta de grupos en servicio IM*
Fuente: *[el Autor]*

Una vez que se hayan registrado todos los usuarios, y los nombres de grupos (como se observa en la figura 5.39), se debe conformar al conjunto de usuarios que pertenecerán al grupo, para ello se entra a ***Grupos***, ***Listado de Grupos***, se selecciona uno, y se procede a incorporar uno a uno los Usuarios que lo conforman, escribiendo el nombre en el casillero de ***Agregar Usuario*** y luego dando click en el botón ***Agregar***.

Para que estos usuarios puedan ser vistos por otros usuarios dentro del mismo servidor, se debe activar la opción, ***Enable contact list group sharing***, luego escribir el mismo nombre del grupo en el cuadro de ***texto Enter contact list group name***, y se debe seleccionar el/los grupo(s) en el listado (***The following groups***), o que puedan verse con todo los usuarios (***All users***), tal como se muestra en la figura 5.40.

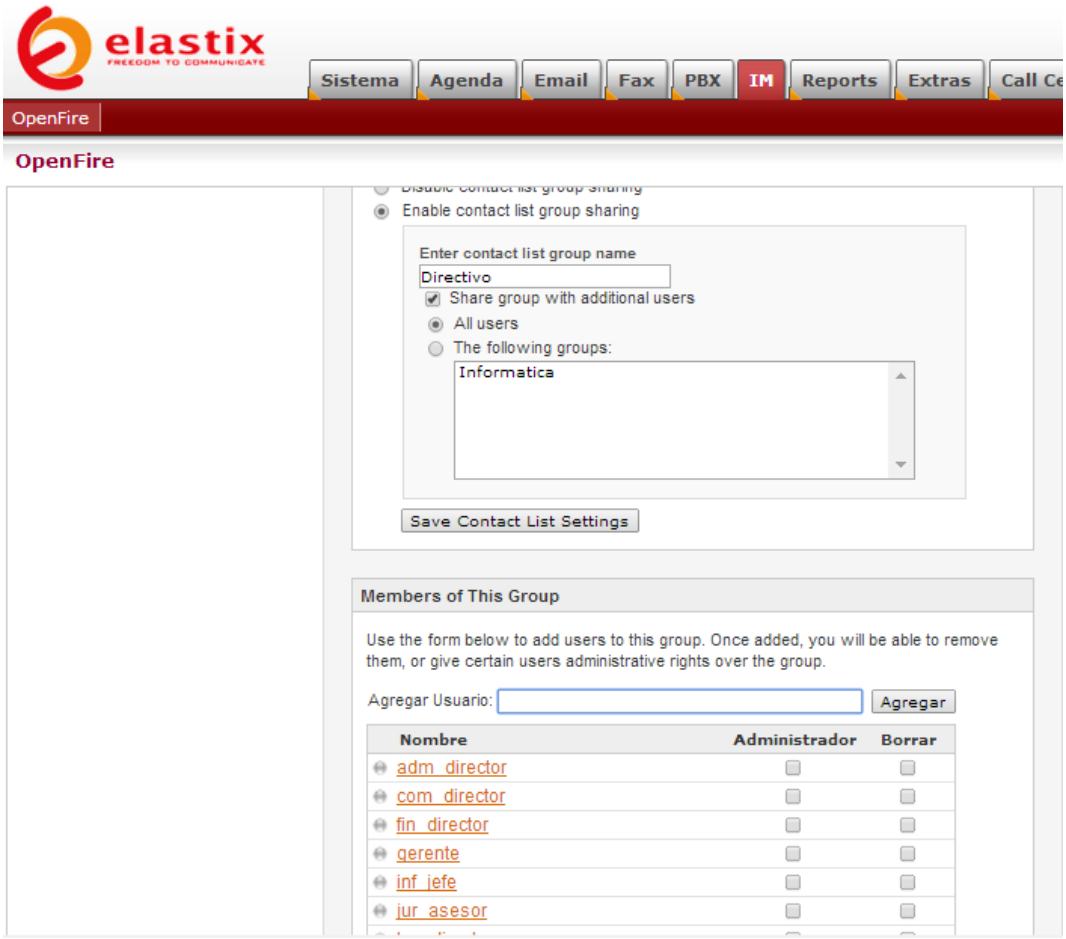


Figura 5.40 *– Configuración de los usuarios en los grupos*
Fuente: *[el Autor]*

5.9. Integración entre servidores del servicio IM

La integración entre servidores IM, es una solución para que los usuarios de cada edificios (configurado localmente), pueda tener acceso entre ellos, esta estrategia es ideal, para que cada grupo de usuarios dentro de un mismo edificio, tenga independencia, y de esta manera, si se llega a caer el enlace que une a cada edificio, todos los usuarios sigan teniendo comunicación con los usuarios locales, a diferencia de que todos los usuarios se configuren en un único servidor para ganar visibilidad y disponibilidad aparente.

Para realizar esta integración, se debe ingresar a las opciones de ***Servidor***, y seleccionar la pestaña ***Configuración de Servidor***, y dar click en la opción ***Servidor a Servidor***, y en el cuadro de texto Dominio, se debe agregar la IP del server remoto al cual se le permitirá la conexión, tal y como se observa en la figura 5.41; esto se debe de realizar en ambos servidores.

Figura 5.41 *– Configuración de los usuarios en los grupos*
Fuente: *[el Autor]*

5.10. Logueo de cuentas, en clientes IM para PC y Smartphone

Para configurar los usuarios *IM*, en la aplicación cliente, basta con instalar un cliente *IM*, en este caso *Spark*, y loquear con el usuario y clave que se configuraron en el servidor, para ello se registra el nombre de usuario, contraseña, y dirección IP del servidor para poder conectarse, luego que inicia sesión el usuario, se mostrara los grupos con los que compartirá comunicación (figura 5.42).

Para que los usuarios entre servidores (ubicados uno en cada edificio), pueden compartir comunicación, primero de debe haber realizado la configuración de integración en los servidores, y luego desde la aplicación cliente IM, o desde las opciones del servidor, se puede realizar invitación de conexión, las cuales una vez aceptadas, los usuarios de un edificio con los otros (a los cuales ha invitado), podrán ser visibles y establecer comunicaciones.

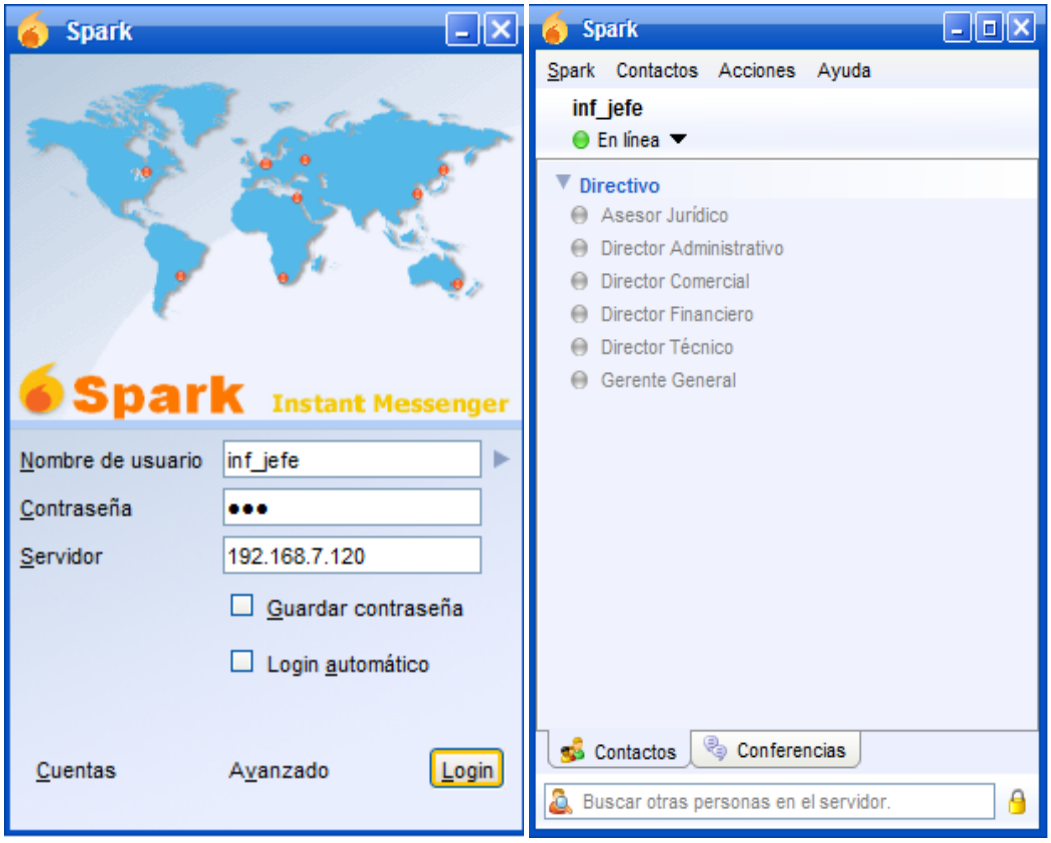


Figura 5.42 *– Cliente IM – Spark*
Fuente: *[el Autor]*

Existen algunos clientes IM (software), que integran una interfaz donde un usuario IM, tiene opciones a recibir o llamar por medio de la *PBX*, para realizar esta integración, se debe proceder a instalar el plugins Asterisk-*IM Openfire Plugin*

(figura 5.43), y luego verificar el archivo, donde consta la definición de la BD, el cual permite el registro de la integración, ya que en las versiones resientes del *Elastix*, existe un problema de compatibilidad.

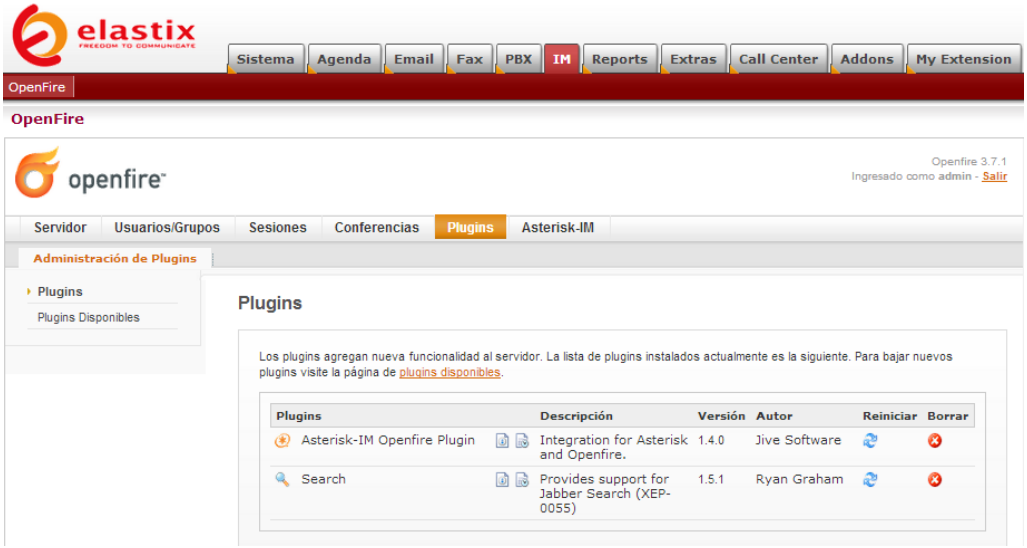


Figura 5.43 *– Instalación, Asterisk-IM OpenFire Plugin*
Fuente: *[el Autor]*

En el archivo /opt/openfire/plugins/asterisk-im/database/asterisk-im_hsqldb.sql se debe verificar que todos los campos de las tablas que aceptan valores nulos, deben no aceptarlos y aumentarle la palabra NOT, tal y como se muestra en la figura 5.44.

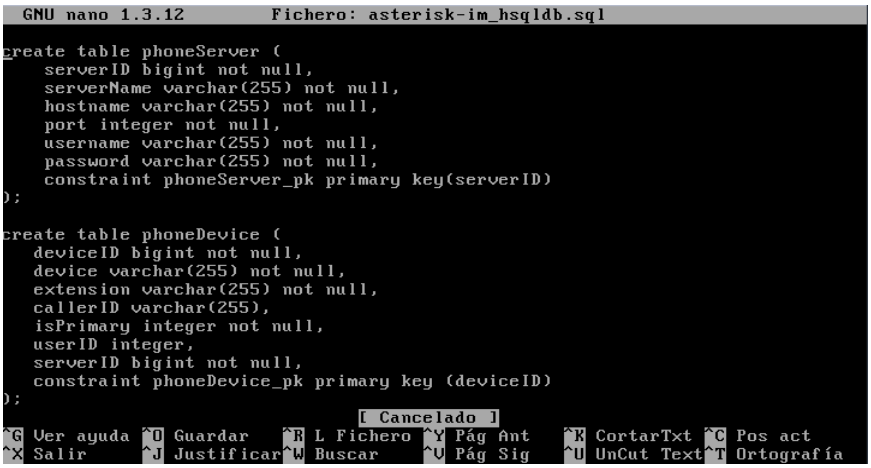


Figura 5.44 *– Edición de archivo asterisk-im_hsqldb.sql*
Fuente: *[el Autor]*

Luego, desde el panel de administración del *Elastix*, en las opciones de *OpenFire*, se debe buscar la pestaña nueva creada "**Asterisk-IM**", luego de la

instalación del *plugins*, donde en la opción ***General Settings***, se debe configurar datos del servidor local para vincular el servicio *VoIP* con el *IM*, tal y como se visualiza en la figura 5.45.

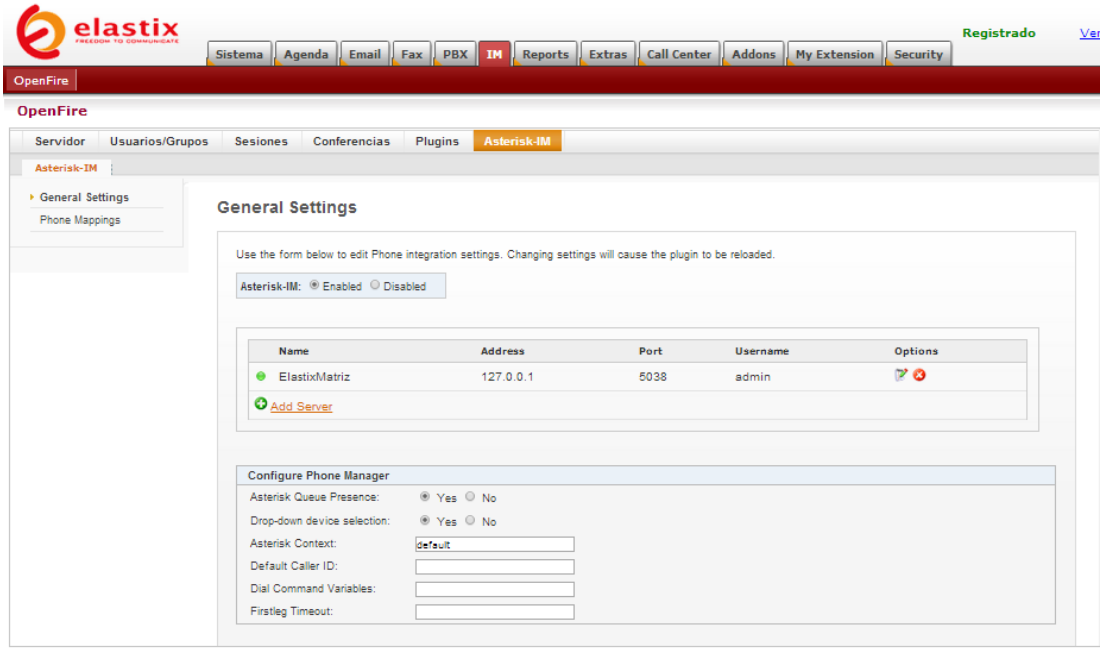


Figura 5.45 *– Vinculación servicios VoIP e IM*
Fuente: *[el Autor]*

Finalmente, en ***Phone Mappings***, se debe registrar las extensión VoIP asignada al funcionario, a la cuenta IM correspondiente, tal y como lo demuestra la figura 5.46.

