UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

Configuración de parámetros de QoS en una Red VoIP-SIP

TESIS
Para obtener el grado de
Ingeniero en Redes

PRESENTA
Alen Arturo Loria Chulim

DIRECTOR DE TESIS
Dr. Homero Toral Cruz

ASESORES

Dr. Jaime Silverio Ortegón Aguilar

M. T. I. Melissa Blanqueto Estrada

Chetumal Quintana Roo, México, Diciembre de 2014

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

Trabajo de Tesis elaborado bajo supervisión del Comité de asesoría y aprobada como requisito parcial para obtener el grado de:

INGENIERO EN REDES

Comité de Trabajo de Tesis

Director: _____

Dr. Homero Toral Cruz

Asesor: _____

Dr. Jaime Silverio Ortegón Aguilar

Asesor: _____

M. T. I. Melissa Blanqueto Estrada

Chetumal Quintana Roo, México, Diciembre de 2014

AGRADECIMIENTOS

A todos mis profesores por haber sido parte fundamental durante mi formación académica y en especial al Dr. Homero Toral Cruz, por haber tenido la paciencia y la dedicación para apoyarme en la realización de este trabajo de tesis.

De la misma forma agradezco al Departamento de Ciencias e Ingeniería por haber financiado este trabajo de tesis.

Este trabajo fue financiado en la convocatoria 2013

"Apoyo a la Titulación de la DCI"

DEDICATORIA

Dedico este trabajo de tesis a mi familia, pero en especial a mi padre Domingo Loría Basto QEPD, que no tuvo la oportunidad de verme lograr este objetivo tan anhelado. A mi madre Ofelia Chulim, que siempre me ha apoyado y nunca me ha dejado solo, a mis hermanos Leydi C. Loría Chulim, Juan Carlos Loría Chulim que siempre me estuvieron apoyando en la medida de lo posible y que a pesar de todo siempre han confiado en mí y han hecho posible que llegue a la culminación de este objetivo que es la conclusión de la carrera.

De igual manera a mi hermano Eduardo Efrén Loría Chulim, que aunque este residiendo en otro Estado, siempre está al pendiente de mí y me ha alentado a seguir adelante en mi camino.

Así mismo dedico este trabajo a mi futura esposa, Jacqueline Estefani Sansores Cuevas y a nuestro futuro hijo que viene en camino, de lo cual me siento muy feliz y orgulloso de saber que voy a tener la experiencia de ser padre y de tener una familia.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ACRÓNIMOS

ACR	Absolute Category Rating
ADLS	Asymmetric Digital Subscriber Line
ATM	Asynchronous Transfer Mode
BRI	Basic Rate Interface
CDMA	Code Division Multiple Access
CDR	Call Detail Report
DCR	Degradation Category Rating
DoS	Denial of Service
FXO	Foreigne Xchange Office
FXS	Foreigne Xchange Subscriber
GPRS	General Packet Radio Service
HTTP	Hypertext Transfer Protocol
IAX	Inter Asterisk Exchange
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ITU	International Telecommunication Union
LDAP	Lightweight Directory Access Protocol
MOS	Mean Opinion Store
PRI	Primary Rate Interface

PSTN	Red Telefónica Púbilca Conmutada
QoS	Quality Of Service
RDSI	Red Digital de Servicios Integrados
RTB	Red Telefónica Básica
RTC	Red Telefónica Conmnutada
RTCP	Real Time Control Protocol
SAP	Session Announcement Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TDMA	Time DivisionMultiple Access
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
VAD	Voice Activity Detection
VoIP	Voz sobre IP

CAPÍTULO 1 INTRODUCCIÓN

1.1. Antecedentes

Debido al creciente uso de la telefonía IP, muchas de las empresas e instituciones gubernamentales han migrado a esta tecnología, mediante el uso de sistemas en software como Elastix, el cual posee la característica de fácil uso y configuración, además ofrece grandes ventajas, ya que integra, Free PBX, E-Mail, Mensajería Instantánea, Fax, entre otros servicios.

Sin embargo en muchas de las ocasiones no se realiza la configuración adecuada de ciertos parámetros del sistema en función de los recursos de la red y en consecuencia la calidad de servicio (QoS) se ve afectada. En los sistemas de voz sobre el protocolo de Internet (VoIP), la calidad de servicio está principalmente determinada por las métricas de retardo. Jitter y pérdida de paquetes.

Por tal motivo, es importante el estudio de las métricas antes mencionadas y la adecuada configuración de parámetros en el sistema VoIP, tales como: tamaño de paquete de voz, uso de detectores de actividad de voz, tipo de códec, tamaño de de-jitter buffer, etc., esto con el objetivo de garantizar cierto nivel de QoS en la transmisión de voz a través de la redes de datos como Internet.

1.2. Justificación

VoIP es hoy en día la tendencia para las comunicaciones de voz, debido a los grandes beneficios que proporciona en comparación con la red telefónica conmutada, tales como: reducción en los costos de llamada derivado de la tarifa plana por el uso del internet; uso más eficiente de la infraestructura; uso de servicios más atractivos de comunicaciones y reducción de costos por concepto de gestión y operación de infraestructura. Sin embargo, debido a que la tecnología VoIP hace uso de Internet para transportar los flujos de voz, e Internet no garantiza calidad de servicio, durante la transmisión se producen ciertos desperfectos como, retardos, jitter y pérdidas de paquetes; que se traducen en un deterioro en la calidad de la señal de voz que percibe el usuario final.

Motivados por los puntos anteriores, en este trabajo, se implementó una Red VoIP bajo el protocolo SIP basado en Elastix y se realizó un estudio de las principales métricas que determinan la QoS (retardo, jitter y pérdida de paquetes), bajo diferentes configuraciones de parámetros en el sistema VoIP (tamaño de paquete de voz, uso de detectores de

actividad de voz, tipo de códec, tamaño de de-jitter buffer, etc.), este con el objetivo de determinar configuraciones óptimas que proporcionen cierto nivel de QoS.

1.3. Objetivo General

Realizar un estudio de las principales métricas que determinan la QoS, bajo diferentes configuraciones de parámetros en un sistema VoIP basado en Elastix, para determinar configuraciones óptimas de dichos parámetros que proporcionen cierto nivel de QoS.

1.3.1. Objetivos Específicos

- Implementar un escenario de medición mediante la plataforma Elastix.
- Configurar las troncales SIP.
- Generar tráfico de voz mediante el establecimiento de un conjunto de llamadas bajo diferente configuración de parámetros de QoS (VAD, CODECs, tamaño de “de jitter buffer”).
- Capturar el tráfico generado mediante el software VoIPmonitor.
- Analizar el comportamiento de parámetros de QoS.
- Evaluar el desempeño de las llamadas de prueba.

CAPÍTULO 2 CONCEPTOS BÁSICOS DE VOIP

Para poder entender los principales conceptos de Voz sobre IP (VoIP), hablaremos un poco de la historia de la red telefónica tradicional.

El término telefonía proviene del griego y se compone por dos vocablos: “tele” (lejos, distancia) y “fonía” (sonidos), éste aparece a finales del siglo XIX, en un principio se le atribuyó a Alexander Graham Bell como el inventor del teléfono, ya que él fue el primero en patentarlo, pero poco más tarde se reconoció al médico italiano Antonio Meucci como el inventor del teléfono, ya que en 1849 hizo una demostración de un dispositivo capaz de transmitir voz en La Habana, pocos años después, en 1854 realiza una nueva demostración en la ciudad de Nueva York.

Este primer teléfono consistía en un altavoz y un micrófono, los cuales estaban conectados con otro teléfono de características similares. Esta conexión se realizó mediante un cable y a través de este cable se transmitía y recibía la señal de voz con alguno de los teléfonos de los extremos, gracias a esto se pudo mantener conversaciones a cierta distancia [1].

En las primeras etapas del uso del teléfono, cada usuario telefónico necesitaba tener una conexión física con el teléfono de la persona con la que deseaba realizar una comunicación. Esta conexión se realizó a través de un alambre de cobre y no disponía de circuitos de marcación, sin embargo la agrupación de la red telefónica no era ordenada, ya que comenzó con una simple agrupación de conexiones entre clientes, dicho de otra manera, una conexión punto a punto.

Debido al crecimiento del número de clientes esta situación se volvió impráctica, por lo que surgió la necesidad de crear una solución, de esta forma surgieron las centralitas (conmutadores) como una entidad que se encargaba de interconectar los cables. Las primeras centralitas telefónicas no eran automáticas, por consiguiente la conexión entre el origen y el destino de la llamada se realizaba de forma manual y se necesitaba de un operador humano.

Más tarde Almon Brown Stroweger inventó un sistema de marcado, para que la llamada se conmute automáticamente al destino requerido que posteriormente patentó. En 1960 empiezan a surgir las primeras centralitas telefónicas automáticas electrónicas analógicas que realizaban la conmutación a través de relés y se aceleró el proceso de conmutación.

En la actualidad todo el proceso se ha automatizado, las centrales modernas se encargan de recibir todas las llamadas y realizan las conexiones de forma casi instantánea [2].

2.1 Redes por Conmutación de Circuitos

Las redes orientadas a circuitos son aquellas donde se establece un circuito exclusivo o dedicado entre los nodos antes de que los usuarios se puedan comunicar, de manera que todos los paquetes llegarán exactamente en el mismo orden en el que se generaron, en este tipo de redes se ofrecen servicios orientados a la conexión. Una vez que se estable el circuito, el resultado es equivalente a conectar físicamente un par de cables de un extremo a otro, de manera que este circuito ya no podrá ser utilizado, ya que hay una reserva de recursos que garantiza que el circuito extremo a extremo reduzca al mínimo la probabilidad de pérdidas. Este tipo de redes es comúnmente utilizado por compañías telefónicas alrededor del mundo y es el mismo que utilizó Bell en sus inicios [2] [3] [4].

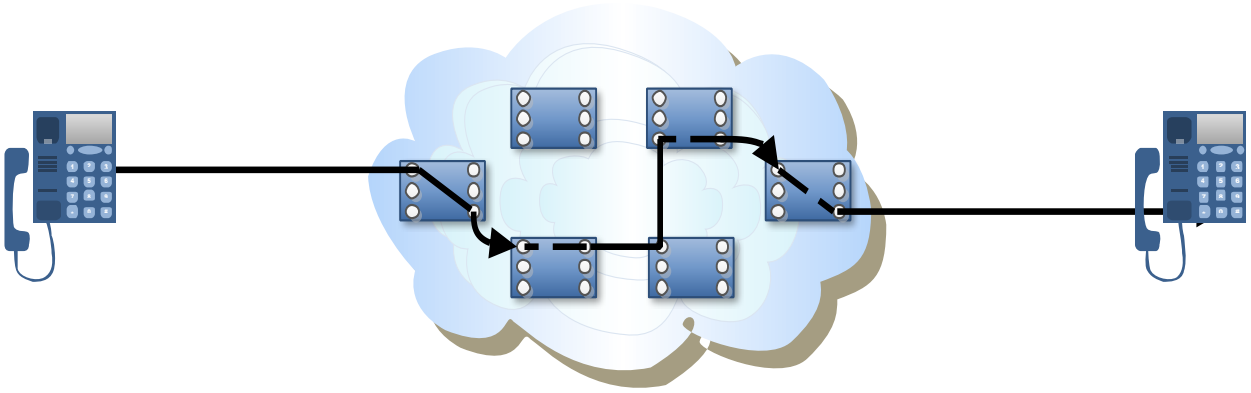


Figura 2-1 Conmutación de Circuitos.

2.1.1 Red Pública Telefónica

La Red Pública Telefónica (PSTN) es esencialmente una red basada en circuitos. Esta red cubre tanto telefonía fija como móvil y es la red que hace posible que podamos comunicarnos con cualquier persona. En sus inicios fue una red analógica pero actualmente es una red en su mayoría digital; de tal manera que existen dos tipos de circuitos: analógicos y digitales [2].

2.1.1.1 Sistemas analógicos

La Red Telefónica Básica (RTB) se define como la agrupación de todos los medios de transmisión y conmutación necesarios para conectar dos equipos terminales a través de un circuito físico que nos permite establecer una comunicación, este circuito es temporal ya que se desconecta al finalizar la llamada, este proceso las realizan las redes de telecomunicaciones conmutadas. Esta fue creada para transmitir la voz humana, además se podía utilizar para trasportar datos; y dada la naturaleza de la información a transmitir y la tecnología en la época en la que fue creada, este fue de tipo analógicos, hasta hace poco se denominaba Red Telefónica Conmutada (RTC), por la aparición de la Red Digital de Servicios Integrados (RDSI), pero también basados en la conmutación de circuitos. Este hecho impuso la terminología RTB para Red Telefónica Analógica y reservando las siglas RTC para la Redes Conmutadas ya sean Analógicas o Digitales. De la misma forma que Internet es la red global de datos, la RTB es la madre de todas las redes de conmutación de circuitos usada para el tráfico de voz.

Sin importar el tipo de tecnología ya sea analógico o digital se requiere de un enlace desde nuestro hogar hasta la central telefónica asignada a nuestra zona, por esta razón es de gran importancia conocer los 2 tipos de conexiones telefónicas analógicas existentes, conocidas como FXS y FXO, dicho de otra manera los nombres de los puertos o interfaces usados por las líneas telefónicas y los dispositivos analógicos [1].

2.1.1.1.1 FXS

Un FXS (Foreigne Xchange Subscriber) es lo que está situado al otro lado de la línea telefónica o bien es el puerto por el cual el abandono accede a la línea telefónica, ya sea de la compañía telefónica o de la central de la empresa. En otras palabras, la interfaz FXS provee el servicio al usuario final (Teléfonos, módems o faxes). Los puertos FXS son, los encargados de: proporcionar tono de marcado, suministrar tensión y corriente al dispositivo final.

La interfaz FXS es el punto donde se conectan los teléfonos del hogar que quieren hacer uso de la línea, de manera más simple la interfaz FXS sería entonces la roseta de telefonía del hogar [1] [5].

2.1.1.1.2 FXO

Un FXO (Foreigne Xchange Office) es cualquier dispositivo que actúa como teléfono tradicional o bien es el puerto por el cual se recibe a la línea telefónica. Los FXO poseen funciones que son capaces de aceptar una señal de llamada o ring o ponerse en estado de colgado o descolgado, enviar y recibir señales de voz conocida como cierre de bucle.

Un ejemplo de esta interfaz es la conexión telefónica que tienen los teléfonos analógicos, fax, etc. Es por ello que a los teléfonos analógicos se les denomina “dispositivos FXO” [1] [5]. Un conmutador que integra periféricos FXO y FXS puede conectarse a la RTB e incorporar teléfonos analógicos. Las líneas telefónicas que vienen del operador se tienen que conectar a una interfaz FXO. Los teléfonos se deben de conectar a las interfaces FXS del conmutador.

Existen 2 reglas que debemos de recordar:

1. Un FXS necesita estar conectado a un FXO (como una línea telefónica necesita estar conectada a un teléfono) o viceversa.
2. Un FXS suministra energía (elemento activo) a un teléfono FXO (elemento pasivo) [6].

2.1.1.2 Sistemas digitales

Los trabajos de desarrollo de la RDSI comenzaron en la década de los 80, pero no sería comercializada hasta principios de los años 90. Se esperaba que la RDSI pudiera revolucionar la industria de las comunicaciones telefónicas; como hoy en día se espera que lo pueda hacer la VoIP. A pesar de que las compañías telefónicas pusieron mucho empeño en extenderlo al mayor número de lugares posibles, muchos consideran a la RDSI un fracaso, debido a que todo lo que prometía no se pudo llevar a cabo. Lo certero es que la RDSI nunca terminó de despegar ya que cuando lo estaba haciendo surgió otra tecnología que tuvo una implementación mucho más barata y rápida, llamada ADSL(Asymmetric Digital Subscriber) [1] [5].La RDSI permite que en una línea haya múltiples canales, pudiendo contener en cada uno de ellos datos (canales B) o señalización (canales D). Pero además, la RDSI no se limita únicamente a la transmisión de voz. A diferencia de la RTB, cada canal de la RDSI tenía un ancho de banda de 64 Kbps, de forma que podían emplearse canales B y D para la transmisión de datos, siempre y cuando no haya datos de señalización por lo que esta característica brindaba una mayor flexibilidad que las que poseen las líneas RTB [1] [5].

El objetivo de la RDSI fue el facilitar las conexiones digitales para ofrecer una amplia gama de servicios integrados a los usuarios. RDSI establece dos tipos de interfaces para cumplir con este fin.

- BRI: Basic Rate Interface

Estuvo orientada a hogares. Contiene 2 canales útiles (llamados canales B) de 64 Kbit/s cada uno más un canal de señalización de 16 Kbit/s (llamado canal D) que en total suman 144 Kbit/s. Este se suponía que iba a ser un estándar para los hogares, pero no fue así del todo y tuvo muy poca popularidad en este segmento del mercado en los Estados Unidos, pero en Europa fue diferente y es utilizado en muchos países de este continente.

- PRI: Primary Rate Interface

Es la opción para usuarios de mayor envergadura como negocios o empresas debido a que puede contener más canales B. Actualmente es muy popular y se transmite sobre circuitos T-carrier y E-carrier [2].

2.1.1.3 E1/T1

Un T1 es un acceso digital que dispone de 24 canales, pudiéndose realizar en cada uno de ellos (menos uno) una llamada. Mientras que el T1 es muy común en Estados Unidos y Japón, en Europa se emplea con mayor frecuencia el E1. A diferencia del T1, esta línea dispone de 32 canales en vez de 24. Tanto los T1s como los E1s tienen que realizar el proceso de señalización de las llamadas de alguna manera. Esto se consigue mediante lo que se conoce como Señalización por Robo de Bit (Robbed Bit Signaling), es decir, que cada cierto tiempo se usa un bit de cada canal para así señalizar y enviar información a través de la línea (T1s), o mediante multiplexación del bit en un canal común, algo que se emplea sobre todo en Europa (E1s) [1].Usar T1s y E1s para proporcionar datos y voz a la vez es muy común. En esta ocasión, algunos de los canales de las líneas son asignados para ser usados para datos y otros son asignados para ser usados para voz. Incluso se puede dar el caso de que existan canales sin usar. Los proveedores de servicios pueden proporcionar en este caso precios más bajos de lo normal, ya que, por ejemplo, unos cuantos canales podrían ser para voz, otros para conectarse a Internet y un último grupo podría ser para conectarse de forma privada a otra oficina de la organización. Por todo lo comentado, si necesita tener, por ejemplo, de 8 a 16 líneas así como conexión de datos, tanto un T1 como un E1 (dependiendo de la zona donde estemos) podrían constituir una buena elección [1].

2.2 Redes por Conmutación de Paquetes

En este tipo de red se pueden transportar simultáneamente diferentes flujos de información por un mismo medio, para hacer esto posible, es dividido cada flujo de información en fragmentos o paquetes que se envían intercaladamente, posteriormente en el destino los paquetes son reensamblados para reproducir el mensaje original [2]. Es importante mencionar que cada paquete es tratado de forma independiente en cada nodo, por lo que debe contener la dirección del destino ya que, de esta manera, el nodo podrá tomar las decisiones de encaminamiento más adecuadas a cada caso, pero sin embargo un nodo no puede reenviar un paquete hasta que no ha sido completamente transmitido por el nodo anterior [3] [4].

En este tipo de red, el servicio suele ser sin conexión, ya que al no existir la reserva de recursos, es posible que algunos paquetes se pierdan. A diferencia de las redes orientadas a circuitos, en este tipo de redes el ancho de banda no es fijo ya que depende del tráfico de la red en un momento dado, así mismo cada paquete de un mismo flujo de información no está obligado a seguir el mismo camino por lo que los paquetes que originalmente fueron generados en secuencia puedan llegar desordenados a su destino. Y estos factores son muy importantes a tener en cuenta cuando se transporta tráfico de voz sobre una red de paquetes ya que afectan la calidad de la llamada [2] [3].

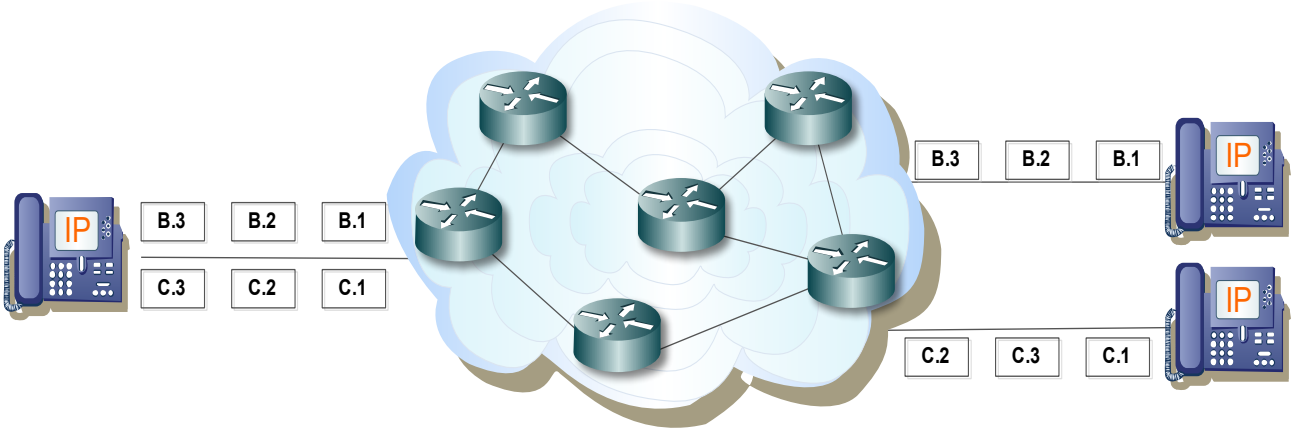


Figura 2-2 Conmutación de Paquetes.

En la Tabla 2-1 podemos visualizar de manera más clara la diferencia entre las redes conmutadas por circuitos y las conmutadas por paquetes.

Tabla 2-1 Comparativa de Redes de Conmutación de Circuito y Conmutación de Paquetes.

Elemento	Conmutación de circuitos	Conmutación de paquetes
Establecimiento de llamada	Requerido	No es necesario
Trayectoria física detallada	Si	No
Cada paquete puede seguir la misma trayectoria	Si	No
Los paquetes llegan en orden	Si	No
Una falla de conmutación es fatal	Si	No
Ancho de banda disponible	Fijo	Dinámico
Instantes donde puede presentarse una congestión	Durante el establecimiento	En cada paquete
Uso óptimo del Ancho de banda	No	Si
Transmisión de almacenamiento y reenvío	No	Si
Tarificación	Por minuto	Tarifa plana

2.2.1 Voz sobre IP

VoIP, es una tecnología que permite transportar voz sobre una red de datos basado en el Protocolo de Internet (IP).La telefonía IP, es una aplicación inmediata de VoIP.

La función principal del VoIP es convertirlos flujos de audio en flujo de paquetes para poder transportarlos sobre redes IP [6].

La Voz sobre IP, permite la unión de dos mundos históricamente separadas, el de transmisión de voz y el de transmisión de datos. Las redes IP fueron diseñas principalmente para datos y muchas de las ventajas de las redes IP para los datos resultan ser una desventaja para la voz pues son muy sensibles a ciertos parámetros como retardos, pérdidas, jitter, etc. [2].

2.2.2 Protocolos usados en VoIP

Los protocolos asociados con VoIP se dividen en 2 grupos: los que soportan el transporte de la voz en tiempo real y aquellos que soportan la señalización de la llamada y las funciones de control. Sin embargo existen otros protocolos involucrados y que proponen formas distintas de establecer una transmisión de voz sobre IP, cabe mencionar que dentro

del mismo protocolo IP se encuentran varios protocolos de red involucrados, tales como los de capa de transporte como TCP y UDP [2].

2.2.3 Protocolos de Transporte en Tiempo Real

Definen los mecanismos para la realización de una comunicación en tiempo real. Los protocolos de transporte en tiempo real más utilizados son RTP y RTCP [3].

2.2.3.1 RTP

RTP (Real Time Protocol) es el protocolo que hace posible la transmisión de audio y video en tiempo real sobre redes IP, asumiendo la existencia de pérdidas, retardos y variación dinámica de las características de la red durante la comunicación. Suministra funciones de transporte de extremo a extremo y ofrece servicios tales como identificación del tipo de carga, numeración de secuencia, estampas de tiempo, etc. Este protocolo no garantiza la entrega de paquetes en tiempo real, pero sí suministra los recursos para que éste se entregue de manera sincronizada.

La Figura 2-3 muestra la estructura de un paquete RTP.

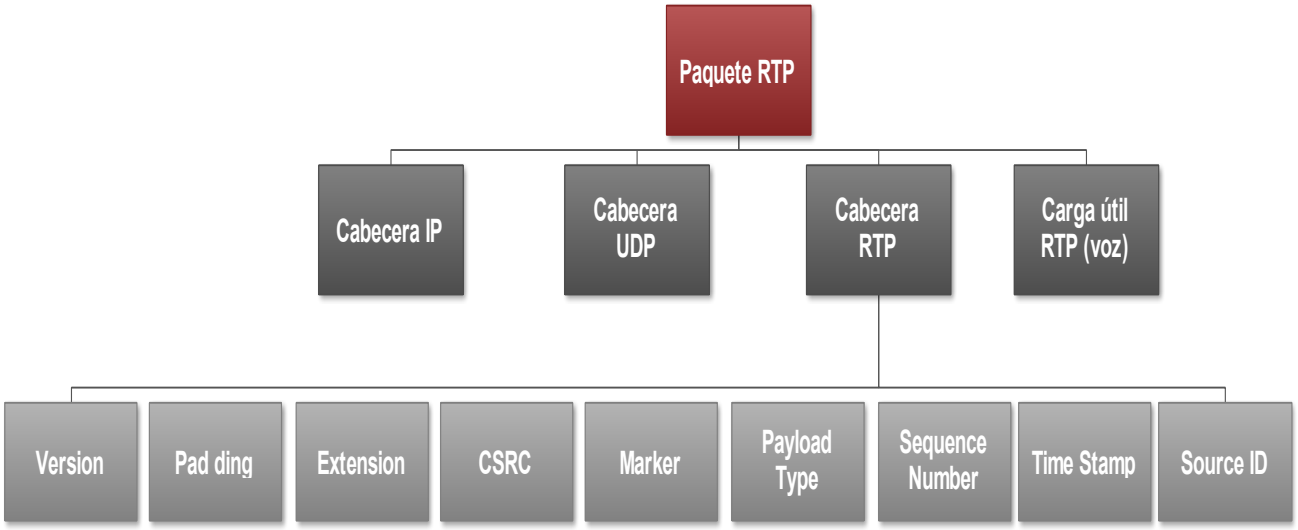


Figura 2-3 División Paquetes RTP.

2.2.3.2 RTCP

RTP dispone de medios para poder continuar con la reproducción del flujo de paquetes en presencia de pérdidas, jitter o retardo, sin embargo, no especifica ningún medio para estimar los valores de dichos parámetros. Para esto existe el protocolo de control en tiempo real, RTCP (Real Time Control Protocol).Este protocolo describe el intercambio de mensajes de control relacionados con la calidad de servicio (retardo, jitter, tasa de pérdidas, etc.) [3].

2.2.4 Protocolos de Señalización

El objetivo de estos protocolos es establecer un canal de comunicaciones a través del cual se pueda transmitir información del usuario y liberar el canal cuando finalice la transmisión. Los protocolos más utilizados en implementaciones comerciales son H323 y SIP [2] [5].

2.2.4.1 H323

El protocolo H323 fue diseñado por ITU, (International Telecommunication Union) en 1996. Fue diseñado para ser un estándar en la transmisión de audio, video y datos a través de las redes IP en las cuales no existe garantía de calidad del servicio. El estándar H.323 ofrece control y señalización de llamada, control medios y señalización RAS (registro, admisión y estado). La señalización de H.323 es muy rápida comparada con la de SIP, la cual utiliza paquetes de gran tamaño, debido a que sus mensajes son en código binario [1]. H.323 es, en realidad, un conjunto de protocolos que definen los componentes y los medios de interacción entre los mismos que deben cumplirse para soportar comunicaciones multimedia sobre las redes IP. H.323 está compuesto por cuatro elementos: Terminales, Gateways, Gatekeepers y Unidades de control multipunto [3].

2.2.4.2 SIP

El propósito del protocolo SIP es establecer la comunicación entre dos dispositivos multimedia a través de dos protocolos RTP/RTCP y SDP. El protocolo se usa para transportar los datos de voz en tiempo real, mientras que el protocolo SDP (Session Description Protocol) se emplea para la negociación de las capacidades de los participantes, como tipo de codificación, etc. Este protocolo tiene una sintaxis similar al HTTP. Tiene métodos para minimizar los efectos de DoS (Denial of Service). Utiliza un mecanismo de transporte seguro mediante TLS (Transport Layer Security). El protocolo SIP establece los siguientes elementos para establecer una comunicación: Agentes de Usuario (UA) y servidores. El UA se compone de dos partes, el UAC (User Agent Client) y el UAS (User Agent Server). El UAC se encarga de generar peticiones SIP y de recibir las respuestas de éstas. Por otro lado, el UAS se encarga de generar respuestas a las peticiones SIP [3].

