TRABAJO ESPECIAL DE GRADO

DESARROLLO E IMPLEMENTACIÓN DE UN GATEWAY BASADO EN CÓDIGO ABIERTO SOBRE LA RED DE DATOS DE LA UNIVERSIDAD CENTRAL DE VENEZUELA

Presentado ante la Ilustre
Universidad Central de Venezuela
por la Br. López D. Sarith V.
para optar al título de
Ingeniero Electricista

Caracas, 2011

TRABAJO ESPECIAL DE GRADO

DESARROLLO E IMPLEMENTACIÓN DE UN GATEWAY BASADO EN CÓDIGO ABIERTO SOBRE LA RED DE DATOS DE LA UNIVERSIDAD CENTRAL DE VENEZUELA

Tutor Académico: Ing. Luis Fernández

Presentado ante la Ilustre
Universidad Central de Venezuela
por la Br. López D. Sarith V.
para optar al título de
Ingeniero Electricista

Caracas, 2011

CONSTANCIA DE APROBACIÓN

Caracas, 04 de noviembre de 2011

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por la Bachiller Sarith V. López D. titulado:

"DESARROLLO E IMPLEMENTACIÓN DE UN GATEWAY BASADO EN CÓDIGO ABIERTO SOBRE LA RED DE DATOS DE LA UNIVERSIDAD CENTRAL DE VENEZUELA"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. Neudith Morales
Jurado

Prof. Carlos Moreno
Jurado

Prof. Luis Fernández
Tutor Académico

DEDICATORIA

A Dios…

A Yaya….

A Papa López…

A Matilo…

A mi Mamá…

Al Hamster….

A Mi familia …

AGRADECIMIENTOS

La presente Tesis y mi Carrera en sí, es un esfuerzo en el cual, directa o indirectamente, participaron varias personas, corrigiéndome, apoyándome, teniéndome paciencia y acompañándome, tanto en los momentos más difíciles, como en los momentos de felicidad. Tomen ésto, como una pequeña muestra de agradecimiento por todo lo que me han dado y espero seguir contando con ustedes de aquí en adelante, así como podrán contar conmigo siempre.

A Dios. Por permitirme llegar hasta este momento tan importante de mi vida y lograr otra meta más; y en especial, por llenar mi vida de dicha y bendiciones. Gracias Papá!.

A Yaya. Mi Mamá-Tía, por ti estoy aquí. Fuiste, eres y serás mi guía y mi ejemplo a seguir siempre, porque me enseñaste todo lo que sé y aún en tu ausencia, sigo aprendiendo de ti. Me diste tanto, que un tomo completo no me bastaría para agradecerte. Te agradezco por tanto amor, dedicación y por hacerme quien soy. En todo momento te llevo conmigo, eres lo mejor que me ha pasado. No te olvidaré nunca. Dios te bendiga y te tenga en su Santa Gloria.

A Papa López. Mi adorado Abuelo. Por infundirme todos los principios y valores y enseñarme el significado de amor y de familia. Tu visión, tu inventiva y tus ganas de aprender, fueron los motivos que me llevaron a escoger esta carrera, la carrera del futuro. Espero haber cumplido tu sueño. Dios te Bendiga.

A Matilo. Por su cariño, amor, comprensión y apoyo sin condiciones ni medidas. Por encomendarme siempre a Dios para que saliera adelante, ya sé que tus oraciones fueron escuchadas. Gracias!. Porque eres mi pilar fundamental y la razón de mi vida. Sin ti no hubiese podido lograr ni la cuarta parte de lo que he logrado. Te adoro Matilo!

A Mi Mamá. Por su amor, comprensión y apoyo, que me permite sentir que puedo lograr todo lo que me proponga. Gracias por tu alegría y tu bondad, eres la luz que ilumina mi vida. Siempre lo he dicho, eres mi héroe, si llego a ser la mitad de lo que

tú has sido, consideraré que he conseguido el éxito, porque siempre he querido ser como tú y continuaré siguiendo tus pasos.

Al Hámster. Mi hermana, mi mejor amiga y mi hámster. No sé que haría sin ti, porque eres mi mano derecha y la persona en quien más confío. Gracias por tu cariño, confianza, por tu apoyo, por escucharme siempre, por tus consejos; para ti éste trabajo!, y para que también continúes superándote y sigas siendo esa persona especial de siempre.

A Mi Familia. Y en especial a mi Tía Coco, mi Tía Carvy, mi Tío José Antonio y mi Tía Tilito. A todos ustedes por su apoyo incondicional y a quienes debo este triunfo profesional, por todo su trabajo y dedicación para darme una formación académica y sobre todo humanista y espiritual. De ustedes es este triunfo y para ustedes es todo mi agradecimiento.

A mis Amigos Kenny, Usbel, Jonás, Jessi, al Negro (gracias por ser parte de mi vida) y a todas aquellas personas que fueron importantes para mí durante todo este tiempo. Con ustedes compartí aventuras, experiencias desveladas y los más divertidos momentos, lo que me dió la fortaleza necesaria para seguir adelante. Gracias por hacer que cada pedazo de tiempo fuera ameno.

A mi Manito y compañero de tesis Max. Quién me enseñó a salir adelante en los momentos más difíciles, me suministró todo su ayuda, enseñanzas y me brindó su amistad y confianza, al igual que nuestro **tutor** y amigo el **Ing. Luis Fernández**, director de este proyecto; gracias por su disposición y apoyo en esta investigación.

A la UCV. La máxima casa de estudios, "La Casa que Vence las Sombras" y mi segundo hogar. **A todos los Profesores,** que participaron en mi desarrollo profesional durante mi carrera, sin su ayuda y conocimientos no estaría en donde me encuentro ahora.

A los que nombré y los que no…A Todos….

¡Gracias!

López D. Sarith V.

DESARROLLO E IMPLEMENTACIÓN DE UN GATEWAY BASADO EN CÓDIGO ABIERTO SOBRE LA RED DE DATOS DE LA UNIVERSIDAD CENTRAL DE VENEZUELA

Tutor Académico: Ing. Luis Fernández. Tesis. Caracas. UCV. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Tesis de Grado 2011. 140h + anexos.

Palabras Claves: Gateway; H.323; SIP; Sistemas de Videoconferencia; Software Libre; Código Abierto.

Resumen. La presente investigación, tiene como objetivo principal desarrollar e implementar un Gateway basado en un software libre que permita administrar, traducir e interconectar los protocolos involucrados en el servicio de videoconferencia de la Universidad Central de Venezuela, procurando la compatibilidad con la plataforma existente de acuerdo a las necesidades y requerimientos de la red; permitiendo así, la interacción de profesores y estudiantes con un software de videoconferencia en tiempo real, de suficiente capacidad y a un bajo costo. Al mismo tiempo, con este proyecto basado en software libre, se pretende expandir la red de datos de la UCV superando las barreras impuestas por los protocolos propietarios y los elevados costos de los equipos terminales. Se podrá intercambiar servicios propios de la videoconferencia que aplicados con diversos fines, bien sea: académicos, técnicos, informativos o educativos; brindarán a cualquier miembro de la comunidad universitaria un libre acceso a este medio, promoviendo así, el desarrollo de los servicios de transmisión de datos a distancia dentro de nuestra casa de estudios. Este proyecto se compone de tres partes principales: en principio, a partir de los requisitos definidos durante el proyecto, se realizará el completo desarrollo de una herramienta modular y escalable, explicando en detalle cada elemento y los protocolos básicos que debiera manejar el software. En segundo lugar, se establecerán las pautas de implementación, considerando la arquitectura, y por último, serán realizadas las pruebas de validación necesarias y requeridas que comprueben la funcionalidad del software.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

ACRÓNIMOS

ATM Asynchronous Transfer Mode

ASCII American Standard Code for Information Interchange

ASN.1 Abstract Syntax Notation number One

CODEC COder/DECoder

DNS Domain Name Servers

DTMF Dual Tone-Multi-Frequence

ENUM Electronic Number/Telephone Mapping

HTTP Hypertext Transfer Protocol

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force's

IP Internet Protocol

ITU-T Telecommunication Standardization Sector of International Telecommunication Union

LAN Local Area Network

MAN Metropolitan Area Network

MBONE Multicast Backbone

MC Multipoint Controller

MCU Multipoint Control Unit

MMUSIC Multiparty Multimedia Session Control

MP Multipoint Processor

MOS Mean Opinion Score

NAPTR Naming Authority Pointer

OSI Open Systems Interconnection

PC Personal Computer

PBN packet based network

PBX Private Branch Exchange

PSTN Public Swicthed Telephone Network

QCIP Quarter Comment Intermediate Format

QoS Quality of Service

RAS Registration Admission and Status

RDSI Red Digital de Servicios Integrados

RFC Request For Comments

RSVP Resource Reservation Protocol

RTC Red telefónica conmutada

RTCP Real Time Control Protocol

RTSP Real Time Streaming Protocol

RTP Real-Time Transport Protocol

SAP Service Advertising Protocol

SDP Session Description Protocol

SMTP Simple Mail Transfer Protocol

SIP Session Initiation Protocol

TEG Trabajo Especial de Grado

TCP Transmission Control Protocol

TLD Top Level Domains

UA User Agent

UAC User Agent Server

UAS User Agent Client

UCV Universidad Central de Venezuela

UDP User Datagram Protocol

URI Universal Resource Identifier

URL Uniform Resource Locator

VoIP Voice over Internet Protocol

WAN Wide Area Network

INTRODUCCIÓN

Cuando establecemos una comunicación con otra persona, en la que adicionalmente podemos observar sus expresiones faciales, obtenemos mayor información de lo que expresa la persona con sus mismas palabras o calidad de voz combinadas. Surge así la videoconferencia, como una solución accesible a esta necesidad de comunicación, con sistemas que permiten el transmitir y recibir información visual y sonora entre puntos o zonas diferentes, evitando el traslado físico de las personas a costos cada vez menores y con señales de mejor calidad. La videoconferencia es un sistema de comunicación cerrada punto a punto o multipunto, que nos permite llevar a cabo el encuentro de varias personas ubicadas en sitios distantes, y establecer una conversación como lo harían si todas se encontraran reunidas en una misma sala.

La Universidad Central de Venezuela cuenta con una plataforma de videoconferencia basada en equipos Polycom, que si bien está apoyada en estándares internacionales (basados en el protocolo H.323), hacen uso de protocolos propietarios que confinan su expansión a la totalidad de la UCV debido a los elevados costos de los equipos terminales y a la problemática de la red provocada por la presencia de diversos protocolos de comunicación que no son interoperables entre sí.