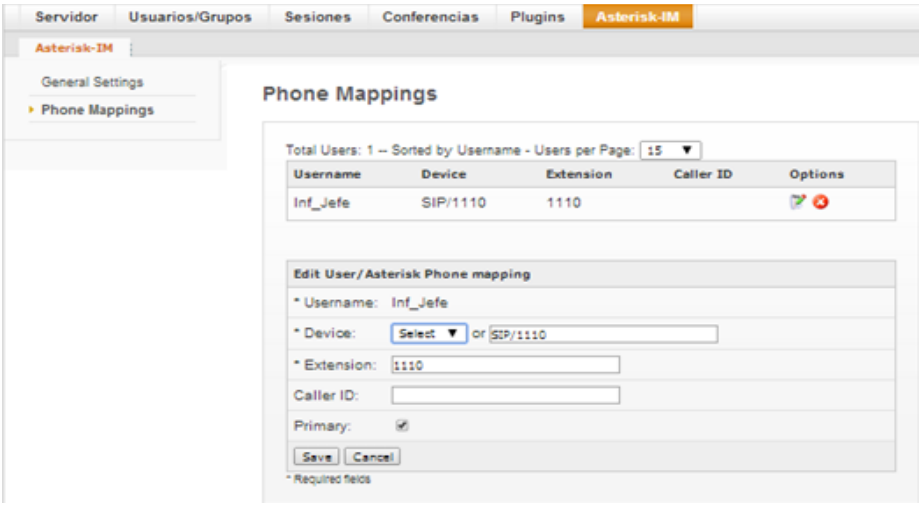


Figura 5.46 *– Vinculación de extensiones VoIP con user IM*
Fuente: *[el Autor]*

5.11. Integración entre PBX Elastix y Central Panasonic TDA-100

La EPMAPAP, cuenta con una central analógica de marca Panasonic TDA-100, la cual actualmente se encuentra funcionando, esta central se puede mantener, y aprovecharla en conjunto con el servidor *Elastix* como un sistema híbrido, tomándola como trocal para la líneas de telefonía fija, además de utilizarla como alternativa de backup, en caso que el servidor Elastix quede inoperativo temporalmente, con este justificativo, se incluye a continuación una alternativa, la cual puede ser acogida por el DSI, si cree conveniente mantener un sistema hibrido de extensiones IP y extensiones análogas, y se justifica el costo de la adquisición de la tarjeta.

Para realizar esta implementación, se debe utilizar una tarjeta E1, que permita la conexión entre el servidor *Elastix* y la central Panasonic, para este caso, una opción es la Digium TE220 PCI Express, la cual consta de 2 puertos (T1/E1), como se muestra en la figura 5.47.

Figura 5.47 *– Tarjeta PCI Express, Digium TE220 2 puertos (T1/E1)*
Fuente: *[internet]*

Luego se procede a la configuración de la tarjeta en el servidor, siempre y cuando no se haya configurado automáticamente, para ello, accedemos al archivo /etc/dahdi/system.conf, donde debe constar las siguientes configuraciones, tal y como se muestra en la figura 5.48, aclarando que en el caso del cancelación de eco, si en la tarjeta se incorporar el módulo opcional (VPMOCT064M), no debe incluirse el parámetro ***oslec***, el cual encarga a la CPU del servidor, realizar la tarea en caso que la tarjeta no incluya el módulo de cancelación de eco.

```
#Span 2: TE2/0/2 “T2XXP (PCI) Card 0 Span 2”
span=2,2,0,ccs,hdb3
bchan=32-46,48-62
dchan=47
echocanceller=oslec,32-46,48-62
```

Figura 5-48 *– Configuración del archivo system.conf* ***¡Error! Marcador no definido.***

Fuente: *[el Autor]*

Cabe indicar, que las configuraciones detalladas, toman al segundo puerto para la interconexión, dejando libre el primero por si en algún momento se contratara una trocal SIP al proveedor de telefonía fija.

Adicional a lo anterior, también se debe realizar la configuración en el archivo /etc/asterisk/dahdi-channels.conf, como se muestra en la figura 5.49.

```
#Span 2: TE2/0/2 “T2XXP (PCI) Card 0 Span 2”
group=1
context=from-internal
switchtype=qsig
signalling=pri_net
channel=>32-46,48-62
```

Figura 5-49 *– Configuración del archivo dahdi-channels.conf*

Fuente: *[el Autor]*

Luego de realizar las configuraciones de la tarjeta, se debe proceder a conectar mediante cable, el servidor (por medio de la tarjeta E1) a la central Panasonic, para ello, hay que fabricar el cable que permita esta conexión, como se indica en la siguiente figura.

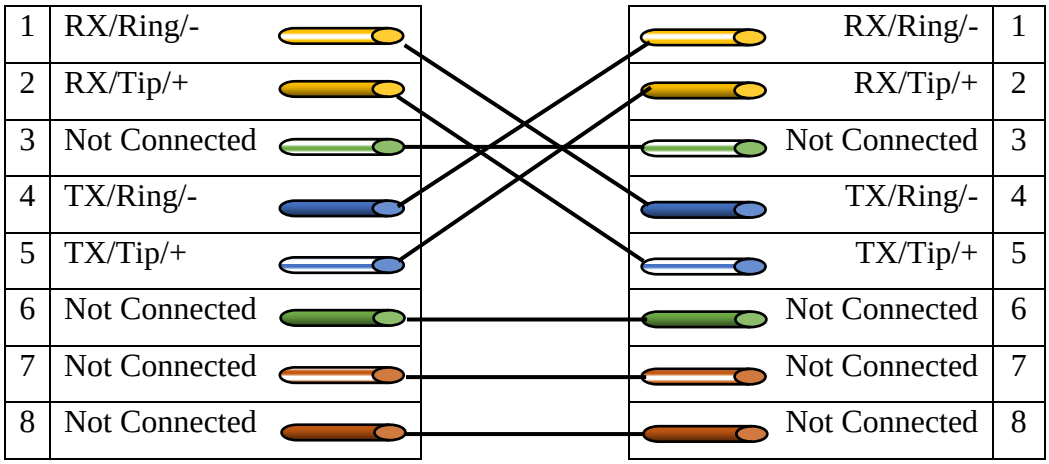


Figura 5-50 *– Diseño de cable para conectar servidor con central Panasonic*

Fuente: *[el Autor]*

Finalmente se debe realizar configuración de troncal, para que cuando se quiera tener acceso a una línea fija y/o extensiones análogas, se enruten las llamadas por medio de esta troncal, para lo cual también hay que realizar la configuración respectiva, tal y como se ha explicó anteriormente, y consta en las figuras 5.26 y 5.27.

Cabe indicar, que la central Panasonic, ya cuenta con su propio plan de marcado, al cual se debe ajustar las configuraciones que se realice en las condiciones de marcado, de la ruta saliente en el servidor PBX.

Conclusiones

De acuerdo a las pruebas realizadas, se pudo determinar que el volumen de tráfico generado por los aplicativos de la empresa, constituyen al 22.92% del ancho de banda, llegando escasamente a un 40% en horarios picos, de lo cual denotamos que la disponibilidad del enlace de datos que interconecta a los edificios, es del 60% al 77,08%. Con este porcentaje de disponibilidad se puede lograr tener de entre 3 a 4 llamadas simultaneas, o 7 a 8 llamadas si se activa la opción de supresión de silencio en los servidores *PBX* (lo cual es lo recomendable), empleando el protocolo G711 u-law que viene por default en Asterisk, cuyo tamaño de paquete generado es de 168 kbps.

Respecto a las pruebas de *QoS,* se pudo determinar que los problemas de, *jitter*, retardo y pérdida de paquetes, se da cuando un paquete pasa por varios ruteadores, o dominios de *broadcast* que puedan incidir en el retardo de los paquetes *VoIP*, y como cada edificio cuenta con su propia red local categoría (5e en uno y 6e en otro), no se experimentaron ninguno de estos problemas, sin embargo, cuando se realizaron llamadas simultaneas inter-edificios, se pudo experimentar aumento de latencia, donde los tiempos de *jitter*, fueron incrementando a medida se aumentaban las llamadas simultaneas, cuyos valores siempre se encontraron dentro de los parámetros normales y no causaron ningún problema en la comunicación. En cuanto a los casos de aumento de latencia, se dieron por la saturación en el ancho de banda, cuando se llevó al máximo de consumo permitido, cuya recomendación, seria de separar el tráfico por *vlan*, y aumentar el *buffer Jitter* en los equipos (teléfonos IP, *SoftPhone*), para garantizar la *QoS* en la comunicación, o implementar el proyecto de enlace propio que fue propuesto por el DSI.

En cuanto, al uso de las líneas de telefonía fija se deja claro que, con la presente propuesta, se dará el 100% de *GOS* para llamadas exclusivamente externas, lo cual no se daba en la realidad, ya que estás líneas eran usadas (según monitoreo tabulado en la tabla 3.1), para llamadas inter-edificios, las cuales ahora serán canalizadas por la red interna empleando el sistema de *VoIP*, y por ende disminuirá la probabilidad de bloqueo o negación del servicio para este tipo de llamadas.

Con todo lo expuesto, se puede determinar que el ***Tráfico de Datos*** generado por el sistema *VoIP* e *IM* utilizando la ***Herramienta Open Source*** *Elastix*, en los parámetros

definidos y con la ***Tecnología de protocolo de comunicación*** escogido, puede ser soportado por la ***Infraestructura de comunicación existente***, lo cual sustenta la factibilidad tecnológica del presente estudio.

La factibilidad económica, es sustentada en el hecho, que al usar un *software Open Source* (sin costo de licencia), cuyo requerimiento de hardware es mínimo, y podría ser instalado sobre PC´s normales, el hecho de aprovechar la infraestructura ya existente, y, utilizar las computadoras como teléfonos por medio de los *SoftPhone*, quedando pendiente solo la compra de la tarjeta para troncalizar las líneas de telefonía fija, las cuales son de bajo costo y fácil acceso, garantiza a la institución, que la implementación de este sistema de comunicación, no significa mayor inversión de costes.

Y finalmente, con los resultados obtenidos en las encuestas (figura 4.13), se demuestra la aceptación que tienen los usuarios de esta tecnología, corroborando así la hipótesis, concluyendo que, a un costo muy bajo, y aprovechando la infraestructura existente en los edificios para la transmisión de datos, se puede transmitir voz, integrando *PBX´s VoIP* y como comunicación complementaria el servicio *IM*, empleando la distribución *Open Source* de comunicación unificada *Elastix* en los edificios de la EPMAPAP, cuya ingeniería de implementación, ha sido definida como una propuesta que garantizará un alto grado de prestaciones, cuyos servicios integrados funcionaran también de forma independencia intra-edificio, con la finalidad de brindar disponibilidad de servicios, para el personal administrativo.

Recomendaciones

- Implementar la propuesta como una solución a las necesidades determinadas, la cual está respaldada en la factibilidad técnica y económica, fundamentada en la presente tesis.

- Realizar las configuraciones necesarias en los equipos activos para mejorar la QoS del servicio de VoIP, cuyas configuraciones se incorporados en la sección de anexo (extraído de los manuales técnicos de los equipos).

- Brindar capacitaciones periódica al personal que presente problema en la utilización de esta tecnología como herramienta de trabajo, para que obtenga los mayores beneficios de la misma.

- Reservar ancho de banda del internet, para que el personal directivo se conecte a la PBX por medio del internet.

- Considerar la propuesta del DSI, de instalar un enlace propio de fibra, para no estar limitado al mega clear channel que esta arrendado al ISP.

Referencia Bibliográfica

1. Ahmed, A., Madini, H., & Siddiqui, T. (2011). *VoIP Perfomance Management and Optimization* (Ingles 1ª ed.). USA: Cisco Press.

2. Cabezas, J. D. (2007). *Sistemas de telefonía* (Español 1ª ed.). España: Thomson.

3. Carballar, J. A. (2007). *VoIP. La Telefonía de Internet* (Español 1ª ed.). España: Thomson.

4. Castro, A., & Fusario, R. J. (1999). *Teleinformática para Ingenieros en Sistemas de Información* (Español 2ª ed.). Barcelona: Reverté.

5. Cisco. (02 de 02 de 2006). *Voice Over IP – Per Call Bandwidth Consumption.* Recuperado el 02 de 10 de 2013, de http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml: http://www.cisco.com/image/gif/paws/7934/bwidth_consume.pdf

6. Corporación Nacional de Telecomunicaciones. (30 de 07 de 1992). *Ley Especial de Telecomunicaciones reformada.* Recuperado el 05 de 10 de 2013, de http://www.cnt.gob.ec/images/Pdfs/normas_regulatorias/LEY%20ESPECIAL%20DE%20TELECOMUNICACIONES%20REFORMADA.pdf

7. Corporación Nacional de Telecomunicaciones. (13 de 03 de 2000). *Reglamento General a la Ley Especial de Telecomunicaciones.* Recuperado el 05 de 10 de 2013, de https://www.cnt.gob.ec/images/Pdfs/normas_regulatorias/REGLAMENTO%20GENERAL%20A%20LA%20LEY%20ESPECIAL%20DE%20TELECOMUNICACIONES.pdf

8. Dwivedi, H. (2008). *Hacking VoIP: Protocols, Attacks, and Countermeasures,* (Ingles 1ª ed.). San Francisco: No Starch Press.

9. Elastix Freedom Communicate. (s.f.). *Características*. Recuperado el 05 de 10 de 2013, de http://www.elastix.org/index.php/es/informacion-del-producto/caracterisiticas.html

10. Elastix Freedom Communicate. (n.d.). *Información del Producto*. Retrieved 10 05, 2013, from http://www.elastix.org/index.php/es/informacion-del-producto/informacion.html

11. Ernesto. (24 de 01 de 2013). *Ancho de banda utilizado por VoIP*. Recuperado el 01 de 11 de 2013, de http://www.3cx.es/ancho-de-banda-voip/

12. Ford, K. (1998). *Tecnologías de interconectividad de redes Cisco Press.*

13. Fryer, B. (31 de 10 de 2010). *Elastix 2.0 – Installation Guide.* Recuperado el 01 de 11 de 2013, de http://sourceforge.net/projects/elastix/files/Tutorials_Docs_Manuals/Elastix%202.0%20Guides/ELASTIX%202%20Installation%20Guide.pdf/download

14. Ganguly, S., & Bhatnagarm, S. (2008). *VoIP: Wireless, P2P and New Enterprise voice over IP* (Ingles 1ª ed.). USA: Wiley.

15. Herrera, E. (2004). *Introducción a las Telecomunicaciones Modernas* (Español 1ª ed.). México: Limusa.

16. Hewlett-Packard. (s.f.). *User Guide - HP 1910 Fast Ethernet Switch Series.* Recuperado el 02 de 11 de 2013, de http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c03941555-1.pdf

17. Huidobro, J. M., & Conesa, P. R. (2006). *Sistemas de Telefonía* (Español 5ª ed.). España: Thomson.

18. Huidoro, J. M., & Ronald, D. (2003). *Integración de Voz y Datos.* Madrid: McGraw-Hill.

19. Iñigo, J., Barceló, J., Cerdá, L., Peig, E., Abella, J., & Corral, G. (2008). *Estructura de redes de computadores* (Español 1ª ed.). España: Edirotial UOC.

20. Iversen, V. B. (2010). *Teletraffic Engineering and Network Planning.* Recuperado el 01 de 11 de 2013, de ftp://ftp.dei.polimi.it/outgoing/Flaminio.Borgonovo/Teoria/teletraffic_Iversen.pdf

21. Keagy, S. (2001). *Integración de Redes de Voz y Datos. .* Madrid: Perason Educación, S.A. Cisco Systems.

22. Landivar, E. (2011). *Comunicaciones Unificadas con Elastix. Volumen 1 (Español 2ª ed.).* Recuperado el 01 de 11 de 2013, de http://www.elastixbook.com/libros/cuce/vol1/es/Indice.html

23. Linksys a Division of Cisco. (s.f.). *User Guide – Business Series.* Recuperado el 02 de 10 de 2013, de http://www.cisco.com/en/US/docs/switches/lan/csbms/srw2048/administration/guide/SRW-US_v10_UG_A-Web.pdf

24. M. Á. M. Diariocrítico. (20 de 06 de 2013). *Un antecedente del espionaje norteamericano y británico: la red Echelon, base del 'programa Prism'*. Recuperado el 02 de 10 de 2013, de http://www.diariocritico.com/nacional/seguridad-en-internet/espionaje-ciudadanos-eeuu/437273

25. Magaña, E., Izkue, E., Prieto, M., & Villadangos, J. (2003). *Comunicaciones y redes de computadores* (Español 1ª ed.). Madrid: Pearson Educación.