CAPÍTULO 3 VOIP SOBRE SIP

SIP fue creado con el propósito de invitar usuarios a participar en sesiones, no fue diseñado desde cero, es decir está basado en la fusión de dos protocolos IETF propuestos para el mismo fin [8].

3.1. Historia del Protocolo SIP

3.1.1. SIP V1

A pesar de que las primeras transmisiones de voz a través de redes de conmutación fueron alrededor de 1974, los primeros sistemas de conferencia aparecieron a principios de 1990. Thierrry Turtelly desarrolló “INRIA Video conferencing System” (IVS) o Sistema de Videoconferencia INRIA, este sistema fue diseñado para la transmisión de audio y video a través del Internet. Un usuario IVS podía llamar a otro usuario y podía mantener una sesión unidifusión. IVS también podía utilizarse en sesiones de multidifusión. Aprovechando el códec de video H.261 a través de Internet, el trabajo realizado sobre IVS fue fundamental en el desarrollo del Protocolo RTP.

Más tarde, Eve Schooler desarrolló el Control de Conferencia Multimedia (MMCC) o Multimedia Conference Control, para conectar varios usuarios utilizaba el Protocolo de Control de Conexión (PCC) que era un protocolo orientado a transacciones. Un ejemplo típico consta de una solicitud realizada por el usuario y de una respuesta realizada desde el usuario remoto. Este protocolo utiliza UDP para su transporte, de esta manera implementó los tiempos de espera y retransmisiones para asegurar la entrega confiable de los mensajes del protocolo. Estos dos primeros sistemas multimedia dieron paso al diseño de Protocolo de Invitación de Sesión creada por Mark Handley y Eve Schoole, ésta fue la primera versión de SIP. SIPv1 fue presentado al IETF como un proyecto de Internet y utilizaba el protocolo SDP para descubrir las sesiones, UDP como transporte y se basaba en texto plano. Cabe destacar que SIPv1 únicamente manejaba el establecimiento de las sesiones y tenía la capacidad de proporcionar un cierto nivel de movilidad a los usuarios, ya que si un usuario se encontraba fuera de su estación de trabajo, el usuario podría optar por registrar su estación de trabajo temporal y recibir invitaciones de conferencias locales [8].

3.1.2. SCIP

De igual manera el 22 de Febrero de 1996, Henning Schulzrinne presentó un proyecto de Internet a la IETF llamado Simple Conference Invitation Protocol (SCIP), que también era un mecanismo para invitar usuarios a sesiones punto a punto y multidifusión. Se basaba en el Protocolo HTTP (Hypertext Transfer Protocol) y utilizaba TCP (Transmission Control Protocol) como protocolo de transporte y se basaba en texto al igual que SIPv1. SCIP utilizaba direcciones de correo electrónico como identificadores para los usuarios, con el fin de proporcionar un identificador universal para ambas comunicaciones tanto síncronas y asíncronas. La señal de SCIP permanece después del establecimiento de la sesión para los cambios de los parámetros en las sesiones en curso y cerraba las sesiones existentes. En lugar de reciclar un mecanismo para la descripción de la sesión como lo hace SDP.

En una sesión de la IETF en Los Ángeles presentaron el Protocolo SIP por Schooler y el Protocolo SCIP por Schulzrinne que finalmente después de una larga discusión se decide fusionarlos y el Protocolo resultante conserva el nombre de SIP pero cambia el significado de las siglas de Protocolo de Inicio de Sesión y avanzó a la versión 2 [8].

3.1.3. SIP V2

SIP es un protocolo de señalización desarrollado en respuesta a las recomendaciones del UIT –T H.323, debido a que el IETF creía que H.323 era inadecuado para la evolución de los requerimientos de la telefonía, ya que su estructura de mando era demasiado centralizada y monolítica. SIP es un protocolo de capa de control que permite el establecimiento, la liberación y la modificación de sesiones multimedia a través del Internet. Estas sesiones pueden ser conferencias, telefonía o transferencias de datos multimedia, con prestaciones como la mensajería instantánea y la movilidad de aplicaciones en entornos de red. La función principal de SIP es distribuir la información de la descripción de la sesión y durante ésta, negociar y modificar sus parámetros y utiliza el puerto 5060 como puerto de destino. SIP admite la asignación de nombres y servicios de redirección, lo que permite la implementación de servicios de ISDN [2].

SIP soporta protocolos como Resource Reservation Protocol (RSVP), RTP, Real – Time Streaming Protocol (RTSP), SAP y SDP, pero también hereda funcionalidades de ciertos protocolos como HTTP, utilizados para navegar sobre la Web y “Simple Mail Transport Protocol” (SMTP) utilizados para transmitir mensajes electrónicos. La Figura 3-1 muestra los protocolos asociados con SIP [9].

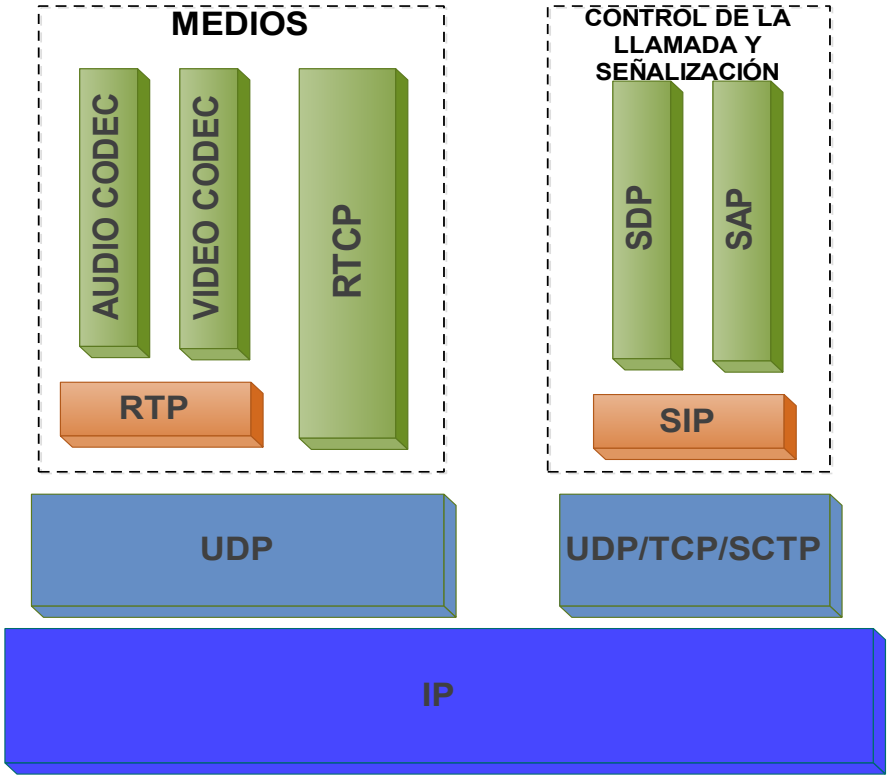


Figura 3-1 Protocolos Asociados con SIP.

3.2. Arquitectura y componentes SIP

SIP está basado en una arquitectura cliente servidor, en la cual los clientes inician llamadas y los servidores responden las llamadas. Debido a la simplicidad, escalabilidad, modularidad y comodidad, SIP es un protocolo abierto basado en estándares; ha sido extendido con el fin de soportar numerosos servicios tales como la mensajería instantánea, el establecimiento de llamada, la conferencia, entre otros. Además SIP ha sido elegido por el 3GPP para la arquitectura “IP Multimedia Subsystem” (IMS) como protocolo para el control de sesión y el control de servicio. Dado que SIP es un protocolo de señalización, una vez establecida la sesión los participantes intercambian directamente tráfico de audio y video a través del protocolo RTP. Por otro lado SIP no es un protocolo de reservación de recursos y por consecuencia no puede asegurar la calidad del servicio, de modo que se trata de un protocolo de control de llamada y no de control del medio. De la misma manera tampoco es un protocolo de transferencia de archivos tal como HTTP, usado con el fin de transportar grandes volúmenes de datos, ya que SIP fue diseñado para transmitir mensajes de señalizaciones cortas con el fin de establecer, mantener y liberar sesiones multimedia [4].

La red SIP cuenta con los siguientes elementos:

- Usuarios: Son los dispositivos que utiliza el usuario final para acceder y utilizar los servicios multimedia.
- Servidores SIP: Se utilizan en modalidades de Proxy o de redireccionamiento, se utiliza para localizar otros usuarios SIP o para reenviar mensajes en el caso de modo Proxy.
- Gateway SIP: Es una aplicación o dispositivos genéricos que permiten la interconexión de una red SIP a otras redes distintas con diferentes protocolos, tales como: H.323, PSTN, etc.

En la Figura 3-2 se muestra la Arquitectura de una red SIP.

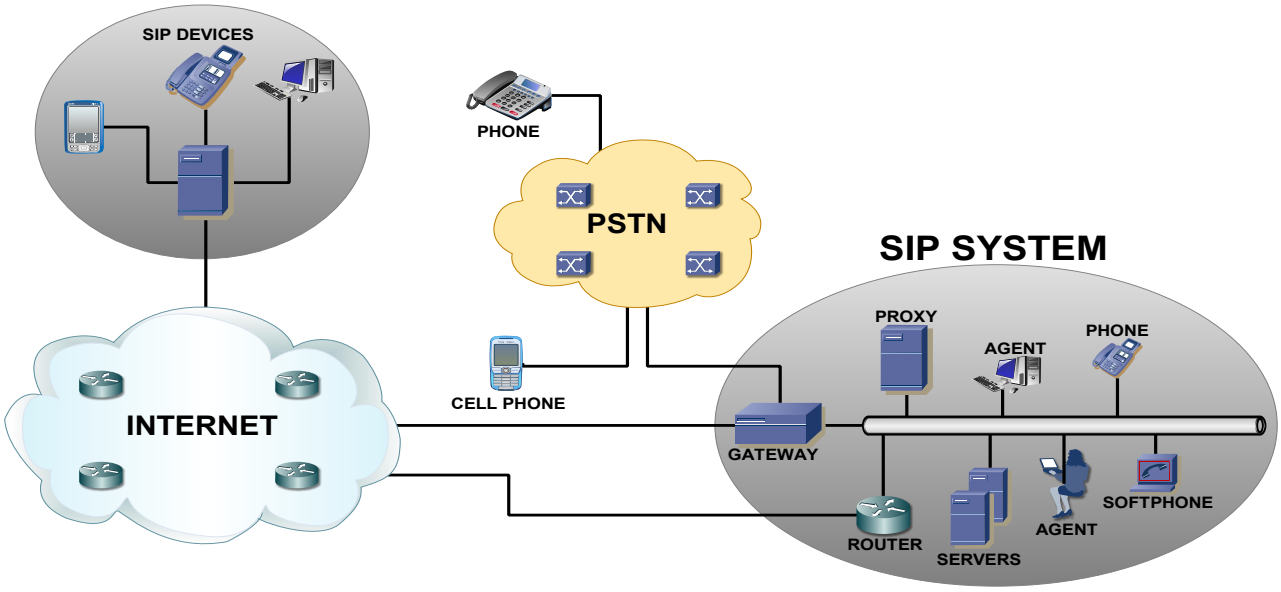


Figura 3-2 Arquitectura Red SIP.

Los dos componentes principales en una red SIP son los Agentes de Usuario y los Servidores de Red [3].

3.2.1. Agentes de Usuario

Los UA, son dispositivos que generan solicitudes para iniciar una llamada o terminar una en curso. Los UA se dividen, a nivel lógico, en dos entidades:

- Un Agente de Usuario Cliente inicia las solicitudes SIP.
- Un Agente de Usuario Servidor recibe las solicitudes y devuelve las respuestas en nombre del usuario, actúa como el agente de usuario llamado.

Ambas partes, UAC y UAS, pueden terminar una sesión en curso, los UA pueden ser teléfonos IP o sotfphones [7] [3].

3.2.2. Servidores SIP

Los servidores de Red son aplicaciones que aceptan las solicitudes SIP y responden a ellos. Los servidores SIP actúan como intermediarios en las comunicaciones entre los Agentes de Usuario y existen de cuatro tipos: Servidor proxy, servidor de localización, servidor de redirección y servidor de registro. Dado de que los Servidores proporcionan servicios y funciones a los Agentes de Usuario, éstos se deben de apoyar tanto de TCP, TLS y UDP para el transporte [10] [3].

3.2.2.1. Servidor de Registro

Es un servidor que acepta solicitudes de registro de los usuarios, de tal forma que el usuario indica por medio de un mensaje REGISTRER la dirección de localización (dirección IP), entonces el servidor actualiza una base de datos y guarda la información de éstas peticiones para suministrar traducción de direcciones en el dominio que controla. Generalmente este Servidor requiere que el UA se registre para ser autenticado, de manera que las llamadas entrantes no puedan ser tomadas por un usuario no autorizado [3] [8].

3.2.2.2. Servidor de Localización

Este tipo de servidor proporciona información acerca de la localización del usuario. Si un usuario A desea comunicarse con un usuario B, en primer lugar A necesita descubrir la localización actual de B en la red, con el fin de que la petición de establecimiento de sesión pueda llegarle. Además hay que tener en cuenta que el usuario B puede estar en diferentes lugares en instantes distintos. Esto es posible ya que hace uso de la información de los usuarios registrados o desde otra base de datos. La mayoría de los usuarios registrados actualizan su ubicación a un servidor de localización tras la recepción. Sin embargo entre la comunicación de los servidores de localización y los servidores SIP no se utiliza el protocolo SIP, sino que se utiliza el protocolo Lightweight Directory Access Protocol (LDAP) [3] [10].

3.2.2.3. Servidor Proxy

Los Servidores Proxy trabajan como dispositivos intermediarios que reciben solicitudes SIP que interpretan y deciden hacia a que otros servidores retransmitirlas después de haber realizado modificaciones en los encabezados sobre estas solicitudes sólo si es necesario.

Este proceso se puede llevar a cabo ya que comúnmente los Servidores tienen acceso a una base de datos o a un servicio de localización.

Al recibir los encabezados se identifica que Servidor Proxy ha sido el iniciador de la petición y asegura que las respuestas sigan el mismo camino de regreso al Servidor Proxy en lugar del cliente. Este servidor tiene la particularidad de actuar como cliente y servidor con el propósito de establecer llamadas entre los usuarios. Poseen una funcionalidad similar a la de un Proxy HTTP que tiene la tarea de encaminar las peticiones que recibe de otras entidades próximas al destinatario, además de proporcionar funciones como autenticación, autorización, control de acceso a la red, enrutamiento, retransmisión confiable de la solicitud y seguridad.

Los Servidores Proxy pueden ser clasificados de acuerdo a la cantidad de información del estado que almacenan durante una sesión. SIP define tres tipos de servidores:

Call Statefull Proxy: Este tipo de servidor necesita estar informado de todas las transacciones SIP que se producen durante una sesión. Ellos siempre están en el camino que toman los mensajes SIP que viajan entre los usuarios. También almacenan la información del estado desde el momento que la sesión es establecida hasta el momento en que se termina.

Statefull Proxy: A menudo son llamados Proxy con Estado de Transacción ya que su única preocupación es la de mantener el estado de las transacciones durante el procesamiento de las peticiones. A diferencia del Call Statefull Proxy no necesita estar en el camino que toman los mensajes SIP para las transacciones posteriores. Permite la división de una petición en varias, a este proceso se le conoce como *Forking Proxies*, cuya finalidad es la de la realizar una búsqueda en paralelo de la llamada dependiendo de su configuración. Una búsqueda en paralelo consiste en tratar de buscar en todo los posibles lugares al mismo tiempo y así obtener la mejor respuesta para enviarla al usuario que realizó la llamada.

Stateless Proxy: No mantienen el estado de las transacciones durante el procesamiento de las peticiones, únicamente reenvía la respuesta basada sólo en el contenido del mensaje al siguiente salto e inmediatamente después elimina todos los estados relacionados a la solicitud. Un Stateless Proxy no vuelve a retransmitir los mensajes y tampoco utiliza ningún temporizador SIP [3] [8].

3.2.2.4. Servidor de Redirección

Servidor que se encarga de aceptar solicitudes SIP, traduce la dirección SIP de destino en una o varias direcciones de red y devuelve las respuestas al cliente que contiene la dirección y redirección a las peticiones hacia el próximo servidor. Utiliza una base de datos o servicio de localización para buscar al usuario. El Redirect Server a diferencia del Proxy Server no inicia transacciones, sino que reciben las solicitudes desde un UAC, remiten al mismo Agente un mensaje indicando el o los servidores con los que debe ponerse en contacto, este proceso es similar al de la búsqueda interactiva del DNS. De igual manera tampoco acepta llamadas ni procesa ni reenvía peticiones SIP. Este tipo de servidores gestionan mayor número de mensajes que los Servidores Proxy, pero con menor procesamiento [3].

3.3. Mensajes SIP

Existen dos tipos de mensajes SIP: Las peticiones iniciadas por los clientes SIP y las respuestas obtenidas por los servidores. Cada mensaje contiene un encabezado que describe los detalles de la comunicación. Ya que SIP es un protocolo basado en texto, estos mensajes tienen una estructura idéntica a la del Protocolo HTTP, con una primera línea, una cabecera y finalmente un cuerpo del mensaje opcional. Los mensajes SIP se envían sobre TCP o UDP con múltiples mensajes transportados en una única conexión TCP o datagrama UDP.

Los mensajes se utilizan para el intercambio de información necesaria entre los clientes, para inicializar llamadas, agregar usuarios a la lista de contactos, eliminar usuarios, mostrar la presencia de los mismos, finalizar llamadas, enviar confirmaciones, etc.

Los Mensajes SIP están formados por tres elementos: Línea de petición, encabezado y cuerpo del mensaje [7].

3.3.1. Peticiones

La especificación principal de SIP describe seis tipos de peticiones SIP:INVITE, REGISTRER, BYE, ACK, CANCEL Y OPTIONS, estas solicitudes también conocidas como Métodos, cada una con un propósito diferente, permite a los UA y a los Servidores de Red localizar, invitar y gestionar llamadas. Los nombres de los Métodos son sensibles a las mayúsculas y convencionalmente se usan en mayúsculas para una mayor claridad visual para poder distinguirlos de los campos de la cabecera ya que se utilizan tanto mayúsculas como minúsculas. Las solicitudes o métodos son considerados como verbos en el

Protocolo SIP, desde que ellos solicitan una acción específica para ser utilizado por otro UA o Servidor de Red [10].

3.3.1.1. INVITE

El método INVITE es usado con el fin de que dos o más User Agent establezcan y participen en una sesión y de igual manera modifica una sesión multimedia existente. Esta petición puede ser reenviada por los Proxy Servers, INVITE corresponde al mensaje ISUP IAM o al mensaje Q.931 SET UP e incluye una descripción de la sesión utilizando el Protocolo SDP para indicar que características tendrá la comunicación, tales como: Direcciones IP del llamante y del llamado, Localización de usuario, Calidad de Servicio (QoS), información de seguridad y los códecs a utilizar. La llamada en curso indica el tipo de flujo que serán intercambiados (Voz, Video, etc.). Con este método simple, los usuarios pueden reconocer las capacidades del otro extremo y abrir una sesión de conversación con número limitado de mensajes y circuitos [10].

3.3.1.2. REGISTER

Este método es empleado por los usuarios para registrar su dirección de contacto actual. Dicho de otra forma, un UAC envía peticiones REGISTER a un servidor de registro-localización para informar de la posición actual en la que se encuentra en un momento determinado. Esto hace posible que UAC pueda ser localizado haciendo uso de una misma dirección user@dominio sin importar dónde se encuentre físicamente. Éste método puede contener un cuerpo de mensaje, aunque su uso no está definido en la norma [3] [1].

3.3.1.3. ACK

Este método es enviado por el usuario origen que envió la petición INVITE para hacer saber al usuario destino que su respuesta 200 OK ha sido recibida. Ahora es cuando ambos pueden empezar a enviar tráfico. Este método ACK no se puede utilizar para modificar una descripción de medios que ya haya sido enviado en el INVITE inicial [1].

3.3.1.4. BYE

El método BYE se utiliza para terminar una sesión de los medios de comunicación establecidos. Una sesión se considera establecida si un INVITE ha recibido una respuesta de clase éxito (2xx) o un ACK ha sido enviado. Un BYE se envía solamente por los Agentes de Usuario que participaron en la sesión, nunca por Servidores Proxy o por terceras partes, ya que éste es un método de extremo a extremo, por lo que las respuestas sólo se generan por el otro Agente de Usuario [10].

3.3.1.5. CANCEL

Este método se utiliza para terminar búsquedas pendientes o intentos de llamadas. Puede ser generado por cualquiera de los Agentes de Usuario o Servidores Proxy. Por ejemplo si el destino está sonando pero aún no ha sido descolgado y el teléfono origen cuelga, se envía un CANCEL, a diferencia del BYE que se enviaría si el teléfono destino hubiera sido descolgado previamente y por tanto la comunicación establecida se cancelaría en unos instantes [10].

3.3.1.6. OPTIONS

El método OPTIONS se utiliza para consultar un Agente de Usuario o un Servidor sobre sus capacidades y descubrir su disponibilidad actual. Un Agente de Usuario o un Servidor responde a la solicitud como lo haría un INVITE. Una solicitud de OPTIONS no puede contener un cuerpo de mensaje. Un Servidor Proxy determina si es una solicitud de OPTIONS mediante el examen de la petición de URI, si la respuesta URI contiene la dirección del Servidor Proxy, la petición es el Servidor Proxy, de lo contrario la petición será reenviada a otro Agente de Usuario o a otro Servidor Proxy [10].

3.3.2. Respuestas

Cada petición SIP lleva asociada una respuesta enumerada con un código que la identifica. Estos códigos son desde el identificador 100 hasta el identificador 699, siendo además colocadas en grupos de respuestas tales como: 1xx, 2xx, 3xx, 4xx, 5xx y 6xx.

- Las respuestas del grupo 1xx indican el estado temporal de la comunicación. Estas se utilizan por ejemplo cuando se tiene en progreso el establecimiento de una comunicación mediante la petición INVITE.
- Las respuestas pertenecientes al grupo 2xx corresponden a respuestas que informan el éxito de una petición SIP. Por ejemplo, cuando se establece con éxito el establecimiento de comunicación con la petición INVITE se envía una respuesta 200 OK informándolo al UAC origen.
- Las respuestas conformadas en el grupo 3xx informan de que la petición SIP debe de ser reenviada a otro UAS. Un Servidor de Redirección nos enviará una respuesta con código “302 Moved Temporarily.”
- Las respuestas del grupo 4xx corresponden a errores en el cliente SIP.
- Las respuestas del grupo 5xx corresponden a errores al Servidor SIP.
- Las respuestas que corresponden al grupo 6xx informan de errores generales [1].

En laTabla3-1 se muestran las posibles respuestas del Protocolo SIP.

Tabla 3.1 Tabla de Respuestas SIP.

TIPO DE RESPUESTA	IDENTIFICADOR	SIGNIFICADO
Informan el estado provisional de la comunicación	100	Trying
	180	Ringing
	181	Call Being Forwarded
	182	Call Queued
	183	Session Progress
Informan el éxito de la comunicación	200	OK
	202	Accepted
Informan el reenvío necesario de la petición SIP	300	Multiple Choices
	301	Moved Permanently
	302	Moved Temporarily
	305	Use Proxy
	380	Alternative Service
Informan errores en el cliente	400	Petition Bad Request
	401	Unauthorized
	402	Payment Required
	403	Forbidden
	404	Not Found
	405	Method Not Allowed
	406	Not Acceptable
	407	Proxy Authentication Required
	408	Request Timeout
	410	Gone
	413	Request Entity too Large
	414	Request URI Too Long
	415	Unsupported Media Type
	416	Unsupported URI Scheme
	420	Bad Extension

	421	Extension Required
	423	Interval Too Brief
	480	Temporarily Unavailable
	481	Call/Transaction Does Not Exist
	482	Loop Detected
	483	Too Many Hops
	484	Address Incomplete
	485	Ambiguoss
	486	Busy Here
	487	Request Terminated
	488	Not Acceptable Here
	491	Request Pending
	493	Undecipherable
Informan errores en el Servidor	500	Server Internal Error
	501	Not Implemented
	502	Bad Gateway
	503	Service Unavailable
	504	Server Time Out
	505	Version Not Supported
	513	Message Too Large
Informan errores generales	600	Busy Everywhere
	603	Declined
	604	Does Not Exist Anywhere
	606	Not Acceptable

En la Figura 3-3 se muestra los pasos básicos del establecimiento de una llamada SIP.

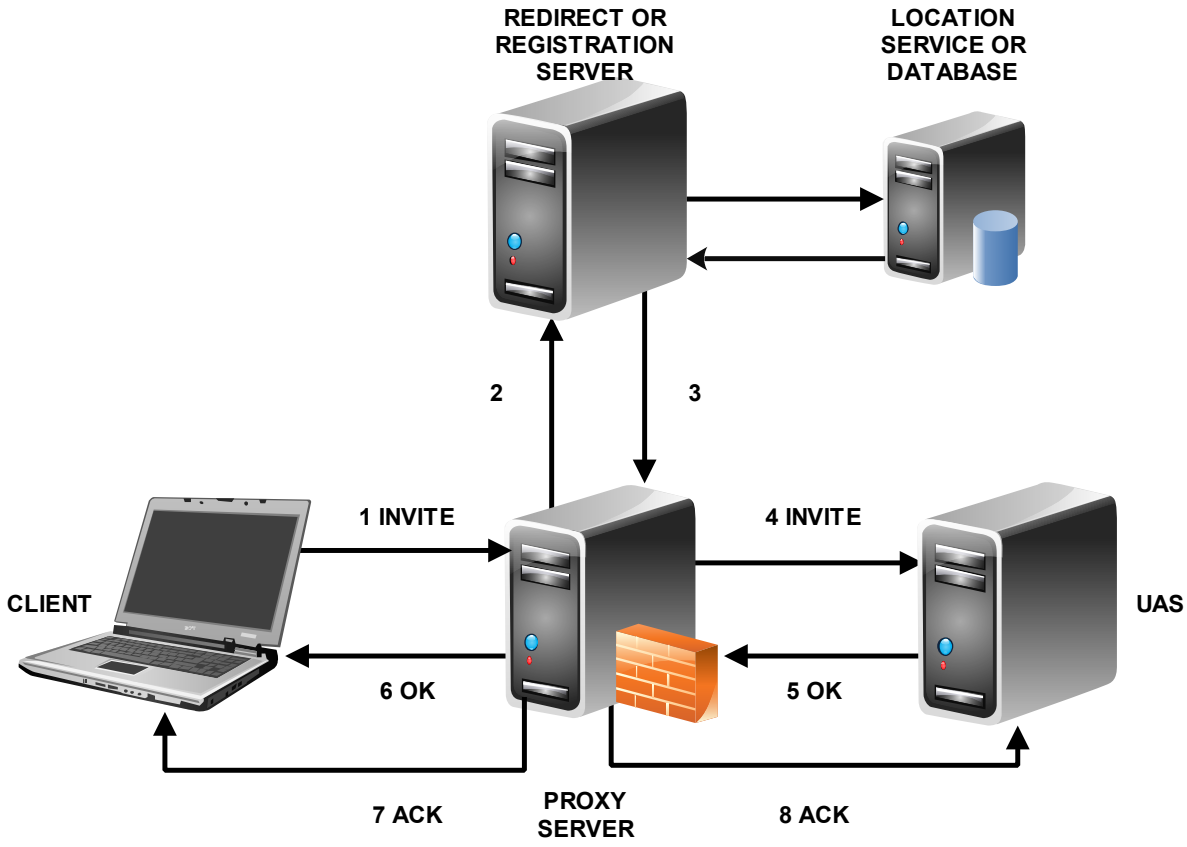


Figura 3-3 Establecimiento de una Llamada SIP.

3.4. Sistemas IP – PBX Basados en Linux

3.4.1. Elastix

Es un software de código abierto para el establecimiento de comunicaciones unificadas y de esta forma incorpora en una única solución todos los medios y alternativas de comunicaciones existentes en el ámbito empresarial.

3.4.1.1. Comunicaciones unificadas

Elastix inició como interfaz de reporte para llamadas Asterisk. Fue liberado en Marzo de 2006. La Figura 3-4 muestra los diversos servicios que proporciona Elastix.