En el mundo se han desarrollado sistemas de videoconferencia basados en software, como es el caso de "Skype", que permite la utilización de PC como equipos terminales; además, existen sistemas soluciones multipunto como "ooVoo" y "Spontania". No obstante, todos ellos, utilizan protocolos propietarios con costos de licencias importantes y muchos de ellos no son compatibles con equipos, como lo son los encontrados en la red de nuestra casa de estudios. Sin embargo, existen proyectos basados en códigos abiertos como los de la "Fundación Xiph.org" que buscan ofrecer una alternativa. Tanto la ITU (Unión Internacional de Telecomunicaciones), como la IETF (Internet Engineering Task Force) han definido marcos de especificaciones que

describen la señalización, arquitectura y la operación de un sistema de comunicación de voz, datos y video sobre una red de paquetes. H.323 y SIP respectivamente. Son recomendaciones que hoy en día han sido ampliamente desplegadas, aportando flexibilidad, sencillez, rapidez, escalabilidad, factibilidad de desarrollo y lo más importante, proporciona servicios de transporte fiable de datos, voz y video.

La recomendación H.323 cubre los requerimientos técnicos para los servicios de comunicaciones entre Redes Basadas en Paquetes (PBN) que no necesariamente proporcionan calidad de servicio (QoS). Por otra parte, protocolos como SIP, son ampliamente utilizados en dispositivos que integran sistemas de videoconferencia y que proporcionan los mismos servicios de comunicación de la recomendación H.323; además, éste es un protocolo que, gracias a su simplicidad, actualmente, es el utilizado con mayor frecuencia, sobre todo, en temas de señalización. Los productos que cumplen con el estándar H.323 pueden interoperar con la mayoría de otros productos, al igual que los que cumplen con el protocolo SIP; sin embargo, no se ha realizado la interconexión de ambos protocolos (SIP y H.323); al menos, no en un ambiente de software libre o no propietario.

Fundamentado en lo anterior, y en búsqueda de una solución alternativa a la problemática presentada; un sistema de videoconferencia interoperable, como el que es precisado por la red de nuestra casa de estudios, debería comprender como base: Terminales, Gateways y Unidades de Control Multipunto (MCU). Los terminales vienen dados por dispositivos que proporcionan comunicación bidireccional en tiempo real (entre otro terminal, Gateway o MCU) y son los puntos finales de toda transmisión. Dentro de la red de la universidad, éstos están conformados generalmente por PCs multimedia (sonido, voz, datos y video), equipos de telefonía SIP y equipos de videoconferencia Polycom. Los MCUs, se encargan de gestionar una conferencia entre los terminales presentes en la red. No trata directamente el flujo de datos, voz y video, sino que los mezcla y conmuta, soportando así la videoconferencia. Un MCU, puede ser un dispositivo físico dedicado a realizar estas operaciones de gestión, así como también, puede ser un software implementado en

PCs adecuadas para tal fin. Los Gateways (o Pasarela***s***), constituyen unos de los elementos principales de una conferencia. Son necesarios para lograr la comunicación con un terminal que está en otro tipo de red. Éstos proporcionan muchos servicios, el más común es la traducción entre formatos de transmisión y entre procedimientos de comunicación, es decir, realizan adaptación de protocolos, por lo que también se les denomina traductores de protocolos. Además, muchos Gateways efectúan la adaptación de modo que también subsane las diferencias que puedan existir, a nivel de infraestructuras, entre dos redes distintas. Por otra parte, el Gateway también realiza traducciones entre los códecs de video y audio usados en ambas redes y procesa la configuración de la llamada y limpieza de ambos lados de la comunicación, logrando de esta manera que los usuarios puedan comunicarse sin preocuparse con problemas de compatibilidad. En cuanto a la implementación de los mismos, una posibilidad que existe a la hora de implementar un Gateway es diseñar un software que realice la traducción de protocolos. Las máquinas donde se instalarán, deberán contar con el hardware apropiado para que el Gateway pueda realizar el intercambio de datos.

Los componentes anteriores integrados, conforman una arquitectura interoperable que permite el establecimiento de una teleconferencia. Se pretende así, un desarrollo local enmarcado dentro de un proyecto de software libre, el cual, en parte se encuentra ya implementado actualmente (en lo concerniente a los terminales existentes). La implementación del sistema descrito, requerirá de la aportación de dos estudiantes: uno dedicado al desarrollo de la unidad MCU gestora y administradora de la red y el otro, enfocado a procurar la compatibilidad con la plataforma existente mediante la implementación de un Gateway. El presente proyecto tendrá como finalidad este último punto.

CAPÍTULO I

1. FUNDAMENTOS DEL TRABAJO DE GRADO

1.1 Planteamiento del Problema

Una plataforma de Videoconferencia como la existente a la red de datos de la Universidad Central de Venezuela, basada en equipos Polycom y caracterizada por el uso de protocolos propietarios que aún cuando son fundamentados en estándares internacionales, producen una latencia en la interconexión con protocolos y arquitecturas dentro de la misma red, la confinan e impiden que ésta se expanda a la totalidad de la UCV. Inclusive, pueden existir restricciones en cuanto al uso en la red de firewalls internos y externos, direcciones privadas y públicas, y conflictos de compatibilidad de equipos de videoconferencia, en especial con aquellos basados en protocolo SIP; ésto no solo impide la interoperabilidad de la plataforma, sino que además, se desperdicia gran parte del potencial de los elementos que conforman la red.

Aunado a ésto, el uso de sistemas de videoconferencias basados en software libre, facilita un desarrollo local de dominio público, libre y más optimizado, ya que, permite la utilización de equipos de más bajo costo e incluso, la implementación de dispositivos ya existentes, obteniéndose con ésto, un mayor aprovechamiento de la plataforma. Por esta razón, se presenta como una solución alternativa válida dentro del entorno universitario.

Surge entonces, la necesidad de realizar la implementación de una arquitectura de videoconferencia conformada entre otros elementos (como terminales y una MCU), por un Gateway basado en software libre con código abierto que permita interconectar las redes y los protocolos involucrados a fin de garantizar la compatibilidad en nuestra red.

1.2 Justificación

Para el sistema de videoconferencia de la UCV, una arquitectura basada en los lineamientos de la recomendación H.323 representa una solución completa para la interconexión de los protocolos utilizados en el servicio de videoconferencia y por lo tanto para la interoperabilidad de la red de datos entre los equipos que la conforman. Por tal motivo, lograr la compatibilidad con la infraestructura de comunicación existente es de suma importancia en la constitución total de la plataforma requerida.

Como se mencionó anteriormente, el hecho de que dicha plataforma requiera del pago de licencias o del manejo de equipos terminales compatibles con la marca Polycom, además del problema que representa la existencia de un gran número de equipos que también prestan servicios de videoconferencia (aquellos basados en protocolos SIP), pero que a su vez no son compatibles en cuanto a protocolos de comunicación; restringe y hasta en muchos casos imposibilita el uso del sistema en sí. De allí, la necesidad de integrar una plataforma alternativa de código abierto y que, regida bajo los lineamientos de la recomendación H.323 sea una solución basada en estándares internacionales, implementada a escala local y de fácil administración, que permita efectuar sesiones interactivas entre varios participantes, empleando los recursos existentes y dispositivos comunes como lo son las computadoras personales (PC's o laptops). De esta forma, no sólo se logra el funcionamiento del sistema sino que se optimiza la red, aprovechando todo el potencial de cada uno de sus elementos.

Es necesario entonces, concatenar los componentes básicos de una videoconferencia: Terminales, Gateway y la Unidad MCU, para desarrollar así el sistema planteado anteriormente. En este sentido, parte del proyecto está ya establecido; tal es el caso de los terminales y equipos existentes. En cuanto a lo restante, el desarrollo de un software, permite el uso de computadoras personales, las cuales pueden ser encontradas en las instalaciones de la universidad o es un recurso común en la población estudiantil.

Así pues, restaría la implementación de un Gateway (Software) que asegure la compatibilidad dentro de los elementos del sistema, además del desarrollo de una Unidad MCU que gestione y controle la videoconferencia en sí. Por esta razón, se precisa de la participación de otro estudiante que desarrolle la Unidad de Control Multipunto y de esta forma lograr conformar por completo el sistema de videoconferencia con suficiente capacidad que pueda atender los requerimientos de la red.

Por otra parte, la videoconferencia integra tecnologías de audio, video y datos en una misma transmisión, logrando una comunicación unificada y entre varios participantes simultáneamente (solución a video multipunto), lo que representa una prioridad en la sociedad actual.

El desarrollo del Gateway que se propone, permitirá entre otras cosas:

- Asegurar la interoperabilidad de la red de datos de la UCV, a través de la adaptación de protocolos (en especial protocolo SIP) promoviendo compatibilidad con la plataforma Cisco existente.
- Reducción del presupuesto (costos de los equipos terminales, así como de los licenciamientos de protocolos) debido al desarrollo del software libre basado en una codificación abierta.
- Optimización de la red. Se utilizarán y se aprovecharán al máximo cada uno de los elementos ya existentes, sin generar desperdicio de equipos y componentes que no sean compatibles.
- Resolución de problemas de presencia de Firewalls internos y externos, direcciones privadas y públicas.
- Comunicación instantánea en tiempo real entre varios participantes como pueden ser profesores, grupos de estudiantes, autoridades y/o cualquier miembro de la comunidad universitaria.
- Intercambio de diferentes aplicaciones de conferencia para satisfacer las necesidades y requisitos de cualquier usuario dentro de la comunidad

universitaria, incluyendo servicios de movilidad, transmisión de grabaciones y emisiones.

- Innovación del software llevándolo al alcance de cada usuario mediante aplicaciones más interactivas que permitan utilizarlo como medio de capacitación e instrucción para los miembros de la comunidad universitaria a través de clases impartidas por videoconferencia o incluso, para la realización de reuniones profesorales o tutoriales virtuales como lo son los consejos de escuela, de facultad, reuniones administrativas, etc.