26. Packetizer, Inc. (s.f.). *VoIP Bandwidth Calculator*. Recuperado el 01 de 11 de 2013, de http://www.bandcalc.com/es/

27. Palosanto Solutions. (s.f.). *Manual del Usuario en Español (Beta) – Elastix 0.9-alpha.* Recuperado el 01 de 11 de 2013, de http://sourceforge.net/projects/elastix/files/Tutorials_Docs_Manuals/User%20Manual%200.9-alpha%20%28Spanish%29/Elastix_User_Manual_Spanish_0.9-alpha.pdf/download

28. Porter, T., Baskin, B., Chaffin, L., Cross, M., Kanclirz, J. R., Shim, C., y otros. (2003). *Practical VoIP Security* (Ingles 1ª ed.). Canada: Syngress.

29. Tom Burghardt Global Research. (13 de 07 de 2013). *ECHELON Today: The Evolution of an NSA Black Program.* Recuperado el 02 de 10 de 2013, de http://www.globalresearch.ca/echelon-today-the-evolution-of-an-nsa-black-program

30. Tomasi, W. (2003). *Sistemas de Comunicaciones Electrónicas* (Español 4ª ed.). México: Pearson Educación.

31. Wallace, K. (2005). *Voice Over IP First-Step* (Ingles 1ª ed.). USA: Cisco Press.

Glosario

3CXPhone = Cliente VoIP

Arpanet = Advanced Research Projects Agency Network

Buffer = Espacio de memoria, reservada para almacenamiento temporal

BRI = Basic Rate Interface

Callback = proceso de volver a llamar a un número, previo a haber colgado..

CAS = Channel-Associated Signaling

CCITT = Consultative Committe International Telegraphy and Telephony

CCS = Common-Channel Signaling

CDR = Call Detail Record

Cisco = Empresa (marca), de equipos de comunicación

Clear Channel = Definición de canal limpio o integro en los tunel de datos

DAHDI = Digium Asterisk Hardware Driver Interface

DataPlan = Plan de marcado de una PBX

DISA = Direct Inward System Access

DTMF = Dual-Tone Multi-Frequency

Elastix = Distribución Linux, con sistemas de comunicación unificada

ERLANG = Medida estadística del volumen de tráfico usada en telefonía

Ethernet = Estándar de redes de área local

Fax-a-email = Servicio de fax por correo por internet

FXO = Foreign eXchange Office

FXS = Foreign eXchange Station

GOS = Grade Of Service (Grado de servicio)

GSTB = General Switched Telephone Network

IAX = Inter-Asterisk eXchange

IM = Instant Messaging

IP = Internet Protocol

ISDN = Integrated Services Digital Network

ISP = Internet Service Provider

IVR = Interactive Voice Response

Jitter = Variabilidad temporal durante el envío de señales digitales

LAN = Local Area Network

LCR = Least Cast Routing

Mbps = Megabit por segundo

MPLS = Multiprotocol Label Switching

OSI = Open System Interconnection

OverHead = Encabezado de un paquete

PBX = Public Branch eXchange

PABX = Private Automatic Branch Exchange

PENTEST = Método de evaluación de seguridad

PRI =Primary Rate Interface

PSTN = Public Switched Telephone Network

PYMES = Pequeñas y medianas empresas

QoS = Quality of Service

RDSI = Red Digital de Servicios Integrados

RTP = Real-time Transport Protocol

SmartPhone = Teléfono móvil inteligente

SoftPhone = Software de PC que emula a un teléfono IP

SOS = Software Open Source

Spark = Cliente de mensajería instantánea

VirtualBox = Software para virtualizar maquinas

VoIP = Voice over IP

Zoiper = Cliente VoIP

Anexos

ANEXO 1

Modelo de Encuesta – Elaborada desde

Google Drive

Configuración del formulario

Mostrar barra de progreso en la parte inferior de las páginas del formulario

Página 1 de 1

Formulario - Encuesta

Encuesta de satisfacción del proyecto piloto de Telefonía VoIP y del servicio IM

Sistema de comunicación telefónico*
Durante la prueba piloto con el sistema VoIP, Ud. logró establecer más llamadas que con el sistema de telefonía tradicional.

- Totalmente de acuerdo
- De acuerdo
- Indiferente
- En desacuerdo
- Totalmente en desacuerdo

Sistema de comunicación telefónico*
Usar un softphone es igual de sencillo que usar un teléfono físico

- Totalmente de acuerdo
- De acuerdo
- Indiferente
- En desacuerdo
- Totalmente en desacuerdo

Sistema de comunicación telefónico*
La calidad de la voz, durante las llamadas telefónicas con el sistema propuesto fue:

- Excelente
- Muy Buena
- Buena
- Regular
- Suficiente

Sistema de comunicación telefónico*
Disponer de su propia extensión telefónica instalada en su smartphone, le permitirá comunicación oportuna.

- Totalmente de acuerdo
- De acuerdo
- Indiferente
- En desacuerdo
- Totalmente en desacuerdo

Sistema de comunicación telefónico*
Preferiría al sistema telefónico tradicional por el sistema propuesto

- Totalmente de acuerdo
- De acuerdo
- Indiferente
- En desacuerdo
- Totalmente en desacuerdo

Mensajería Instantánea*
Considera útil el servicio de IM para sus labores diarías

- Totalmente de acuerdo
- De acuerdo
- Indiferente
- En desacuerdo
- Totalmente en desacuerdo

Mensajería Instantánea*
Disponer del servicio IM instalado en su smartphone, le permitirá comunicación oportuna.

- Totalmente de acuerdo
- De acuerdo
- Indiferente
- En desacuerdo
- Totalmente en desacuerdo

Añadir elemento

Página de confirmación

Hemos registrado tu respuesta.

- Mostrar enlace para enviar otra respuesta
- Publicar y mostrar un enlace público a los resultados del formulario
- Permitir que los encuestados editen las respuestas después de enviarlas

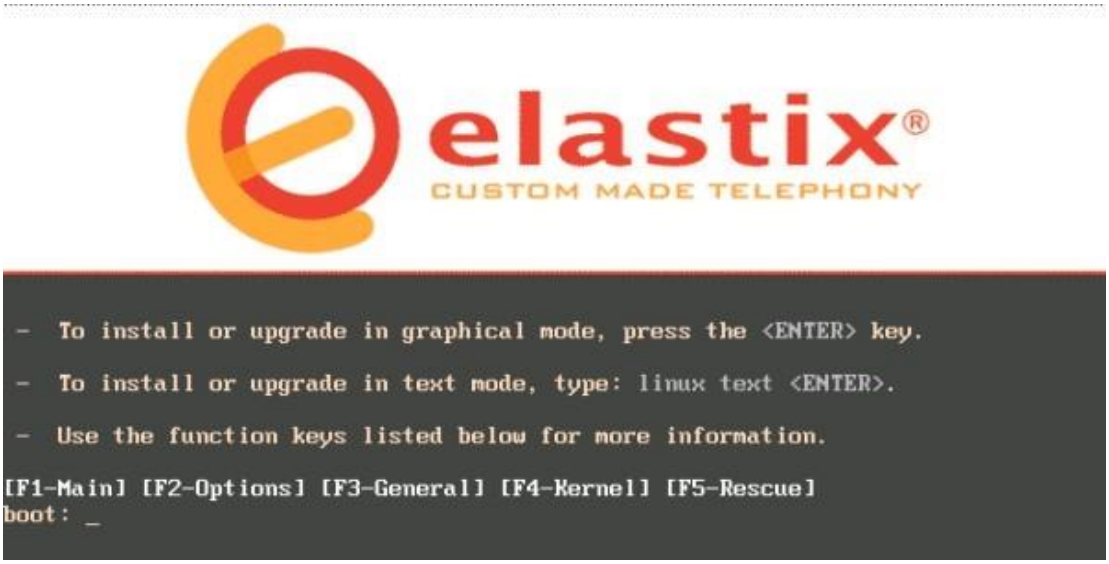
Enviar formulario

ANEXO 2

INSTALACIÓN DE ELASTIX

Instalación ELASTIX

Inserte el CD de instalación de Elastix al momento de encender su máquina. Una vez hecho esto aparecerá una pantalla como la siguiente:

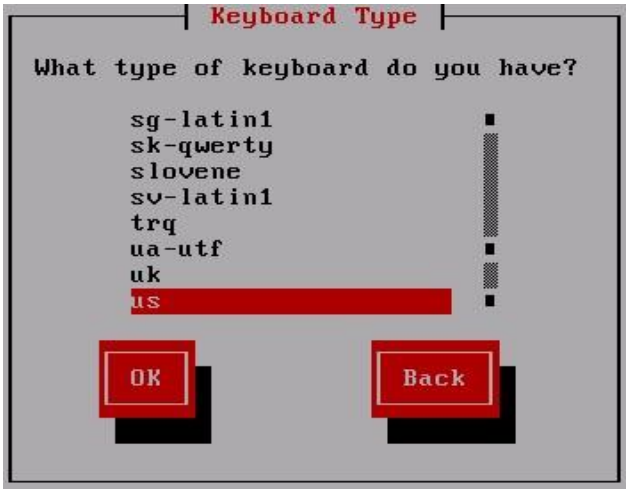


Si usted es un usuario experto puede ingresar en modo avanzado digitando el comando:

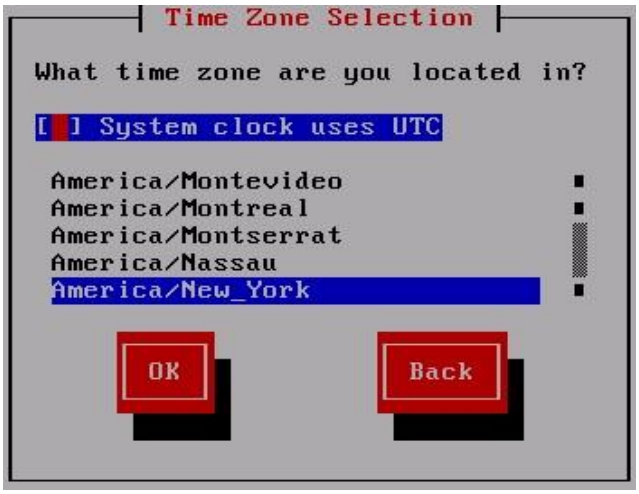
advanced

Caso contrario espere, el CD de instalación iniciará la instalación automáticamente o presione enter.

Proceda a escoger el tipo de teclado de acuerdo al idioma. Si su teclado es de idioma español seleccione la opción es:



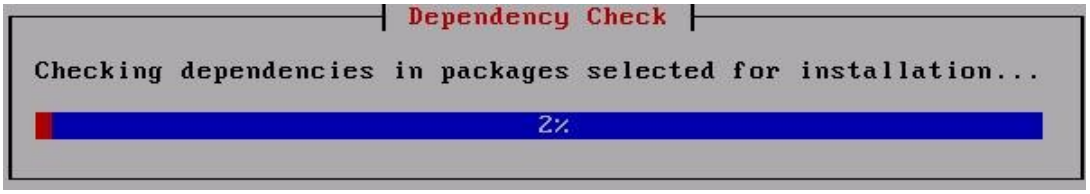
Seleccione la hora zona horaria de su región:



Digite la contraseña que será usada por el administrador de Elastix. Recuerde que esta es una parte crítica para la seguridad del sistema.

Nota: Los procedimientos a continuación los realizará el CD de instalación de manera automática.

Primero se buscará las dependencias necesarias para la instalación:



Luego se procede con la instalación, inicialmente usted verá algo como esto:

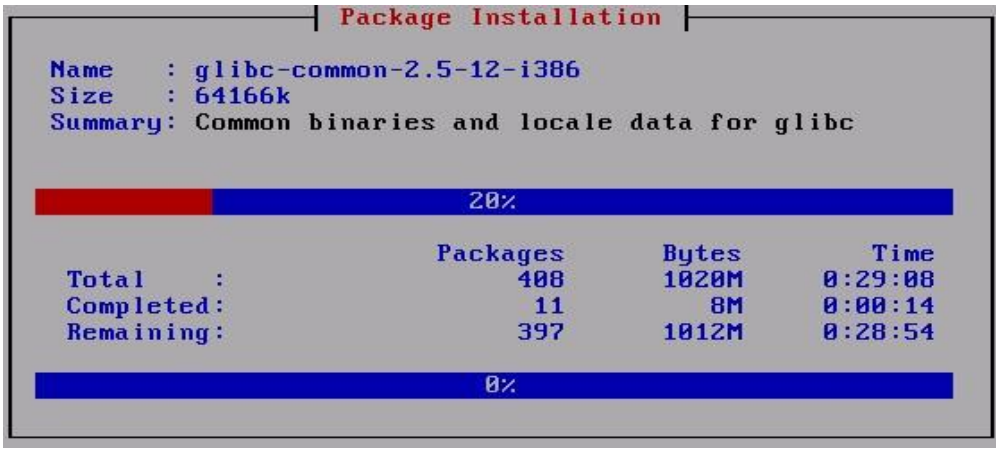
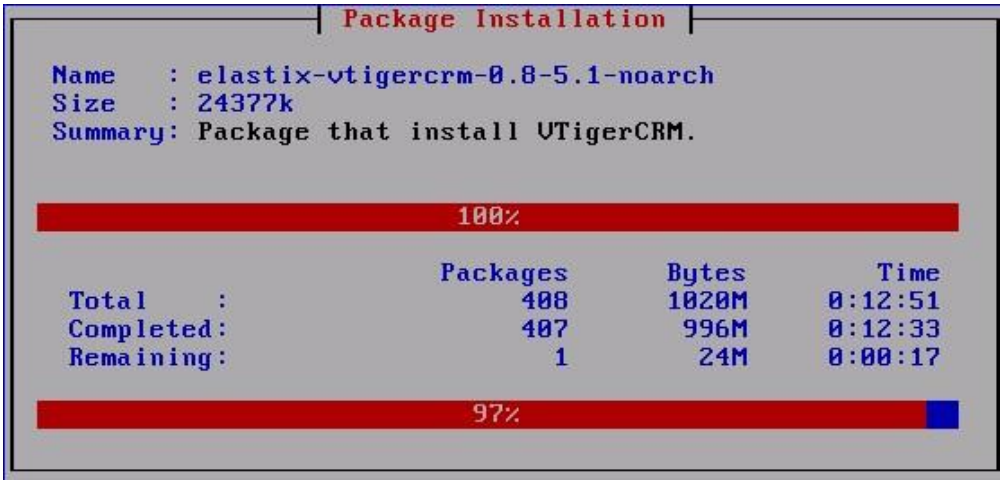
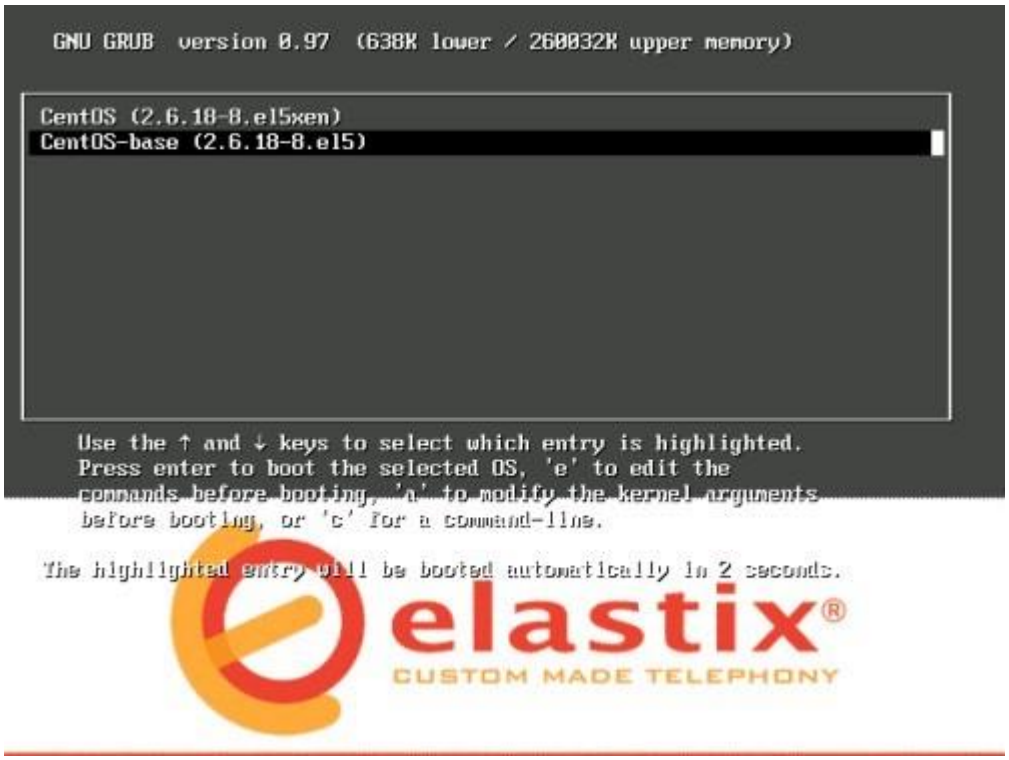


Imagen del proceso de instalación por finalizar:

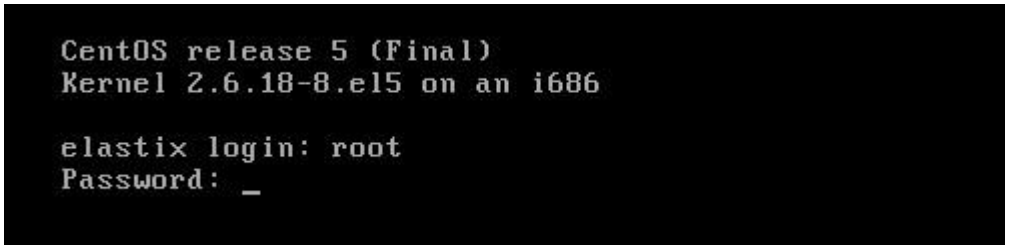


Una vez se realice la instalación completa, se procede a reiniciar el sistema.