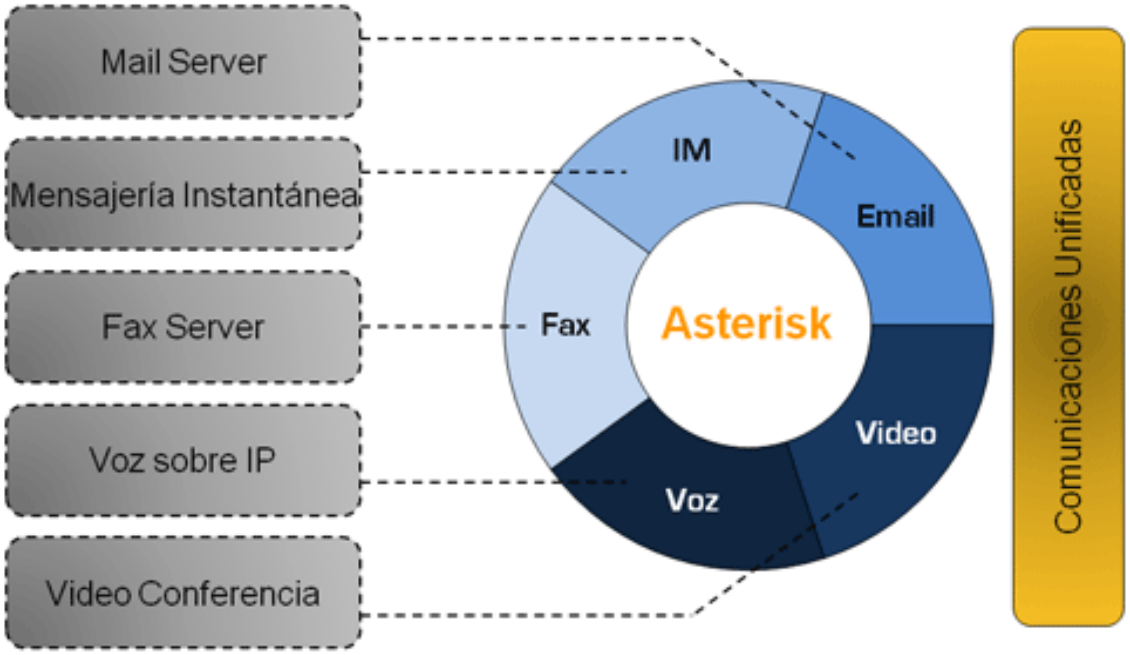


Figura 3-4 Comunicaciones Unificadas –Elastix.

3.4.1.2. Características y funcionalidades

3.4.1.2.1. PBX

Grabación de llamadas.

Correo de voz.

Correo de voz a E – mail.

Interfaz de detección de hardware.

Servidor DHCP para asignación dinámica de IP's.

Panel de Operador basado en Web.

Reporte de destalle de llamadas (CDR).

Centro de Conferencias con Salas Virtuales.

Soporte para protocolos SIP e IAX, entre otros.

Codecs 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).

3.4.1.2.2. Fax

Servidor fax basado en Hylafax.

Visor de faxes integrado con PDF's descargables.

Aplicación Fax a E – mail.

Personalización de faxes-a-email.

Control de acceso para clientes de fax.

Puede ser integrada con Winprint Hylafax.

3.4.1.2.3. IM

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.

Soporte a conexión a otras redes de mensajería como MSN, Yahoo, Gtalk, ICQ.

3.4.1.2.4. E – MAIL

Servidor de E – mail con soporte multidominio.

Administración centralizada vía Web.

Cliente de E – mail basado en Web.

Soporte Antispam.

3.4.1.2.5. General

Monitor de Recursos del Sistema.

Configurador de parámetros de red.

Configuración de apagado/re-encendido de la central vía Web.

Control de Acceso a la interfaz, basado en ACL's [2].

3.4.2. Asterisk

Es una plataforma software de Dominio Público (Open Software) para el desarrollo de centrales telefónicas y es considerado por algunos como el sistema de telefonía más flexible y extensible de los que actualmente existen en el mercado. Proporciona todas las funcionalidades de los grandes sistemas propietarios y ofrece algunas posibilidades y servicios todavía no disponibles en ellos. Además, es el más competitivo en precio.

Está sujeto a la licencia de distribución de software GPL y utiliza para su funcionamiento el sistema operativo Linux, también de libre distribución. Fue creado por Mark Spencer como respuesta a la estrategia de la mayoría de los fabricantes de telefonía de mantener sus

sistemas completamente cerrados para cautivar a sus clientes y evitar la libre competencia. Actualmente es uno de los proyectos de Dominio Público de más difusión y con una de las comunidades de usuarios y desarrolladores más activa. Además, Digium, la empresa fundada por Mark Spencer, se encuentra detrás de este proyecto soportándolo comercialmente [5].

3.4.2.1. Características

Interoperabilidad.

Flexibilidad y capacidad de crecimiento.

Funcionalidad.

La arquitectura de Asterisk está basada en un sistema modular que depende del núcleo principal del sistema.

El núcleo del sistema se basa principalmente en cuatro componentes:

- Gestión de Módulos
- Temporizador de Sistema
- Gestión de Canales
- Interfaces del Sistema

La Figura 3-5 se muestra la Arquitectura de Asterisk [5].

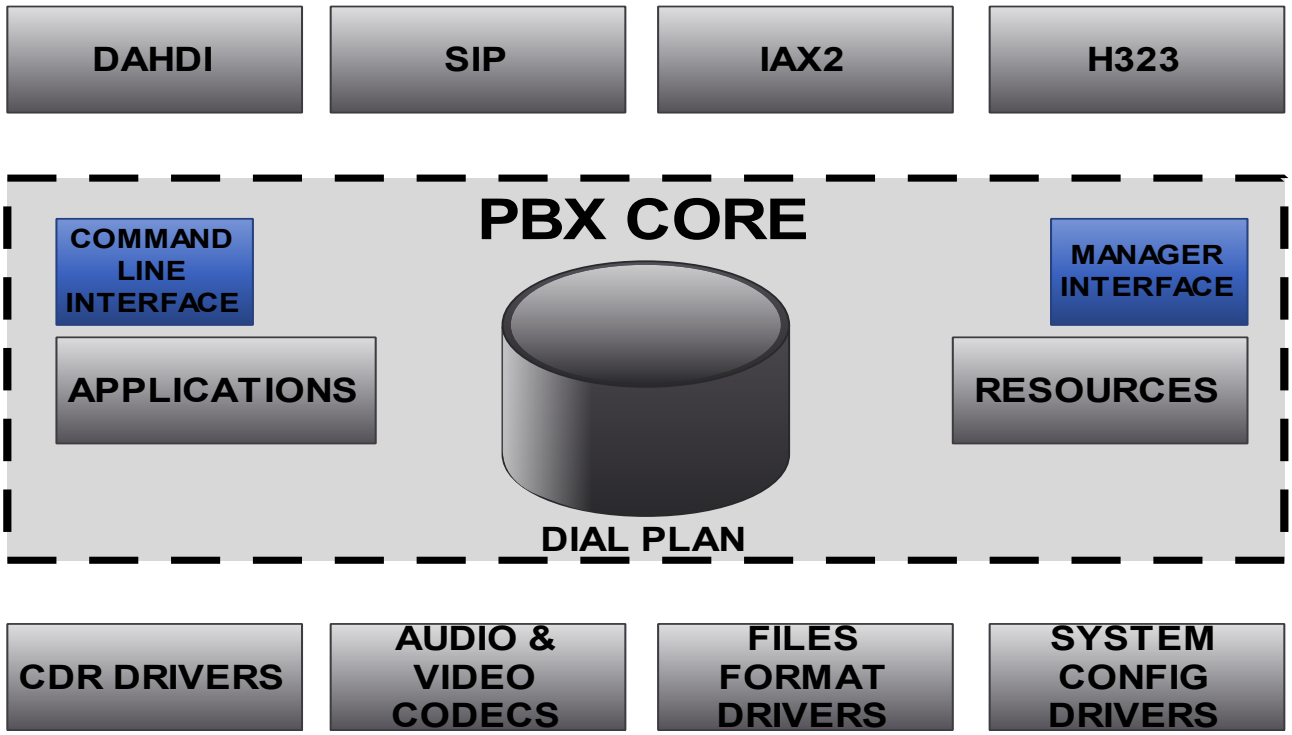


Figura 3-5 Arquitectura de Asterisk.

CAPÍTULO 4 CALIDAD DE SERVICIO EN VOIP

La calidad de servicio de una red o **QoS** es la capacidad de la misma para transportar el tráfico procedente de una fuente determinada, dadas sus características de pérdidas, retardo, jitter, ancho de banda, etc. Estas características forman parte de lo que se denomina perfil de tráfico de la fuente. El perfil de las fuentes de tráfico en tiempo real suele caracterizarse por un bajo retardo, una tolerancia al jitter, un ancho de banda garantizado y una tasa de pérdidas lo más bajo posible [2].

Los mecanismos de QoS tiene como objetivo proporcionar unas prestaciones adecuadas a cada fuente de tráfico de acuerdo con su perfil, para ello es necesario:

- Clasificar el tráfico.
- Gestión del Ancho de banda.
- Control de situaciones de congestión en la red (dando prioridad a fuentes de tráfico más restrictivas).

Otros mecanismos relacionados son:

- Fragmentación del tráfico
- Prevención de la congestión
- Adaptación del tráfico.
- Control de admisión

Otras características referentes a QoS son:

- La accesibilidad: La capacidad de iniciar una llamada cuando se desee
- Velocidad de enrutamiento: La velocidad con la que se establecen las llamadas
- Fiabilidad de conexión: La fiabilidad del proceso del establecimiento de la llamada
- Fiabilidad del enrutamiento: La fiabilidad del proceso de enrutamiento de la conexión con el destino solicitado
- Continuidad de conexión: La capacidad de mantener la conexión con una calidad aceptable hasta que ya no sea necesario
- Fiabilidad de la desconexión: La fiabilidad de las respuestas del sistema a las instrucciones de terminar y por lo tanto detener la conexión [11]

Los mecanismos de clasificación del tráfico o el control de admisión, resultan más adecuadas en los bordes de la red (edge routers), mientras que los mecanismos de control de congestión en los routers del backbone [3].

Los problemas de la calidad del servicio en VoIP vienen derivados de dos factores principalmente:

- Las redes IP están basadas en la conmutación de paquetes y por tanto la información no viaja siempre por el mismo camino. Esto produce efectos como la pérdida de paquetes o el jitter.
- Las comunicaciones VoIP son en tiempo real, por tal motivo los efectos del eco, pérdida de paquetes y retardo o latencia son no deseados en una comunicación [6].

Decimos que una red o un proveedor ofrecen QoS cuando se garantiza el valor de uno o varios de los parámetros que definen la calidad de servicio que ofrece la red. El contrato que especifica los parámetros de QoS acordados entre el proveedor y el usuario (cliente) se denomina SLA (Service Level Agreement) y se refiere a la habilidad de la red, de ofrecer prioridad a unos determinados tipos de tráfico, sobre diferentes tecnologías, incluyendo: Frame Relay, ATM, LANs y líneas dedicadas [11].

4.1. Parámetros de Calidad de Servicio

La calidad de servicio en VoIP puede discutirse bajo los siguientes apartados:

- Calidad en redes IP
- Calidad de la VoIP
- Ingeniería de tráfico
- Seguridad VoIP

QoS lo definen principalmente 4 parámetros: ancho de banda, retardo, variación de retardo (jitter) y probabilidad de error (o pérdida de paquetes).

4.1.1. Retardo

La latencia o retardo se define como el tiempo que tarda un paquete en llegar desde la fuente al destino.

4.1.2. Jitter

El jitter es la variación del tiempo de arribo entre paquetes consecutivos. El jitter es ocasionado principalmente por congestiones en la red, pérdida de paquetes, y cambios de rutas. Par atenuar los efectos del jitter se utiliza un de-jitter buffer. La idea básica del de-

jitter buffer es reordenar a los paquetes si es necesario y retrasar deliberadamente la reproducción del sonido para garantizar que los paquetes más “lentos” hayan llegado.

4.1.3. Pérdida de paquetes

En las redes de datos, la pérdida de paquetes es común y esperada. Representa el porcentaje de paquetes transmitidos que se descartan en la red.

Estas pérdidas pueden ser producto de alta tasa de error en alguno de los medios de enlace o por sobrepasar la capacidad de un buffer de una interfaz en momentos de congestión.

4.2. Evaluación de Calidad de Servicio

Existen diversos métodos para evaluar la calidad de servicio, los cuales se clasifican en métodos subjetivos y métodos objetivos.

En el método subjetivo la calidad de la voz se establece a través de la opinión del usuario. La calidad de audio puede ser evaluada directamente (ACR) Absolute Category Rating o en forma comparativa contra un audio de referencia (DCR) Degradation Category Rating. Con evaluaciones directas ACR se califica el audio con valores entre 1 y 5, siendo 5 “Excelente” y 1 “Malo”. El MOS (Mean Opinion Score) es el promedio de los ACR medidos entre un gran número de usuarios. Si la evaluación es DCR, el audio se califica también entre 1 y 5, siendo 5 cuando no hay diferencias apreciables entre el audio de referencia y el medido, 1 cuando la degradación es muy molesta [13].

Cabe mencionar que los métodos subjetivos se caracterizan por ser caros y lentos a la vez, ya que requiere de un gran panel de usuarios y dependen del idioma y de lo que el usuario obtuvo de sus experiencias.

El promedio de los valores DCR es conocido como DMOS (Degradation MOS). La metodología de evaluación subjetiva más ampliamente usada es la del MOS (Mean Opinión Score), estandarizada en la recomendación ITU-T P.800 [12].

La ITU ha recomendado el modelo E para cuantificar la calidad de la voz que percibe el usuario final.

En el modelo E, los efectos de los retardos, los paquetes perdidos y otros desperfectos relevantes dentro de una red, se combinan dentro de un valor llamado factor R, que varía de 0 (en el peor de los casos) hasta 100 (en el mejor caso). El factor R esta expresado como la suma de cuatro términos como sigue:

$$R = R_0 - I_s - I_d - I_e + A \quad (1)$$

Dónde R_0 representa la relación señal a ruido (SNR) que puede llegar a tomar hasta un valor de 100, I_s es la combinación de todos los desperfectos que aparecen de forma casi simultánea con la señal de voz, I_d representa los errores causados por los retardos, I_e son las degradaciones causadas por los CODECs, y A es el factor de expectación, el cual captura el hecho que los usuarios pueden aceptar algo de degradación de la calidad por el hecho que están usando VoIP. Para opciones prácticas se puede reducir la ecuación 1 como sigue:

$$R = 93.2 - I_d(T) - I_e(\text{CODEC}, \text{PLR}) \quad (2)$$

$$I_d = 0.024(T) + 0.11(T - 177.3)y(T - 177.3)$$
$$T = \text{OWD} = \frac{1}{2}\text{RTT}, \quad y(x) = \begin{cases} 0, & x < 0 \\ 1, & x > 0 \end{cases} \quad (3)$$

$$I_e(\text{G.711}) \sim 0 + 30\ln(1 + 15 \cdot \text{PLR})$$
$$I_e(\text{G.729}) \sim 11 + 40\ln(1 + 10 \cdot \text{PLR}) \quad (4)$$

Dónde $I_d$está en función del retardo T e I_e está en función del tipo de CODEC usado (G.711 ó G.729) y la tasa de paquetes perdidos (PLR).

La relación entre el factor R y el MOS está dado por la siguiente expresión:

$$\begin{aligned} &\text{MOS} = 1; && R < 0 \\ &\text{MOS} = 1 + 0.035 + 7 \cdot 10^{-6}\, R(R - 60)(100 - R); && 0 \le R \le 100 \\ &\text{MOS} = 4.5; && R > 100 \end{aligned} \quad (5)$$

La Figura 4-1 muestra el grado de satisfacción de los usuarios de acuerdo al factor R y MOS.

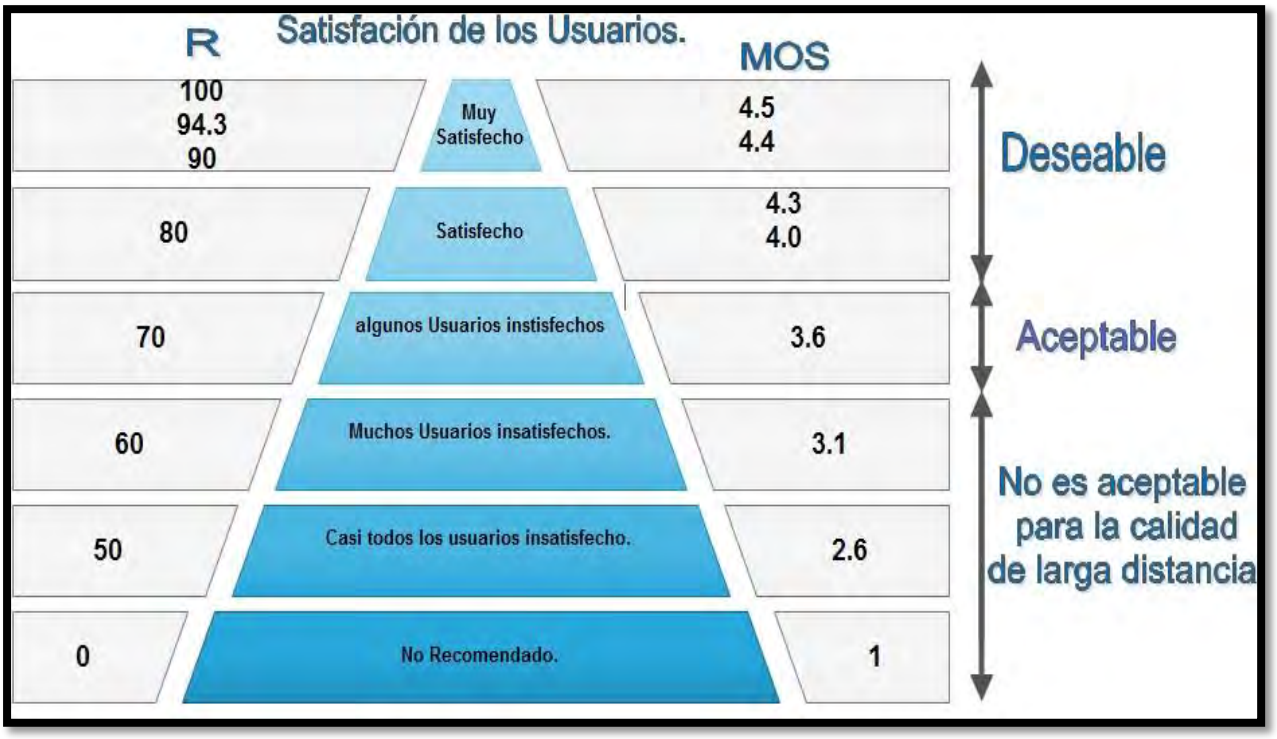


Figura 4-1 Satisfacción de los Usuarios.

4.3. Habilitación y Configuración de parámetros

Como hemos visto hasta ahora, hay muchos factores que afectan la QoS en una red VoIP, sin embargo hay parámetros que a continuación se describirán y pueden ser habilitados o configurados para obtener una mejor calidad de servicio.

4.3.1. Detectores de actividad de voz (VAD)

Cuando está habilitada la detección de actividad de voz (VAD, Voice Activity Detection). El VAD funciona detectando la magnitud en decibelios (dB) y decidiendo cuando debe realizar la paquetización, en función de la presencia de silencios o flujos de voz. Cuando detecta una disminución de amplitud de la voz, espera un tiempo determinado antes de poner tramas de voz en paquetes. Este tiempo determinado se conoce como *hangover* y suele ser de 200ms.

El VAD padece determinados problemas inherentes a la hora de determinar cuándo finaliza y empieza la voz y a la hora de distinguir la voz de un ruido de fondo, es decir, que si está en un espacio ruidoso, el VAD es incapaz de distinguir entre la voz y el ruido de fondo, también conocido como el *umbral de señal de ruido* [7].

También es importante mencionar que la supresión de silencio tiene dos efectos perjudiciales sobre la precepción del usuario. La primera es que si las señales de voz son de bajo volumen, el VAD será lento para percibir los inicios suaves y finales de las palabras y sílabas, produciendo lo que se le conoce como recorte de voz frontal (Front-end speech clipping), tal recorte puede convertirse en un factor importante de irritación cuando un usuario trata de mantener una conversación. El segundo efecto es que la supresión de silencio produce una completa ausencia señal en el extremo de la otra línea, por lo tanto, para los usuarios que están acostumbrados a al menos un poco de ruido en la línea, puede dar lugar a una percepción errónea de que la línea este muerta [7] [11].

Una ventaja al habilitar la detección de actividad de voz en una comunicación VoIP es hacer uso óptimo del ancho de banda.

4.3.2. Códecs

La voz es de naturaleza analógica, mientras que la red de datos es digital. El proceso de convertir ondas analógicas a información digital se realiza mediante un códec (codificador/decodificador), que, además de llevar a cabo la conversión analógica-digital, comprime la secuencia de datos, y proporciona la cancelación del eco.

El proceso de codificación puede ser realizada mediante tres técnicas principales: por codificación de forma de onda, por codificación basada en modelos matemáticos sobre la producción de la voz y en modelos híbridos que combinan ambas técnicas.

4.3.3. De-Jitter Buffer

El de-jitter buffer es el elemento dónde los paquetes se almacenan para luego ser enviados al codificador a la misma tasa como fueron transmitidos. El tamaño del de-jitter buffer se mide en milisegundos. Si el tamaño de un de-jitter buffer es de 200 ms significa que introducimos un retardo de 200 ms previo a la reproducción de la voz.

Existen dos tipos de de-jitter buffers:

- Estático: está implementado como parte del equipo y configurado de manera fija por el fabricante.
- Dinámico: se configura usando un programa y lo puede cambiar el usuario. Un valor común del jitter buffer es de 100 ms.

Al incrementar el tamaño del de-jitter buffer se disminuye la probabilidad de pérdida de paquetes en el lado del receptor, sin embargo incrementa el retardo extremo a extremo [6].

CAPÍTULO 5 ESCENARIO DE PRUEBA Y MEDICIONES

5.1. Escenario de prueba

El escenario de medición en el cual se midió el tráfico VoIP está conformado por dos redes de área local (LAN), interconectadas mediante una troncal SIP a través de Internet entre los servidores Elastix como lo muestra la Figura 5-1.Donde la LAN A: Red de la Universidad de Quintana Roo y LAN B: Red ISP.

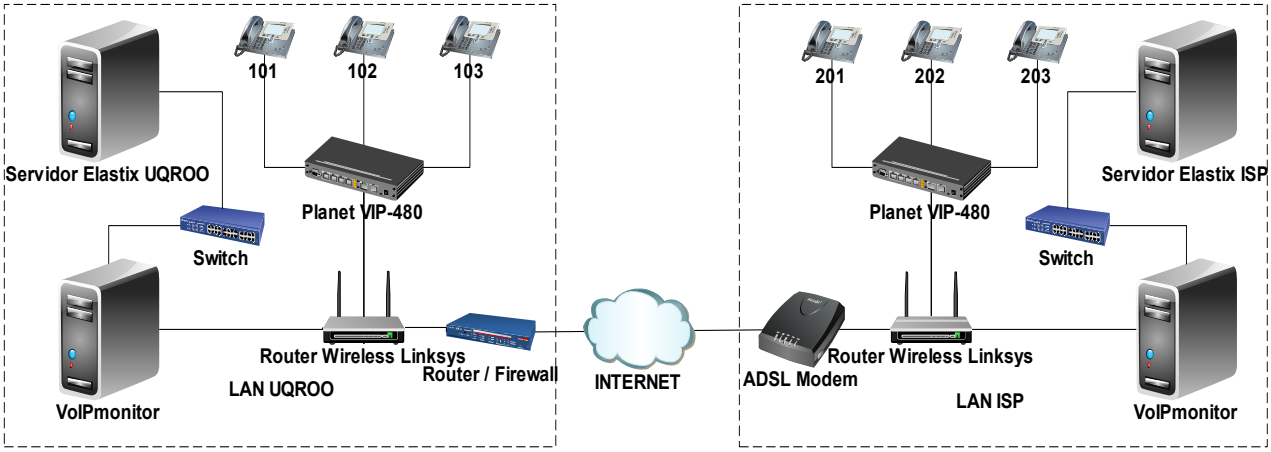


Figura 5-1 Escenario de Medición.

La Figura 5-1 muestra una arquitectura SIP formada por dos redes LAN interconectadas a través de un troncal SIP entre los servidores Elastix, cada red LAN está conformada por un Servidor Elastix, un Switch, el VoIPmonitor instalado en Linux Mint 15 con 2 tarjetas en modo Bridge, un Router Wireless Linksys y dos equipos Internet Telephony Gateway Planet VIP-480 con 6 teléfonos cada uno con sus respectivas extensiones.

5.1.1. Características de los Equipos

Cada Red LAN cuenta con:

- 2 computadoras
- 1Routers Inalámbricos Linksys
- 1Tarjeta de Red Ethernet PCI
- 2 Gateway Planet VIP-480

HP Compaq dc7700: Servidor Elastix UQROO

- Sistema Operativo: Elastix 2.4.0

- Procesador: Intel Core 2 Duo 6300 @ 1.86
- Memoria RAM: 1Gb
- Disco Duro: 160Gb
- Gráficos: Intel (R) Q965/Q963 Express Chipset Family

HP Compaq 6000 Pro Small form Factor: VoIPmonitor en Linux Mint 15 UQROO

- Procesador: Pentium(R) Dual-Core CPU E5700 @ 3.00GHz
- Memoria (RAM): 4.00 GB
- Gráficos: Intel(R) Q45/Q43 Express Chipset (Microsoft Corporation - WDDM 1.1)
- Gráficos de juego: 1547 MB (memoria de gráficos total disponible)
- Disco duro principal: 346GB disponibles (455GB en total)
- Linux Mint 15
- Fabricante: Hewlett-Packard
- Modelo: HP Compaq 6000 Pro SFF PC
- Tipo de sistema: Sistema operativo de 32 bits
- Número de procesadores principales: 2
- Compatible con 64 bits: Sí
- Tarjeta Ethernet PCI Linksys Gigabit

4-Port H.323/SIP VoIP Gateway: UQROO

- H.323 / SIP Comunicación Modo Dual
- SIP 2.0 (RFC3261), compatible con H.323v4
- Peer-to-Peer / H.323 GK / SIP proxy calls
- Soporte para Códec de Video: G.711 (A-law / u-law), G.729 AB, G.723 (6.3Kbps / 5.3Kbps)
- Procesamiento de voz: detección de actividad de voz, detección DTMF,G.165/G.168 compatible con cancelación de eco, detección de silencio, FAX (T.38 /T.30).
- Construido con búfer adaptable que ayuda a suavizarlas variaciones de retardo (jitter) para el tráfico de voz.
- Visualización del estado de los canales de voz.

Dell Optiplex: Servidor Elastix ISP

- Sistema Operativo: Elastix 2.4.0
- Processor: Intel 865G chipset, Intel® Pentium® 4

- Memoria (RAM): 1GB
- Gráficos: Integrated Intel Extreme® Graphics 2
- Disco Duro: 80GB

HP Compaq 6000 Pro Small form Factor: VoIPmonitor en Linux Mint 15, ISP

- Procesador: Pentium(R) Dual-Core CPU E5700 @ 3.00GHz
- Memoria (RAM): 4.00 GB
- Gráficos: Intel(R) Q45/Q43 Express Chipset (Microsoft Corporation - WDDM 1.1)
- Gráficos de juego: 1547 MB (memoria de gráficos total disponible)
- Disco duro principal: 346GB disponibles (455GB en total)
- Linux Mint 15
- Fabricante: Hewlett-Packard
- Modelo: HP Compaq 6000 Pro SFF PC
- Tipo de sistema: Sistema operativo de 32 bits
- Número de procesadores principales: 2
- Compatible con 64 bits: Sí
- Tarjeta Ethernet PCI Broadcom Corporation NetXtreme Gigabit

4-Port H.323/SIP VoIP Gateway: ISP

- H.323 / SIP Comunicación Modo Dual
- SIP 2.0 (RFC3261), compatible con H.323v4
- Peer-to-Peer / H.323 GK / SIP proxy calls
- Soporte para Códec de Video: G.711 (A-law / u-law), G.729 AB, G.723 (6.3Kbps / 5.3Kbps)
- Procesamiento de Voz: Detección de Actividad de Voz, detección DTMF, G.165/G.168 compatible con cancelación de eco, detección de silencio, FAX (T.38 / T.30).
- Construido con búfer adaptable que ayuda a suavizarlas variaciones de retardo (jitter) para el tráfico de voz.
- Visualización del estado de los canales de voz.