1.3 Objetivos de la Investigación

1.3.1 Objetivo General

Desarrollo e Implementación de un Gateway basado en software libre de código abierto adaptado a la red de datos de la UCV

1.3.2 Objetivos Específicos

- Estudiar las arquitecturas y protocolos de los sistemas de videoconferencia para redes basadas en equipos Polycom, y aquellos basados en protocolo SIP.
- Analizar en detalle el funcionamiento de un Gateway así como las arquitecturas y protocolos para llevar a cabo su implementación en una red (recomendaciones del ITU H.323 y protocolos como: SIP, IP, TCP, RTP y UDP).
- Caracterizar los atributos presentes en un Gateway como lo son: capacidad, velocidad de enlace, protocolos involucrados, señalización, códecs utilizados, algoritmos de encriptado que soporta, rango de direccionado, control y adaptación de medios.
- Identificar los elementos de la plataforma que se pueden desarrollar e implementar bajo un software libre.
- Implementación del Gateway basado en un software libre.
- Procurar la compatibilidad con la red existente mediante la adaptación de protocolos.

- Solucionar problemas con el uso en la red de Firewalls internos y externos, direcciones públicas y privadas.
- Realizar las pruebas de validación necesarias y requeridas, esto implica evaluar el desempeño y la funcionalidad del código.

CAPÍTULO II
2. MARCO TEÓRICO

2.1 ANTECEDENTES

El interés en la comunicación utilizando video se ha incrementado con la disponibilidad de la televisión comercial iniciada en 1940. Hoy en día, los humanos han crecido utilizando el televisor como un medio de información y de entretenimiento, nos hemos acostumbrado a tener un acceso visual a los eventos mundiales más relevantes en el momento en que estos ocurren.

El crecimiento y fuerte implantación de las redes IP, tanto en local como en remoto, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir no sólo telefonía sobre IP, sino audio y video; lo que no significará en absoluto la desaparición de las redes telefónicas modo circuito, sino que habrá, al menos temporalmente, una fase de coexistencia entre ambas, y por supuesto la necesaria interconexión mediante pasarelas (gateways). En Enero de 1996, un grupo de fabricantes de soluciones de redes y de ordenadores propuso la creación de un nuevo estándar ITU-T para incorporar videoconferencia en la LAN. Inicialmente, las investigaciones se centraron en las redes de área local, pues éstas son más fáciles de controlar. Sin embargo, con la expansión de Internet, el grupo hubo de contemplar todas las redes IP dentro de una única recomendación, lo cual marcó el inicio de H.323.

El Protocolo H.323 soporta vídeo en tiempo real, audio y datos sobre redes de área local, metropolitana, regional o de área extensa. Soporta así mismo Internet e intranets. En Mayo de 1997, el Grupo 15 del ITU redefinió el protocolo H.323 como

la recomendación para los sistemas multimedia de comunicaciones en aquellas situaciones en las que el medio de transporte sea una red de conmutación de paquetes que no pueda proporcionar una calidad de servicio garantizada.

Para el período comprendido entre los años 1994 y 2000, el IETF MMUSIC Working Group, desarrolló el protocolo denominado SIP, con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuarios, donde intervienen elementos multimedia, como el video, voz, mensajería instantánea, entre otros. Posterior al año 2000, SIP fue aceptado como protocolo de señalización de 3GPP; a partir de este momento, pasó a convertirse, paralelamente con el protocolo H.323, en la base de señalización para la transmisión de voz en redes IP (o en redes sobre VoIP). Debido a la simplicidad, flexibilidad e interoperabilidad del protocolo SIP, actualmente afirman que éste, será el que sustituya al protocolo H.323; sin embargo, H.323 no pierde vigencia y al igual que SIP, no tiene límites en las comunicaciones, logrando mediar en cualquier tipo de sesión comunicativa que va desde voz hasta video; añadiendo características como lo es la conferencia y otras futuras aplicaciones que hoy en día en este tipo de plataformas son prácticamente indispensables.

En la actualidad, existen diversas empresas que ofrecen soluciones propietarias de servicios de videoconferencia sobre IP que incluso desarrollan MCUs y Gateways creados para enlazar y administrar videoconferencia en redes, tales como lo son el trabajo de Kundan Singh [1] en el Departamento de Ciencias Computacionales de la Universidad de Columbia de USA, o el trabajo de M. Jeffries y W. Tucker [2] en la Universidad de Western Cape. Ambos proyectos inicialmente fueron de uso y de dominio libre y público en la web y posteriormente fueron clausurados, para pasar a formar parte de grandes empresas de redes y telecomunicaciones. Existen otros software creados para la realización de llamadas sobre IP o inclusive videoconferencias vía internet; tal es el caso de Skype [3], Spontania [4], Ekiga [5] o más específicamente ooVoo [6]; sin embargo el código y los protocolos de éstos permanecen cerrados y bajo la propiedad de empresas

fabricantes, y aún no se ha logrado comprobar su funcionamiento con otros equipos como lo son los equipos Polycom.

Así mismo, existen en desarrollo proyectos de software libre. Algunos son los propuestos por la Fundación Xiph.org [7], la cual es una organización sin fines de lucro, fundada por Christopher Montgomery y dedicada a la producción de herramientas de dominio público para el manejo de archivos multimedia. Adicionalmente, existen proyectos de implementación de MCU y Gateways basados en las recomendaciones del ITU H.323 como lo son los proyectos OpenH323 [8] y OpenMCU , existentes desde 1992 y desarrollado por una compañía Australiana denominada Equivalence Pty Ltd; la cual tiene como meta principal la implementación de códigos fundamentados en H.323 sobre protocolos VoIP.

Por último, se sabe de desarrollos de proyectos que tienen como expectativa el funcionamiento de MCU con equipos Polycom, Tandberg, y clientes H.323, como es el caso de la implementación desarrollada en la UTN de Uruguay por Santiago Aggio [9] en Mayo del presente año y el proyecto de tesis de Antonio Pinzón [10] en España. En tales desarrollos, si bien fueron enfocados en la compatibilidad de sistemas de videoconferencia con equipos Polycom, sólo se logró comprobar el funcionamiento del audio, pero en cuanto a video surgieron problemas de implementación y no existe información (ni siquiera en internet) respecto a la funcionalidad en sí; además, estos trabajos se enfocaron en un desarrollo puramente sobre protocolo H.323, nunca se ha probado compatibilidad con otros protocolos ni en audio ni en video hasta el momento.

2.2 LA VIDEOCONFERENCIA

2.2.1 Definición de Videoconferencia: Se puede definir la videoconferencia como la combinación tecnológica de audio, video y redes de comunicación que permiten la interacción en tiempo real entre personas remotas. La videoconferencia aumenta las posibilidades de comunicaciones añadiendo interactividad visual además de la escrita y la verbal. Con esta nueva tecnología se simula a un mayor nivel la experiencia del diálogo "cara a cara". La videoconferencia ofrece una solución accesible a las necesidades de comunicación, con sistemas que permiten transmitir y recibir información visual y sonora entre dos puntos que pueden estar en cualquier lugar del planeta.

2.2.2 Tipos de Videoconferencia: Cuando la videoconferencia es utilizada para una comunicación donde existen solamente dos puntos remotos, se denomina videoconferencia punto a punto, pero cuando ésta puede reunir a más de dos participantes, se denomina videoconferencia multipunto o multiconferencia. Esta última, por sus características, consumirá obviamente mayor cantidad de recursos. Entre otras, la videoconferencia se puede dividir en: Desktop (son de escritorio y más pequeños, utilizan computadores con cámaras y sistema de audio), Rollabout (diseñados para alojarse en un gabinete con ruedas), Interconstruidos (son los más grandes y se disponen de salas fijas adecuadas para ellos) y Videoconferencia a través de internet.

2.2.2.1 Videoconferencia a través de internet: posee grandes ventajas y a su vez también grandes inconvenientes. Como ventajas se puede indicar que tanto la instalación como las llamadas son de bajo costos (se cancela únicamente la conexión de datos con la compañía de telecomunicaciones que suministre el servicio). Otra de las ventajas, al ser una videoconferencia basada en internet, muchos de los dispositivos actuales, como laptops, tablets PC, smartphones, entre otros; soportan este tipo de aplicaciones, ya que en su mayoría, estos componentes se manejan a

través de la web. Como inconvenientes, la calidad es muy baja, debido a que no se puede asegurar una continuidad en la transmisión de audio y/o video comprimido o no, esto dado a que son redes basadas en IP, donde la pérdida de paquetes, no permiten garantizar la calidad del servicio.

2.2.3 Componentes Necesarios en una Videoconferencia: Los componentes básicos utilizados en un sistema de videoconferencia suelen dividirse en tres elementos que son: la red de comunicaciones, la sala de videoconferencia y el Códec.

2.2.3.1 Red de Comunicaciones: en los sistemas de videoconferencias se requiere que el medio de comunicación proporcione una conexión digital bidireccional y de alta velocidad entre los puntos a conectar. Desde hace poco tiempo, se han desarrollado tecnologías de red que pueden cumplir con los requerimientos de un sistema de videoconferencia, utilizando cada una de ellas, diferentes medios de transmisión (cobre, fibra, inalámbrico) para el transporte de información. Estas tecnologías consiguen un mayor ancho de banda tanto en entornos de red de área local como en áreas extensas. Entre estas tecnologías están: RDSI (Red Digital de Servicios Integrados), Frame Relay, ATM (Asynchronus Transfer Mode), Fast-Ethernet, Gigabit-Ethernet, etc. La opción más económica y sencilla de aplicar videoconferencia es sobre internet, aunque su calidad a veces puede variar dependiendo del presupuesto con el que se cuente para obtener equipos con tecnología de punta y redes de alta velocidad con gran ancho de banda.

2.2.3.2 Sala de Videoconferencia: se subdivide en cuatro compontes esenciales: el ambiente físico, el sistema de audio, el sistema de video y el sistema de control. En la actualidad, existen dispositivos que conjugan todos los elementos anteriores, como por ejemplo equipos celulares, tablets PC, etc.

2.2.3.3 El Códec: las señales de audio y video que se desean transmitir se encuentran por lo general en forma de señales analógicas. Para poder transmitir dicha información a través de una red digital, ésta debe ser transformada mediante algún

método a una señal digital. Una vez realizado lo anterior, se debe comprimir para su transmisión. El elemento, conformado por hardware y software, encargado de comprimir las imágenes y el sonido al enviarlo y descomprimirlos al ser recibidos, es el códec. Cuanto mayor es la compresión, la velocidad de transmisión del video será mayor, pero a cambio de sacrificar la calidad de imagen, por la que habrá que establecer un equilibrio entre ambas. La UIT se encarga de desarrollar Recomendaciones formales para Códecs de audio y video, para asegurar que las comunicaciones a nivel mundial se cumplan de manera efectiva y eficiente. Más adelante, los códec serán estudiados en detalle.