Luego de reiniciar el sistema usted podrá escoger entre las opciones de boot la distro de Elastix.



Ingrese como usuario root y la contraseña digitada al momento de la instalación.



FUENTE:

http://sourceforge.net/projects/elastix/files/Tutorials_Docs_Manuals/User%20Manual%200.9-alpha%20%28Spanish%29/Elastix_User_Manual_Spanish_0.9-alpha.pdf/download

http://sourceforge.net/projects/elastix/files/Tutorials_Docs_Manuals/Elastix%202.0%20Guides/ELASTIX%202%20Installation%20Guide.pdf/download

ANEXO 3

CONFIGURACIÓN DE QoS EN UN LINSYS SRW2024 Switch

Security > Storm Control

Security > Storm Control

Port Displays the port number for which storm control is enabled.

Broadcast Control Indicates whether broadcast packet types are forwarded on the specific interface.

Mode Specifies the Broadcast mode currently enabled on the device. The possible field values are:

- **Unknown Unicast, Multicast & Broadcast** Counts Unicast, Multicast, and Broadcast traffic. This option is not available on the SRW224G4 and SRW248G4.
- **Multicast & Broadcast** Counts Broadcast and Multicast traffic together.
- **Broadcast Only** Counts only Broadcast traffic.

Rate Threshold The maximum rate (packets per second) at which unknown packets are forwarded. The default value is **3500**. The range is **70–100,000**.

QoS

Network traffic is usually unpredictable, and the only basic assurance that can be offered is best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria, and that specific traffic receives preferential treatment. QoS in the network optimizes network performance and entails two basic facilities:

Classifying incoming traffic into handling classes, based on an attribute, including:

- The ingress interface
- Packet content
- A combination of these attributes

Providing various mechanisms for determining the allocation of network resources to different handling classes, including:

- The assignment of network traffic to a particular hardware queue
- The assignment of internal resources
- Traffic shaping

The terms Class of Service (CoS) and QoS are used in the following context:

CoS provides varying Layer 2 traffic services. CoS refers to classification of traffic to traffic-classes, which are handled as an aggregate whole, with no per-flow settings. CoS is usually related to the 802.1p service that classifies flows according to their Layer 2 priority, as set in the VLAN header.

QoS refers to Layer 2 traffic and above. QoS handles per-flow settings, even within a single traffic class.

QoS > CoS Settings

The *CoS Settings* screen contains fields for enabling or disabling CoS. In addition, the Trust mode can be selected. The Trust mode relies on predefined fields within the packet to determine the egress queue settings.

QoS > CoS Settings

The *CoS Settings* screen has two areas, CoS Settings and CoS to Queue.

QoS Mode Indicates if QoS is enabled on the interface. The possible values are:

- **Disable** Disables QoS on the interface.
- **Basic** Enables QoS on the interface.
- **Advanced** Enables Advanced mode QoS on the interface. This feature has been added to version 1.2 of the SRW2024/SRW2016 and version 1.1 of the SRW224G4/SRW248G4.

Class of Service Specifies the CoS priority tag values, where **0** is the lowest and **7** is the highest.

Queue Defines the traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported.

The **Restore Defaults** button restores the device factory defaults for mapping CoS values to a forwarding queue.

CoS Default

Interface Interface to which the CoS configuration applies.

Default CoS Determines the default CoS value for incoming packets for which a VLAN tag is not defined. The possible field values are **0–7**. The default CoS is **0**.

Restore Defaults Restores the device factory defaults for mapping CoS values to a forwarding queue.

LAG LAG to which the CoS configuration applies.

QoS > Queue Settings

The *Queue Setting* screen contains fields for defining the QoS queue forwarding types.

NOTE: Individual queues cannot be assigned on the SRW224G4 and SRW248G4.

QoS > Queue Settings

Queue Displays the queue for which the queue settings are displayed. The range is **1–4**.

Strict Priority Indicates that traffic scheduling for the selected queue is based strictly on the queue priority.

WRR Indicates that traffic scheduling for the selected queue is based strictly on weighted round-robin (WRR).

WRR Weight Displays the WRR weights to queues.

% of WRR Bandwidth Displays the amount of bandwidth assigned to the queue. These values are fixed and are not user defined.

QoS > DSCP Settings

The *DSCP Settings* screen enables mapping DSCP values to specific queues.

QoS > DSCP Settings

The *DSCP Settings* screen contains the following fields:

DSCP Indicates the Differentiated Services Code Point value in the incoming packet.

Queue Maps the DSCP value to the selected queue.

QoS > Bandwidth

The *Bandwidth* screen allows network managers to define the bandwidth settings for a specified egress interface. Modifying queue scheduling affects the queue settings globally. The *Bandwidth* screen is not used with the Service mode, as bandwidth settings are based on services. This feature has been added to version 1.2 of the SRW2024/SRW2016 and version 1.1 of the SRW224G4/SRW248G4.

QoS > Bandwidth

Queue shaping can be based per queue and/or per interface. Shaping is determined by the lower specified value. The queue shaping type is selected in the *Bandwidth* screen.

Interface Indicates the interface for which the queue shaping information is displayed. The possible field values are:

- **Port** Indicates the port for which the bandwidth settings are displayed.
- **LAG** Indicates the LAG for which the bandwidth settings are displayed.

Ingress Rate Limit Status Indicates if rate limiting is defined on the interface.

Egress Shaping Rate on Selected Port Indicates if rate limiting is enabled on the interface.

Committed Information Rate (CIR) Defines CIR as the queue shaping type. The range is **64–1,000,000** Kbps.

Committed Burst Size (CBS) Defines CBS as the queue shaping type. The possible field value is **4096–16,769,020** bits.

Use the **Add to List** button to add the Bandwidth configuration to the Bandwidth Table at the bottom of the screen.

QoS > Basic Mode

QoS > Basic Mode

The *Basic Mode* screen contains the following fields:

Trust Mode Displays the trust mode. If a packet's CoS tag and DSCP tag are mapped to different queues, the Trust Mode determines the queue to which the packet is assigned. Possible values are:

- **CoS** Sets trust mode to CoS on the device. The CoS mapping determines the packet queue
- **DSCP** Sets trust mode to DSCP on the device. The DSCP mapping determines the packet queue

QoS > Advanced Mode

Advanced QoS mode provides rules for specifying flow classification and assigning rule actions that relate to bandwidth management. The rules are based on the ACLs (see Access Control Tab). This feature has been added to version 1.2 of the SRW2024/SRW2016 and version 1.1 of the SRW224G4/SRW248G4.

QoS > Advanced Mode

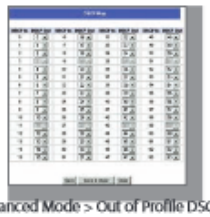
MAC ACLs and IP ACLs can be grouped together in more complex structures, called policies. Policies can be applied to an interface. Policy ACLs are applied in the sequence they appear within the policy. Only a single policy can be attached to a port.

In advanced QoS mode, ACLs can be applied directly to an interface in Security > ACL Binding. However, a policy and ACL cannot be simultaneously applied to an interface.

After assigning packets to a specific queue, services such as configuring output queues for the scheduling scheme, or configuring output shaping for burst size, CIR, or CBS per interface or per queue, can be applied.

Out of Profile DSCP Assignments This button opens up the *Out of Profile DSCP* screen.

Advanced Mode > Out of Profile DSCP



Advanced Mode > Out of Profile DSCP

DSCP In Displays the DSCP In value.

DSCP Out Displays the current DSCP Out value. A new value can be selected from the pull-down menu.

Use the **Policy Settings** button to open the *Policy Name* screen.

Advanced Mode > Policy Name

Advanced Mode > Policy Name

Policy Name Defines a new Policy name.

Add to List The **Add to List** button lets you add the policy to the Policy Name table.

Advanced Mode > New Class Map

Advanced Mode > New Class Map

Class Map Name Defines a new Class Map name.

Preferred ACL Indicates if packets are first matched to an IP-based ACL or a MAC based ACL. The possible field values are:

- **IP Based ACLs** Matches packets to IP-based ACLs first, then matches packets to MAC based ACLs.
- **MAC Based ACLs** Matches packets to MAC-based ACLs first, then matches packets to IP-based ACLs.

IP ACL Matches packets to IP-based ACLs first, then matches packets to MAC-based ACLs.

Match Criteria used to match IP addresses and/or MAC addresses with an ACL's address. The possible field values are:

- **And** Both the MAC-based and the IP-based ACL must match a packet.
- **Or** Either the MAC-based or the IP-based ACL must match a packet.

MAC ACL Matches packets to MAC-based ACLs first, then matches packets to IP-based ACLs.

Advanced Mode > New Aggregate Policer

Advanced Mode > New Aggregate Policer

Aggregate Policer Name Enter a name in this field.

Ingress Committed Information Rate (CIR) Defines the CIR in bits per second. This field is only relevant when the Police value is **Single**.

Ingress Committed Burst Size (CBS) Defines the CBS in bytes per second. This field is only relevant when the Police value is **Single**.

Exceed Action Action assigned to incoming packets exceeding the CIR. This field is only relevant when the Police value is **Single**. Possible values are:

- **Drop** Drops packets exceeding the defined CIR value.
- **Remark DSCP (Out of Profile DSCP)** Remarks packet's DSCP values exceeding the defined CIR value.
- **None** Forwards packets exceeding the defined CIR value.

Spanning Tree

Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The device supports the following Spanning Tree versions:

- **Classic STP** Provides a single path between end stations, avoiding and eliminating loops.
- **Rapid STP** Detects and uses network topologies that provide faster convergence of the spanning tree, without creating forwarding loops.
- **Multiple STP** Provides full connectivity for packets allocated to any VLAN. Multiple STP is based on the RSTP. In addition, Multiple STP transmits packets assigned to different VLANs through different MST regions. MST regions act as a single bridge.

Fuente:
http://www.cisco.com/en/US/docs/switches/lan/csbms/srw2048/administration/guide/SRW-US_v10_UG_A-Web.pdf

ANEXO 4

CONFIGURACIÓN DE QoS EN UN HP V1910-48G Switch

Configuring QoS

Overview

Quality of Service (QoS) reflects the ability of a network to meet customer needs. In an internet, QoS evaluates the ability of the network to forward packets of different services.

The evaluation can be based on different criteria because the network might provide various services. Generally, QoS performance is measured with respect to bandwidth, delay, jitter, and packet loss ratio during packet forwarding process.

Networks without QoS guarantee

On traditional IP networks without QoS guarantee, devices treat all packets equally and handle them using the first in first out (FIFO) policy. All packets share the resources of the network and devices. How many resources the packets can obtain completely depends on the time they arrive. This service is called "best-effort." It delivers packets to their destinations as possibly as it can, without any guarantee for delay, jitter, packet loss ratio, and so on.

This service policy is only suitable for applications insensitive to bandwidth and delay, such as Word Wide Web (WWW) and email.

QoS requirements of new applications

The Internet has been growing along with the fast development of networking technologies.

Besides traditional applications such as WWW, email and FTP, network users are experiencing new services, such as tele-education, telemedicine, video telephone, videoconference and Video-on-Demand (VoD). Enterprise users expect to connect their regional branches together with VPN technologies to carry out operational applications, for instance, to access the database of the company or to monitor remote devices through Telnet.

These new applications all have special requirements for bandwidth, delay, and jitter. For example, videoconference and VoD require high bandwidth, low delay and jitter. As for mission-critical applications, such as transactions and Telnet, they might not require high bandwidth but do require low delay and preferential service during congestion.

The emerging applications demand higher service performance of IP networks. Better network services during packets forwarding are required, such as providing dedicated bandwidth, reducing packet loss ratio, managing and avoiding congestion, and regulating network traffic. To meet these requirements, networks must provide more improved services.

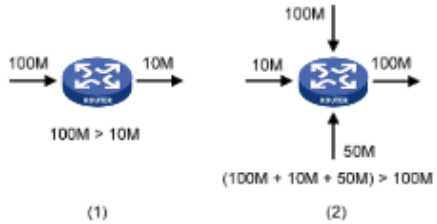
Congestion: causes, impacts, and countermeasures

Network congestion is a major factor contributed to service quality degrading on a traditional network. Congestion is a situation where the forwarding rate decreases due to insufficient resources, resulting in extra delay.

Causes

Congestion easily occurs in complex packet switching circumstances in the Internet. Figure 432 shows two common cases:

Figure 432 Traffic congestion causes



- The traffic enters a device from a high speed link and is forwarded over a low speed link.
- The packet flows enter a device from several incoming interfaces and are forwarded out of an outgoing interface, whose rate is smaller than the total rate of these incoming interfaces.

When traffic arrives at the line speed, a bottleneck is created at the outgoing interface causing congestion.

Besides bandwidth bottlenecks, congestion can be caused by resource shortage in various forms such as insufficient processor time, buffer, and memory, and by network resource exhaustion resulting from excessive arriving traffic in certain periods.

Impacts

Congestion might bring these negative results:

- Increased delay and jitter during packet transmission
- Decreased network throughput and resource use efficiency
- Network resource (memory in particular) exhaustion and even system breakdown

It is obvious that congestion hinders resource assignment for traffic and degrades service performance. Congestion is unavoidable in switched networks and multi-user application environments. To improve the service performance of your network, you must address the congestion issues.

Countermeasures

A simple solution for congestion is to increase network bandwidth, however, it cannot solve all the problems that cause congestion because you cannot increase network bandwidth infinitely.

A more effective solution is to provide differentiated services for different applications through traffic control and resource allocation. In this way, resources can be used more properly. During resources allocation and traffic control, the direct or indirect factors that might cause network congestion should be controlled to reduce the probability of congestion. Once congestion occurs, resource allocation should be performed according to the characteristics and demands of applications to minimize the effects of congestion.

End-to-end QoS

Figure 433 End-to-end QoS model

As shown in Figure 433, traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance are the foundations for a network to provide differentiated services. Mainly they implement the following functions:

- **Traffic classification**—Uses certain match criteria to organize packets with different characteristics into different classes. Traffic classification is usually applied in the inbound direction of a port.
- **Traffic policing**—Polices particular flows entering or leaving a device according to configured specifications and can be applied in both inbound and outbound directions of a port. When a flow exceeds the specification, some restriction or punishment measures can be taken to prevent overconsumption of network resources.
- **Traffic shaping**—Proactively adjusts the output rate of traffic to adapt traffic to the network resources of the downstream device and avoid unnecessary packet drop and congestion. Traffic shaping is usually applied in the outbound direction of a port.
- **Congestion management**—Provides a resource scheduling policy to arrange the forwarding sequence of packets when congestion occurs. Congestion management is usually applied in the outbound direction of a port.
- **Congestion avoidance**—Monitors the usage status of network resources and is usually applied in the outbound direction of a port. As congestion becomes worse, it actively reduces the amount of traffic by dropping packets.