5.1.2. Configuración de los Equipos

5.1.2.1. Servidor Elastix

5.1.2.1.1. Configuración de las extensiones

Para la creación de una nueva extensión le damos clic en la pestaña PBX, la cual nos mandará a la siguiente ventana y nos mostrará la opción de agregar un nuevo Dispositivo Genérico SIP tal y como se muestra en la Figura 5-2.

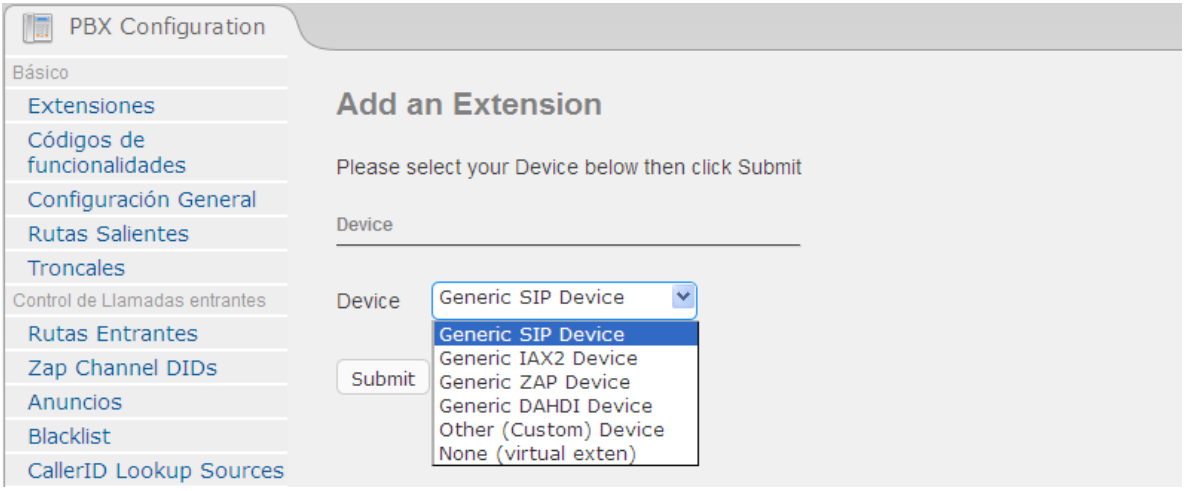


Figura 5-2 Agregando la Extensión SIP.

En la Figura 5-3 se da un ejemplo de la ventana donde agregaremos la nueva extensión SIP y en la cual llenaremos los campos User Extension, Display y Secret

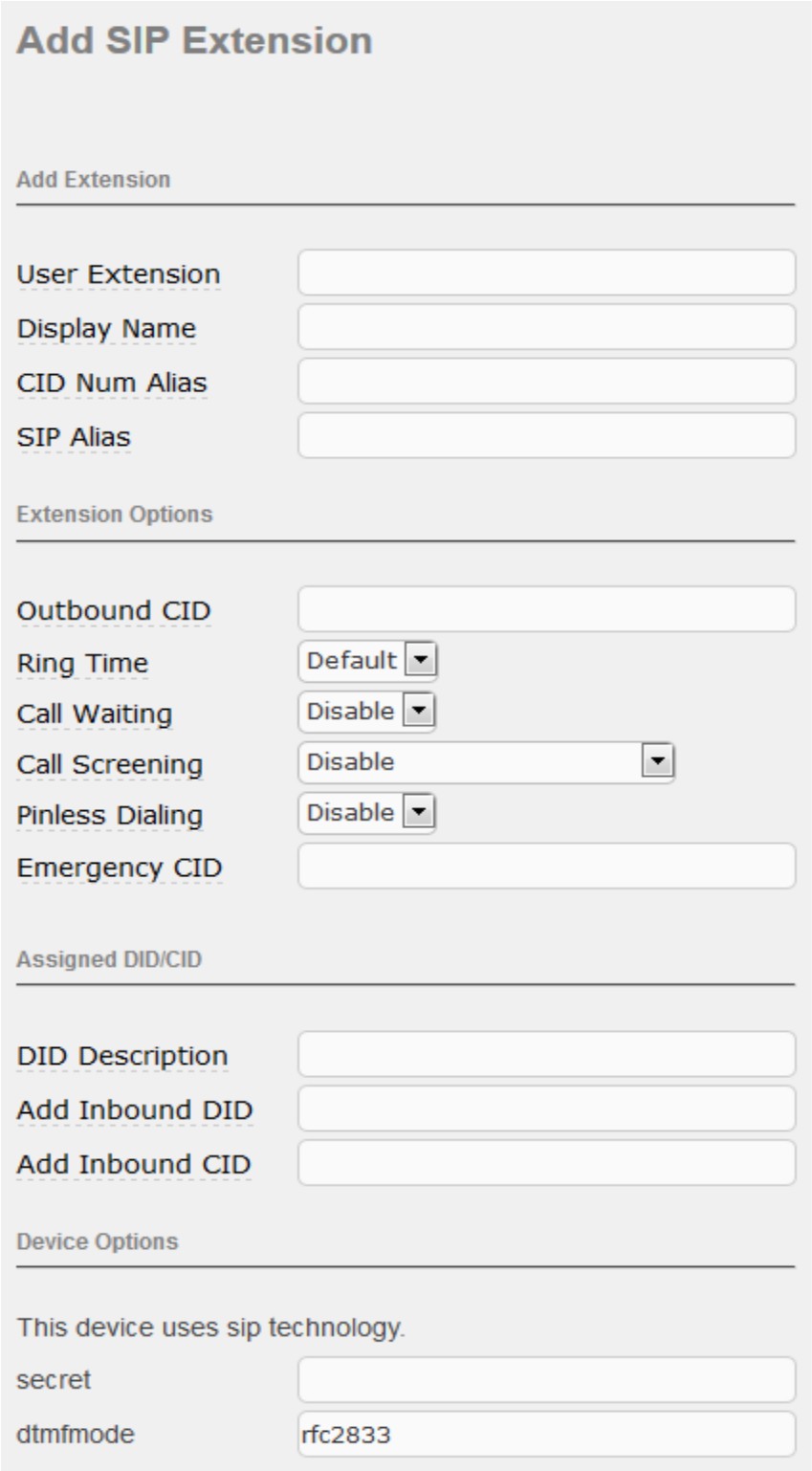


Figura 5-3 Parámetros de la Extensión SIP.

Extensión del Usuario: En el Servidor UQROO se les asignaron las extensiones del 101 a la extensión 106 y en el Servidor ISP se le asignaron las extensiones del 201 a la extensión 206.

Display Name: Para cada extensión se le asignó el nombre de Planet01 hasta el nombre de Planet06, respectivamente en ambos Servidores.

Secret: En este caso se usó el mismo password para las 12 extensiones las cuales fueron pc1234.

5.1.2.1.2. Configuración del Troncal SIP

Para cada Servidor se creó una troncal SIP y para esto nos dirigimos a la pestaña PBX, le damos clic a Trunks y agregamos una troncal SIP, en la Figura 5-4 se muestra la configuración utilizada en el servidor UQROO y en la Figura 5-5 se muestra la configuración del servidor ISP.

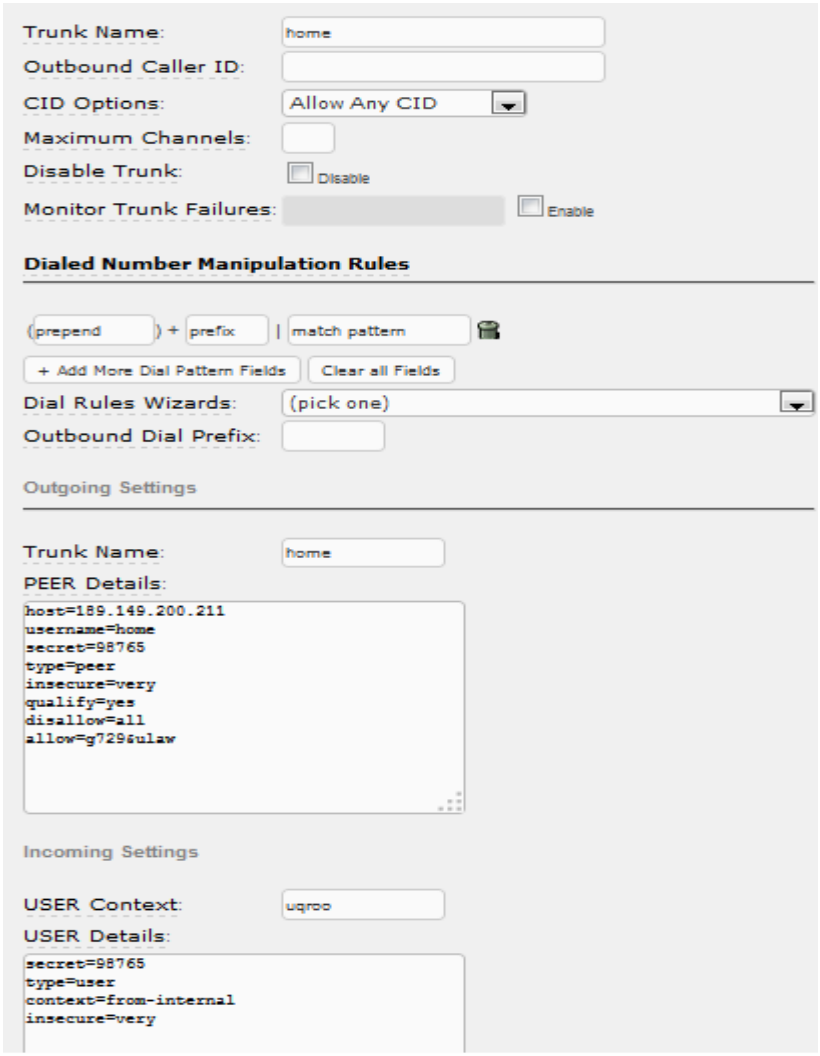
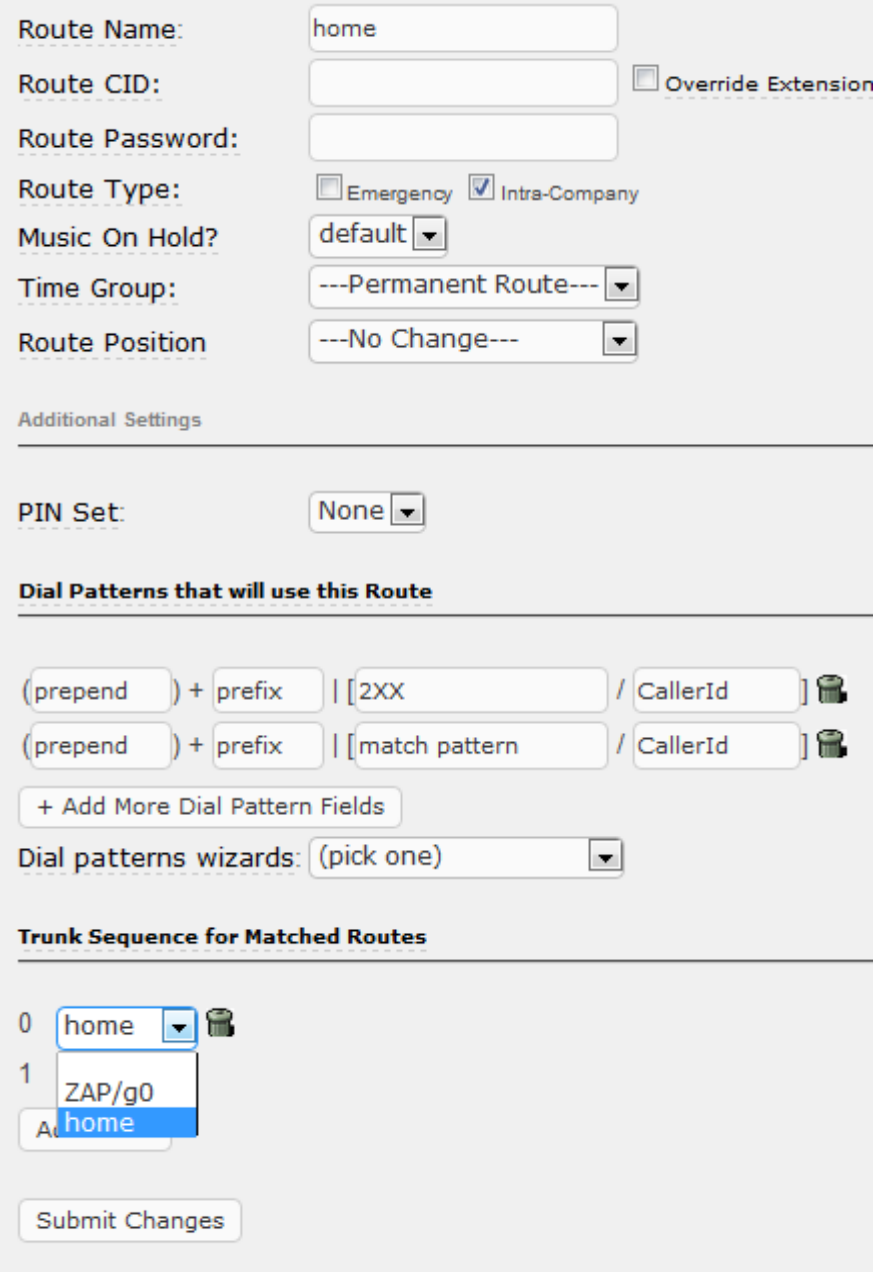


Figura 5-4 Troncal SIP UQROO.

Figura 5-5 Troncal SIP ISP.

Para que cada extensión pueda llamar hacia la otra extensión del Servidor Remoto, se debe crear una ruta de salida, en la Figura 5-6 se muestra la configuración del Servidor UQROO y la Figura 5-7 la del Servidor ISP.



.

Figura 5-6 Ruta de Salida UQROO.

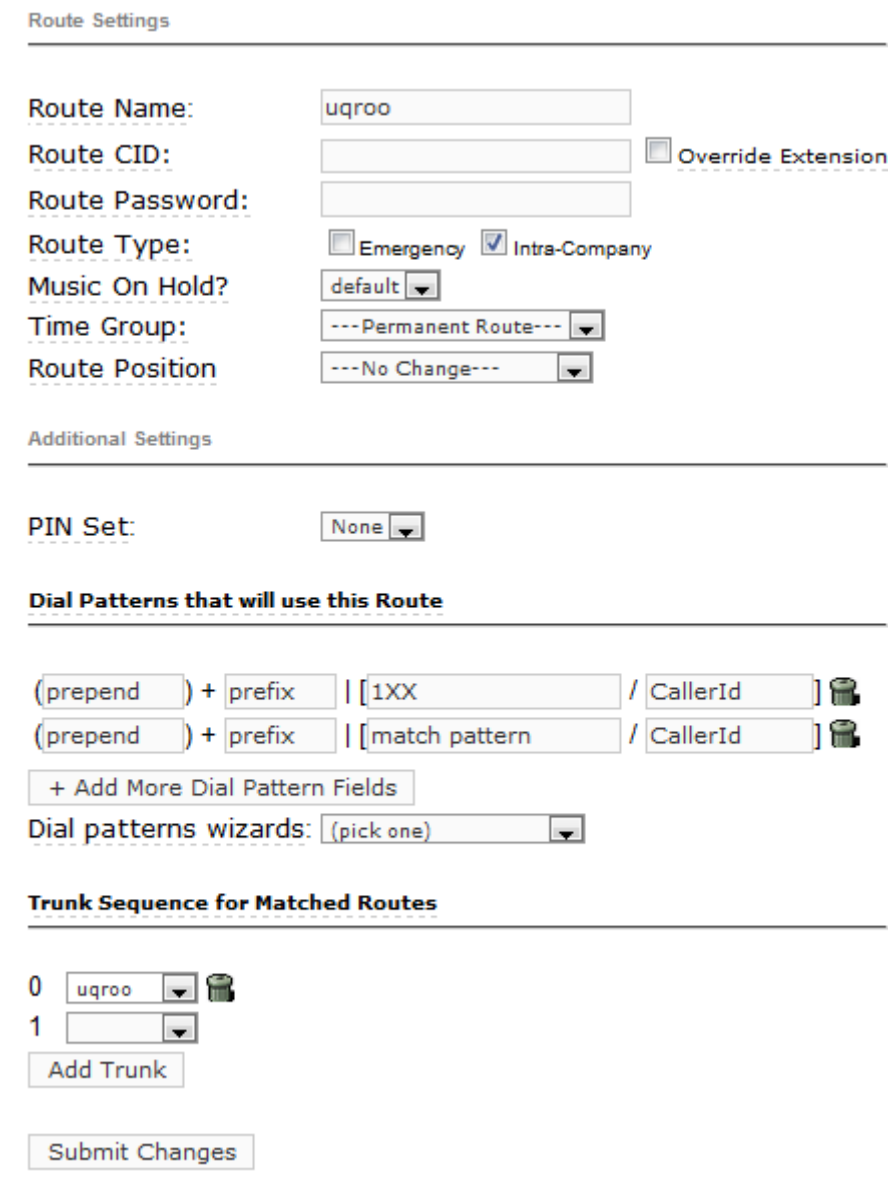


Figura 5-7 Ruta de Salida ISP.

En la Figura 5-8 y en la Figura 5-9 se muestra la configuración del archivo sip_nat.conf de cada Servidor debido a que el protocolo SIP necesita NAT para salir a través de Internet por encontrarse detrás de un Firewall.

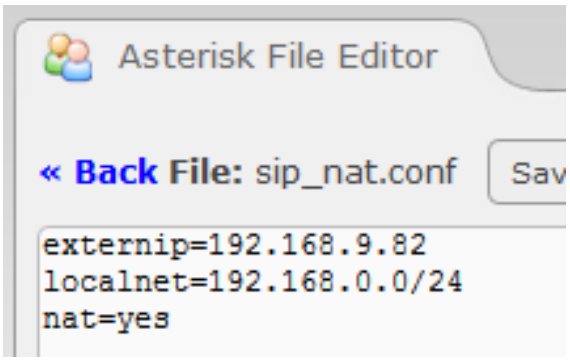


Figura 5-8 Configuración UQROO.

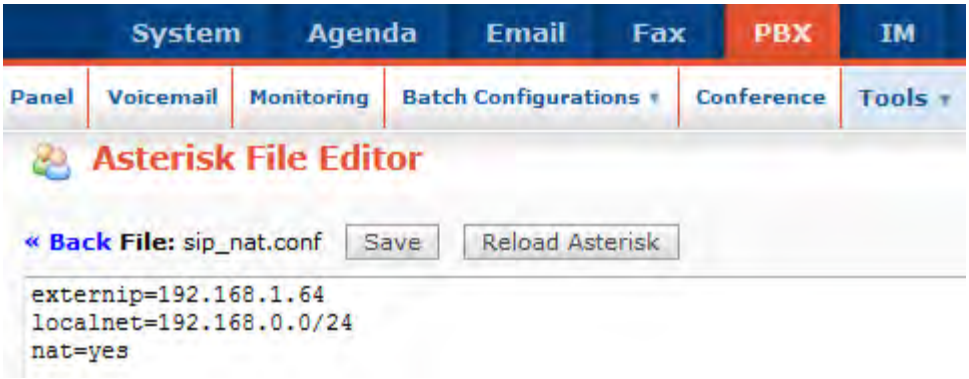


Figura 5-9 Configuración ISP.

5.1.2.2. Router Wireless Linksys

Para que los servidores puedan tener comunicación a través de Internet fue necesario abrir puertos en cada Router Linksys para redirigir el tráfico hacia el servidor, tal y como se muestran las Figuras 5-10 y Figura 5-11.

Figura 5-10 Reenvío de Puertos Router UQROO.

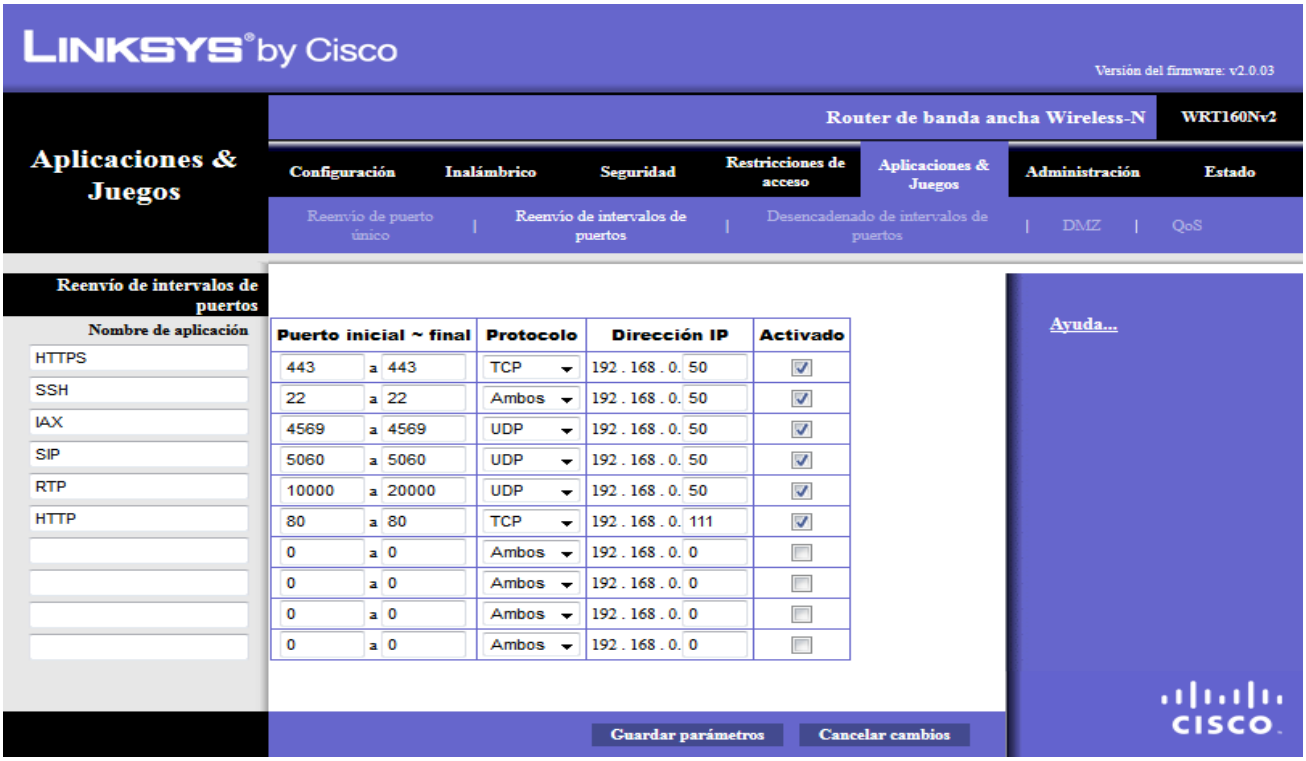


Figura 5-11 Reenvío de Puertos Router ISP.

5.1.2.3. Internet Telephony Gateway: Planet VIP-480

Para poder generar tráfico de voz mediante las llamadas, se crearon las extensiones en cada Equipo Planet VIP-480, en la Figura 5-12 se muestra la configuración del Planet VIP-480 de la UQROO y en la Figura 5-13 la de ISP.

Figura 5-12 Creación de las Extensiones UQROO.

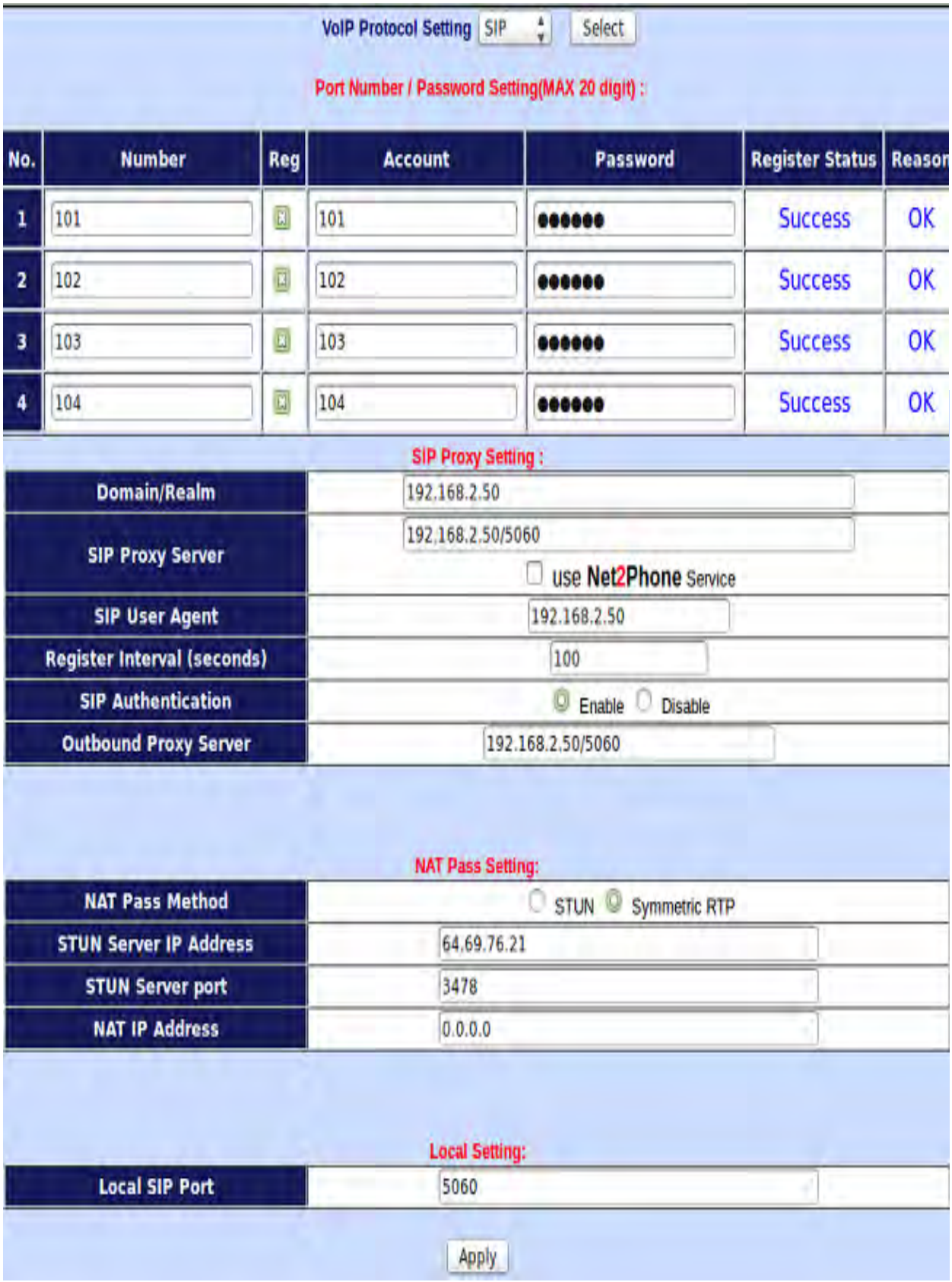


Figura 5-13 Creación de las Extensiones ISP.