2.2.5 Tecnologías para la Transmisión de Videoconferencia

2.2.5.1 Tecnologías LAN (Local Area Network)

Una LAN es una red privada en la cual los computadores conectados a ella normalmente situados dentro de un mismo edificio, lugar o entorno. Entre sus características principales están: un campo de acción no mayor a unos cuantos kilómetros, una velocidad total de transmisión de 100Mbps, 1Gbps, 10Gbps y pertenencia a una única organización. En las redes LAN Ethernet/IEEE802.3 con topología en bus y en estrella (10Base5, 10Base2, 10Base-T y 10Base-F), el control de acceso se hace por medio del protocolo de acceso múltiple como lo son OFDMA, QAM, CDMA u otra. Aparecieron luego, las redes LAN de alta velocidad, las conocidas como Fast-Ethernet y Gigabit-Ethernet, conmutadas y no conmutadas y posteriormente las tecnologías LAN inalámbricas (WLAN), especificadas en el estándar 802.11. Estas últimas, están ocupando rápidamente la preferencia de los usuarios, debido a que proporcionan libertad de desplazamiento entre distintas áreas de cobertura, sin las limitaciones de los cables. Por la importancia que en la actualidad tienen este tipo de redes, se realizará un breve resumen de algunos estándares.

2.2.5.1.1 Fast-Ethernet: Sigue la norma 802.3u. Al estar basado en el estándar IEEE 802.3 le permite mantener la compatibilidad con las tecnologías Ethernet

tradicionales. Fast-Ethernet mantiene todos los elementos de dicha norma en cuanto a interfaces, estructura y longitud de tramas, detección de errores, método de acceso al medio, etc; la única modificación, es una reducción del tiempo de bit en un factor de diez, permitiendo un ancho de banda de 100Mbps. El cableado que se emplea es par trenzado, bien sea UTP o STP (categoría 5) y fibra óptica. Estas características permiten una fácil migración de Ethernet a Fast-Ethernet con componentes actuales y redes ya instaladas, además conlleva a un bajo costo de implementación.

2.2.5.1.2 Gigabit-Ethernet: Descrito bajo el estándar 802.3z, con una velocidad de transmisión de alrededor de los 1000Mbps, soporta dos modos diferentes de funcionamiento: modo dúplex total y modo semi-dúplex, adicionalmente, utiliza mecanismos de adaptación de velocidad y control de flujos. Basados en esta tecnología se desarrollaron versiones de mayor velocidad como 10Gigabit-Ethernet, cuya velocidad nominal es de 10Gbps. Este último, posee un amplio potencial en el mercado, es compatible con estándares anteriores y además contiene diferentes tipos de medios para LAN, MAN y WAN. Estas tecnologías son implementadas sobre fibra óptica, además dividen a la capa física en dos subcapas, las cuales definen los transreceptores ópticos y realizan las funciones de codificación, la señalización y la multiplexación por división de longitud de onda (WDM).

2.2.3.1.3 Switched-Ethernet: una red conmutada de Ethernet está controlada por un Switch en vez de un Hub compartido. El Switch permite la interconexión de todos los clientes, servidores y demás dispositivos de red, asignándoles un par dedicado de alta velocidad a la transmisión y recepción. Para Ethernet, la velocidad de transmisión dada por los switches es de 10Mbps Half-Dúplex (10BaseT) y 100Mbps Half-Dúplex para Fast-Ethernet (100Base-T). Otra ventaja de este tipo de redes, es que posibilita la extensión de la red interconectando switches entre sí o conectando switches con hub. La migración hacia las redes Switched-Ethernet proveé un gran optimización en la transmisión. Por ejemplo, un hub de 24 puertos 100Base-T comparte el total de 200Mbps de ancho de banda entre los 24 nodos, en cambio si se sustituye éste por un

switch cada uno de los pares transmisores/receptores poseerá una capacidad de 200Mbps. (para más información véase anexos)

2.2.5.2 Redes LAN Inalámbricas (WLAN)

Las LAN inalámbricas proveen todas las características y beneficios de las redes LAN tradicionales, sin las limitaciones de los cables. Además proveen varias ventajas en comparación con las redes LAN cableadas como: facilidad de instalación, el alcance a lugares inaccesibles y reducción de costos. Su limitante es su bajo ancho de banda.

Equipos Polycom de Videoconferencia

Polycom es una compañía que ofrece soluciones en cuanto a equipos de videoconferencia, voz, telefonía y telepresencia, así como también soporte remoto y en línea a usuarios. Esta empresa ofrece una completa gama de soluciones de telepresencia en alta definición que se adaptan a distintas aplicaciones. Las soluciones de telepresencia y vídeo de Polycom hacen que resulte fácil comunicarse y trabajar visualmente con cualquier persona en organizaciones dispersas geográficamente, mejorando el trabajo en equipo, la productividad y la toma de decisiones de cualquier organización. Por otra parte, las soluciones de voz de Polycom se integran con plataformas de telefonía fijas alámbricas e inalámbricas líderes en el sector para facilitar y ayudar a que las comunicaciones de los negocios y /o cualquier organización funcionen de forma efectiva. Tanto para el sistemas de escritorio como de conferencias o móviles, Polycom posee productos que se adaptan a cualquier requisito de comunicación y ofrece máxima productividad.

Los productos pertenecientes a la marca Polycom que ofrecen servicios y soluciones de videoconferencia, se basan en la recomendación H.323 para la transmisión, implementación y establecimiento de sesiones interactiva multimedia. Dentro de la arquitectura de esta recomendación, los Polycom pertenecen a la clase de Terminales H.323 cumpliendo con todas las especificaciones descritas en dicha

recomendación. Los Productos Polycom por lo tanto, poseen la particularidad de obligar al uso de la familia de protocolos de comunicaciones asociados al protocolo H.323 junto con toda la normativa correspondiente especificada para equipos terminales de este tipo.

En lo concerniente al presente TEG, se utilizaron sólo aquellos equipos de videoconferencias existentes en la plataforma de datos de la UCV que fueran autónomos y que proporcionaran funciones como MCU. Principalmente se utilizó el equipo MGC-100, el cual es el único equipo existente de esta marca que presta servicios de videoconferencia en forma autónoma dentro de la red de la UCV, sin embargo, algunos terminales como los IPELA (equipos de la marca SONY) y algunos modelos de Polycom y Lifesize existentes en la plataforma de videoconferencia de la UCV, también proveen funciones de MCU a pesar de carecer de autonomía en su funcionamiento.

La descripción y el estudio exhaustivo de los protocolos y estándares internacionales como lo es el protocolo H.323 en el cual se fundamentan los equipos Polycom de videoconferencia, es parte fundamental para cumplimiento de los objetivos del presente trabajo, por ello a continuación se realiza una descripción en detalle de cada protocolo en cuestión.

2.3 PROTOCOLOS DE COMUNICACIONES

2.3.1 Protocolo de Internet (IP): Protocolo no orientado a la conexión usado por los computadores para la comunicación de datos a través de una red de paquetes conmutados, estos son enviados en bloques denominados datagramas (paquetes). Este protocolo provee un servicio de datagramas no fiable, también llamado del mejor esfuerzo, es decir no provee ningún mecanismo para determinar si un paquete alcanza o nó su destino (no proporciona calidad de servicio QoS) y únicamente proporciona

seguridad mediante sumas de comprobación de sus cabeceras (checksums) y no de los datos transmitidos.

2.3.1.1 Arquitectura TCP/IP: la Suite TCP/IP consta de cuatro capas: Acceso de Red, Red, Transporte y Aplicación, cada una con sus respectivos protocolos.

2.3.1.1.1 Capa de Aplicación: constituye el nivel más alto de TCP/IP. Corresponde a los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como: correo electrónico con SMTP (Simple Mail Transfer Protocol), transferencias de ficheros con FTP (File Transfer Protocol), conexión remota con TELNET y HTTP (Hypertext Transfer Protocol).

2.3.1.1.2 Capa de Transporte: coincide con el nivel de transporte del modelo OSI. Los protocolos de esta capa, TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

- TCP (Transport Control Protocol): El protocolo TCP se encarga de corregir deficiencias como paquetes perdidos, duplicados o con errores en la información, fragmentando la información y numerando cada uno de los paquetes de manera que el receptor pueda ordenarlos al recibirlos. Si algunos de los paquetes desaparecen, el receptor pide al transmisor que retransmita los paquetes de nuevo. Cuando toda la información recogida está en su orden, se pasan los datos a la capa de aplicaciones.
- UDP (User Datagram Protocol): es un protocolo de transporte no orientado a la conexión, no añade fiabilidad, control de flujo ni recuperación de errores, usa el concepto de puerto para redirigir los datagramas a la aplicación adecuada, usándose por aquellos procesos de usuario que no necesitan los recursos más amplios de TCP, como TFTP, SNMP, etc.

- ICMP (Internet Control Message Protocol): protocolo para mensajes de control de internet, se utiliza para informar de errores y proporciona los recursos necesarios para el tráfico de mensajes.
- IGMP (Internet Group Management Protocol): se le utiliza en computadoras o dispositivos que emplean IP multicast, es decir, datagramas con múltiples destinatarios.

2.3.1.1.3 Capa de Internet: se ocupa de la transmisión de los datagramas en función de la dirección de destino. Consta de tres protocolos principales: IP, ARP, RARP.

- Protocolo IP: implementa dos funciones básicas: el direccionamiento y la fragmentación. Mediante el direccionamiento encuentra un camino para que el datagrama llegue a su destino.
- ARP (Address Resolution Protocol): el módulo ARP realiza la traducción de direcciones y para lo cual posee tablas donde se guardan las direcciones IP y físicas.
- RARP (Reverse Address Resolution Protocol): trabaja de forma inversa al protocolo ARP y es utilizado por las estaciones que no conocen su propia dirección IP para solicitar información de servidor de información RARP.