Among these QoS technologies, traffic classification is the basis for providing differentiated services. Traffic policing, traffic shaping, congestion management, and congestion avoidance manage network traffic and resources in different ways to realize differentiated services.

This section is focused on traffic classification, and the subsequent sections will introduce the other technologies in details.

Traffic classification

When defining match criteria for classifying traffic, you can use IP precedence bits in the type of service (ToS) field of the IP packet header, or other header information such as IP addresses, MAC addresses, IP protocol field and port numbers. You can define a class for packets with the same quintuple (source address, source port number, protocol number, destination address and destination port number for example), or for all packets to a certain network segment.

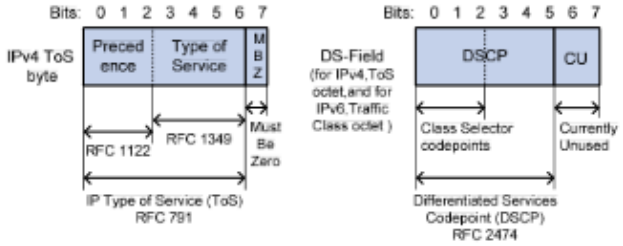
When packets are classified on the network boundary, the precedence bits in the ToS field of the IP packet header are generally re-set. In this way, IP precedence can be directly used to classify the packets in the network. IP precedence can also be used in queuing to prioritize traffic. The downstream network can either use the classification results from its upstream network or classify the packets again according to its own criteria.

To provide differentiated services, traffic classes must be associated with certain traffic control actions or resource allocation actions. What traffic control actions to use depends on the current phase and the resources of the network. For example, CAR polices packets when they enter the network. GTS is performed on packets when they flow out of the node. Queue scheduling is performed when congestion happens. Congestion avoidance measures are taken when the congestion deteriorates.

Packet precedences

IP precedence and DSCP values

Figure 434 ToS field and DS field



As shown in Figure 434, the ToS field of the IP header contains eight bits: the first three bits (0 to 2) represent IP precedence from 0 to 7. The subsequent four bits (3 to 6) represent a ToS value from 0 to 15. According to RFC 2474, the ToS field of the IP header is redefined as the differentiated services (DS) field, where a differentiated services code point (DSCP) value is represented by the first six bits (0 to 5) and is in the range 0 to 63. The remaining two bits (6 and 7) are reserved.

Table 139 Description on IP Precedence

IP Precedence (decimal)	IP Precedence (binary)	Description
0	000	Routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

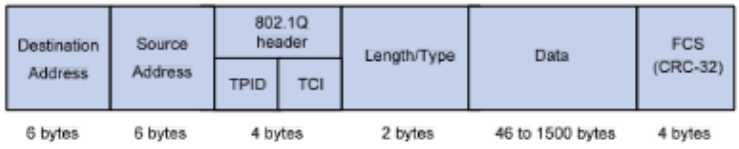
Table 140 Description on DSCP values

DSCP value (decimal)	DSCP value (binary)	Description
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (default)

802.1p priority

802.1p priority lies in Layer 2 packet headers and applies to occasions where Layer 3 header analysis is not needed and QoS must be assured at Layer 2.

Figure 435 An Ethernet frame with an 802.1Q tag header



As shown in Figure 435, the 4-byte 802.1Q tag header consists of the tag protocol identifier (TPID, two bytes in length), whose value is 0x8100, and the tag control information (TCI, two bytes in length). Figure 436 presents the format of the 802.1Q tag header. The priority in the 802.1Q tag header is called "802.1p priority," because its use is defined in IEEE 802.1p. Table 141 presents the values for 802.1p priority.

Figure 436 802.1Q tag header

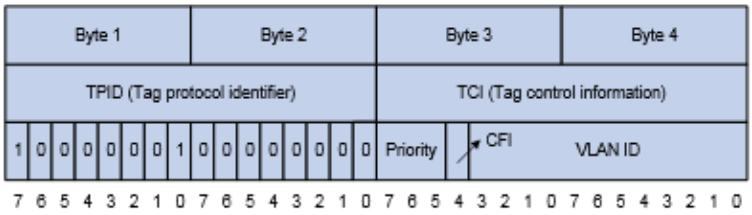


Table 141 Description on 802.1p priority

802.1p priority (decimal)	802.1p priority (binary)	Description
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

Queue scheduling

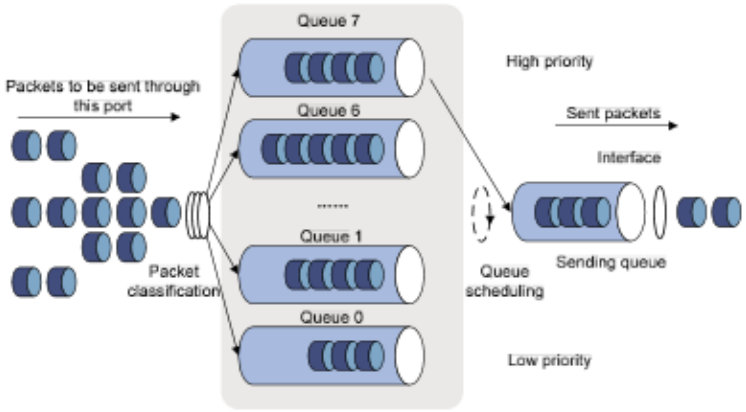
In general, congestion management uses queuing technology. The system uses a certain queuing algorithm for traffic classification, and then uses a certain precedence algorithm to send the traffic. Each queuing algorithm handles a particular network traffic problem and has significant impacts on bandwidth resource assignment, delay, and jitter.

In this section, two common hardware queue scheduling algorithms Strict Priority (SP) queuing and Weighted Round Robin (WRR) queuing are introduced.

SP queuing

SP queuing is designed for mission-critical applications, which require preferential service to reduce response delay when congestion occurs.

Figure 437 SP queuing



A typical switch provides eight queues per port. As shown in Figure 437, SP queuing classifies eight queues on a port into eight classes, numbered 7 to 0 in descending priority order.

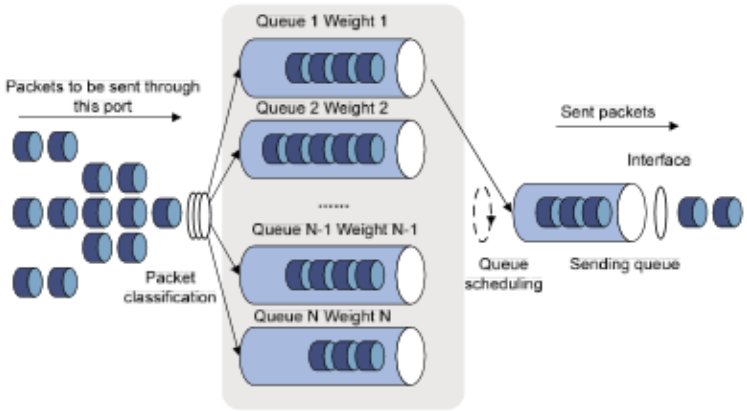
SP queuing schedules the eight queues strictly according to the descending order of priority. It sends packets in the queue with the highest priority first. When the queue with the highest priority is empty, it sends packets in the queue with the second highest priority, and so on. You can assign mission-critical packets to the high priority queue to make sure they are always served first and common service (such as Email) packets to the low priority queues to be transmitted when the high priority queues are empty.

The disadvantage of SP queuing is that packets in the lower priority queues cannot be transmitted if the higher priority queues have packets. This might cause lower priority traffic to starve to death.

WRR queuing

WRR queuing schedules all the queues in turn to make sure every queue can be served for a certain time, as shown in Figure 438.

Figure 438 WRR queuing



A typical switch provides eight output queues per port. WRR assigns each queue a weight value (represented by w7, w6, w5, w4, w3, w2, w1, or w0) to decide the proportion of resources assigned to the queue. On a 100 Mbps port, you can set the weight values of WRR queuing to 50, 30, 10, 10, 50, 30, 10, and 10 (corresponding to w7, w6, w5, w4, w3, w2, w1, and w0, respectively). In this way, the queue with the lowest priority is assured of at least 5 Mbps of bandwidth, and the disadvantage of SP queuing (that packets in low-priority queues might fail to be served for a long time) is avoided.

Another advantage of WRR queuing is that while the queues are scheduled in turn, the service time for each queue is not fixed. If a queue is empty, the next queue will be scheduled immediately. This improves bandwidth resource use efficiency.

WRR queuing involves:

- **Basic WRR queuing**—Contains multiple queues. You can configure the weight, percentage (or byte count) for each queue and WRR schedules these queues based on the user-defined parameters in a round robin manner.
- **Group-based WRR queuing**—All the queues are scheduled by WRR. You can assign the output queues to WRR priority queue group 1 and WRR priority queue group 2. Round robin queue scheduling is performed for group 1 first. If group 1 is empty, round robin queue scheduling is performed for group 2.

You can implement SP+WRR queue scheduling on a port by assigning some queues on the port to the SP scheduling group when you configure WRR. Packets in the SP scheduling group are scheduled preferentially by SP. When the SP scheduling group is empty, the other queues are scheduled by WRR.

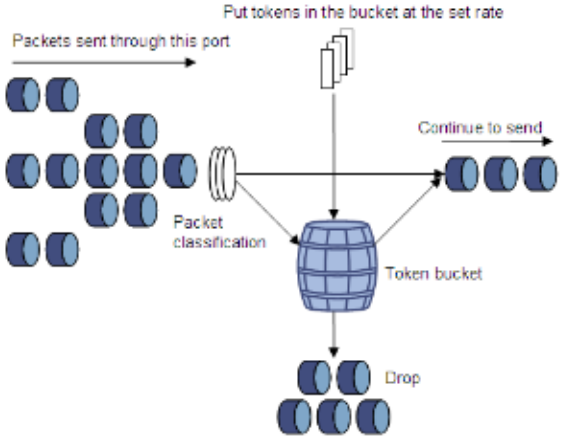
Line rate

Line rate is a traffic control method using token buckets. The line rate of a physical interface specifies the maximum rate for forwarding packets (including critical packets). Line rate can limit all the packets passing a physical interface.

Traffic evaluation and token bucket

A token bucket can be considered as a container holding a certain number of tokens. The system puts tokens into the bucket at a set rate. When the token bucket is full, the extra tokens will overflow.

Figure 439 Evaluate traffic with the token bucket



The evaluation for the traffic specification is based on whether the number of tokens in the bucket can meet the need of packet forwarding. If the number of tokens in the bucket is enough to forward the packets (usually, one token is associated with a 1-bit forwarding authority), the traffic conforms to the specification, and the traffic is called "conforming traffic." Otherwise, the traffic does not conform to the specification, and the traffic is called "excess traffic."

A token bucket has the following configurable parameters:

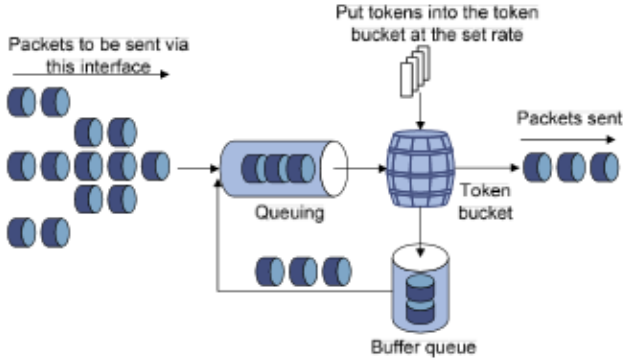
- **Mean rate**—Rate at which tokens are put into the bucket, or the permitted average rate of traffic. It is usually set to the committed information rate (CIR).
- **Burst size**—The capacity of the token bucket, or the maximum traffic size permitted in each burst. It is usually set to the committed burst size (CBS). The set burst size must be greater than the maximum packet size.

One evaluation is performed on each arriving packet. In each evaluation, if the number of tokens in the bucket is enough, the traffic conforms to the specification and the tokens for forwarding the packet are taken away. If the number of tokens in the bucket is not enough, it means that too many tokens have been used and the traffic is excessive.

Working mechanism of line rate

With line rate configured on an interface, all packets to be sent through the interface are firstly handled by the token bucket of line rate. If the token bucket has enough tokens, packets can be forwarded. Otherwise, packets are put into QoS queues for congestion management. In this way, the traffic passing the physical interface is controlled.

Figure 440 Line rate implementation



With a token bucket used for traffic control, when the token bucket has tokens, the bursty packets can be transmitted. When no tokens are available, packets cannot be transmitted until new tokens are generated in the token bucket. In this way, the traffic rate is restricted to the rate for generating tokens, the traffic rate is limited, and bursty traffic is allowed.

Priority mapping

Concepts

When a packet enters a network, it is marked with a certain priority to indicate its scheduling weight or forwarding priority. Then, the intermediate nodes in the network process the packet according to the priority.

When a packet enters a device, the device assigns to the packet a set of predefined parameters (including the 802.1p priority, DSCP values, IP precedence, and local precedence).

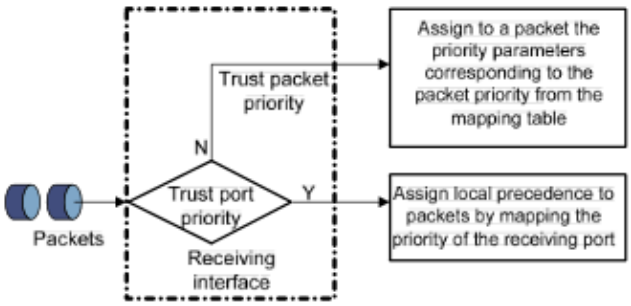
- For more information about 802.1p priority, DSCP values, and IP precedence, see "Packet precedences."
- Local precedence is a locally significant precedence that the device assigns to a packet. A local precedence value corresponds to an output queue. Packets with the highest local precedence are processed preferentially.

The device provides the following priority trust modes on a port:

- **Trust packet priority**—The device assigns to the packet the priority parameters corresponding to the packet's priority from the mapping table.
- **Trust port priority**—The device assigns a priority to a packet by mapping the priority of the receiving port.

You can select one priority trust mode as needed. Figure 441 shows the process of priority mapping on a device.

Figure 441 Priority mapping process



Introduction to priority mapping tables

The device provides the following types of priority mapping tables:

- **CoS to Queue**—802.1p-to-local mapping table.
- **DSCP to Queue**—DSCP-to-local mapping table, which applies to only IP packets.

Table 142 through Table 143 list the default priority mapping tables.

Table 142 Default CoS to Queue mapping table

Input CoS value	Local precedence (Queue)	DSCP
0	2	0
1	0	8
2	1	16
3	3	24
4	4	32
5	5	40
6	6	48
7	7	56

Table 143 Default DSCP to Queue mapping table

Input DSCP value	Local precedence (Queue)	CoS
0 to 7	0	0
8 to 15	1	1
16 to 23	2	2
24 to 31	3	3
32 to 39	4	4
40 to 47	5	5
48 to 55	6	6

Input DSCP value	Local precedence (Queue)	CoS
56 to 63	7	7

Configuration guidelines

When you configure QoS, follow these guidelines:

- When you configure line rate and traffic policing for a behavior, make sure the ratio of CBS to CIR is more than 100:16. Otherwise, the handling for bursty traffic might be affected.
- If the outgoing port configured for a traffic redirecting action is bound to a NAT virtual interface, packets are redirected to the L3 NAT card, which can cause traffic redirecting failure.
- If an ACL is referenced by a QoS policy for defining traffic classification rules, the operation of the QoS policy varies by interface. The specific process is as follows:
  - If the QoS policy is applied to a software interface and the referenced ACL rule is a **deny** clause, the ACL rule does not take effect and packets go to the next classification rule.
  - If the QoS policy is applied to a hardware interface, packets matching the referenced ACL rule are organized as a class and the behavior defined in the QoS policy applies to the class regardless of whether the referenced ACL rule is a **deny** or **permit** clause.
- If a QoS policy is applied in the outbound direction of a port, the QoS policy cannot influence local packets. Local packets refer to the important protocol packets that maintain the normal operation of the device. QoS must not process such packets to avoid packet drop. Commonly used local packets are: link maintenance packets, ISIS packets, OSPF packets, RIP packets, BGP packets, LDP packets, RSVP packets, and SSH packets and so on.
- When you configure queuing for a traffic behavior:
  - In a policy, a traffic behavior with EF configured cannot be associated with the default class, while a traffic behavior with WFQ configured can only be associated with the default class.
  - In a policy, the total bandwidth assigned to the AF and EF classes cannot be greater than the available bandwidth of the interface to which the policy applies. The total bandwidth percentage assigned to the AF and EF classes cannot be greater than 100%.
  - In the same policy, the same bandwidth unit must be used to configure bandwidth for AF classes and EF classes, either absolute bandwidth value or percent.