Para realizar las llamadas con los códecs y habilitar el VAD, se configuró la sección "Advance Setting" en cada Planet VIP-480 como se muestran en La Figura 5-14:

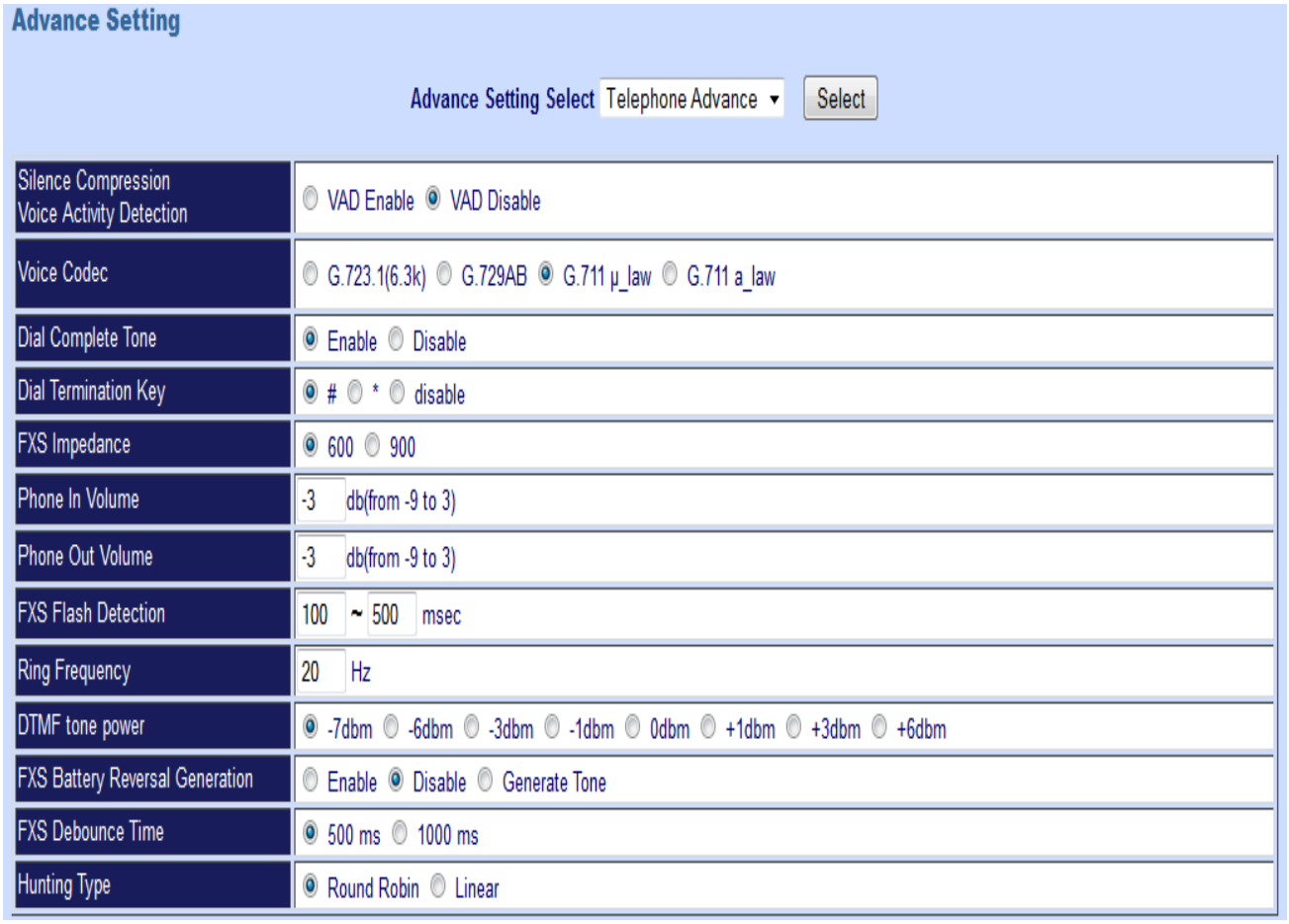


Figura 5-14 Selección de Códec y Modo de Compresión de Voz.

5.1.3. Software de Monitoreo: VoIPmonitor

En cada equipo que se utilizó como monitor se instaló bajo el sistema operativo Linux MInt 15 el software de monitoreo VoIPmonitor, así mismo se le agregó una tarjeta de Red Ethernet PCI Linksys Gigabit en el equipo de la red UQROO y por el lado del equipo de la red del ISP una tarjeta Broadcom NetXtreme Gigabit, a cada equipo se configuraron las tarjetas en modo Bridge para poder hacer la capturas mediante VoIPmonitor, en la Figura 5-15 se muestra la configuración del archivo interfaces de cada equipo:

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
auto br0
iface br0 inet static
        bridge_ports eth0 eth2
        bridge_stp on
        address 192.168.0.14
        netmask 255.255.255.0
        gateway 192.168.0.1
```

Figura 5-15 Configuración del Modo Bridge en Linux Mint 15.

Una vez configurado el modo Bridge en cada equipo, se debe de modificar un archivo de configuración del Software VoIPmonitor para que realice la captura en la interfaz virtual creada en el modo Bridge como se muestra en la Figura 5-16:

```
 GNU nano 2.2.6                File: /etc/voipmonitor.conf

#
# voipmonitor.org configuration file
#
# location of this file is at ~/.voipmonitor.conf or /etc/voipmonitor.conf
# command line parameters overrides configuration directives in this file
# allowed comments are ; or #.
#

[general]

# in case of running more voipmonitor instances on the same or another servers configured to save to one database and t$
# it is possible to differentiate CDR by id_sensor column. If you set id_sensor >= 0 the number will be saved in cdr.id$
#id_sensor = 1