2.3.1.2 La Telefonía IP o VoIP: VoIp es un estándar de la ITU (Internacional Telecomunications Union), creado en 1996 con el objeto de proporcionar una base desde la cual los desarrolladores puedan evolucionar en conjunto. El concepto de Telefonía IP es sinónimo de VoIP, es decir, posibilita la transmisión de paquetes de voz y datos a través de una red de datos, la comunicación se realiza por medio del Protocolo IP para tráfico de voz full dúplex, permitiendo establecer las llamadas (voz, datos, fax) sobre conexiones IP (Redes Privadas, Redes Corporativas, Intranets, Internet, etc). Los componentes claves de la tecnología telefonía IP, son los equipos que convierten la señal de voz analógica en datagramas IP; estos equipos pueden ser tarjetas o software específicas para PC o incluso, servidores de pasarela de voz. Para

conformar un sistema de VoIP, es necesario contar con: teléfonos IP, adaptadores para PC, Hubs, instalación de Gateways (pasarelas) y paquetes de software, Gatekeepers, Unidades de Control Multipunto (MCU) y servicios de directorios. Gracias a la concatenación de éstos, la telefonía IP, permite el transporte de voz sobre redes IP, produciendo versatilidad y un efectivo ahorro en el gasto que incurren las corporaciones para sus llamadas y conferencias (especialmente larga distancia nacional e internacional); en otras palabras; la implementación de software en dependencias estratégicas, sustituye minutos de larga distancia por minutos de voz sobre IP a un costo mucho menor, posibilitando la obtención de beneficios económicos tangibles a corto plazo.

2.3.1.2.1 Escenarios de la VoIP: se distinguen dos escenarios de aplicación de la voz IP en servicios de telefonía. El primero es cuando la voz IP es transportada a través de redes privadas empresariales y el segundo, cuando la red de transporte usada entre los dos extremos de la conversación es Internet. La telefonía VoIP se manifiesta en tres formas básicas, estas son:

- Llamadas PC a PC: En este caso ambos ordenadores necesitan tener instalada la misma aplicación encargada de gestionar la llamada telefónica, y estar conectados a la red IP, para poder efectuar una llamada IP.
- Llamadas teléfono a teléfono: En este caso tanto el origen como el destino necesitan ponerse en contacto con un gateway. Supongamos que el teléfono A descuelga y solicita efectuar una llamada a B. el gateway de A solicita información al gatekeeper sobre como alcanzar a B, y éste le responde con la dirección IP del gateway que da servicio a B. entonces el gateway de A convierte la señal analógica del teléfono A en un caudal de paquetes IP que encamina hacia el gateway de B, el cuál va regenerando la señal analógica a partir del caudal de paquetes IP que recibe con destino al teléfono B. El gateway de B se encarga de enviar la señal analógica al teléfono B.
- Llamadas PC a teléfono o viceversa: En este caso sólo un extremo necesita ponerse en contacto con un gateway. El PC debe contar con una aplicación

que sea capaz de establecer y mantener una llamada telefónica. supongamos que un ordenador A trata de llamar a un teléfono B. en primer lugar la aplicación telefónica de A ha de solicitar información al gatekeeper, que le proporcionará la dirección IP del gateway que da servicio a B. entonces la aplicación telefónica de A establece una conexión de datos, a través de la red IP, con el gateway de B, el cuál va regenerando la señal analógica a partir del caudal de paquetes IP que recibe con destino al teléfono B. se observa como el gateway de B se encarga de enviar la señal analógica al teléfono B. Por tanto tenemos una comunicación de datos a través de una red IP, entre el ordenador A y el gateway de B, y una comunicación telefónica convencional entre el gateway que da servicio al teléfono B (gateway B), y éste. Es decir, una llamada telefónica convencional, y una comunicación IP.

2.3.2 Protocolo H.323 (ITU-T H.323)

El protocolo H.323 fue diseñado por la Unión Internacional de Telecomunicaciones (ITU, Internacional Comunication Union) y fue publicado por primera vez en 1996. La séptima es la versión más actual publicada en el año 2009. Se creó originalmente para proveer un mecanismo de transporte (audio, video y datos) a través de la red IP (donde no se garantiza QoS) para la videoconferencia en redes de área local (LAN), pero evolucionó rápidamente para convertirse en un método de transporte de aplicaciones multimedia en redes de conmutaciones de paquetes tanto LAN como WAN. El estándar fue diseñado específicamente con los siguientes objetivos:

- Basarse en los estándares existentes, incluyendo H.320, RTP y Q.931.
- Incorporar algunas de las ventajas que las redes de conmutación de paquetes ofrecen para transportar datos.
- Solucionar la problemática que plantea el envío de datos en tiempo real sobre redes de conmutación de paquetes.

Los diseñadores de H.323 sabían que los requisitos de la comunicación difieren de un lugar a otro, entre usuarios, entre compañías y obviamente con el tiempo. Dados estos factores, los diseñadores definieron al H.323 de tal manera que las empresas fabricantes de los equipos puedan agregar su propias especificaciones al protocolo y pueden definir otras estructuras de estándares que permitan a los dispositivos adquirir nuevas características o capacidades. H.323 es una parte del estándar de Audivisual and Multimedia System, the series H.32X, donde se define la transmisión multimedia a través de diferentes tipos de medios. Tales son: H.320 (Comunicaciones multimedia sobre RDSI), H.310 y H.321 (Comunicaciones multimedia sobre ATM), H.324 (Comunicaciones multimedia sobre RTC) y H.323 (Comunicaciones multimedia sobre IP).

2.3.2.1 Protocolos Asociados a H.323: H.323 incluye entre otros, parte de los siguientes protocolos: H.225.0, H.245, RTP/RTCP, RAS, T.120, RSVP, UDP, TCP, RFC 1006, IP todos estos protocolos se ilustran en la siguiente Figura.

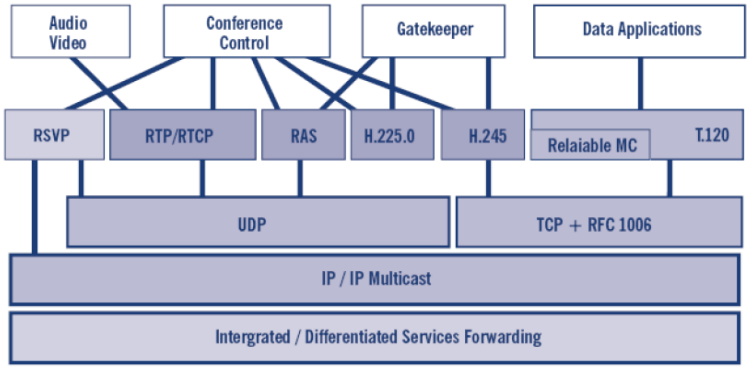


Figura 2.1- Familia de Protocolos H.323

Fuente: Elaboración Propia

- Protocolo H.225.0: define los mensajes de señalización de establecimiento, control y finalización de llamada (conexión y desconexión), además de la señalización RAS (Registration, Admission and Status). RAS lleva a cabo los procedimientos de registro, admisión, cambios de ancho de banda, estado y desconexión, entre terminales y un Gatekeeper H.323. La señalización

H.225.0 está basada en los procedimientos de establecimiento de llamada de ISDN (Integrated Services Digital Networks, estándar Q.931).

- Protocolo H.245: transmite y proporciona la información necesaria para una comunicación multimedia (protocolo de control usado en el establecimiento y control de una llamada), tal como opciones de codificación, control de flujo, gestión de jitter, etc. Digamos, que este protocolo asegura que hay una aplicación y un códec compatible entre los terminales implicados en una comunicación.
- Protocolo RTP: RTP (Real Time Protocol) es similar al protocolo utilizado en SIP, H.323 utiliza RTP como protocolo de transporte. Su característica principal es proveer servicios para la transmisión y entrega de la información en tiempo real como el audio o el video. Es un protocolo situado en la capa de sesión del modelo OSI y aunque fue diseñado para ser independiente de las capas de transporte y red, en redes IP se usa mayoritariamente con UDP. A pesar de ser RTP diseñado inicialmente como un protocolo multicast, éste es también utilizado en aplicaciones del tipo unicast. RTP no proporciona ningún mecanismo que garantiza calidad de servicio ni la entrega a tiempo de los paquetes, confinando estas funciones a capas más bajas del modelo OSI. RTP va de la mano con RTCP.
- Protocolo RTCP: es el protocolo de control de RTP, su función principal es informar de la calidad de servicio proporcionada por RTP. Así, RTCP recoge estadísticas de la conexión y a su vez información como por ejemplo: bytes enviados, paquetes enviados, paquetes perdidos, jitter entre otros. Esta información puede ser usada por una aplicación para incrementar la calidad de servicio (QoS), ya sea limitando el flujo de información o usando un códec de compresión más bajo, etc.
- Q.931: (Digital Subscriber Signalling) Este protocolo se define para señalización de accesos RDSI básico.
- RSVP: (Resource ReSerVation Protocol) protocolo de reserva de recursos en la red para cada flujo de información de usuario.

- T.120: esta recomendación define un conjunto de protocolos para conferencia de datos.
- UDP: Explicado en detalle en la sección "Protocolo UDP" del presente documento.
- TCP: permite establecer la configuración de conexión inicial entre los terminales y gateways/gatekeepers. Explicado en detalle en la sección "Protocolo TCP" del presente documento.
- Protocolo RAS (Registration, Admission and Status): sirve para registrar, controlar y admitir. Administra además el ancho de banda, el estado y desconexión de los participantes. Su función será explicada más adelante con más detalle.