Recommended QoS configuration procedures

Recommended QoS policy configuration procedure

A QoS policy involves the following components: class, traffic behavior, and policy. You can associate a class with a traffic behavior using a QoS policy.

1. Class

   Classes identify traffic.

   A class is identified by a class name and contains some match criteria.

   You can define a set of match criteria to classify packets. The relationship between criteria can be **and** or **or**.

   - **and**—The device considers a packet belongs to a class only when the packet matches all the criteria in the class.

- **or**—The device considers a packet belongs to a class as long as the packet matches one of the criteria in the class.

2. Traffic behavior

   A traffic behavior, identified by a name, defines a set of QoS actions for packets.

3. Policy

   You can apply a QoS policy to a VLAN or a port.

   - **VLAN Policy**—Applies a QoS policy to a VLAN to regulate all traffic of the VLAN. QoS policies cannot be applied to dynamic VLANs, such as VLANs generated by GVRP.
   - **Port Policy**—Applies a QoS policy to a port to regulate the inbound or outbound traffic of the port. A QoS policy can be applied to multiple ports. Only one policy can be applied in one direction (inbound or outbound) of a port.

Perform the tasks in Table 144 to configure a QoS policy:

Table 144 Recommended QoS policy configuration procedure

Step	Remarks
1. Adding a class	Required. Add a class and specify the logical relationship between the match criteria in the class.
2. Configuring classification rules	Required. Configure match criteria for the class.
3. Adding a traffic behavior	Required. Add a traffic behavior.
4. Configure actions for the behavior: - Configuring traffic mirroring and traffic redirecting for a traffic behavior - Configuring other actions for a traffic behavior	Use either method. Configure various actions for the traffic behavior.
5. Adding a policy	Required. Add a policy.
6. Configuring classifier-behavior associations for the policy	Required. Associate the traffic behavior with the class in the QoS policy. A class can be associated with only one traffic behavior in a QoS policy. Associating a class already associated with a traffic behavior will overwrite the old association.
7. Applying a policy to a port	Required. Apply the QoS policy to a VLAN or a port.

Recommended queue scheduling configuration procedure

Step	Remarks
1. Configuring queue scheduling on a port	Optional. Configure the queue scheduling mode for a port.

Recommended line rate configuration procedure

Step	Remarks
1. Configuring line rate on a port	Required. Limit the rate of incoming packets or outgoing packets of a physical port.

Recommended priority mapping table configuration procedure

Step	Remarks
1. Configuring priority mapping tables	Required. Set priority mapping tables.

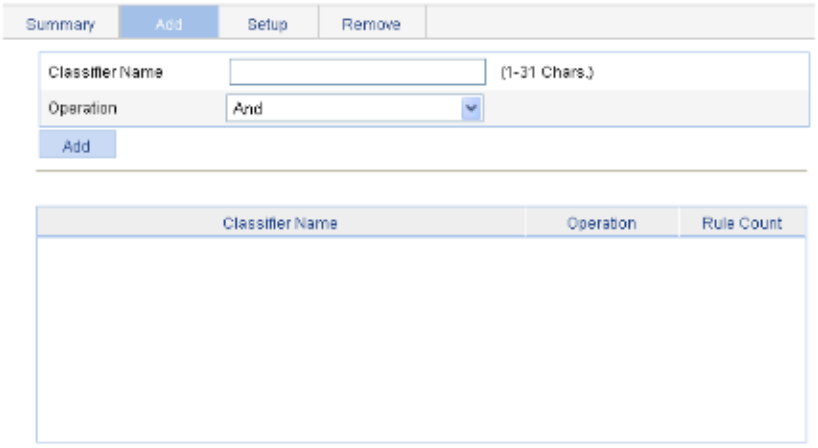
Recommended priority trust mode configuration procedure

Step	Remarks
1. Configuring priority trust mode on a port	Required. Set the priority trust mode of a port.

Adding a class

1. Select **QoS> Classifier** from the navigation tree.
2. Click the **Add** tab to enter the page for adding a class.

Figure 442 Adding a class



3. Add a class as described in Table 145.
4. Click **Add**.

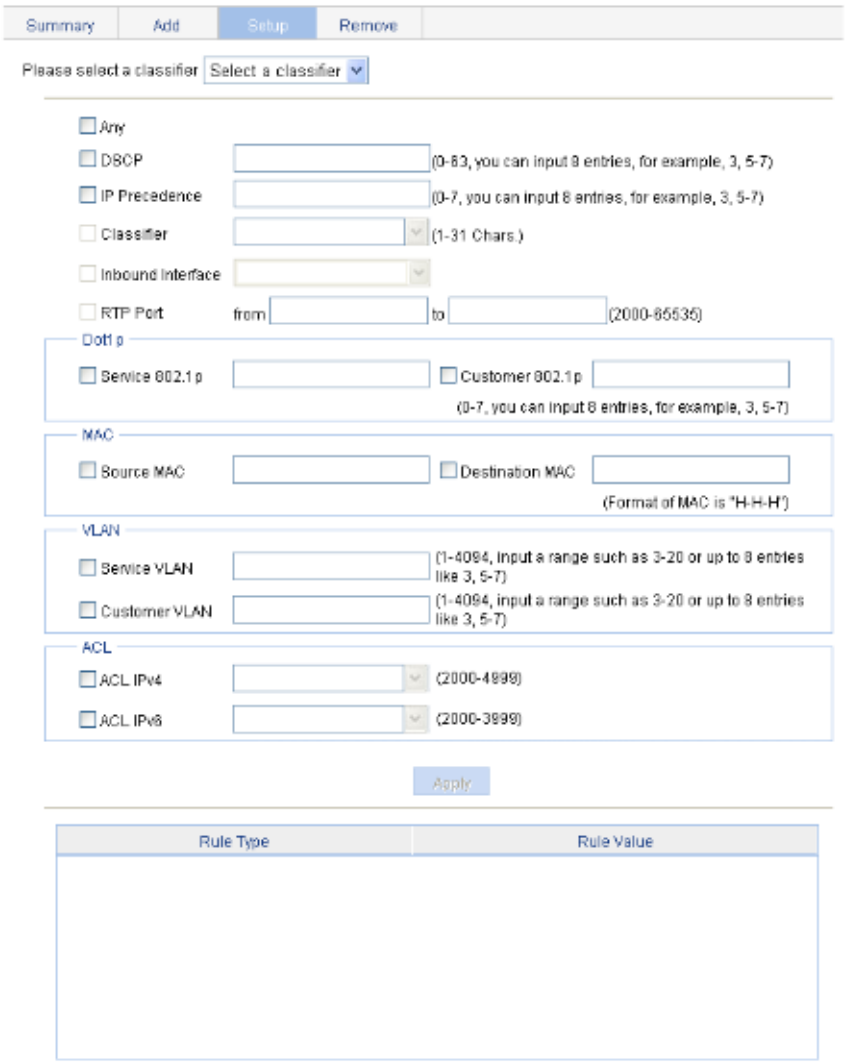
Table 145 Configuration items

Item	Description
Classifier Name	Specify a name for the classifier to be added. Some devices have their own system-defined classifiers. The classifier name you specify cannot overlap with system-defined ones. The system-defined classifiers include: default-class, ef, af1, af2, af3, af4, ip-prec0, ip-prec1, ip-prec2, ip-prec3, ip-prec4, ip-prec5, ip-prec6, ip-prec7, mpls-exp0, mpls-exp1, mpls-exp2, mpls-exp3, mpls-exp4, mpls-exp5, mpls-exp6, and mpls-exp7.
Operator	Specify the logical relationship between rules of the classifier. • **and**—Specifies the relationship between the rules in a class as logic AND. The device considers a packet belongs to a class only when the packet matches all the rules in the class. • **or**—Specifies the relationship between the rules in a class as logic OR. The device considers a packet belongs to a class as long as the packet matches one of the rules in the class.

Configuring classification rules

1. Select **QoS> Classifier** from the navigation tree.
2. Click **Setup** to enter the page for setting a class.

Figure 443 Configuring classification rules



3. Configure classification rules for a class as described in Table 146.
4. Click **Apply**.

Table 146 Configuration items

Item		Description
Please select a classifier		Select an existing classifier in the list.
Any		Define a rule to match all packets. Select the box to match all packets.
DSCP		Define a rule to match DSCP values. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. You can configure up to eight DSCP values each time. If multiple identical DSCP values are specified, the system considers them as one. The relationship between different DSCP values is **OR**. After such configurations, all the DSCP values are arranged in ascending order automatically.
IP Precedence		Define a rule to match IP precedence values. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. You can configure up to eight IP precedence values each time. If multiple identical IP precedence values are specified, the system considers them as one. The relationship between different IP precedence values is **OR**. After such configurations, all the IP precedence values are arranged in ascending order automatically.
Classifier		Define a rule to match a QoS class.
Inbound Interface		Define a rule to match inbound interfaces.
RTP Port		Define a rule to match a range of RTP ports. Specify the start port in the **from** field and the end port in the **to** field.
Dot1p	Service 802.1p	Define a rule to match the service 802.1p priority values. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. You can configure up to eight 802.1p priority values each time. If multiple identical 802.1p priority values are specified, the system considers them as one. The relationship between different 802.1p priority values is **OR**. After such configurations, all the 802.1p priority values are arranged in ascending order automatically.
	Customer 802.1p	Define a rule to match the customer 802.1p priority values. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. You can configure up to eight 802.1p priority values each time. If multiple identical 802.1p priority values are specified, the system considers them as one. The relationship between different 802.1p priority values is **OR**. After such configurations, all the 802.1p priority values are arranged in ascending order automatically.
MAC	Source MAC	Define a rule to match a source MAC address. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. A rule to match a source MAC address is significant only to Ethernet interfaces.

Item		Description
	Destination MAC	Define a rule to match a destination MAC address. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. A rule to match a destination MAC address is significant only to Ethernet interfaces.
VLAN	Service VLAN	Define a rule to match service VLAN IDs. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. You can configure multiple VLAN IDs each time. If the same VLAN ID is specified multiple times, the system considers them as one. The relationship between different VLAN IDs is logical **OR**. After such a configuration. You can specify VLAN IDs in either of the following ways: • Enter a range of VLAN IDs, such as 10-500. The number of VLAN IDs in the range is not limited. Specify a combination of individual VLAN IDs and VLAN ID ranges, such as 3, 5-7, 10. You can specify up to eight VLAN IDs in this way.
	Customer VLAN	Define a rule to match customer VLAN IDs. If multiple such rules are configured for a class, the new configuration does not overwrite the previous one. You can configure multiple VLAN IDs each time. If the same VLAN ID is specified multiple times, the system considers them as one. The relationship between different VLAN IDs is logical **OR**. You can specify VLAN IDs in either of the following ways: • Enter a range of VLAN IDs, such as 10-500. The number of VLAN IDs in the range is not limited. • Specify a combination of individual VLAN IDs and VLAN ID ranges, such as 3, 5-7, 10. You can specify up to eight VLAN IDs in this way.
ACL	ACL IPv4	Define an IPv4 ACL-based rule.
	ACL IPv6	Define an IPv6 ACL-based rule.

Adding a traffic behavior

1. Select **QoS> Behavior** from the navigation tree.
2. Click the **Add** tab to enter the page for adding a traffic behavior.

Figure 444 Adding a traffic behavior

3. Add a traffic behavior as described in Table 147.
4. Click **Add**.

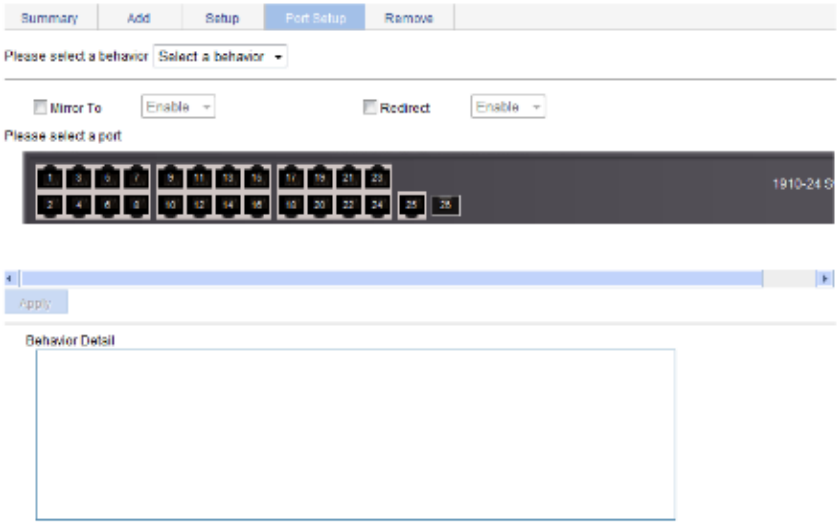
Table 147 Configuration items

Item	Description
Behavior name	Specify a name for the behavior to be added. Some devices have their own system-defined behaviors. The behavior name you specify cannot overlap with system-defined ones. The system-defined behaviors include **ef**, **af**, and **be**.

Configuring traffic mirroring and traffic redirecting for a traffic behavior

1. Select **QoS> Behavior** from the navigation tree.
2. Click **Port Setup** to enter the port setup page for a traffic behavior.

Figure 445 Port setup page for a traffic behavior



3. Configure traffic mirroring and traffic redirecting as described in Table 148.
4. Click **Apply**.

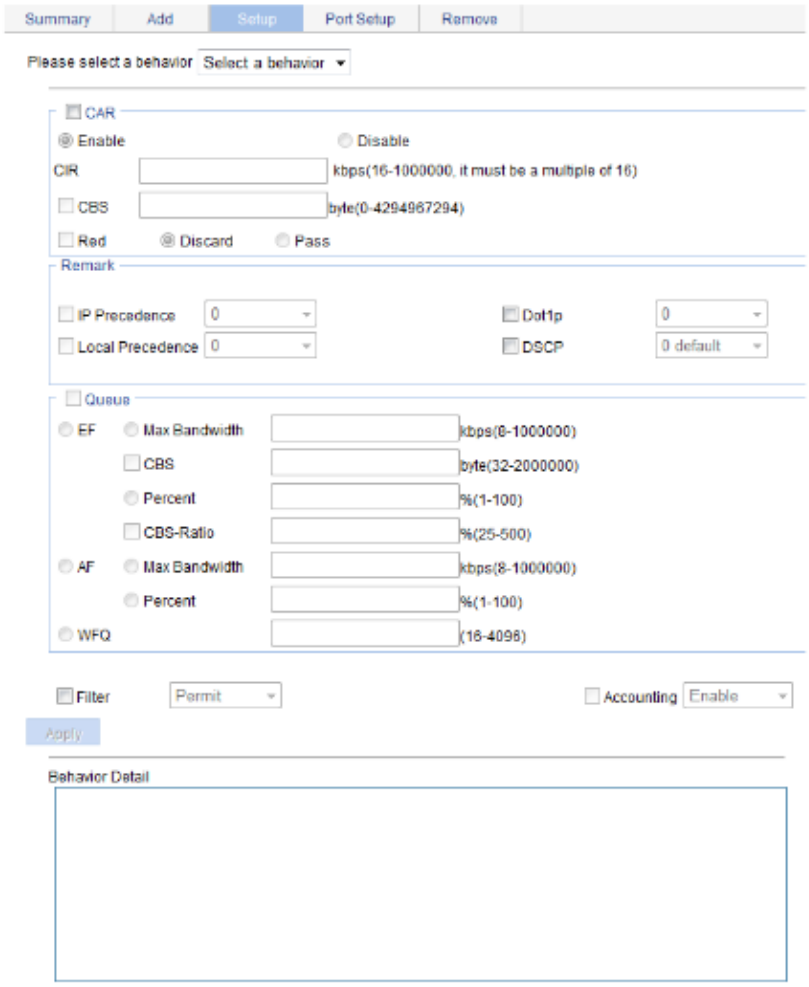
Table 148 Configuration items

Item	Description
Please select a behavior	Select an existing behavior in the list.
Mirror To	Set the action of mirroring traffic to the specified destination port.
Redirect	Set the action of redirecting traffic to the specified destination port.
Please select a port	Specify the port to be configured as the destination port of traffic mirroring or traffic directing on the chassis front panel.