# voipmonitor is able to sniff directly on network interface or it can read files.

# listening interface. Can be 'any' which will listen on all interfaces - NOTE that "any" will not put intefaces into p$
# check if you are not using -i ethX argument in command line as it has more priority
# than this configuration file
interface = br0
```

Figura 5-16 Configuración del Archivo voipmonitor.conf.

5.1.3.1. Captura de tráfico con VoIPmonitor

Una vez configurado todo lo anterior, se procede a capturar el tráfico entre las llamadas en el troncal SIP, la Figura 5-17 muestra el inicio de captura de tráfico entre las llamadas.

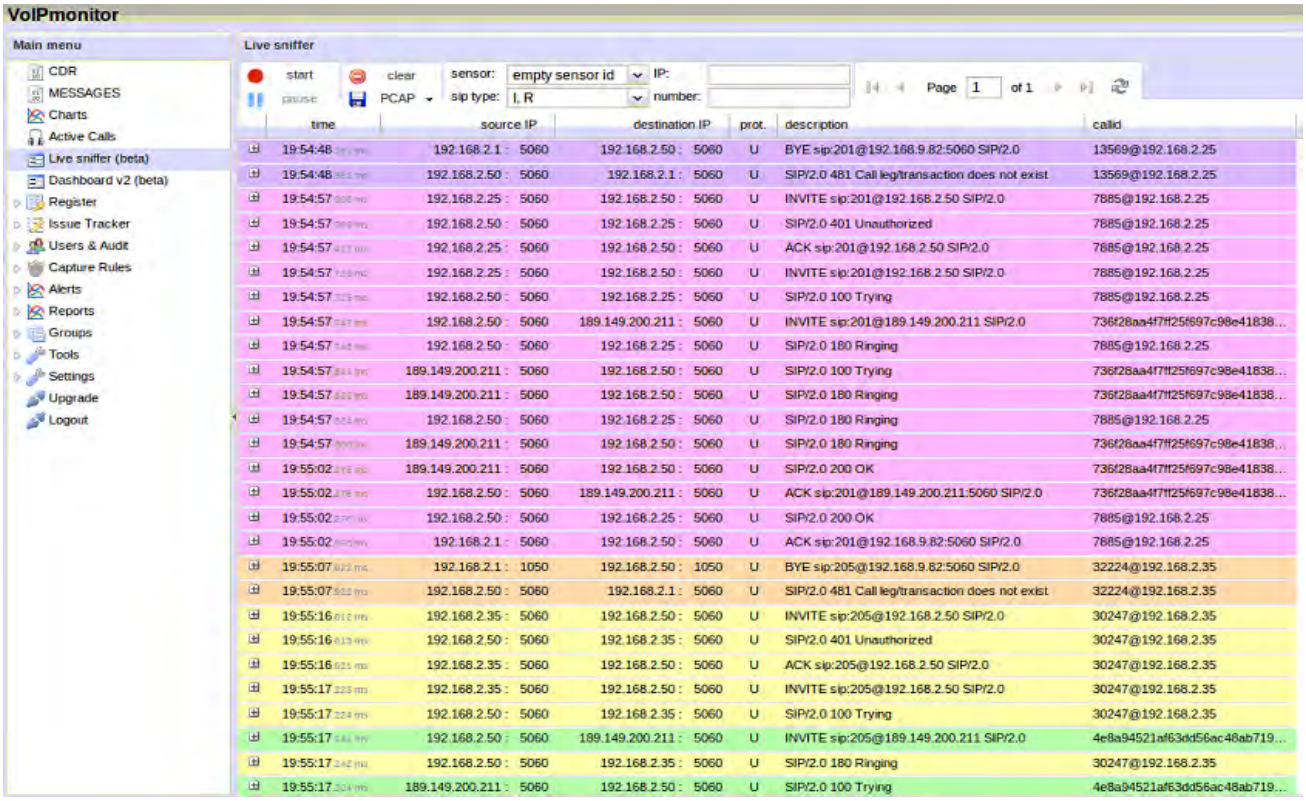


Figura 5-17 Captura de Tráfico con Live Sniffer (VoIPmonitor).

Una vez capturado el tráfico entre las llamadas nos dirigimos a la pestaña de CDR (Call Detail Record) para visualizar los valores de cada métrica obtenida por el VoIPmonitor, tal como se muestra en la Figura 5-18:

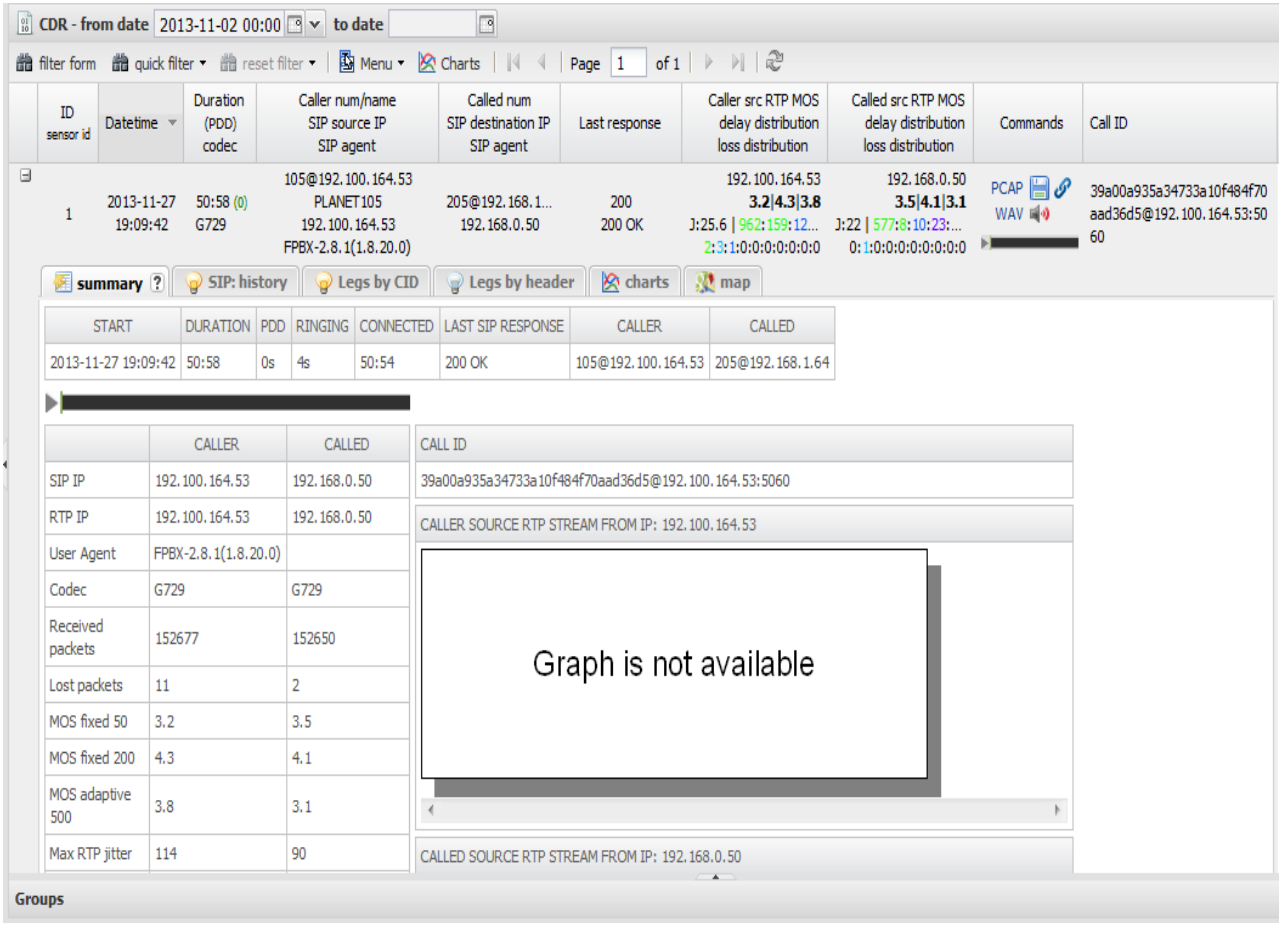


Figura 5-18 Métricas CDR.

5.2. Mediciones

En este capítulo se presenta la metodología para la medición de tráfico en una red SIP. Para poder llevar a cabo esta tarea, se generó tráfico VoIP mediante el establecimiento de un conjunto de llamadas de prueba a través de unos equipos H.323/SIP VoIP Gateway. Posteriormente se capturó tráfico mediante VoIPmonitor. El principal objetivo de estas mediciones fue colectar un conjunto de patrones de tráfico, tales como: jitter de arribo, pérdida de paquetes y retardo extremo a extremo.

Para colectar el conjunto de trazas, las llamadas de prueba realizadas se llevaron a cabo con las siguientes configuraciones en función del códec, tal como se muestra en la Tabla 5-1.

Tabla 5-1 Configuración de Llamadas de Prueba.

SET DE MEDICIONES	PLANET VIP-480 UQROO (10Mb/s)		PLANET VIP-480 ISP (3Mb/s)	
	CODEC	Detección de Actividad de Voz	CODEC	Detección de Actividad de Voz
SET 1	G729	No VAD	G729	No VAD
	G711	No VAD	G711	No VAD
SET 2	G729	VAD	G729	VAD
	G711	VAD	G711	VAD
SET 3	G729	VAD	G729	VAD
	G729	No VAD	G729	No VAD
SET 4	G711	VAD	G711	VAD
	G711	No VAD	G711	No VAD

Como se muestra en la Tabla 5-1, las llamadas de prueba se realizaron bajos los dos esquemas de codificación de voz más importantes G729 y G711. Las llamadas de prueba tuvieron una duración de 50 minutos, y se realizaron en horas de trabajo, de 9am a 9pm.

CAPÍTULO 6 ANÁLISIS DE MÉTRICAS DE QoS BAJO DIFERENTE CONFIGURACIÓN DE PARÁMETROS EN UNA RED VOIP-SIP.

En este capítulo se presenta el estudio de las principales métricas que determinan la QoS (jitter y pérdida de paquetes), bajo diferentes configuraciones de parámetros en una red VoIP-SIP (uso de detectores de actividad de voz, tipo de códec y tamaño de de-jitter buffer), con el objetivo de determinar las configuraciones óptimas que proporcionen cierto nivel de QoS. Este estudio se realizó mediante un conjunto de llamadas con las configuraciones mostradas en la Tabla 5-1 sobre el escenario de medición descrito en la sección 5.1.

Se realizó un conjunto de llamadas de prueba y se comparó el desempeño obtenido mediante el códec G.711 (Figura 6-1) y G.729 (Figura 6-2) sin habilitar la detección de actividad de voz, bajo diferentes configuraciones en el tamaño del de-jitter buffer (50ms, 200ms y 500ms).

De este conjunto de llamadas se observó que el códec G.711, utilizando un tamaño de de-jitter búffer fijo de 50ms presenta un valor promedio de MOS igual a 3.89, mientras que con un de-jitter búffer fijo de 200ms presenta un valor promedio de MOS de 3.79, y con de-jitter búffer adaptativo de 500ms presenta un valor promedio de MOS de 3.21. Estos valores en función del nivel de satisfacción de los usuarios se traduce de la siguiente manera: algunos usuarios insatisfechos cuando se usa un de-jitter búffer fijo de 50ms y 200ms; mientras que para el de-jitter búffer adaptativo de 500ms, muchos usuarios insatisfechos. Por lo tanto, cuando configuramos los tamaños de de-jitter buffer de 50ms y 200ms y usamos un códec G.711 obtenemos una calidad aceptable para llamada.

Por otro lado, en el conjunto de llamadas realizadas mediante el códec G.729 se observó que con un de-jitter búffer fijo de 50ms se obtuvo un valor promedio de MOS igual a 3.4, con un de-jitter búffer fijo de 200ms se obtuvo un valor promedio de MOS de 4.04 y finalmente con un de-jitter búffer adaptativo de 500ms se presenta un valor promedio de MOS de 3.6. De acuerdo al nivel de satisfacción de los usuarios, se puede decir que hay muchos usuarios insatisfechos, usuarios satisfechos y muchos usuarios insatisfechos,

respectivamente. Por lo tanto, con una configuración en el tamaño del de-jitter buffer de 200ms y un códec G.729 obtenemos una calidad deseable en la llamada.

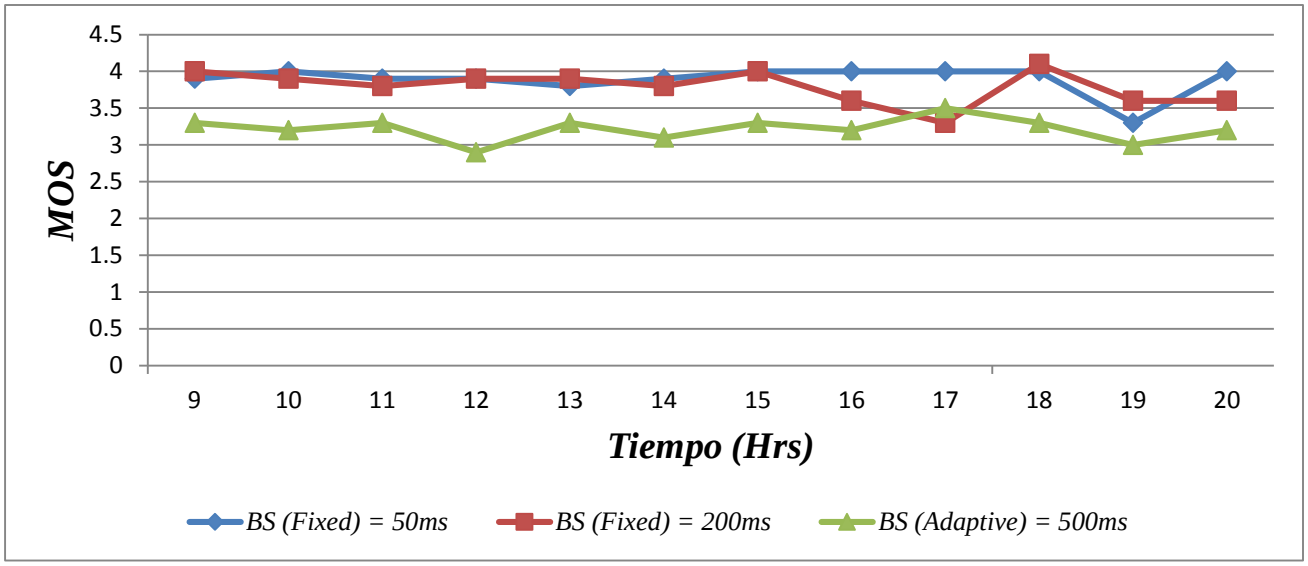


Figura 6-1 G711 No VAD

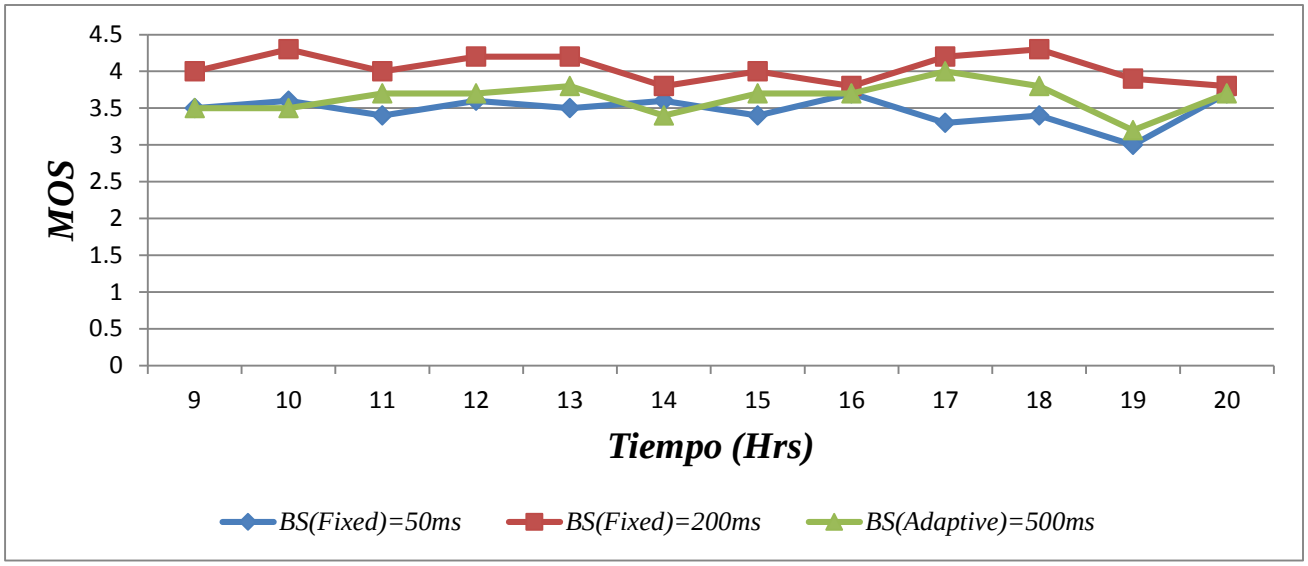


Figura 6-2 G729 No VAD

Posteriormente se repitió el análisis anterior habilitando la detección de actividad de voz, y usando un códec G.711 (Figura 6-3) se observó lo siguiente: con un de-jitter búffer fijo de 50ms se obtuvo un valor promedio de MOS de 3.7, para un de-jitter búffer fijo de 200ms se presentó un valor promedio de MOS 3.75 y para un de-jitter búffer adaptativo de 500ms se obtuvo un valor promedio de MOS de 3.01; de acurdo al nivel de satisfacción de los usuarios, estos resultados se traducen como algunos usuarios insatisfechos cuando se usa un de-jitter búffer fijo de 50ms y 200ms, y todos los usuarios insatisfechos cuando se usa

un de-jitter buffer adaptativo de 500ms. Por lo tanto, cuando configuramos el de-jitter buffer a 50ms y 200ms y usamos un códec G.711 obtenemos una calidad aceptable de llamada.

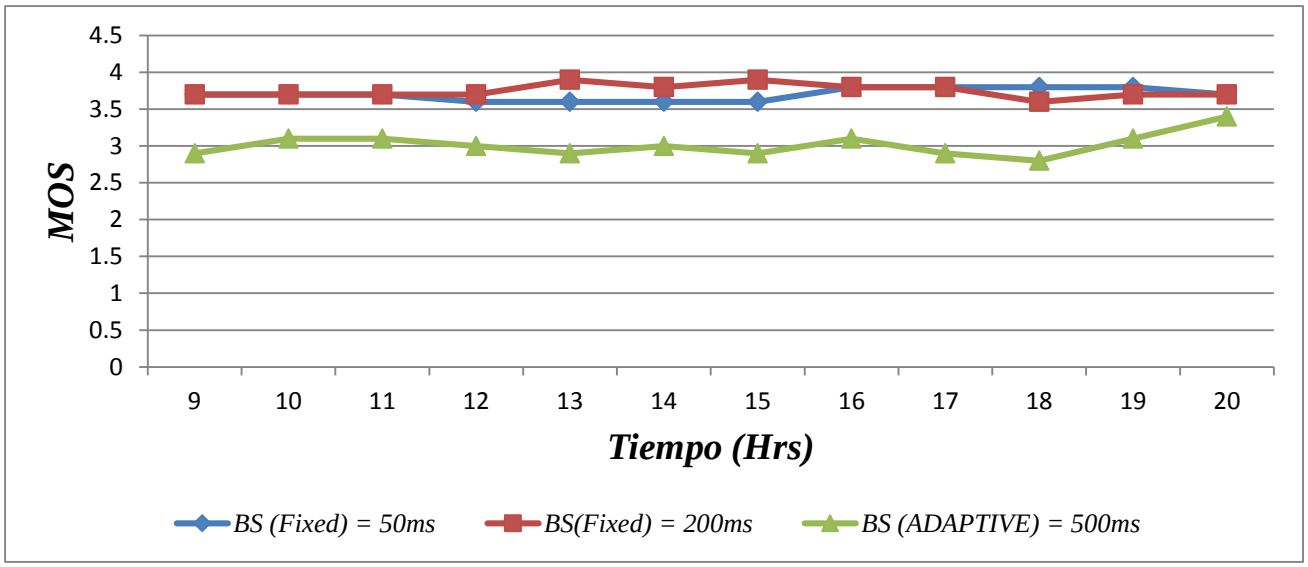


Figura 6-3 G711 VAD

Por otro lado, con el códec G729 se obtuvieron los siguientes resultados: con un de-jitter búffer fijo de 50ms se obtuvo un valor promedio de MOS de 3.34 y para un de-jitter búffer fijo de 200ms se obtuvo un valor promedio de MOS de 3.51 y para un de-jitter búffer adaptativo de 500ms se obtuvo un valor promedio de MOS de 3.51; en función del nivel de satisfacción del usuario, se tiene muchos usuarios insatisfechos para las tres configuraciones de tamaño de de-jitter buffer. En consecuencia la calidad obtenida es no aceptable.

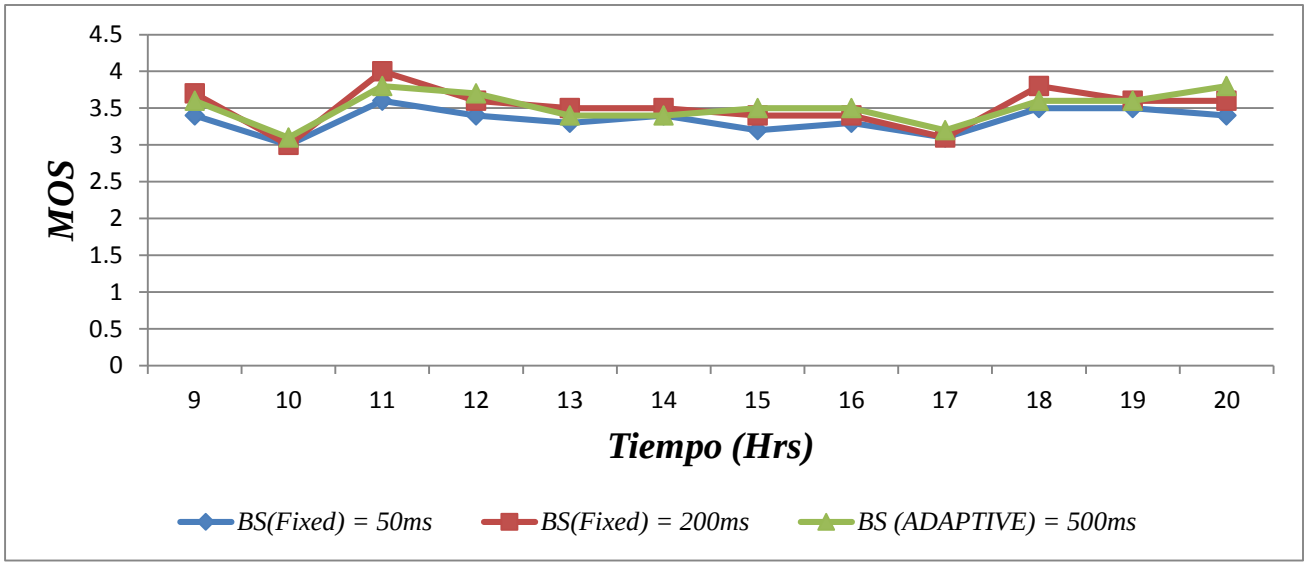


Figura 6-4 G729 VAD

En la Figura 6-5 y Figura 6-6 se comparan los promedios de MOS del códec G.711 con la habilitación de la detección de actividad de voz y sin la habilitación de la detección de actividad de voz y podemos apreciar lo siguiente: con el tamaño de de-jitter buffer de 50ms se obtienen los valores promedio de MOS de 3.9 con VAD y 3.8 sin VAD; con el de-jitter buffer de 200ms valores promedio de MOS de 4.0 con VAD y de 3.9 sin VAD; y con un de-jitter buffer adaptativo de 500ms valores promedio de 3.4 con VAD y de 3.1 sin VAD. Por lo tanto, cuando configuramos los tamaños de de-jitter buffer de 50ms y 200ms, habilitamos el VAD y usamos un códec G.711obtenemos una calidad aceptable para llamada, con valores de MOS superiores a cuando se encuentra deshabilitado el VAD.

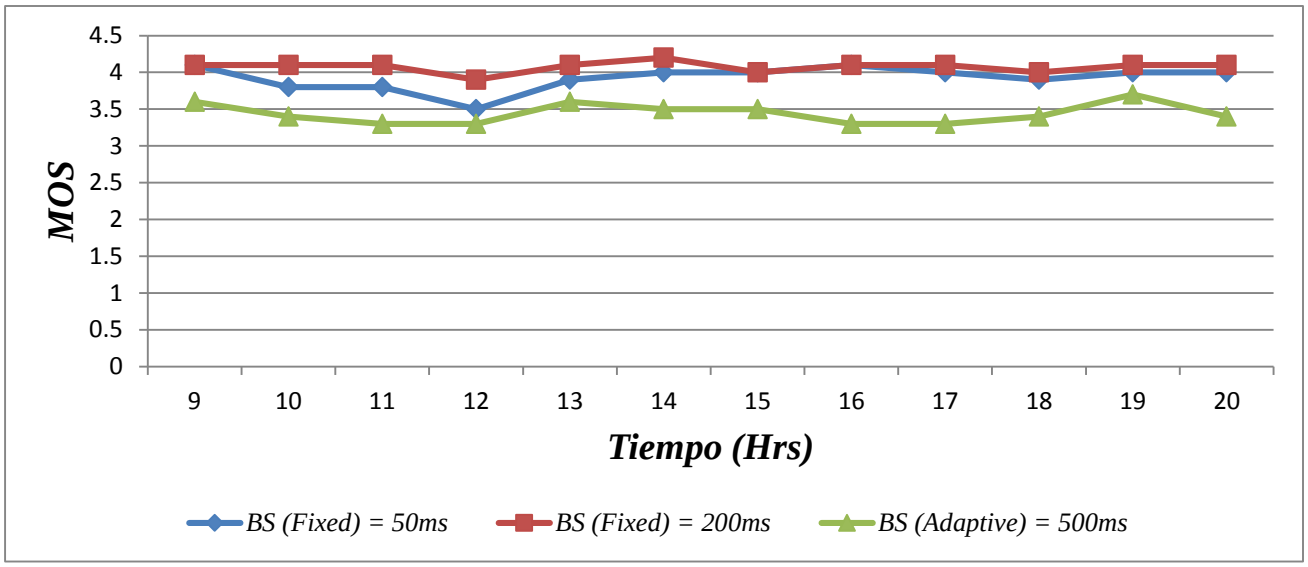


Figura 6-5 G711 VAD

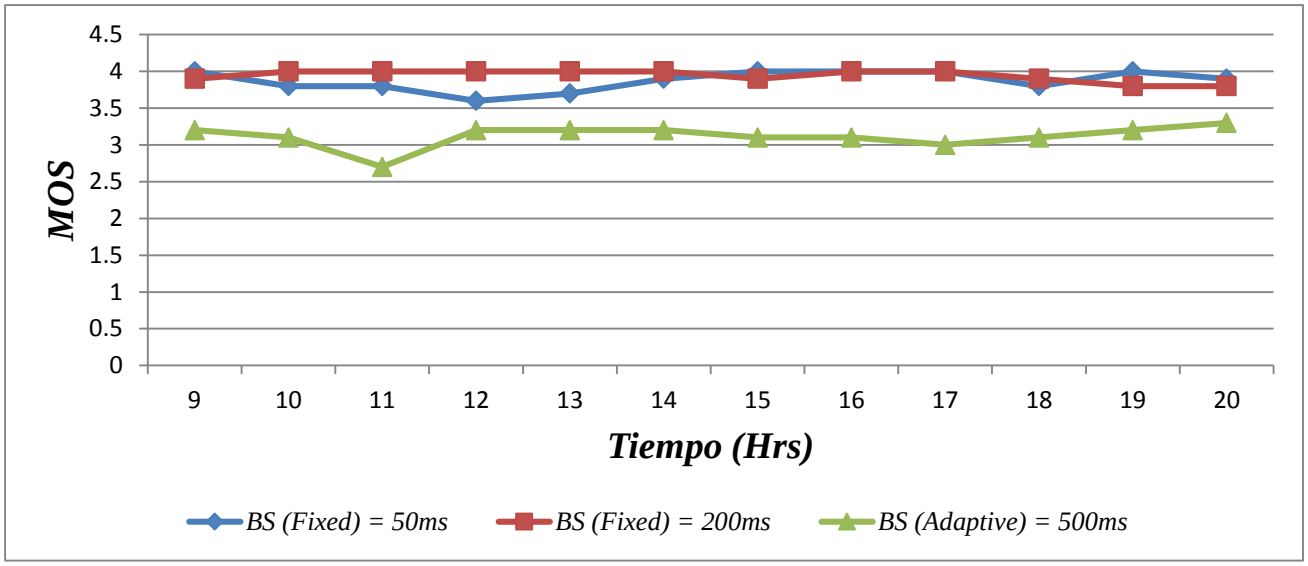


Figura 6-6 G711 No VAD

Por otro lado, se presenta también la comparación cuando habilitamos la detección de actividad de voz y sin la habilitación de la detección de actividad de voz para el códec G729, como se muestra en las Figuras 6-7 y la Figura 6-8: para los diferentes tamaños de de-jitter buffer (50ms, 200ms y 500ms) y con la habilitación del VAD se obtuvieron los valores promedio de MOS de 3.3, 3.5 y de 3.5 respectivamente; en contraste, sin la habilitación del VAD se obtuvieron los valores promedios de MOS de 3.3, 3.7 y 3.0. Por lo tanto, cuando configuramos el tamaño del de-jitter buffer en 200ms, sin la habilitación del VAD y usamos un códec G.729 obtenemos una calidad aceptable para llamada.

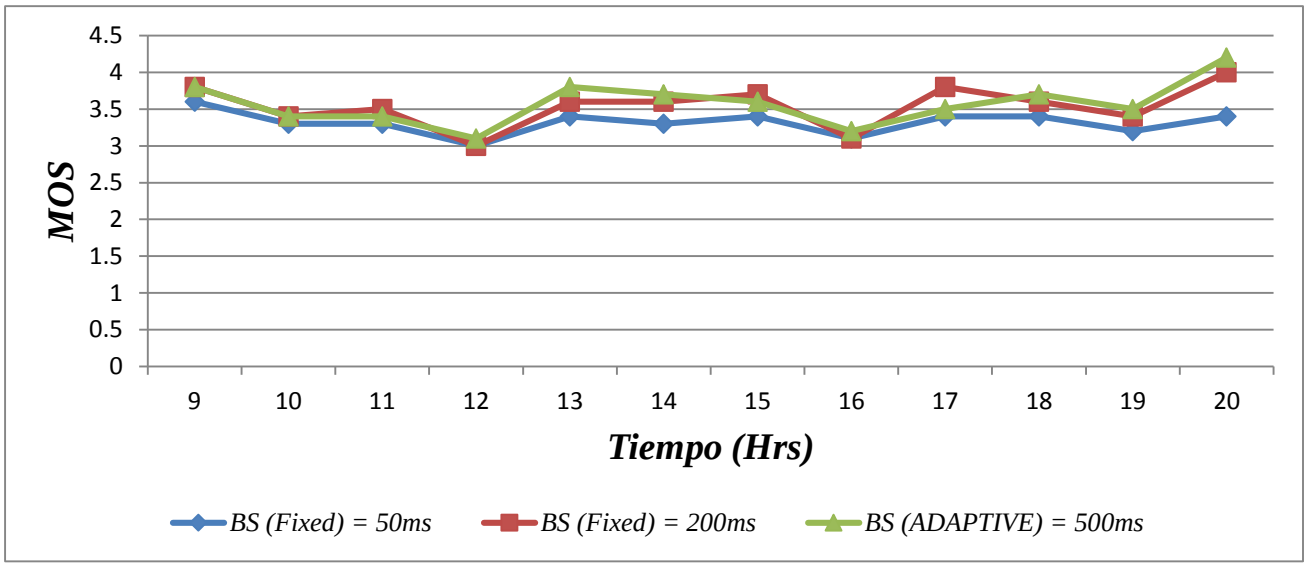


Figura 6-7 G729 VAD

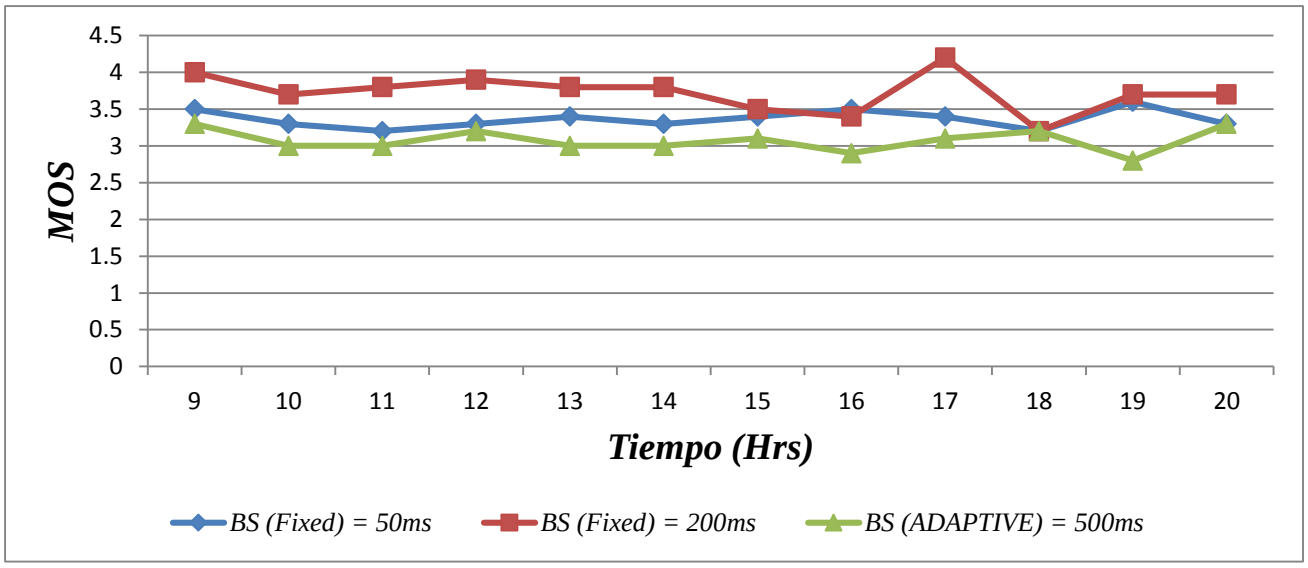


Figura 6-8 G729 No VAD

Otro análisis que se realizó, fue referente a verificar que codificador es más sensible al jitter. Los resultados se muestran en las Figuras 6.9 y 6.10 y puede observarse que el códec G729 es más sensible al jitter sin importar si se habilita o deshabilita la detección de actividad de voz.

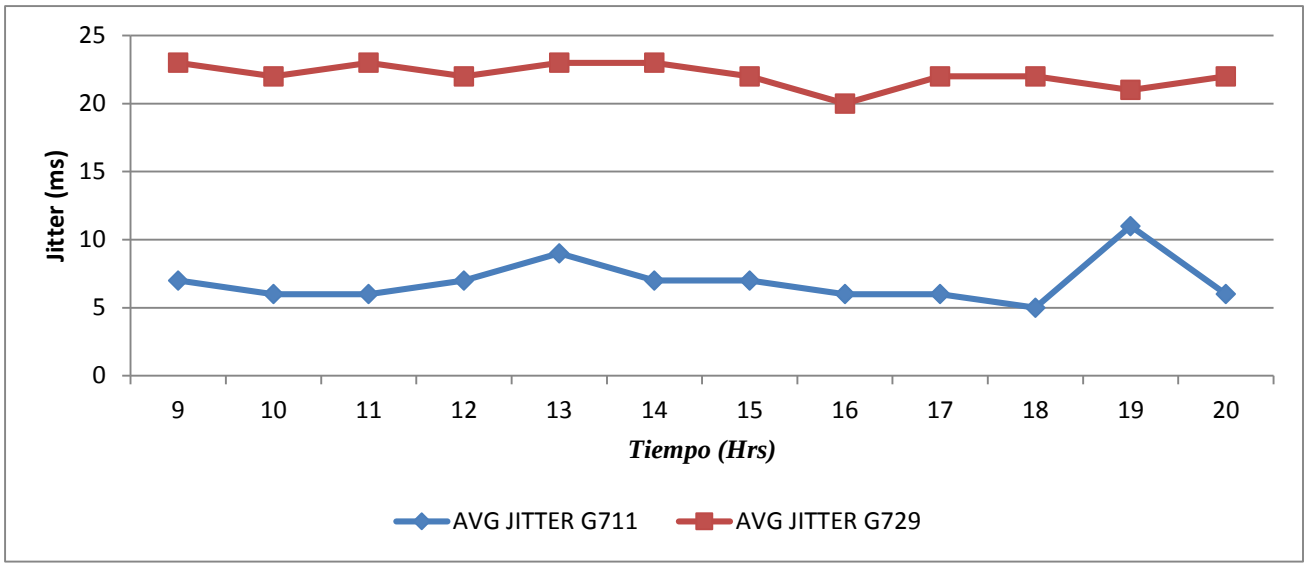


Figura 6-9 AVG Jitter G711 G729 (No VAD)

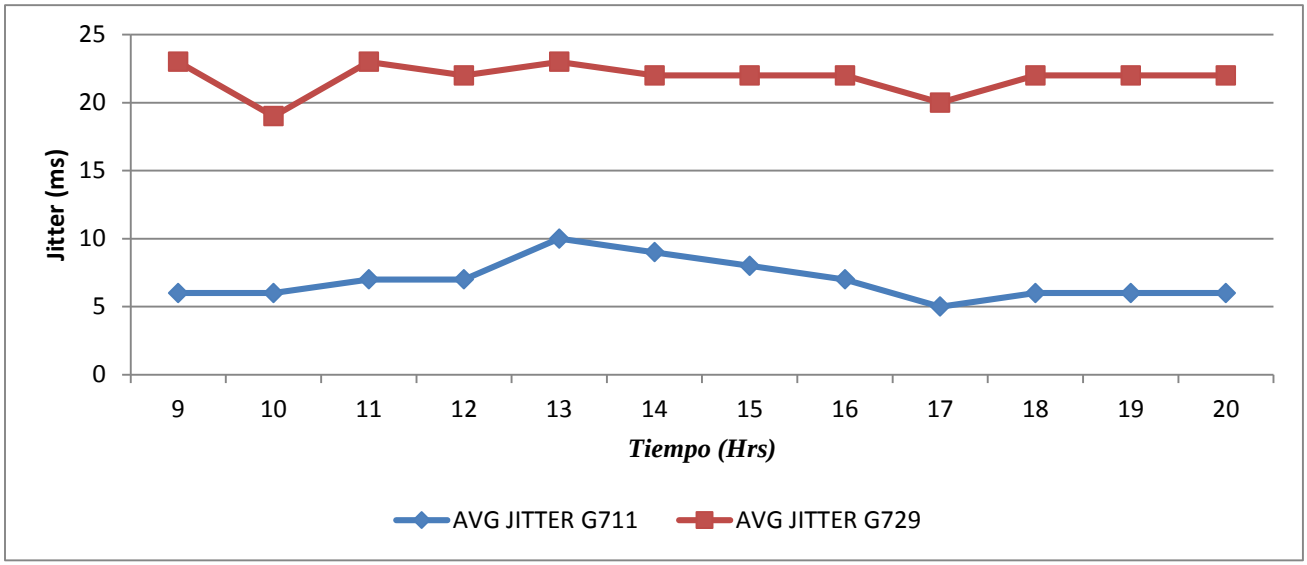


Figura 6-10 AVG Jitter G711 - G729 (VAD)

De igual manera se hizo un análisis de sensibilidad a las pérdidas de paquetes (PLR) entre los códecs G7.11 y G.729, como se muestra en las Figuras 6.11 y 6.12. Como se puede observar en las Figuras 6.11 y 6.12, el códec G.711 es menos sensible a las pérdidas de paquetes sin importar si se habilita o deshabilita el VAD. Los porcentajes promedio de PLR del códec G711 fueron de 0.09 con VAD y 0.09 sin VAD, en contraste para el códec G.729 se obtuvieron los porcentajes promedio de 0.10 con VAD y de 0.15 sin VAD. Este resultado explica el motivo por el cual, el códec G.729 es más sensible al jitter. Es decir, mientras mayor es el porcentaje de PLR, mayor será el valor de jitter.