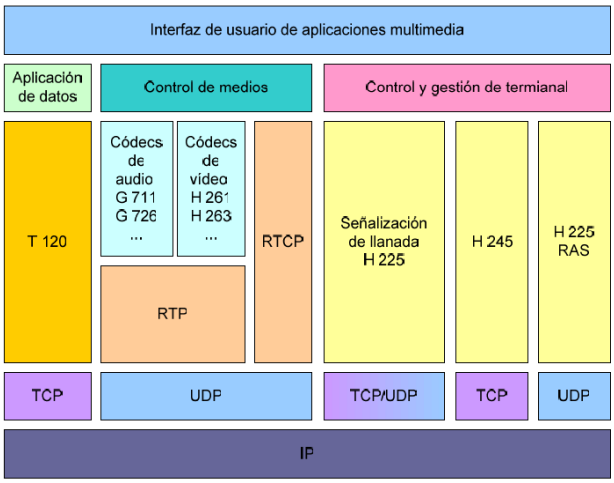


Figura 2.2- Bloques de Protocolos asociados a H.323 utilizando el protocolo IP
Fuente: Elaboración Propia

2.3.2.2 Arquitectura de una Red H.323. Elementos Componentes de una Red H.323: En una red H.323 podemos identificar los siguientes elementos: Gatekeeper, Terminal, Gateway y MCU. Se describirán cada uno a continuación:

2.3.2.2.1 Terminal: Un terminal H.323 es un dispositivo de usuario final que facilita las comunicaciones bidireccionales en tiempo real con otro terminal, pasarela

o MCU. El Terminal puede dar soporte de audio, video y datos. Un Terminal dispone de funciones y capacidades descritas a continuación:

- La unidad de control del sistema, (H.245 y H.225.0), que proporciona control de llamada, el intercambio de capacidad, el envío de mensajes y la señalización para un funcionamiento adecuado del terminal H.323.
- Transmisión de media, que se encarga de recibir los flujos de audio, video, datos, control y mensajes hacia la interfaz de red.
- Códec de Audio, el cual codifica la señal de audio del micrófono para transmisión y decodifica el audio recibido hacia el altavoz. Requiere funciones de codificación y decodificación de G.711μ y G711a y opcionalmente soportar otros códecs de audio como G722, G723.1, G728 y G729.
- Interfaz de red, debe dar servicio de extremo a extremo fiable para el canal de control H.245, los canales de datos y el canal de señalización de llamada; y para los canales de audio, los canales de vídeo y el canal de RAS debe dar un servicio no fiable.
- Códec de video, esta función es opcional y su función es codificar y decodificar video de acuerdo con la recomendación H.261 Quarter Comment Intermediate Format (QCIF).
- Canal de datos. Soporta aplicaciones tales como acceso a bases de datos, transferencias de ficheros, pizarras electrónicas, etc.

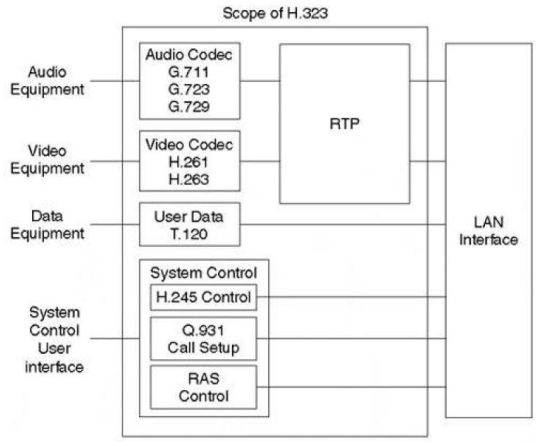


Figura 2.3- Diagrama de Equipo Terminal H.323

Fuente: Prentice Hall PTR, "Voice Gateways and Gatekeepeer" CAP 9 Voice Over IP, Uyless Back August 04, 1999.

2.3.2.2.2 Unidad de Control de Multipunto (MCU): La unidad de control multipunto (MCU) soporta conferencias entre tres o más terminales y/o uno o más gateways en una conferencia multipunto. Una MCU puede negociar capacidades de los terminales en una conferencia y revisar las capacidades durante la conferencia para garantizar un nivel común de comunicaciones.

2.3.2.2.3 Gateway (Pasarela): Un dispositivo importante para la integración de una red H.323 es la pasarela o Gateway. Este dispositivo proporciona comunicaciones entre terminales H.323 y otros terminales de otras redes, realizando funciones de traductor entre ambas redes. En de una conversación donde el equipo terminal no sea H.323, la llamada deberá pasar por un Gateway (pasarela) para que la comunicación sea posible. Generalmente las funciones o el propio Gatekeeper viene integrado en los gateways, conformando un solo dispositivo. En lo cotidiano, este dispositivo proporciona la interfaz entre una red H.323 y la red telefónica básica (RTB) e ISDN (Integrated Services Digital Network).

Los Gateways (o Pasarela***s***) constituyen unos de los elementos principales de una conferencia H.323. Son necesarios para lograr la comunicación con un terminal que está en otra red, éstos proporcionan muchos servicios, el más común es la traducción entre formatos de transmisión y entre procedimientos de comunicación, es decir, realizan adaptación de protocolos, por lo que también se les denomina traductores de protocolos. Su área de trabajo son las capas superiores del modelo OSI, llegando desde el nivel de aplicación al nivel de transporte, e incluso hasta los niveles más inferiores. Aunque muchos Gateways efectúan la adaptación de modo que también subsane las diferencias que puedan existir, a nivel de infraestructuras, entre dos redes distintas. Además el Gateway también realiza traducciones entre los códecs de video y audio usados en ambas redes y procesa la configuración de la llamada y limpieza de ambos lados de la comunicación. Es un tipo particular de terminal y es una entidad llamable (tiene una dirección). Las principales aplicaciones de los Gateways son:

- Establece enlaces con terminales conectados a redes de diversa índole.
- Establecer enlaces con terminales remotos que cumple H.320.
- Establecer enlaces con terminales remotos que cumple H.323.

Un Gateway puede incluir otras funciones opcionales, de las que las más importantes:

- Firewall.
- Servidor proxy.
- Servidores de dominios de nombre (DNS).
- Servidores de web (HTTP/1.1).

En cuanto a la implementación de los mismos, al abarcar los Gateways principalmente los niveles 4, 5 6 y 7 del modelo OSI, una posibilidad que existe a la hora de implementar un Gateway es diseñar un software que realice la traducción de protocolos. Las máquinas donde se instalarán, deberán contar con el hardware apropiado para que el Gateway pueda realizar el intercambio de datos. Normalmente los Gateways software están destinados a trabajar en la World Wide Web y para su desarrollo requieren entre otros:

- Una Librería con acceso a cualquier información independiente de su formato.
- Un Servidor que contenga una bases de datos y aplicaciones específicas.
- Un Estándar para programas que conectan aplicaciones externas con servidores de información.

2.3.2.2.4 Gatekeeper: el Gatekeeper (GK) o controlador de acceso (este dispositivo es opcional), proporciona servicio de control de llamada a los puntos finales. En una red H.323 puede existir más de un gatekeeper que se interaccionan entre sí. En cada una de las zonas puede haber un o más gatekeeper y deben prestar las siguientes funciones:

- Conversión de dirección. El gatekeeper traduce alias a dirección IP o a dirección E.164 necesarios para el establecimiento de las comunicaciones a través de una tabla de traducciones.
- Control de admisiones. El gatekeeper controla el establecimiento de llamadas mediante mensajes Admission Request /Admission Confirm /Admission Reject (ARQ/ACF/ARJ).
- Control de ancho de banda. El gatekeeper controla el número de usuarios simultáneos soportados mediante mensajes de Bandwidth Request /Bandwidth Confirm / Bandwidth Reject (BRQ/BCF/ BRJ).
- Gestión de zona. El gatekeeper coordina acciones entre dispositivos de la misma zona como terminales registrados, Gateways y MCU.
- Control de señalización (opcional). Usa el modelo gatekeeper Router Call Signaling GKRCS.

2.3.2.3 Direccionamiento H.323: H.323 soporta varios tipos de direcciones tales como direcciones alias, URL's, y números de teléfono tradicional (éstos siguen la recomendación ITU E.164).

2.3.2.3.1 Función RAS: (Registration Admission and Status) utiliza los mensajes H.225.0 para la comunicación entre terminal y Gatekeepers y entre gatekeepers. Los terminales usan RAS para registrarse en sus Gatekeeper, realizar

peticiones de permiso, utilizar sus recursos del sistema, obtener direcciones de usuarios remotos, etc. Los Gatekeeper usan RAS para vigilar el estado de los terminales y recoger información de los recursos después de la finalización de una llamada. RAS provee de un mecanismo para los usuarios de autentificación y autentificación de llamada. Se utiliza esta función para registro, control de admisión, control del ancho de banda y estado de la llamada.

2.3.2.3.2 Descubrimiento de Gatekeeper: Los terminales H.323 se registran en un gatekeeper provisto de servicios básicos como resolución de direcciones para llamadas a otros terminales. Hay dos posibilidades para que los terminales encuentren su gatekeeper:

- Multicast discovery: Los terminales envían un GRQ (gatekeeper request) a una dirección multicast conocida y un puerto conocido (en general puerto 1719). Uno o más gatekeeper pueden responder con un mensaje de confirmación GCF (Gatekeeper Confirmation) conteniendo la dirección de transporte del canal de RAS del Gatekeeper o un mensaje de GRJ (Gatekeeper Reject) en caso negativo.
- Configuración: Los terminales conocen la IP del gatekeeper, envían un mensaje GRQ vía unicast y el gatekeeper o confirma o descarta. Adicionalmente, el gatekeeper puede proporcionar gatekeepers alternativos con un mensaje GCF.

2.3.2.3.3 Registro: Después de que el terminal descubra cual es su gatekeeper, el terminal debe registrarse con un mensaje de RRQ (Registration Request) en el gatekeeper. El gatekeeper responderá con una confirmación de registro RCF, (Registration Confirmation) o un rechazo de registro RRJ (Registration Reject). De igual manera si un terminal quiere desregistrarse deberá enviar un mensaje URQ (Unregistration Request).

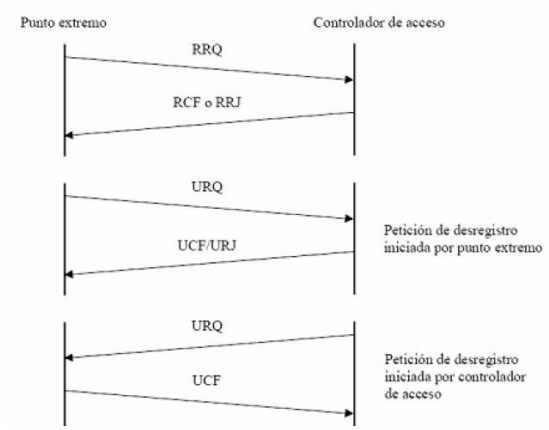


Figura 2.4- Registro/Desregistro de un Usuario H.323

Fuente: Elaboración propia

2.3.2.3.4 Localización de los terminales: Los terminales o gatekeepers pueden determinar información de contacto emitiendo un mensaje de localización LRQ (Location Request) indicando el alias. Este mensaje puede ser enviado al gatekeeper por el canal de RAS o puede ser enviado mediante un GRQ a la dirección multicast. El gatekeeper contestará con LCF, (Location Confirmation) que contendrá información del terminal. Todos los Gatekeepers que reciban el mensaje y no contengan como usuario registrado devolverán un mensaje de rechazo de localización LRJ (Location Reject).