Configuring other actions for a traffic behavior

1. Select **QoS> Behavior** from the navigation tree.
2. Click **Setup** to enter the page for setting a traffic behavior.

Figure 446 Setting a traffic behavior



3. Configure other actions for a traffic behavior as described in Table 149.
4. Click **Apply**.

Table 149 Configuration items

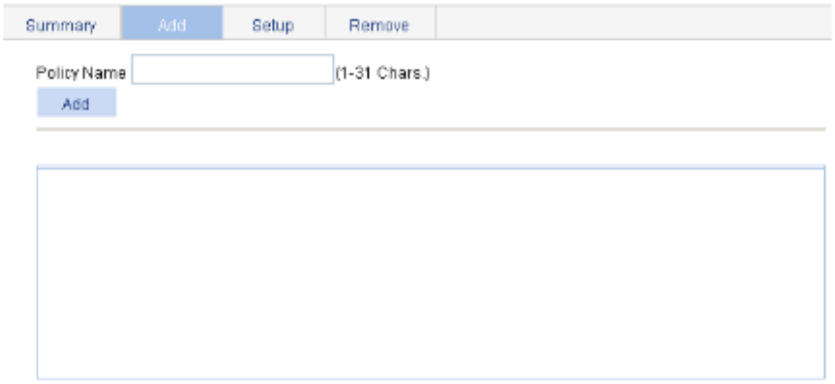
Item			Description
Please select a behavior			Select an existing behavior in the list.
CAR	Enable/Disable		Enable or disable CAR
	CIR		Set the committed information rate (CIR), the average traffic rate.
	CBS		Set the committed burst size (CBS), number of bytes that can be sent in each interval.
	Red	Discard	Set the action to perform for exceeding packets. After selecting the **Red** box, you can select one of the following options: • **Discard**—Drops the exceeding packet. • **Pass**—Permits the exceeding packet to pass through.
		Pass	
Remark	IP Precedence		Configure the action of marking IP precedence for packets. Select the **IP Precedence** box and then select the IP precedence value to be marked for packets in the following list. Select **Not Set** to cancel the action of marking IP precedence.
	Dot1p		Configure the action of marking 802.1p priority for packets. Select the **Dot1p** box and then select the 802.1p priority value to be marked for packets in the following list. Select **Not Set** to cancel the action of marking 802.1p priority.
	Local Precedence		Configure the action of marking local precedence for packets. Select the **Local Precedence** box and then select the local precedence value to be marked for packets in the following list. Select **Not Set** to cancel the action of marking local precedence.
	DSCP		Configure the action of marking DSCP value for packets. Select the **DSCP** box and then select the DSCP value to be marked for packets in the following list. Select **Not Set** to cancel the action of marking DSCP value.
Queue	EF	Max Bandwidth	Configure the maximum bandwidth for Expedited Forwarding (EF).
		CBS	Configure the CBS for EF.
		Percent	Configure the percent of available bandwidth for EF.
		CBS-Ratio	Configure the ratio of CBS to CIR for EF.
	AF	Min Bandwidth	Configure the minimum guaranteed bandwidth for Assured Forwarding (AF).
		Percent	Configure the percent of available bandwidth for AF.
	WFQ		Configure WFQ for the default class by entering the total number of fair queues, which must be the power of two.
Filter			Configure the packet filtering action. After selecting the **Filter** box, select one item in the following list: • **Permit**—Forwards the packet. • **Deny**—Drops the packet. • **Not Set**—Cancels the packet filtering action.

Item	Description
Accounting	Configure the traffic accounting action. Select the **Accounting** box and select **Enable** or **Disable** in the following list to enable/disable the traffic accounting action.
Type	When you select the **Accounting** box, set the traffic counting unit. • **Packet**—Counts packets in the unit of packets. **Byte**—Counts packets in the unit of bytes.

Adding a policy

1. Select **QoS> QoS Policy** from the navigation tree.
2. Click the **Add** tab to enter the page for adding a policy.

Figure 447 Adding a policy



3. Add a policy as described in Table 150.
4. Click **Add**.

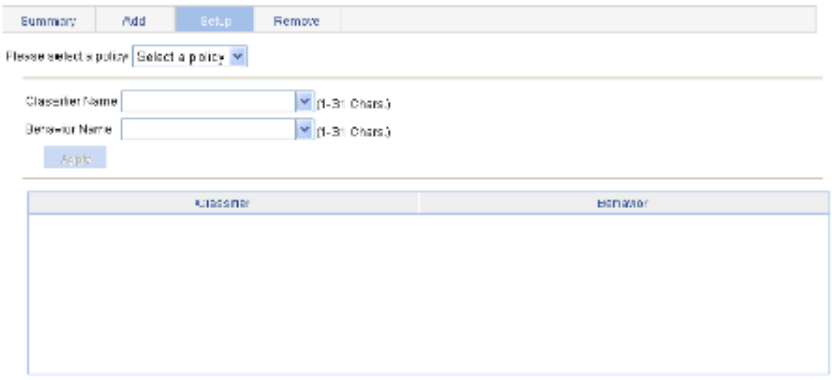
Table 150 Configuration items

Item	Description
Policy Name	Specify a name for the policy to be added. Some devices have their own system-defined policies. The policy name you specify cannot overlap with system-defined ones. The system-defined policy is the policy **default**.

Configuring classifier-behavior associations for the policy

1. Select **QoS> QoS Policy** from the navigation tree.
2. Click **Setup** to enter the page for setting a policy.

Figure 448 Setting a policy



3. Configure a classifier-behavior association for a policy as described in Table 151.
4. Click **Apply**.

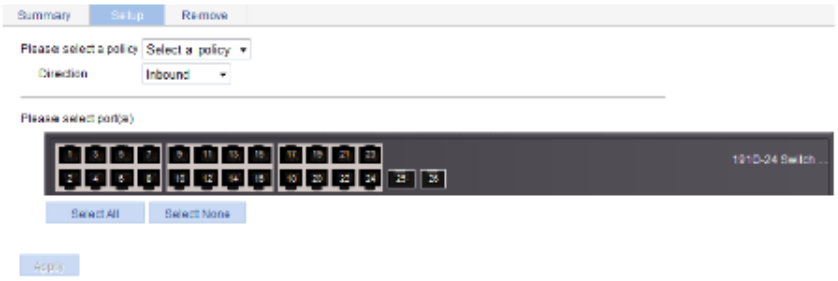
Table 151 Configuration items

Item	Description
Please select a policy	Select an existing policy in the list.
Classifier Name	Select an existing classifier in the list.
Behavior Name	Select an existing behavior in the list.

Applying a policy to a port

1. Select **QoS> Port Policy** from the navigation tree.
2. Click **Setup** to enter the page for applying a policy to a port.

Figure 449 Applying a policy to a port



3. Apply a policy to a port as described in Table 152.
4. Click **Apply**.

Table 152 Configuration items

Item	Description
Please select a policy	Select an existing policy in the list.
Direction	Set the direction in which the policy is to be applied. • **Inbound**—Applies the policy to the incoming packets of the specified ports. • **Outbound**—Applies the policy to the outgoing packets of the specified ports.
Please select port(s)	Click to select ports to which the QoS policy is to be applied on the chassis front panel.

Configuring queue scheduling on a port

1. Select **QoS> Queue** from the navigation tree.
2. Click **Setup** to enter the queue scheduling configuration page.

Figure 450 Configuring queue scheduling

3. Configure queue scheduling on a port as described in Table 153.
4. Click **Apply**.

Table 153 Configuration items

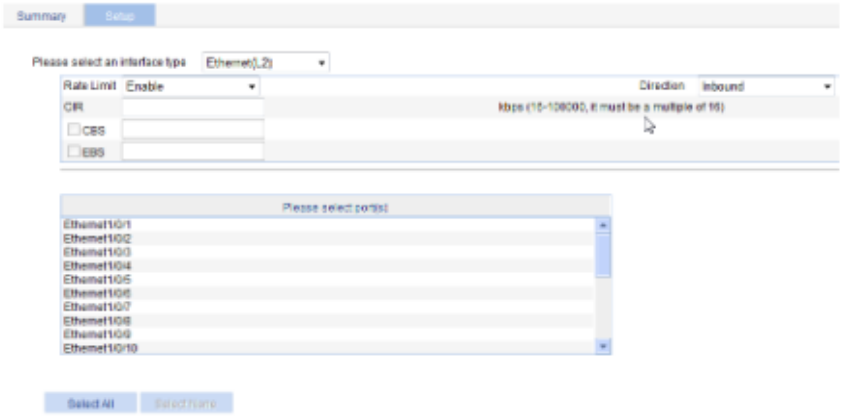
Item	Description
SP	Enable or disable the SP queue scheduling mechanism on selected ports. The following options are available: • **Enable**—Enables SP on selected ports. • **Not Set**—Restores the default queuing algorithm on selected ports.

Item		Description
WRR Setup	WRR	Enable or disable the WRR queue scheduling mechanism on selected ports. The following options are available: • **Enable**—Enables WRR on selected ports. • **Not Set**—Restores the default queuing algorithm on selected ports.
	Queue	Select the queue to be configured. The value range for a queue ID is 0 to n-1 (n is the maximum number of queues on an interface).
	Group	Specify the group the current queue is to be assigned to. This list is available after you select a queue ID. The following groups are available for selection: • **SP**—Assigns a queue to the SP group. • **1**—Assigns a queue to WRR group 1. • **2**—Assigns a queue to WRR group 2.
	Weight	Set a weight for the current queue. This list is available when group 1 or group 2 is selected.
Please select port(s)		Click to select ports to be configured with queuing on the chassis front panel.

Configuring line rate on a port

1. Select **QoS> Line rate** from the navigation tree.
2. Click the **Setup** tab to enter the line rate configuration page.

Figure 451 Configuring line rate on a port



3. Configure line rate on a port as described in Table 154.
4. Click **Apply**.

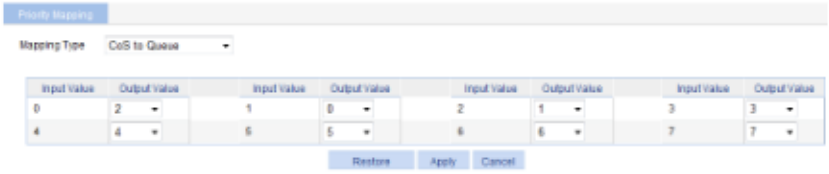
Table 154 Configuration items

Item	Description
Please select an interface type	Select the types of interfaces to be configured with line rate.
Rate Limit	Enable or disable line rate on the specified port.
Direction	Select a direction in which the line rate is to be applied. • **Inbound**—Limits the rate of packets received on the specified port. • **Outbound**—Limits the rate of packets sent by the specified port. • **Both**—Limits the rate of packets received and sent by the specified port.
CIR	Set the committed information rate (CIR), the average traffic rate.
Please select port(s)	Specify the ports to be configured with line rate. Click the ports to be configured with line rate in the port list. You can select one or more ports.

Configuring priority mapping tables

1. Select **QoS> Priority Mapping** from the navigation tree.

Figure 452 Configuring priority mapping tables



2. Configure a priority mapping table as described in Table 155.
3. Click **Apply**.

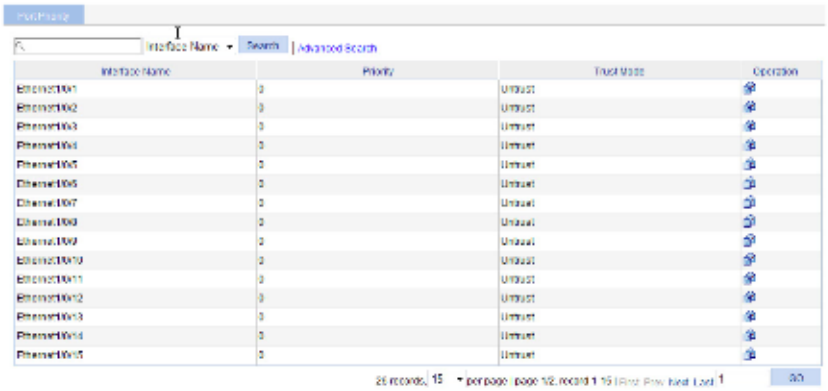
Table 155 Configuration items

Item	Description
Mapping Type	Select the priority mapping table to be configured: • **CoS to Queue**. • **DSCP to Queue**.
Input Priority Value	Set the output priority value for an input priority value.
Output Priority Value	
Restore	Click **Restore** to display the default settings of the current priority mapping table on the page. To restore the priority mapping table to the default, click **Apply**.

Configuring priority trust mode on a port

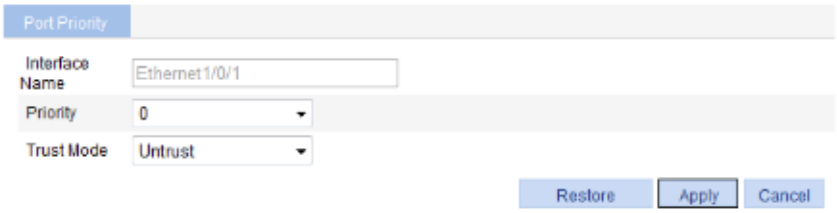
1. Select **QoS**> **Port Priority** from the navigation tree.

Figure 453 Configuring port priorities



2. Click the icon for a port.

Figure 454 Modifying the port priority



3. Configure the port priority for a port as described in Table 156.
4. Click **Apply**.

Table 156 Configuration items

Item	Description
Interface	Interface to be configured.
Priority	Set a local precedence value for the port.
Trust Mode	Select a priority trust mode for the port: • **Untrust**—Packet priority is not trusted. • **Dot1p**—802.1p priority of the incoming packets is trusted and used for priority mapping. **DSCP**—DSCP value of the incoming packets is trusted and used for priority mapping.

ACL and QoS configuration example

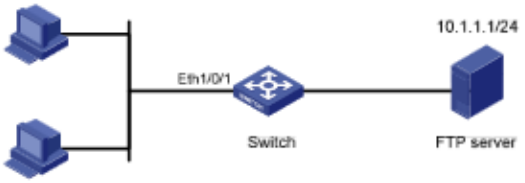
Network requirements

As shown in Figure 455, the FTP server (10.1.1.1/24) is connected to the Switch, and the clients access the FTP server through Ethernet 1/0/1 of the Switch.

Configure an ACL and a QoS policy as follows to prevent the hosts from accessing the FTP server from 8:00 to 18:00 every day:

1. Add an ACL to prohibit the hosts from accessing the FTP server from 8:00 to 18:00 every day.
2. Configure a QoS policy to drop the packets matching the ACL.
3. Apply the QoS policy in the inbound direction of Ethernet 1/0/1.