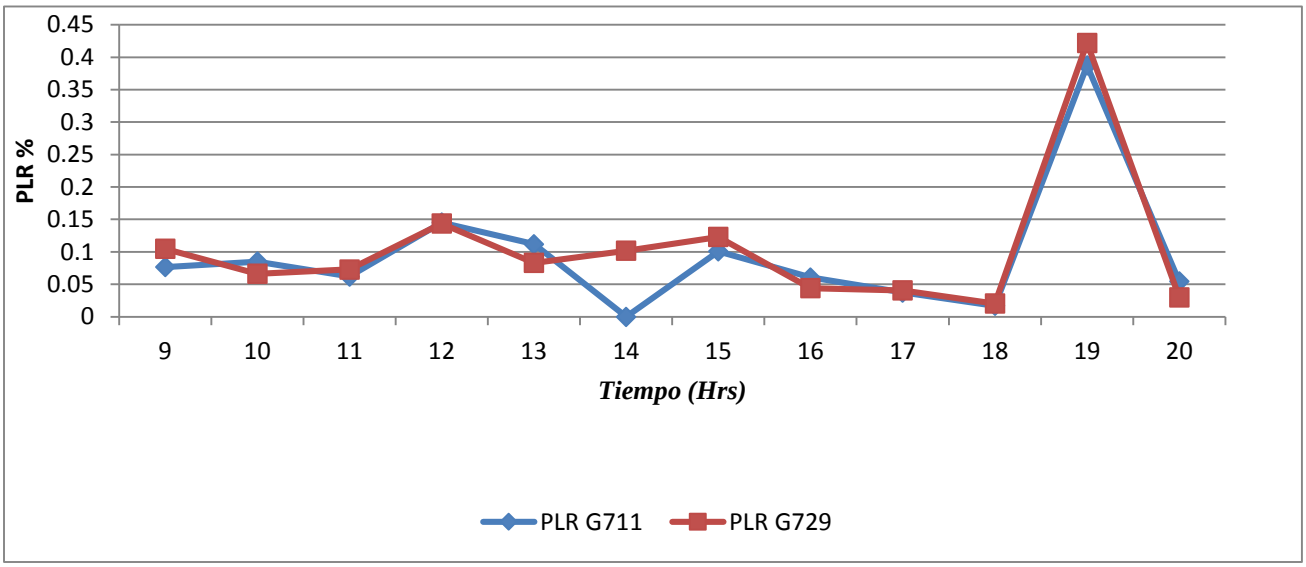


Figura 6-11 Comparación PLR G711-G729 (No VAD)

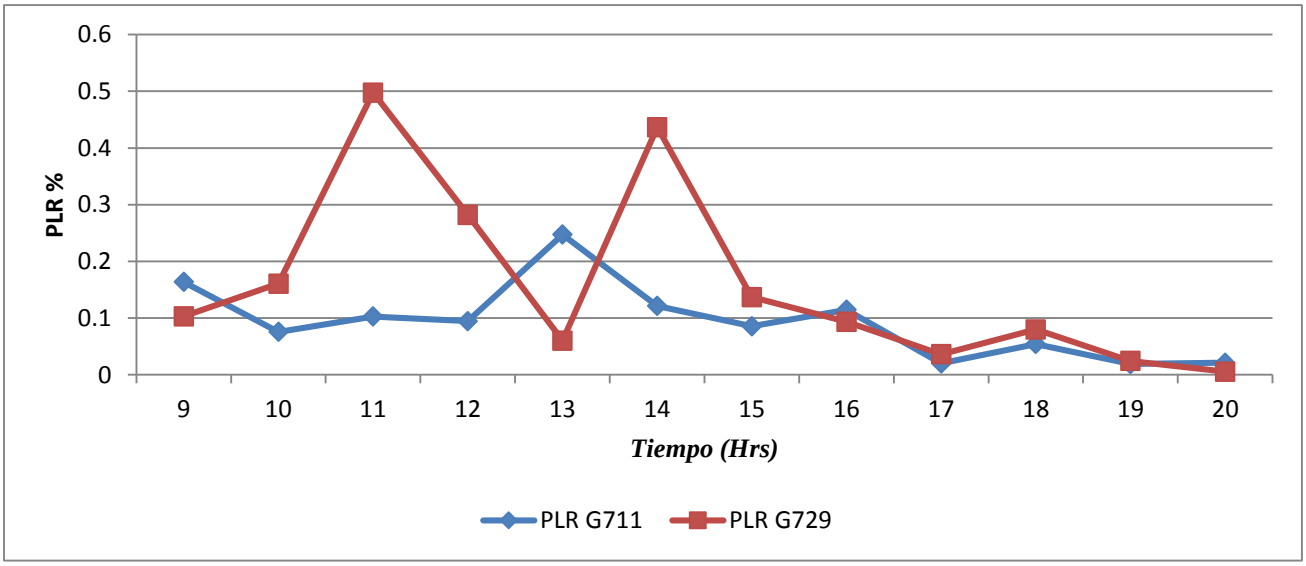


Figura 6-12 Comparación PLR G711-G729 (VAD)

Otro parámetro que se analizó fue el porcentaje de paquetes que presentaron un determinado valor de jitter o variación de retardo entre paquetes PDV (Packet Delay

Variation) a diferentes rangos de PDV (50ms-70ms, 70ms-90ms, 90ms-120ms, 120ms-150ms, 150ms-200ms, 200ms-300ms y mayor a 300ms). En las Figuras 6-13 y 6-14, se puede observar que un mayor porcentaje de paquetes presentaron un valor de PDV en el rango de 50ms-70ms cuando trasmitimos mediante el códec G.29.

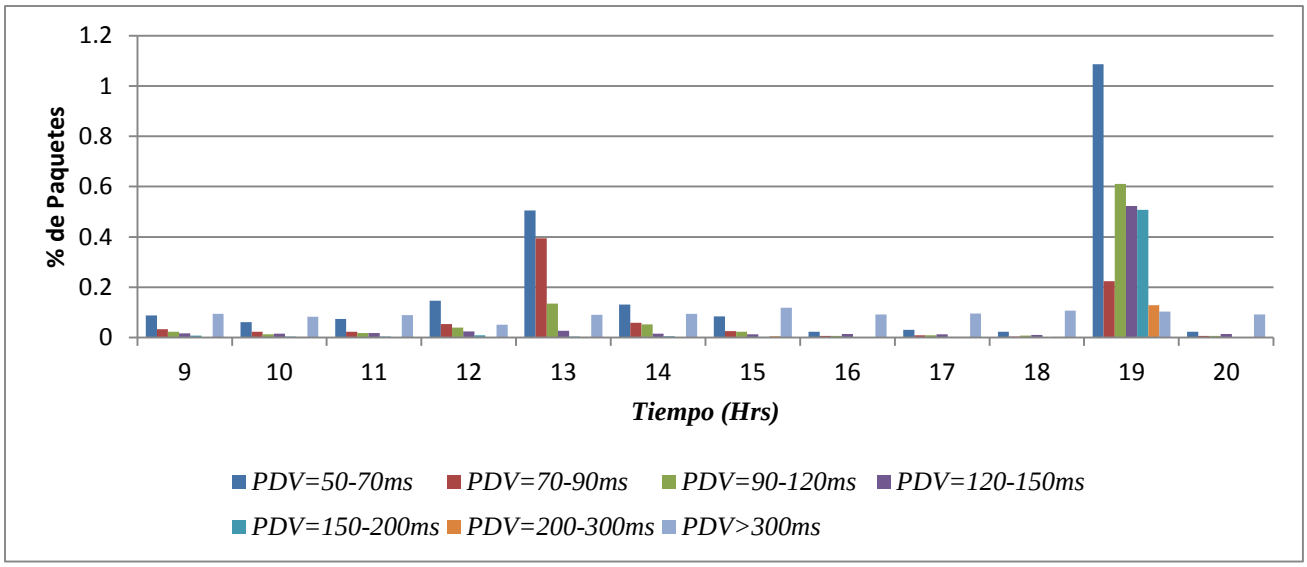


Figura 6-13 PDV G711

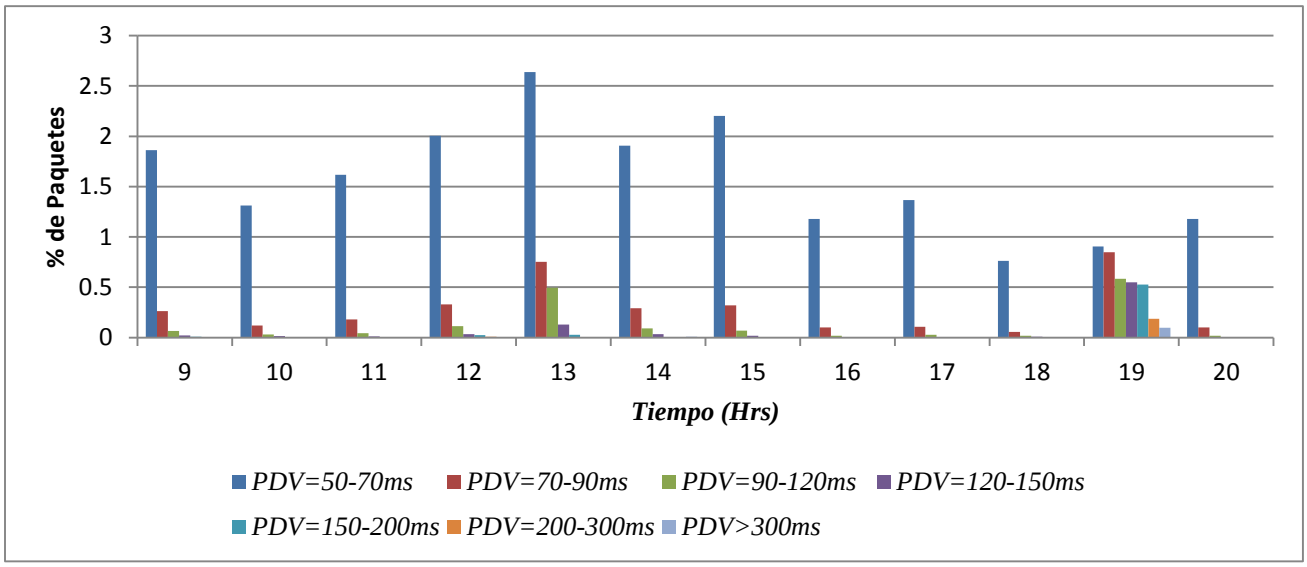


Figura 6-14 PDV G729

Este resultado explica el motivo por el cual, el valor promedio de MOS indica que muchos usuarios están insatisfechos o que existe una calidad no aceptable cuando utilizamos el códec G.729 y configuramos el tamaño del de-jitter buffer en el valor de 50ms. Al tener un porcentaje alto de paquetes con valores superiores a 50ms, traerá como consecuencia un porcentaje alto en la pérdida de paquetes debido a que el tamaño del de-jitter buffer no es lo suficientemente grande para poder almacenar de manera temporal los paquetes.

También se analizó el tamaño de las ráfagas (Burst Size) de las pérdidas presentadas en ambos códecs. La Figura 6-15 muestra que cuando usamos el códec G711 el mayor porcentaje de pérdidas presentaron un tamaño de ráfaga de BS=1 BS=2, mientras que con el códec G729 BS=1, BS=2, y BS=3. Este resultado confirma la existencia de mayor pérdida de paquetes bajo el esquema de codificación G.729.

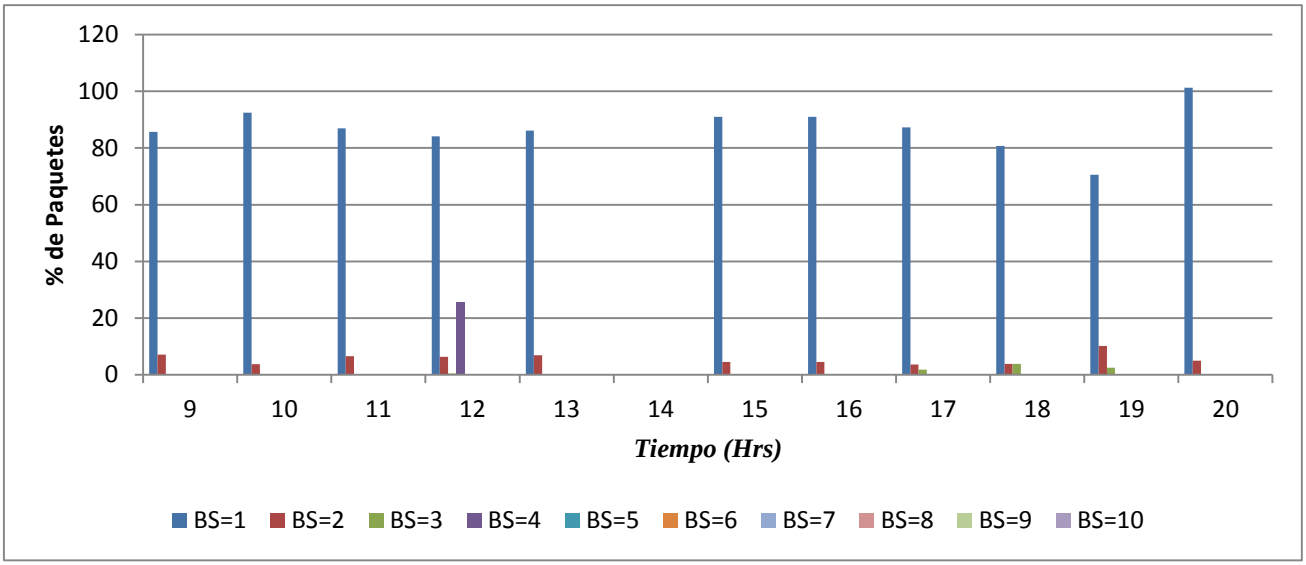


Figura 6-15 Porcentaje BS G711

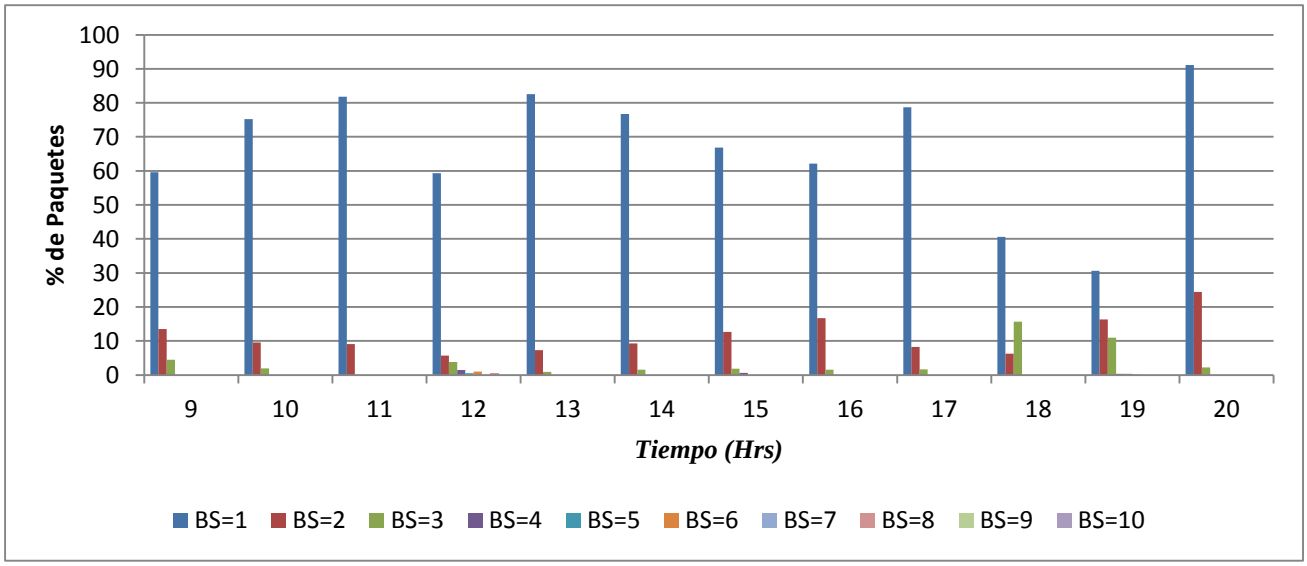


Figura 6-16 Porcentaje BS G729.

CAPÍTULO 7 CONCLUSIONES

En VoIP los dos protocolos más usados son el protocolo H.323 y el protocolo SIP, a pesar de que H.323 es un protocolo robusto, el protocolo SIP presenta una diferencia marcada sobre el protocolo H.323, debido a que este protocolo está basado en texto plano como el protocolo HTTP por lo que su codificación y su decodificación resultan mucho más fáciles de realizar a diferencia del protocolo H.323, así también es un protocolo de fácil implementación. Por esta razón, en este estudio se decidió utilizar el protocolo SIP como base para las llamadas de prueba. De igual forma, en las llamadas de prueba se utilizaron los esquemas de codificación G711 y G729 por ser los más utilizados en el transporte de voz.

En el presente trabajo se presenta el estudio de las métricas de desempeño jitter y pérdida de paquetes, bajo diferentes configuraciones de parámetros en una red VoIP-SIP: habilitación / deshabilitación de la detección de actividad de voz, codificación G.711/G.729 y diversos tamaños de de-jitter buffer (50ms, 200ms y 500ms). Este estudio se realizó mediante un conjunto de llamadas con las configuraciones mostradas en la Tabla 5-1sobre el escenario de medición descrito en la sección 5.1.

El análisis realizado en este trabajo se puede resumir de la siguiente manera:

Cuando configuramos los tamaños de de-jitter buffer de 50ms y 200ms, habilitamos el VAD y usamos un códec G.711 obtenemos una calidad aceptable para llamada, con valores de MOS superiores a cuando se encuentra deshabilitado el VAD.

Cuando configuramos el tamaño del de-jitter buffer en 200ms, sin la habilitación del VAD y usamos un códec G.729 obtenemos una calidad aceptable para llamada.

El códec G729 es más sensible al jitter sin importar si se habilita o deshabilita la detección de actividad de voz.

El códec G.711 es menos sensible a las pérdidas de paquetes sin importar si se habilita o deshabilita el VAD. Este resultado explica el motivo por el cual, el códec G.729 es más sensible al jitter. Es decir, mientras mayor es el porcentaje de PLR, mayor será el valor de jitter.

Cuando se transmite mediante el códec G.729, un mayor porcentaje de paquetes presentaron un valor de PDV en el rango de 50ms-70ms. Este resultado explica el motivo por el cual, el valor promedio de MOS indica que muchos usuarios están insatisfechos o que existe una calidad no aceptable cuando utilizamos el códec G.729 y configuramos el tamaño del de-jitter buffer en el valor de 50ms. Al tener un porcentaje alto de paquetes con valores superiores a 50ms, traerá como consecuencia un porcentaje alto en la pérdida de paquetes debido a que el tamaño del de-jitter buffer no es lo suficientemente grande para poder almacenar de manera temporal los paquetes.

Cuando usamos el códec G711 el mayor porcentaje de pérdidas presentaron un tamaño de ráfaga de BS=1 BS=2, mientras que con el códec G729 BS=1, BS=2, y BS=3. Este resultado confirma la existencia de mayor pérdida de paquetes bajo el esquema de codificación G.729.

REFERENCIAS

[1] Francisco Gil Montoya, Julio Gómez López, **"VoIP y Asterisk: Redescubriendo la telefonía"**, RA-MA Editorial Madrid, España 2009.

[2] Edgar Landívar, **"Comunicaciones Unificadas con Elastix, Volumen 1"**, GNU Free Documentation License. 2009.

[3] Juan Manuel Huidobro Moya, David Roldán Martínez, **"Tecnología VoIP y Telefonía IP"**, Creadores Copyright, S. L., España 2006.

[4] William Stallings, **"Data and Computer Communications,"** PRENTICE-HALL INC., 2004.

[5] Nefta Anaya, **"Fundamentos de Telefonía IP e Introducción a Asterisk/Elastix"**, ElastixTech, 2013.

[6] Alberto Escudero Pascual, Louise Berthilson, **"VoIP para el Desarrollo"**, IT+46, www.it46.se, 2006.

[7] Jonathan Davidson, James Peters, "**Voice over IP Fundamentals"**, Cisco Press, 201

[8] Gonzalo Camarillo, **"SIP Demystified"**, McGraw-Hill Companies, Inc., 2002.

[9] Allan Sulkin, **PBX Systems for IP telephony**, Migrating Enterprise Communication, McGraw-Hill TELECOM, 2003.

[10] Alan B. Johnston, **"SIP: Understanding the Session Initiation Protocol"**, ARTECH HOUSE, INC. 2004.

[11] William C. Hardy, **"VoIP Service Quality: Measuring and Evaluating Packet-Switched Voice"**, McGraw-Hill Companies, Inc., USA, 2003.

[12] ITU-T Rec P. 800, **"Methods for Subjective Determination of Transmission Quality"**, 1996.

[13]José Joskowics, R. S., **"Medida de la Calidad de Voz en Redes IP"**, IIE/FING/UDELAR, Uruguay, 2003.

APÉNDICE

Instalación de Elastix

Primeramente al introducir el CD de instalación de Elastix aparece la pantalla de bienvenida de Elastix, como se muestra en la Figura A-1.

Figura A-1 Pantalla de Bienvenida de Elastix

Para proceder con la instalación de Elastix, presionamos ENTER y nos aparecerá la siguiente pantalla en la cual seleccionaremos el lenguaje de nuestra preferencia, por defecto viene seleccionado el idioma inglés. Como se muestra en la Figura A-2.

Figura A-2 Seleccionando Lenguaje

Una vez seleccionado el idioma de nuestra preferencia, que en mi caso seleccioné el Idioma Español, nos aparecerá que tipo de teclado deseamos seleccionar, en este caso el tipo de teclado Español, como se muestra en la Figura A-3:

Figura A-3 Tipo de Teclado

Posteriormente seleccionaremos el Disco Duro donde instalaremos Elastix, para proceder con la instalación le presionamos la opción **SI**, la Figura A-4 muestra un ejemplo de esta ventana.

Figura A-5 Inicializar el Disco Duro

Una vez seleccionado esta opción procedemos a seleccionar y particionar el espacio del Disco Duro donde queremos instalar Elastix, en este caso seleccionamos el Utilizar el espacio disponible en dispositivos seleccionados y crear diseño predeterminado y presionamos la opción Aceptar, como muestra la Figura A-5.

Figura A-5 Tipo de Particionamiento

Seguidamente en la siguiente pantalla nos pedirá configurar la interfaz de red, el cual seleccionaremos la opción **SI**, como se muestra en la Figura A-6.

Figura A-6 Configuración de la Tarteja de Red

La Figura A-7 muestra la pantalla en donde se nos pedirá la configuración de red para la interfaz Ethernet que deseamos aplicar para la instalación del sistema, el cual marcaremos las opciones Activar al Inicio y Activar soporte IPv4 y seleccionamos la opción Aceptar,

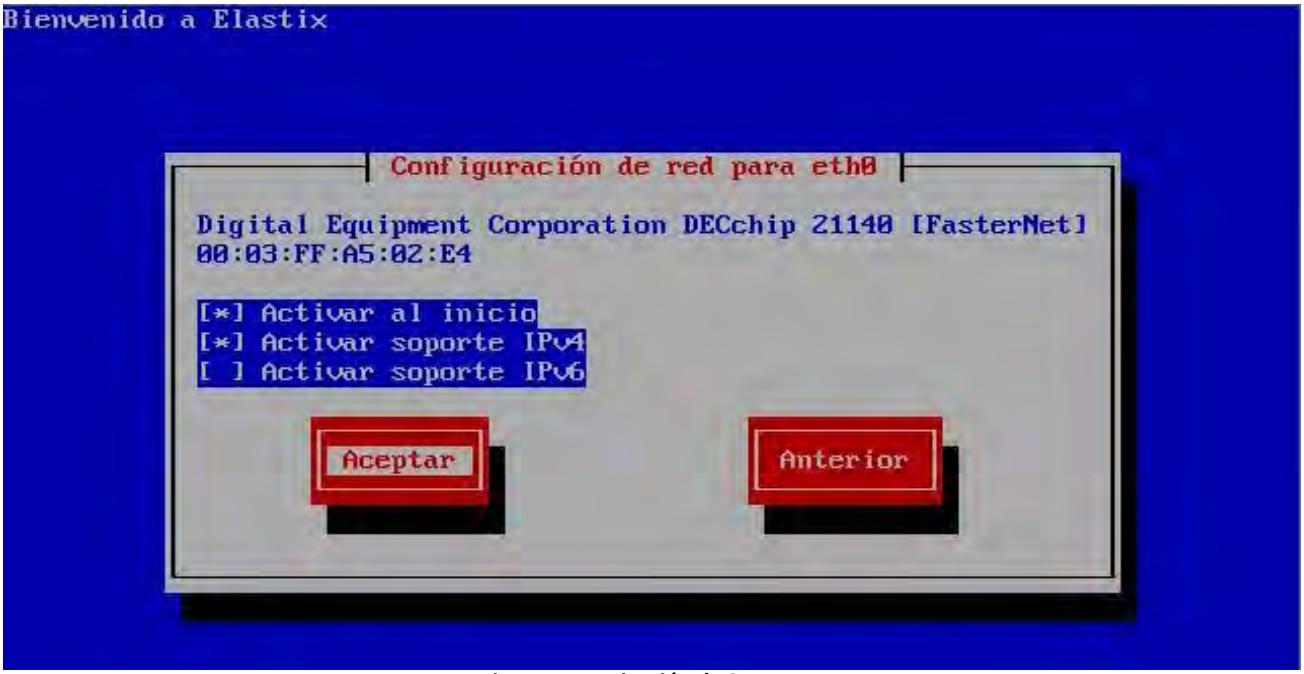


Figura A-7 Activación de Soporte IPv4

Una vez seleccionado esta opción, nos aparecerá la siguiente pantalla para la configuración IPv4 para Ethernet, en el cual marcaremos la Configuración manual TCP/IP y procedemos a introducir la Dirección IP de nuestro servidor, la Máscara de Red, la puerta de enlace, así como el DNS Primario, como lo muestra las Figuras A-8 y Figura A-9, respectivamente.

Figura A-8 Direccionamiento IP

Figura A-9 Configuración DNS

Posteriormente procedemos a configurar el nombre del servidor el cual marcamos la opción Manualmente, como lo muestra la Figura A-10:

Figura A-10 Nombre de Host