2.3.2.3.5 Admisiones y control de ancho de banda: Estos mensajes se producen entre terminal y gatekeeper para proporcionar funciones de control de admisión y gestión del ancho de banda. Los gatekeepers autorizados acceden a la red H.323 mediante los mensajes de petición de admisión ARQ (Admission Request) especificando el ancho de banda de la llamada. El gatekeeper puede reducir el ancho de banda de llamada en el mensaje de confirmación de admisión ACF (Admission Confirm). El terminal o el gatekeeper pueden intentar modificar el ancho de banda durante la llamada con un mensaje de petición de ancho de banda (BRQ, bandwidth

change request) con una aceptación (BCF, bandwidth confirm) o negación (BRJ, bandwidth reject).

2.3.2.3.6 Función de señalización de llamada: La función de señalización está basada en la recomendación H.225, que especifica el uso y soporte de mensajes de señalización Q.931/Q932. Las llamadas son enviadas sobre TCP por el puerto 1720. Sobre este puerto se inician los mensajes de control de llamada Q.931 entre dos terminales para la conexión, mantenimiento y desconexión de llamadas. Los mensajes más comunes de Q.931/Q.932 usados como mensajes de señalización H.323 son:

- Setup. Es enviado para iniciar una llamada H.323 para establecer una conexión con una entidad H.323. Entre la información que contiene el mensaje se encuentra la dirección IP, puerto y alias del llamante o la dirección IP y puerto del llamado.
- Call Proceeding. Enviado por el Gatekeeper a un terminal advirtiendo del intento de establecer una llamada una vez analizado el número llamado.
- Alerting. Indica el inicio de la fase de generación de tono.
- Connect. Indica el comienzo de la conexión.
- Release Complete. Enviado por el terminal para iniciar la desconexión.
- Facility. Es un mensaje de la norma Q.932 usado como petición o reconocimiento de un servicio suplementario.

2.3.2.3.7 Función de Control H.245: El canal de control H.245 es un conjunto de mensajes ASN.1 usados para el establecimiento y control de una llamada. Unas de las características que se intercambian más relevantes son:

- MasterSlaveDetermination (MSD). Este mensaje es usado para prevenir conflictos entre dos terminales que quieren iniciar la comunicación. Decide quién actuará de Master (Maestro) y quién de Slave (Esclavo).
- TerminalCapabilitySet (TCS). Mensaje de intercambio de capacidades soportadas por los terminales que intervienen en una llamada.

- OpenLogicalChannel (OLC). Mensaje para abrir el canal lógico de información y de esta manera permitir la recepción y codificación de los datos. Contiene la información del tipo de datos que serán transportados.
- CloseLogicalChannel (CLC). Mensaje para cerrar el canal lógico de información.

2.3.2.3.8 Modelos de Señalización: existen tres métodos para transmitir la señalización de las llamadas en una red H.323:

- Directamente a través del terminal: Los mensajes de señalización son enviados directamente entre los dos terminales.

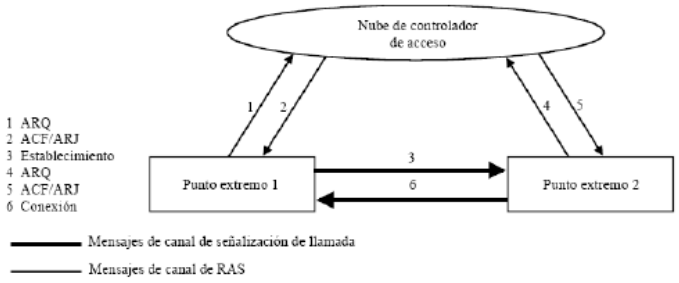


Figura 2.5- Señalización H.323. Método directo.

Fuente: Elaboración Propia

- Señalización encaminada por el gatekeeper (menos los mensajes de control de conferencia: Los mensajes H.225.0 de RAS y los H.225.0 de señalización de llamada se encaminan a través del Gatekeeper, mientras que los mensajes de control de conferencia H.245 son encaminados directamente entre los dos terminales. Este método permite al gatekeeper reencaminar el canal de control H.245 a una MCU. cuando una conferencia multipunto ad hoc pasa de conferencia punto a punto a conferencia multipunto. El gatekeeper realiza esta elección. Cuando se utiliza la señalización de llamada de punto extremo directa, el canal de control H.245 sólo puede ser conectado directamente entre los puntos extremos.

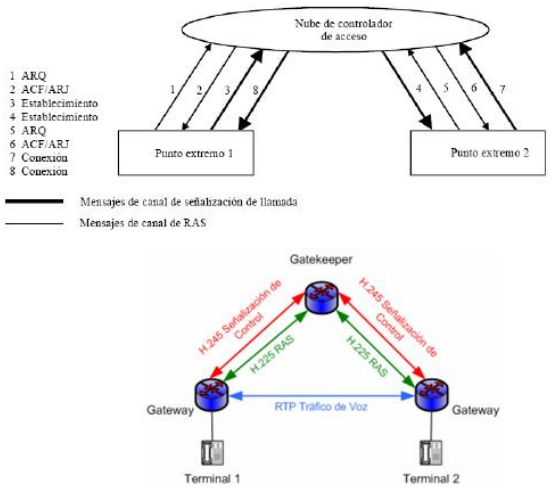


Figura 2.6- Señalización H.323. Modo Enrutado por el Gatekeeper menos los mensajes de control de conferencia. Fuente: Elaboración Propia

- Señalización encaminada por el gatekeeper: Los mensajes de señalización entre los terminales son enrutados a través del gatekeeper.

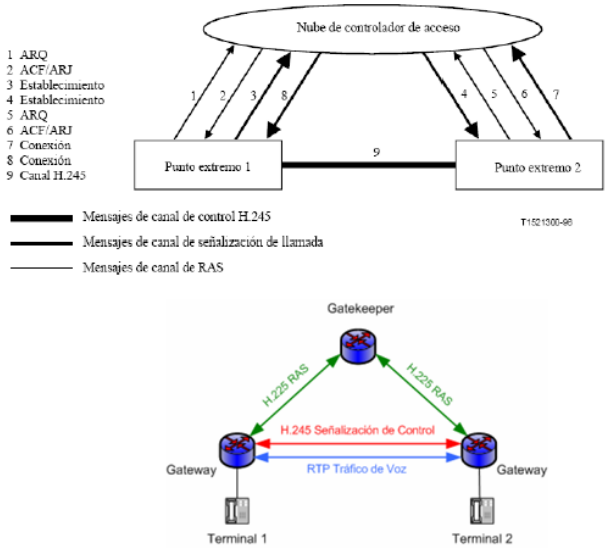


Figura 2.7- Señalización H.323. Modo Gatekeeper Enrutado Fuente: Elaboración Propia

2.3.2.3.9 Fases de una Llamada H.323: una llamada H.323 consta de diferentes fases entre ellas:

- Establecimiento de la comunicación
- Comunicación inicial e intercambio de capacidades
- Establecimiento de la comunicaciones
- Servicios de llamadas
- Terminación de la llamada.

Una llamada H.323 se caracteriza por las siguientes fases:

- Establecimiento de la comunicación: En principio, si existe la presencia de un Gatekeeper (caso contrario este paso se omite), el primer paso de la llamada es registrarse y solicitar una admisión al Gatekeeper, para lo cual se utilizan los mensajes de RAS. Posteriormente, el usuario que desea establecer la comunicación envía un mensaje de SETUP, posteriormente este terminal debe ser registrado y admitido por el Gatekeeper a través de mensajes RAS, una vez admitido (si no existe Gatekeeper se omite este paso), el remitente contesta con un mensaje de CallProcceding y Alerting indicando el inicio de establecimiento de la comunicación. Este mensaje Alerting es similar al Ring Back Tone de las redes telefónicas actuales. Cuando el usuario descuelga el teléfono, se envía un mensaje de Connect.
- Negociación de los parámetros: En esta fase se abre una negociación mediante el protocolo H.245 (control de canal), el intercambio de los mensajes (petición y respuesta) entre los dos terminales establecen quién será master (maestro) y quién slave (esclavo), así como también las capacidades de los participantes y códecs de audio y video soportados (Mensajes TCS, Terminal Capability Set). Como punto final de esta negociación se abre el canal de comunicación (direcciones IP, puerto), mediante los mensajes OLC (Open Logical Channel).

- Comunicación: los terminales inician la comunicación mediante el protocolo RTP/RTCP. En esta fase comienza la transmisión de la información (audio y video).
- Finalización de una llamada: Por último, cualquiera de los participantes activos en la comunicación puede iniciar el proceso de finalización de llamada mediante mensajes CloseLogicalChannel (CLC) y EndSessionComand (ESC) para indicar la finalización de ésta. Una vez realizado esto, ambos terminales deben informarle al Gatekeeper sobre el fin de la comunicación. Para ello se hace uso nuevamente de los mensajes RAS DRQ (Disengage Request) y DCF (Disengage Confirm).

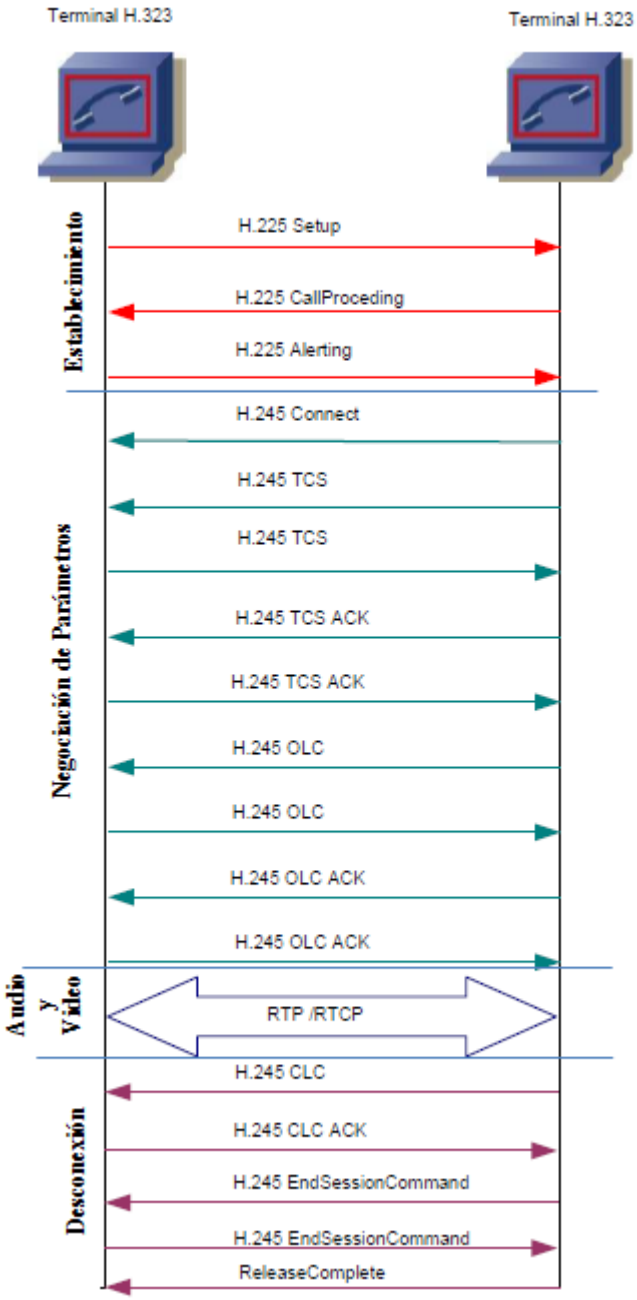


Figura 2.8. Fases de una llamada H.323.