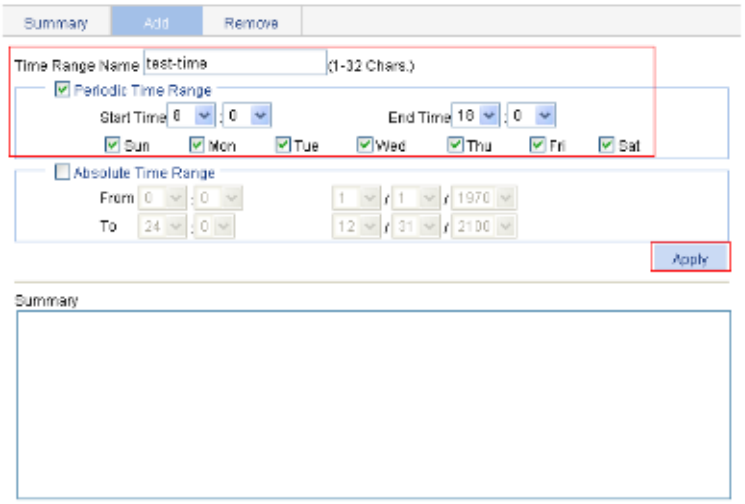
Figure 455 Network diagram



Configuring Switch

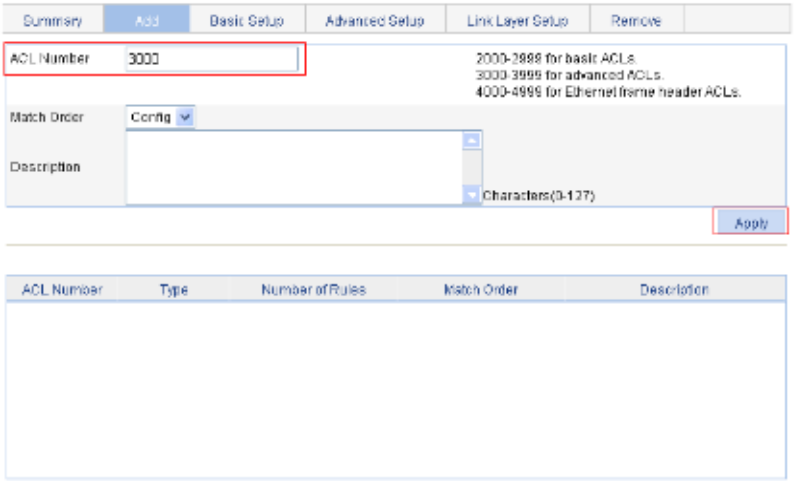
1. Define a time range to cover the time range from 8:00 to 18:00 every day:
   a. Select **QoS> Time Range** from the navigation tree.
   b. Click the **Add** tab.
   c. Enter the time range name **test-time**.
   d. Select the **Periodic Time Range** box.
   e. Set the **Start Time** to 8:00 and the **End Time** to 18:00.
   f. Select the options **Sun** through **Sat**.
   g. Click **Apply**.

Figure 456 Defining a time range covering 8:00 to 18:00 every day



2. Add an advanced IPv4 ACL:
   a. Select **QoS> ACL IPv4** from the navigation tree.
   b. Click the **Add** tab.
   c. Enter the ACL number 3000.
   d. Click **Apply**.

Figure 457 Adding an advanced IPv4 ACL



3. Define an ACL rule for traffic to the FTP server:
   a. Click the **Advanced Setup** tab.
   b. Select **3000** in the **ACL** list.

c. Select the **Rule ID** box, and enter rule ID 2.

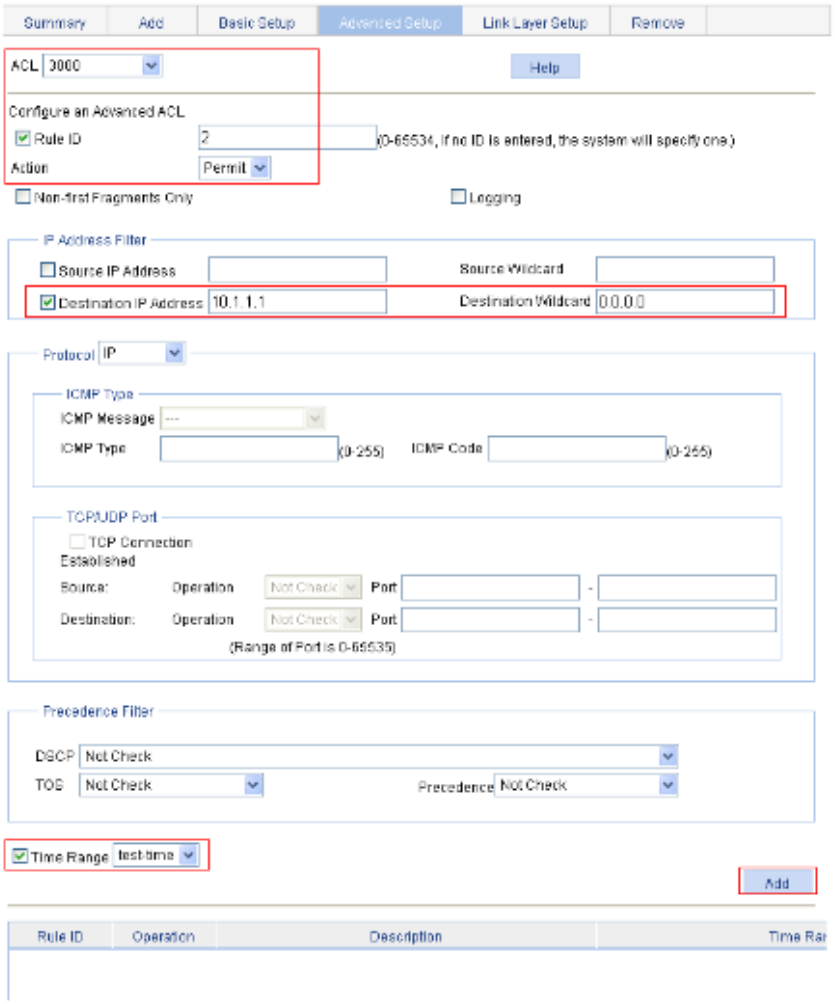
d. Select **Permit** in the **Action** list.

e. Select the **Destination IP Address** box, and enter IP address 10.1.1.1 and destination wildcard 0.0.0.0.

f. Select **test-time** in the **Time Range** list.

g. Click **Add**.

Figure 458 Defining an ACL rule for traffic to the FTP server



4. Add a class:

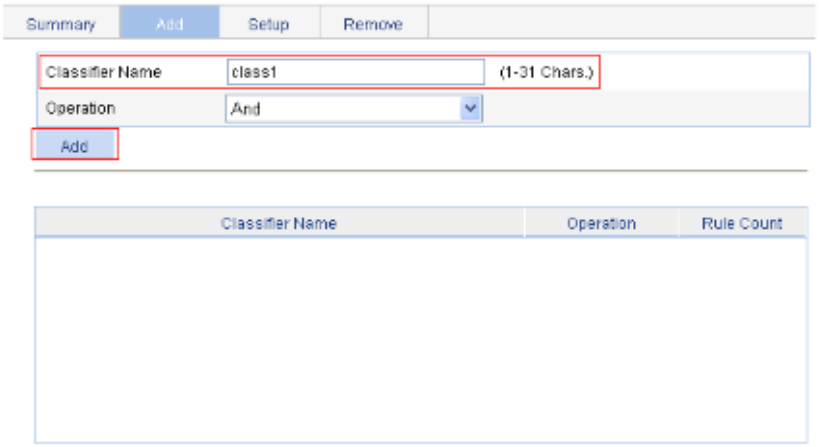
a. Select **QoS> Classifier** from the navigation tree.

b. Click the **Add** tab.

c. Enter the class name **class1**.

d. Click **Add**.

Figure 459 Adding a class



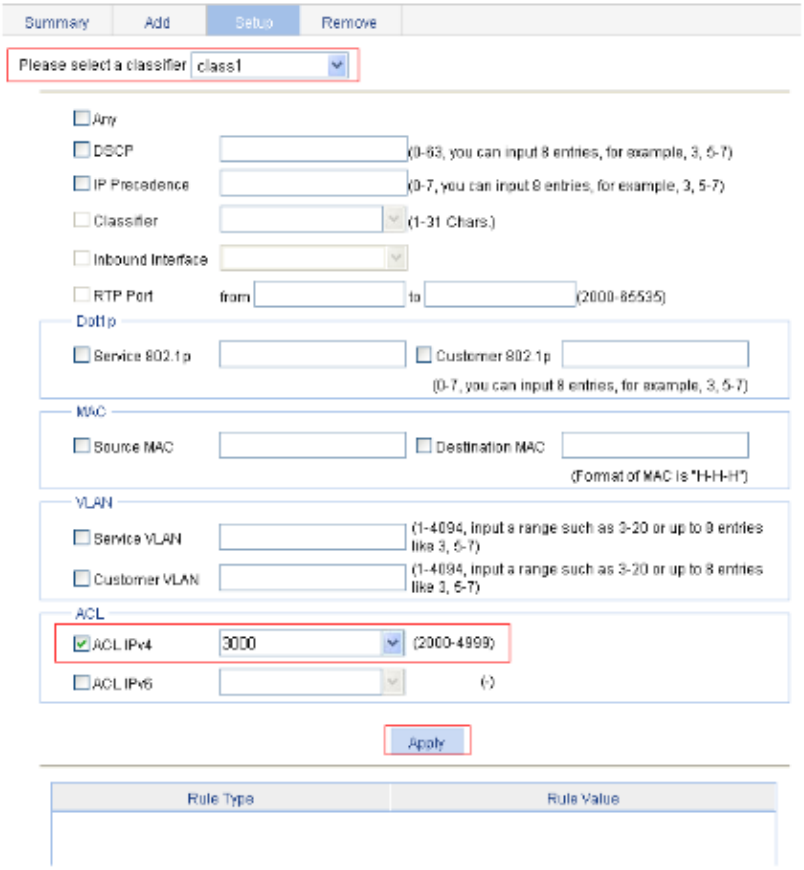
5. Define classification rules:

a. Click the **Setup** tab.

b. Select the class name **class1** in the list.

c. Select the **ACL IPv4** box, and select ACL 3000 in the following list.

Figure 460 Defining classification rules

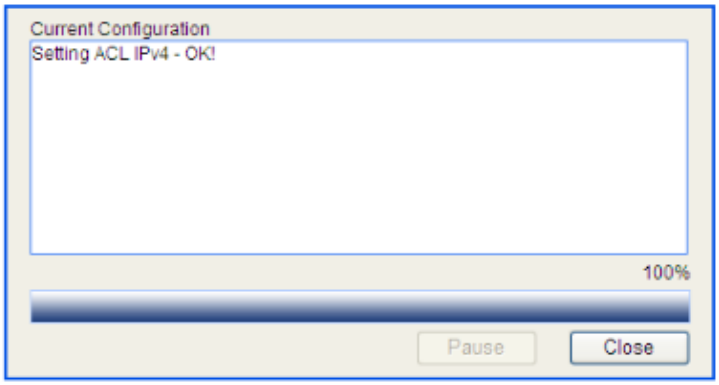


d. Click **Apply**.

A progress dialog box appears, as shown in Figure 461.

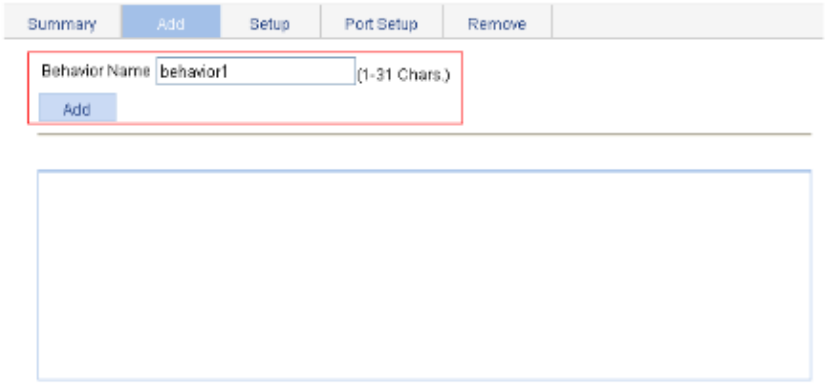
e. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

Figure 461 Configuration progress dialog box



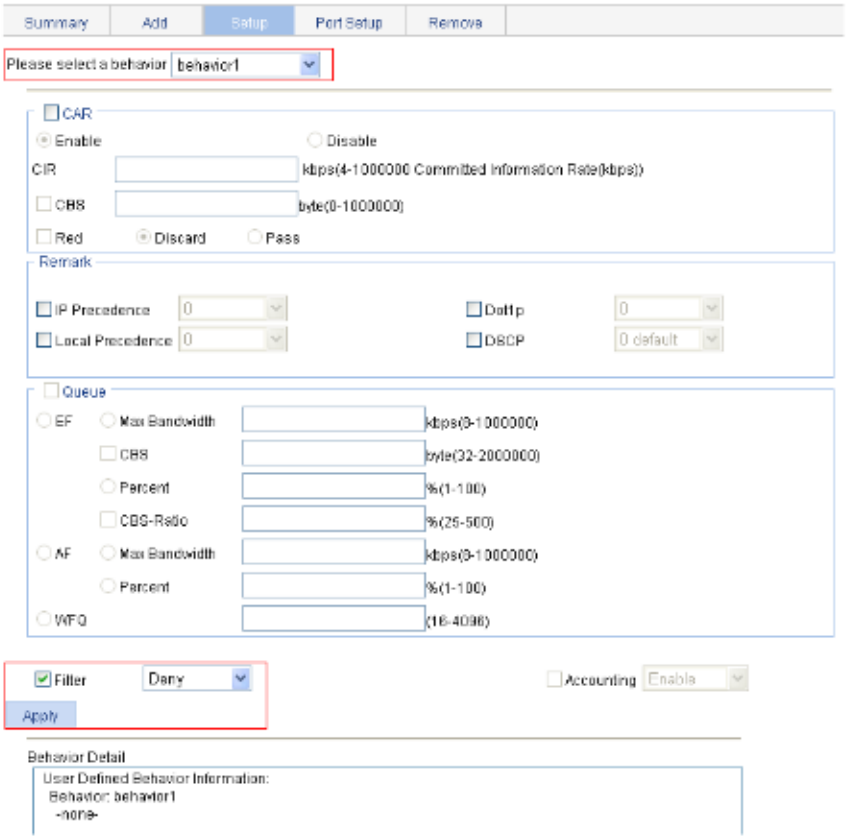
6. Add a traffic behavior:
   a. Select **QoS> Behavior** from the navigation tree.
   b. Click the **Add** tab.
   c. Enter the behavior name **behavior1**.
   d. Click **Add**.

Figure 462 Adding a traffic behavior



7. Configure actions for the traffic behavior:
   a. Click the **Setup** tab.
   b. Select **behavior1** in the list.
   c. Select the **Filter** box, and then select **Deny** in the following list.
   d. Click **Apply**.
      A progress dialog box appears.
   e. Click **Close** when the progress dialog box prompts that the configuration succeeds.

Figure 463 Configuring actions for the behavior

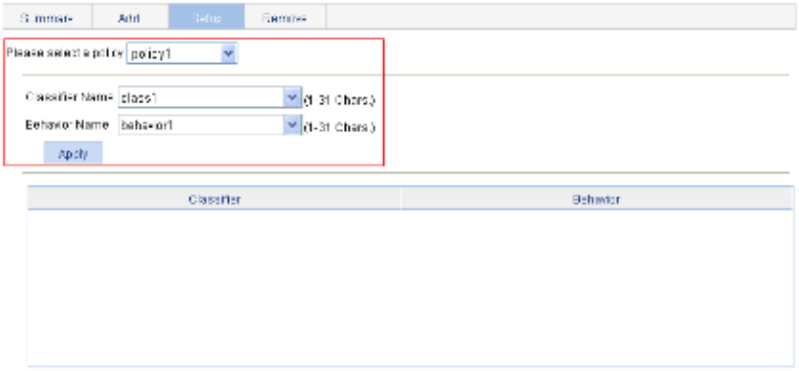


8. Add a policy:
   a. Select **QoS> QoS Policy** from the navigation tree.
   b. Click the **Add** tab.
   c. Enter the policy name **policy1**.
   d. Click **Add**.

Figure 464 Adding a policy

9. Configure classifier-behavior associations for the policy:
   a. Click the **Setup** tab.
   b. Select **policy1**.
   c. Select **class1** from the **Classifier Name** list.
   d. Select **behavior1** from the **Behavior Name** list.
   e. Click **Apply**.

Figure 465 Configuring classifier-behavior associations for the policy



10. Apply the QoS policy in the inbound direction of interface Ethernet 1/0/1:
    a. Select **QoS> Port Policy** from the navigation tree.
    b. Click the **Setup** tab.
    c. Select **policy1** from the **Please select a policy** list.
    d. Select **Inbound** from the **Direction** list.
    e. Select port Ethernet 1/0/1.
    f. Click **Apply**.
       A configuration progress dialog box appears.
    g. Click **Close** when the progress dialog box prompts that the configuration succeeds.

Figure 466 Applying the QoS policy in the inbound direction of Ethernet 1/0/1

490

FUENTE:
http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c03941555-1.pdf