En la Figura A-11 se muestra la pantalla donde se nos pedirá elegir una contraseña de root, la cual será de nuestra libre elección, sin dejar a un lado la seguridad de la contraseña.

Figura A-11 Contraseña de Root

Después de confirmar la contraseña de root dará inicio la instalación de todos los paquetes necesarios para el funcionamiento de Elastix, una vez finalizada la instalación, se nos pedirá la crear una contraseña para root de la base de datos MySQL, como lo muestra la Figura A-12:

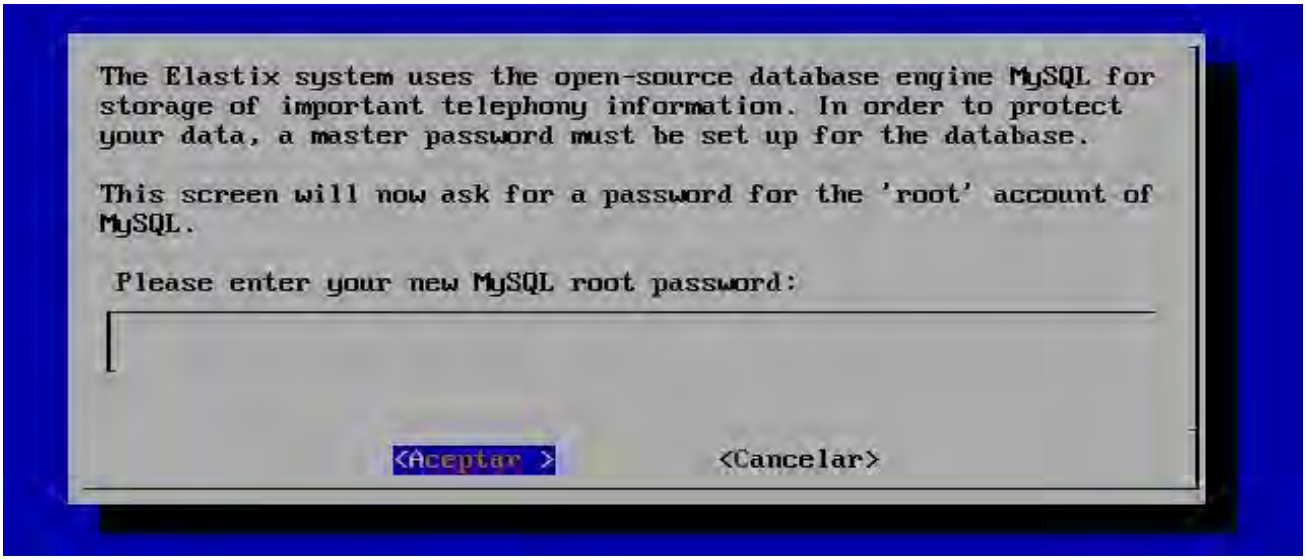


Figura A-12 Contraseña Root para MySQL

Una vez creada la contraseña de root de MySQL, se nos pedirá la contraseña de admin para la administración vía Web, como se muestra en la Figura A-13.

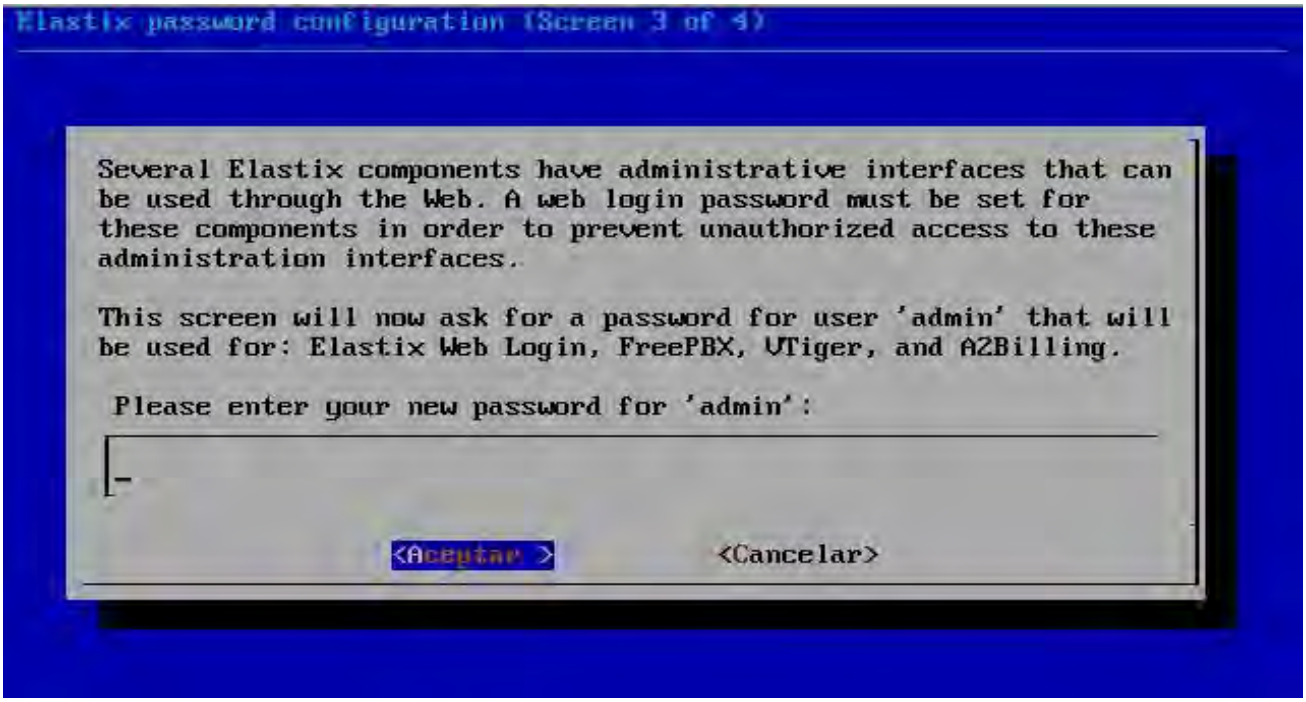


Figura A-13 Contraseña para la Interfaz Gráfica

Configuración de Elastix a través de la interfaz WEB

Una vez terminada la instalación de Elastix procedemos a configurarlo mediante acceso vía Web tal y como se muestra en la Figura A-14:

Figura A-14 Ingreso Vía Web

Dashboard (Tablero de Instrumentos)

Una vez iniciada la sesión como administrador se nos muestra la ventana principal de Elastix que es la de Dashboard (Tablero de instrumentos) que la primer menú de la pestaña Sistema, ésta contiene además de contener este menú, contiene los menús Network, Usuarios, Shutdown, Hardware Detector, Updates, Backup/Restore y Preferencias, tal como se muestra en la Figura A-15.

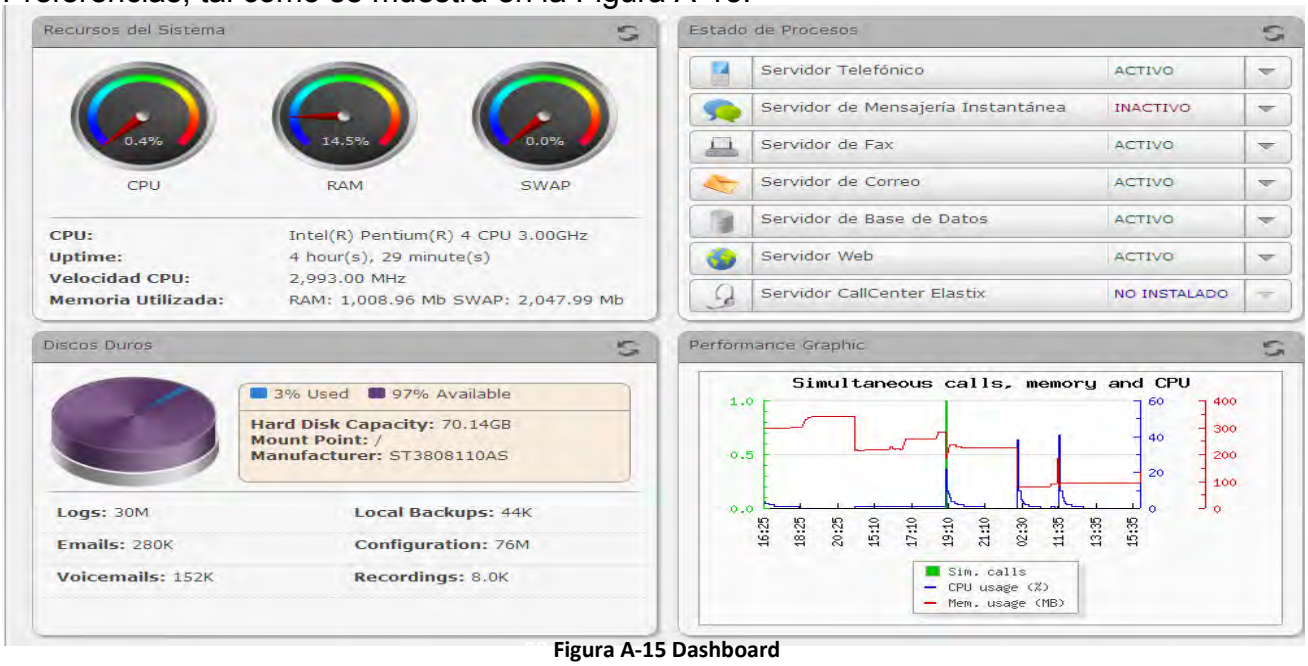


Figura A-15 Dashboard

Dentro del menú Dashboard, está contenida la información del sistema y las actividades que realiza el sistema, para poder modificar el Dashboard, le damos clic en la opción de Dashboard Applet Admin y se nos mostrará la siguiente pantalla donde podremos seleccionar la información de actividades que deseemos mostrar en la pantalla principal tal y como se muestra en la Figura A-16:

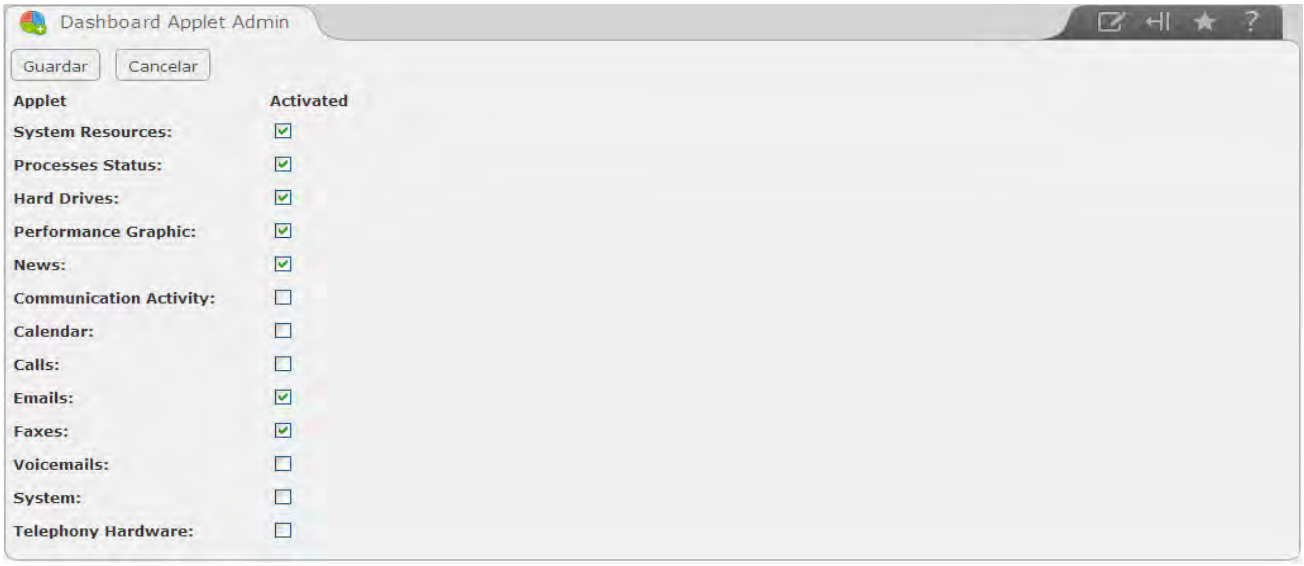


Figura A-16 Configuración Dashboard

Network

En el siguiente menú Network, se muestran los parámetros de red como son nombre del equipo (Hostname), DNS, Puerta de Enlace. De igual manera contiene una descripción de las interfaces Ethernet conectadas como se muestra en la Figura A-17:

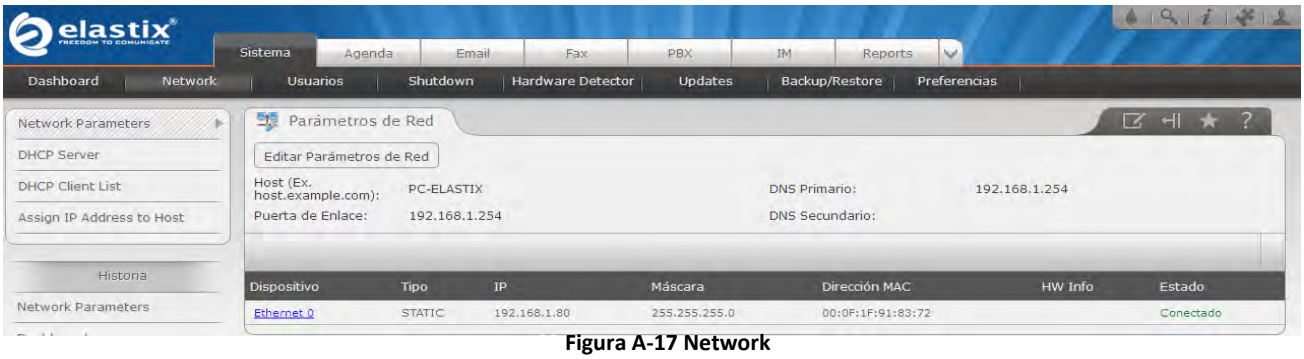


Figura A-17 Network

DHCP

En la opción DHCP Server asignamos de forma automática direcciones a los demás equipos de nuestra red como son: Teléfonos IP, ATAs, etc. Así como se muestra en la Figura A-18.

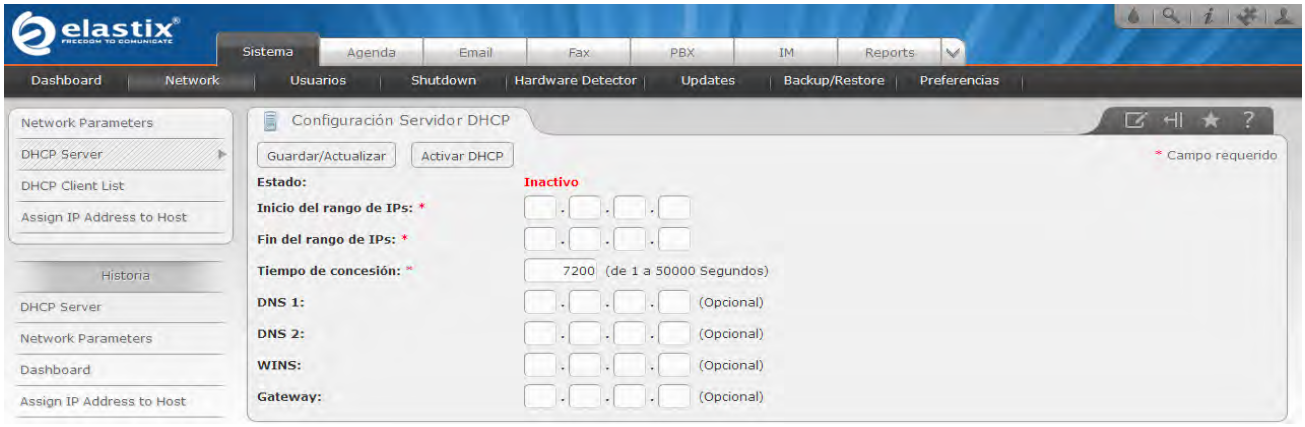


Figura A-18 DHCP Server

Creación de Usuarios

En este menú se crean usuarios, grupos y otorgar permisos a los grupos creados, para poder crear un usuario debemos llenar los siguientes campos requeridos que se muestran en la Figura A-19:

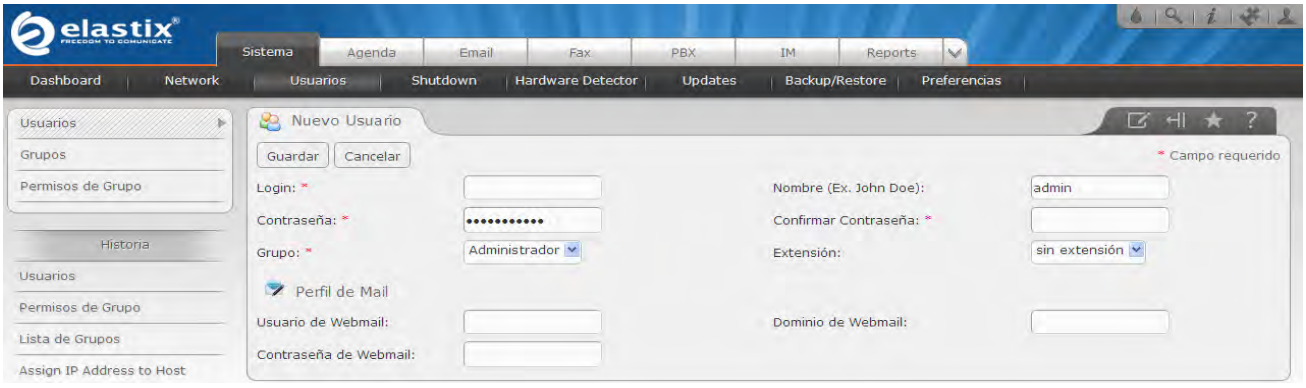


Figura A-19 Users

Configuración del Correo Electrónico

Para configurar el correo electrónico nos vamos a la pestaña Email y nos aparecerá la siguiente ventana y dentro de ella procedemos a crear el dominio para nuestro servidor E – mail, como se muestra en la Figura A-20.

Figura A-20 E-Mail

Una vez creado el dominio, nos disponemos a crear las cuentas de E – mail con los que contará nuestro servicio, por lo cual llenaremos los campos como lo muestra la Figura A-21.

Figura A-21 E-Mail Users

Servicio Follow Me

Para poder activar este servicio nos dirigimos a la opción Follow Me dentro de la pestaña PBX, seleccionamos la extensión a la cual deseamos activar el servicio y agregamos las extensiones a las cuales se marcará para localizar a la persona deseada, como se muestra en la Figura A-21.

Figura A-21 Servicio Follow Me

Conferencia

Para crear una conferencia no dirigimos a la opción Conferencia de la PBX, donde nos aparecerá una ventana en la cual llenaremos los campos Número de Conferencia, nombre de la conferencia, PIN de Usuario y PIN de administrador, como lo muestra la Figura A-22.

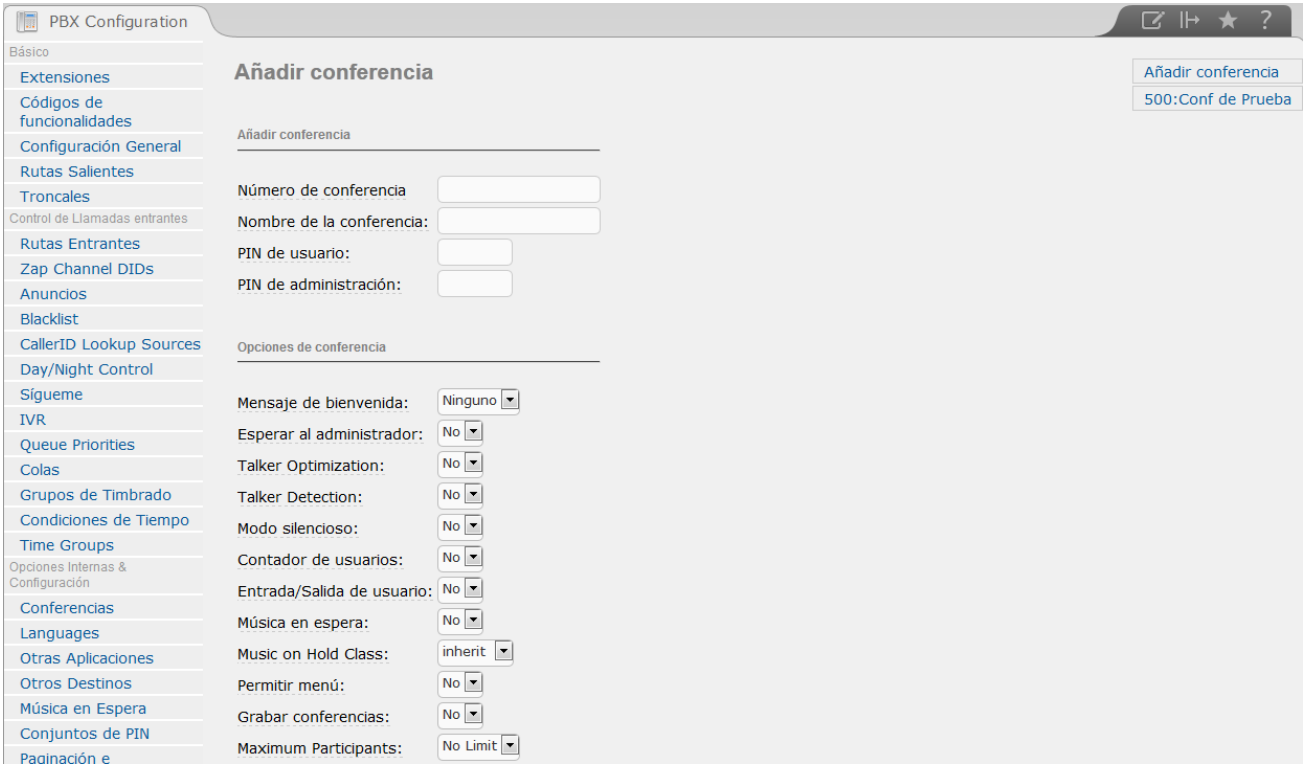


Figura A-22 Conferencia

Música en espera

Para configurar la llamada en espera, nos vamos a la pestaña PBX y nos vamos a la opción Música en Espera y nos aparecerá la siguiente ventana en donde podremos seleccionar los sonidos que hay predeterminados o bien podemos agregar uno personalizado, pero para poder agregarlo el sonido debe estar codificado en PCM A 16 BITS y 8 KHZ, como lo muestra la Figura A-23.

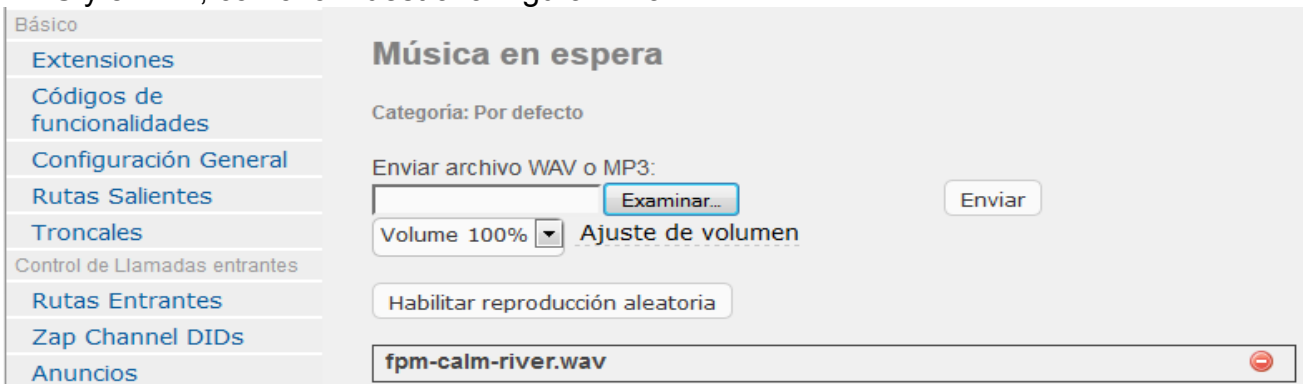


Figura A-23 Música en Espera

Servicio de Voicemail

Para configurar el servicio de Voicemail, nos vamos al menú PBX, seleccionamos una de las extensiones ya creadas y se nos mostrará en donde habilitaremos el servicio y llenamos los campos Voicemail Password y Email Address y para poder escuchar el buzón marcamos *97, como se muestra en la Figura A-24.

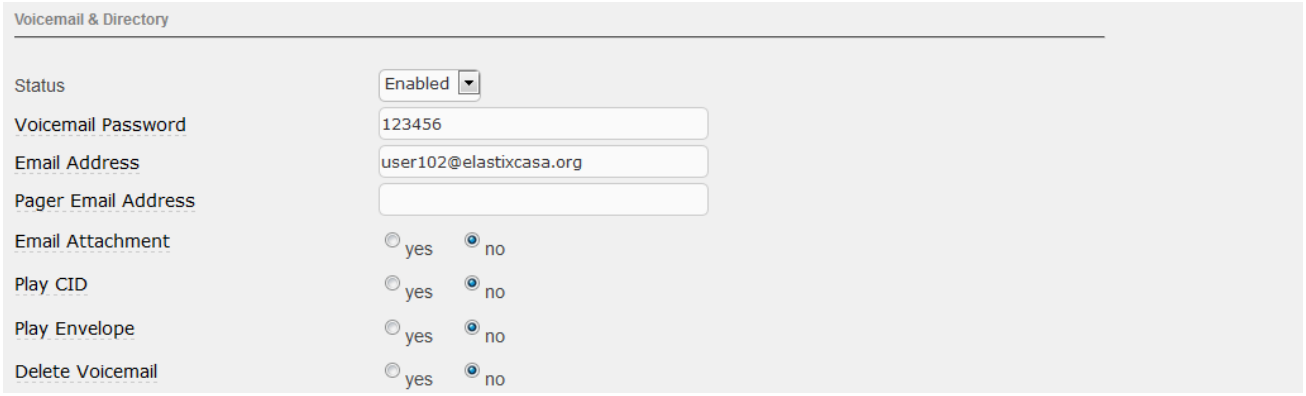


Figura A-24 Voicemail

Configuración llamada de video

Para configurar la llamada de video debemos editar un archivo de configuración llamado Sip.conf, para ello en la opción de Asterisk-CLI buscamos el archivo y le agregamos las líneas que se muestran sombreadas en la Figura A-25:

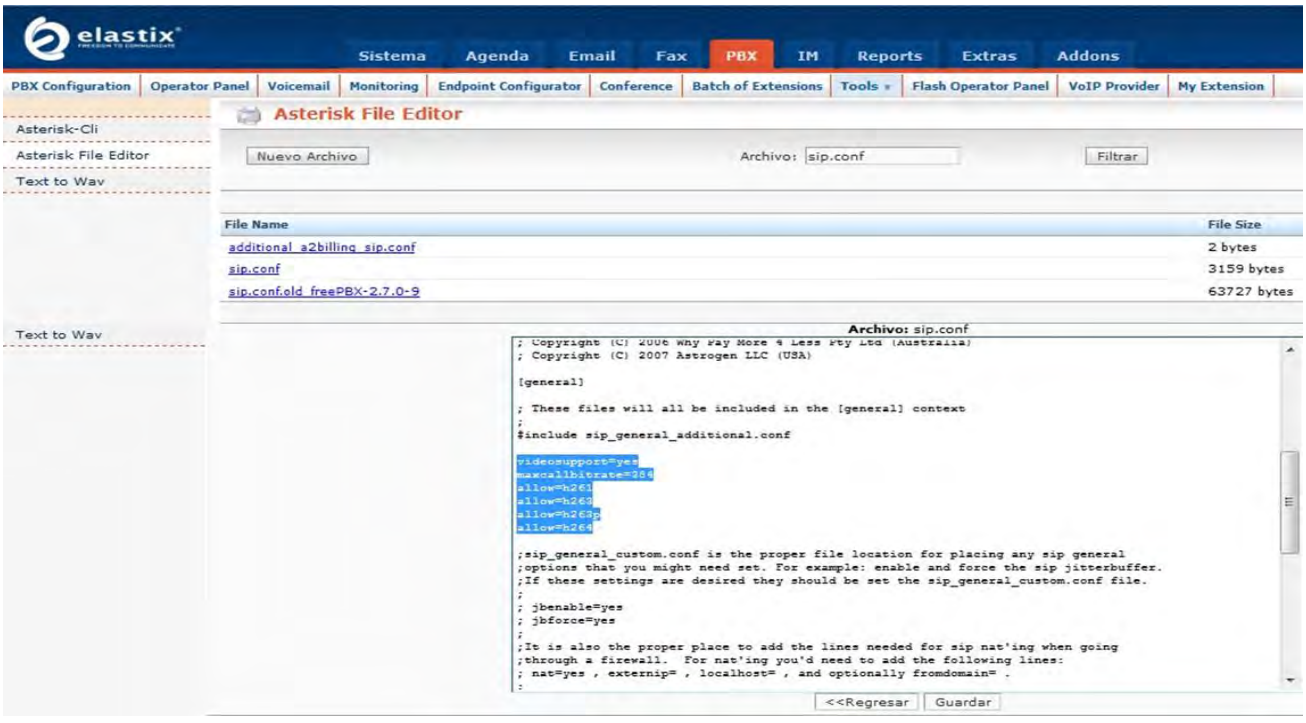


Figura A-25 Configuración para la Video Llamada

Configuración del servicio de mensajería instantánea

Para configurar el servicio de Mensajería Instantánea, nos dirigimos al menú IM y activamos el servicio de Openfire, seguidamente se nos mostrará la ventana donde deberemos escoger el idioma de nuestra interfaz como se muestra en la Figura A-26.

Figura A-26 Activación de Openfire

En esta parte de la activación de Openfire, deberemos escribir el nombre del dominio de nuestro servidor, en este caso es la dirección IP. Y por defecto ya vienen agregados los puertos para la Administración de la Consola, como se muestra en la Figura A-27.

Figura A-27 Configuración del Servidor

Posteriormente deberemos seleccionar la base de datos con la que interactuará Openfire, la seleccionaremos la de base de Interna, como se muestra en la Figura A-28.

Figura A-28 Selección de la Base de datos

A continuación configuraremos en dónde se almacenarán los usuarios de Openfire, por la que dejaremos la opción que seleccionada por defecto, como se muestra en la Figura A-29

Figura A-29 Selección de Almacenaje

Administración Web de Openfire

Una vez que hemos ingresado a la interface de administración como administrador con la cuenta creada previamente, podremos crear usuarios y comenzar a usar la mensajería instantánea en Elastix, como se muestra en la Figura A-30.

Figura A-30 Interfaz Web Openfire

En esta parte nos encargaremos de crear los usuarios para la mensajería instantánea, dónde deberemos llenar los campos con los datos de los usuarios previamente creados, como se muestra en la Figura A-31.

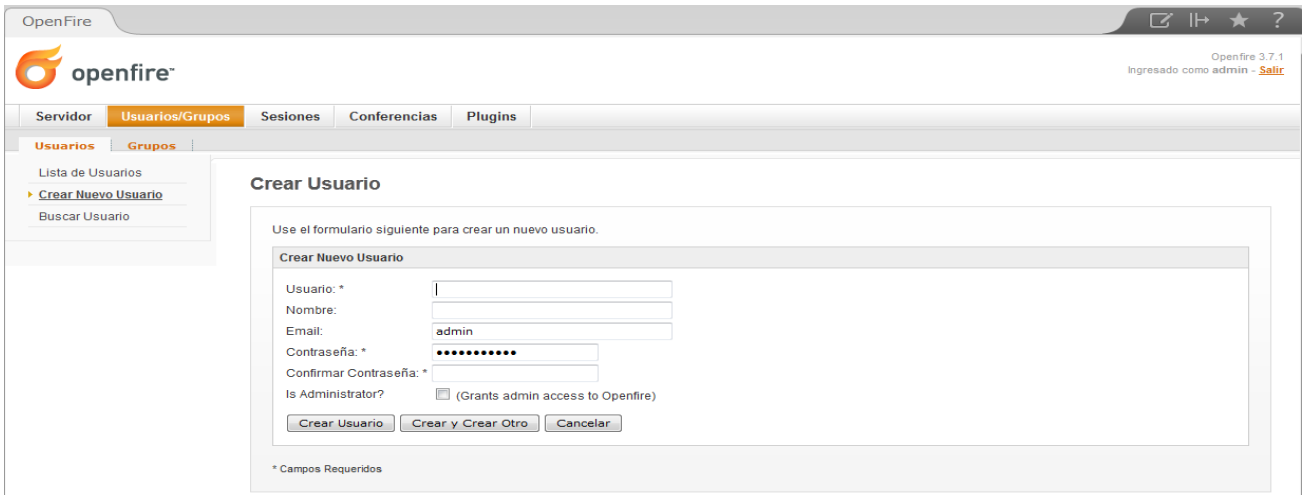


Figura A-31 Creación de Usuarios Openfire

Una vez creados los usuarios se nos mostrará una pantalla similar a esta, dónde podremos observar los status de cada usuario, como se muestra en la Figura A-32.

Figura A-32 Lista de Usuarios

Seguidamente instalaremos un plugin que nos permitirá la interacción con Asterisk y gracias a este plugin podremos realizar tareas de interconexión con el cliente de mensajería. Para ellos nos dirigiremos al menú plugins y presionamos plugins disponibles y procedemos a instalar el plugin Asterisk-IM Openfire Plugin, como se muestra en la Figura A-33.

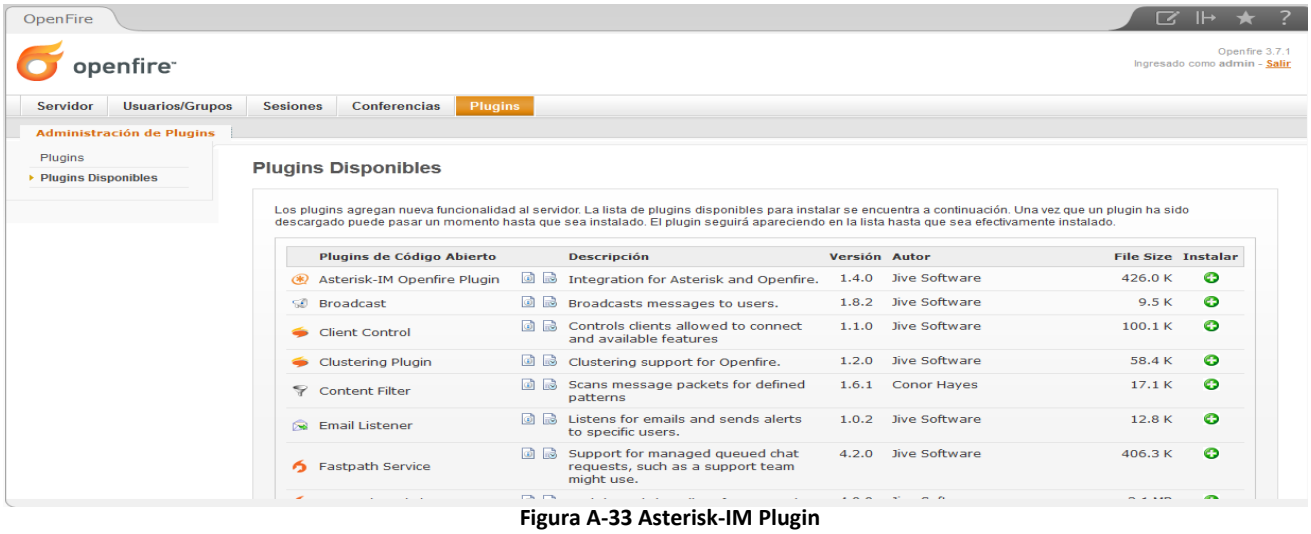


Figura A-33 Asterisk-IM Plugin

Una vez que el plugin se haya instalado correctamente, deberemos de contar con un nuevo Menú llamado Asterisk-IM, en donde podremos configurar la integración de OpenFire con Asterisk. Para ello marcamos Enable para habilitarlo y únicamente llenaremos el campo Asterisk Context con la palabra default, como se muestra en la Figura A-34.

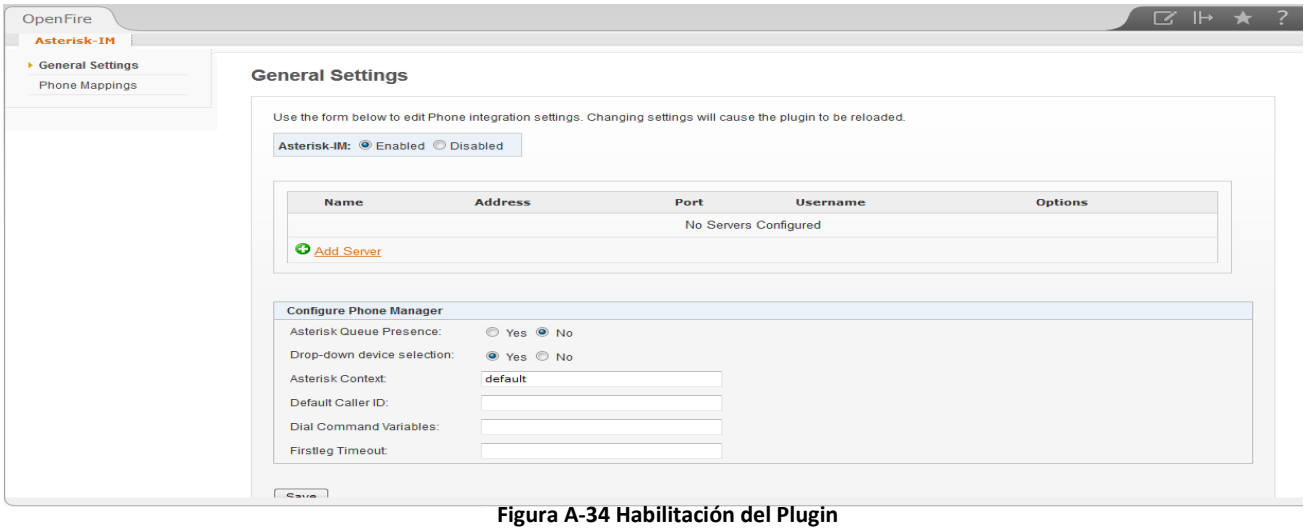


Figura A-34 Habilitación del Plugin

Antes de agregar el servidor que utilizaremos para el servicio de mensajería instantánea, deberemos editar un archivo llamado asterisk-im_hsqldb.sql. Por lo tanto nos iremos a la consola de nuestro servidor y escribiremos cd /opt/openfire/plugins/asterisk-im/database/ damos enter y con nano editaremos el archivo como lo muestra la Figura A-35.

Figura A-35 Modificación del Archivo

Una vez modificado el archivo, ahora podemos procedemos a crear nuestro de servidor de mensajería instantánea. Para ello en el menú Asterisk-IM agregamos el servidor y llenaremos los campos que se muestran en la Figura A-36.

Figura A-36 Creación del Servidor

Concluido la creación del servidor, nos debe de aparecer una ventana donde se nos muestra que el servidor ha sido agregado y de que se ha conectado de manera exitosa, como se muestra en la Figura A-37.

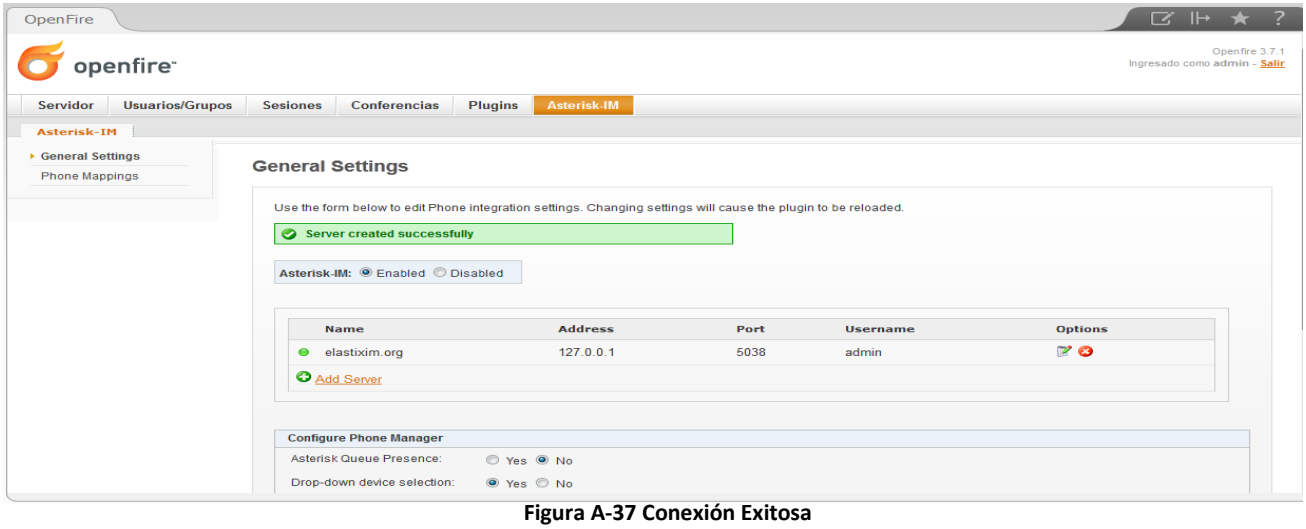


Figura A-37 Conexión Exitosa

Ahora bien, para poder utilizar este servicio, instalaremos un cliente llamado Spark. Una vez instalado, nos logearemos con uno de los usuarios ya creados y en la Figura A-38 se muestra la interacción de los usuarios.

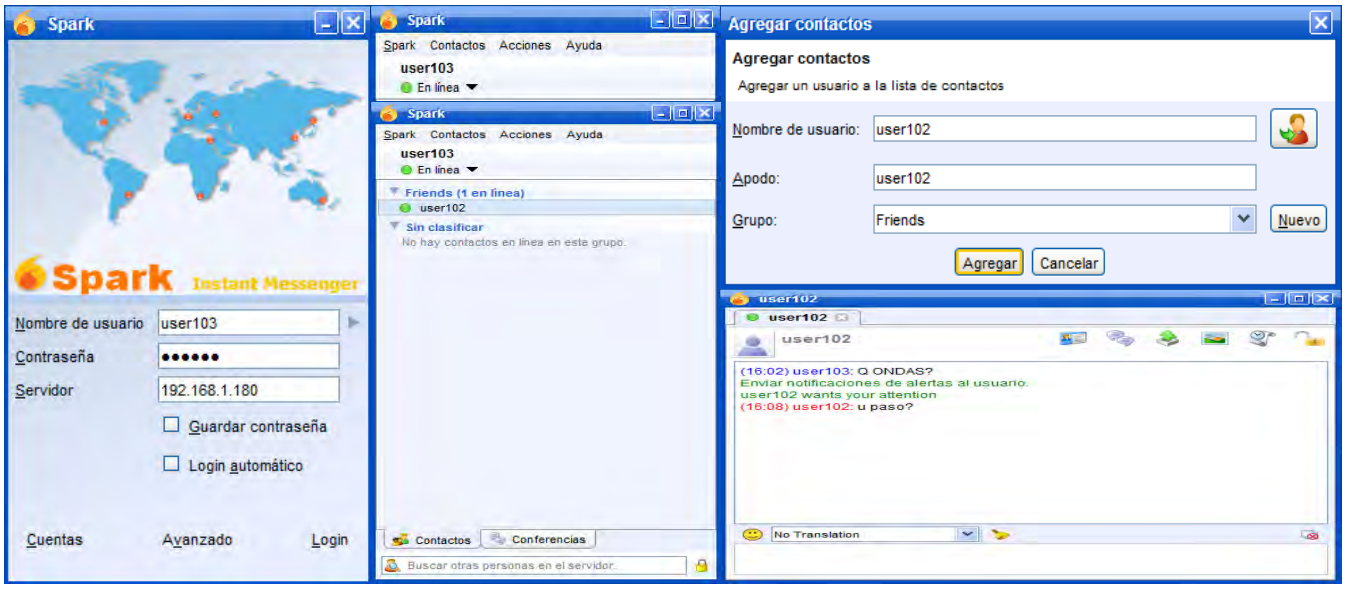


Figura A-38 Live Chat