Fuente: Elaboración Propia

2.3.3 Protocolo SIP (Session Initiation Protocol)

El protocolo SIP fue desarrollado por el grupo MMUSIC (Multimedia Session Control) del IETF (Internet Engineering Task Force), definiendo una arquitectura de señalización y control para VoIP. Inicialmente fue publicado en febrero del 1996 en la RFC 2543, ahora obsoleta con la publicación de la nueva versión RFC 3261 que se publicó en junio del 2002. El propósito de SIP es la comunicación entre dispositivos multimedia. SIP hace posible esta comunicación gracias a dos protocolos que son RTP/RTCP y SDP. El protocolo RTP se usa para transportar los datos de voz en tiempo real (igual que para el protocolo H.323), mientras que el protocolo SDP se usa para la negociación de las capacidades de los participantes, tipo de codificación, etc. Este protocolo fue diseñado de acuerdo al modelo de Internet. Es un protocolo de señalización de extremo a extremo en el que toda la lógica es almacenada en los dispositivos finales (excepto por el enrutamiento de los mensajes SIP). El estado de la conexión es también almacenado en los dispositivos finales. El precio a pagar por esta capacidad de distribución y su gran escalabilidad es una sobrecarga en la cabecera de los mensajes producto de tener que mandar toda la información entre los dispositivos finales. SIP es un protocolo de señalización a nivel de aplicación para establecimiento y gestión de sesiones con múltiples participantes. Se basa en mensajes de petición y respuesta y reutiliza muchos conceptos de estándares anteriores como HTTP (HyperText Transfer Protocol) y SMTP (Simple Mail Transfer Protocol).

2.3.3.1 Protocolos Asociados a SIP: El propósito de SIP es la comunicación entre dispositivos multimedia. Para llevar a cabo este cometido, SIP se sirve de otros protocolos para realizar tareas como la señalización y transporte. En siguiente figura, se ilustran los protocolos involucrados en SIP

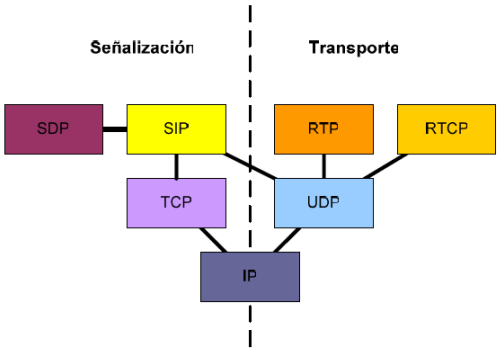


Figura 2.9- Pila de Protocolos de SIP

Fuente: Elaboración propia

- RTP (Real Time Protocol): explicado anteriormente en la sección "Protocolos Asociados a H.323" del presente documento
- RTCP (Real Time Control Protocol): explicado también anteriormente en la parte "Protocolos Asociados a H.323" del presente trabajo
- SDP (Session Description Protocol): El protocolo SDP (Session Description Protocol) RFC 2327, se utiliza para describir sesiones multicast en tiempo real, siendo útil para invitaciones, anuncios, y cualquier otra forma de inicio de sesiones. La propuesta original de SDP fue diseñada para anunciar información necesaria para los participantes y para aplicaciones de multicast MBONE (Multicast Backbone). Actualmente, su uso está extendido para el anuncio y la negociación de las capacidades de una sesión multimedia en Internet. Puesto que SDP es un protocolo de descripción, los mensajes SDP se pueden transportar mediante distintos protocolos con SIP, SAP, RTSP, correo electrónico con aplicaciones MIME o protocolos como HTTP. Como el SIP, el SDP utiliza la codificación del texto. Un mensaje del SDP se compone de una serie de líneas, denominados campos, dónde los nombres son abreviados por una sola letra, y está en una orden requerida para simplificar el análisis. El SDP no fue diseñado para ser fácilmente extensible. La única manera de ampliar o de agregar nuevas capacidades al SDP es definir un nuevo atributo. Sin embargo, los atributos desconocidos pueden ser ignorados. En la tabla siguiente se pueden observar todos los campos.

2.3.3.2 Arquitectura SIP. Componentes de una Red SIP: SIP soporta funcionalidades para el establecimiento y finalización de las sesiones multimedia: localización, disponibilidad, utilización de recursos, y características de negociación. Para implementar estas funcionalidades, en una red SIP, existen dos elementos fundamentales: los agentes de usuario (UA) y los servidores.

2.3.3.2.1 User Agent (UA): Consisten en dos partes distintas, el User Agent Client (UAC) y el User Agent Server (UAS). Un UAC es una entidad lógica que genera peticiones SIP y recibe respuestas a esas peticiones. Un UAS es una entidad lógica que genera respuestas a las peticiones SIP. Ambos se encuentran en todos los agentes de usuario, así permiten la comunicación entre diferentes agentes de usuario mediante comunicaciones de tipo cliente-servidor.

2.3.3.2.2 Servidores SIP: Los servidores SIP pueden ser de tres tipos (la división de estos servidores es conceptual, cualquiera de ellos puede estar físicamente una única máquina):

- Proxy Server: retransmiten solicitudes y deciden a qué otro servidor deben remitir, alterando los campos de la solicitud en caso necesario. Es una entidad intermedia que actúa como cliente y servidor con el propósito de establecer llamadas entre los usuarios. Este servidor tienen una funcionalidad semejante a la de un Proxy HTTP que tiene una tarea de encaminar las peticiones que recibe de otras entidades más próximas al destinatario. Existen dos tipos de Proxy Servers: Statefull Proxy y Stateless Proxy.
- Statefull Proxy: mantienen el estado de las transacciones durante el procesamiento de las peticiones. Permite división de una petición en varias (forking), con la finalidad de la localización en paralelo de la llamada y 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 reenvían mensajes.

- Registrar Server: es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla.
- Redirect Server: es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor.

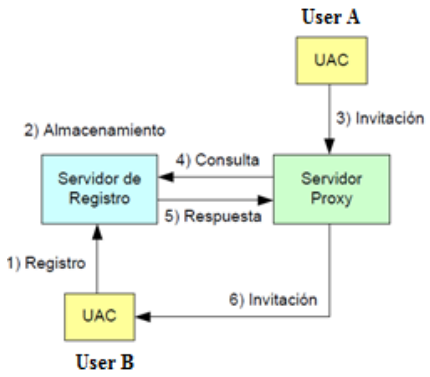


Figura 2.10- Tipos de Servidores SIP

Fuente: Elaboración Propia

2.3.3.3 Mensajes SIP: SIP es un protocolo textual que usa una semántica semejante a la del protocolo HTTP. Los UAC realizan las peticiones y los UAS retornan respuestas a las peticiones de los clientes. SIP define la comunicación a través de dos tipos de mensajes. Las solicitudes (métodos) y las respuestas (códigos de estado) emplean el formato de mensaje genérico establecido en el RFC 2822[12] , que consiste en una línea inicial seguida de un o más campos de cabecera (headers), una línea vacía que indica el final de las cabeceras, y por último, el cuerpo del mensaje que es opcional.

2.3.3.3.1 Métodos SIP: Las peticiones SIP son caracterizadas por la línea inicial del mensaje, llamada Request-Line, que contiene el nombre del método, el identificador del destinatario de la petición (Request-URI) y la versión del protocolo

SIP. Existen seis métodos básicos SIP (definidos en RFC 2543[13]) que describen las peticiones de los clientes:

- INVITE: Permite invitar un usuario o servicio para participar en una sesión para modificar parámetros en una sesión ya existente.
- ACK: Confirma el establecimiento de una sesión.
- OPTION: Solicita información sobre las capacidades de un servidor.
- BYE: Indica la terminación de una sesión.
- CANCEL: Cancela una petición pendiente.
- REGISTER: Registrar al User Agent.

Sin embargo, existen otros métodos adicionales que pueden ser utilizados, publicados en otros RFCs como los métodos INFO, SUBSCRIBER, etc.

2.3.3.3.2 Respuestas (Códigos de estado) SIP: Después de la recepción e interpretación del mensaje de solicitud SIP, el receptor del mismo responde con un mensaje. Este mensaje, es similar al anterior, difiriendo en la línea inicial, llamada Status-Line, que contiene la versión de SIP, el código de la respuesta (Status–Code) y una pequeña descripción (Reason-Phrase). El código de la respuesta está compuesto por tres dígitos que permiten clasificar los diferentes tipos existentes (véase Tabla 2.2). El primer dígito define la clase de la respuesta.

Tabla 2.1 Tabla de códigos de respuestas SIP

Fuente: Elaboración Propia

Código	Clases
1xx	Mensajes provisionales.
2xx	Respuestas de éxito.
3xx	Respuestas de redirección.
4xx	Respuestas de falla de método.
5xx	Respuestas de fallas de servidor.
6xx	Respuestas de fallas globales.

2.3.3.3.3 Cabeceras SIP: Las cabeceras se utilizan para transportar información necesaria a las entidades SIP. A continuación, se detallan los campos:

- Vía: Indica el transporte usado para el envío e identifica la ruta del request, por ello cada proxy añade una línea a este campo.
- From: Indica la dirección del origen de la petición.
- To: Indica la dirección del destinatario de la petición.
- Call-Id: Identificador único para cada llamada y contiene la dirección del host. Debe ser igual para todos los mensajes dentro de un diálogo.
- Cseq: Inicia el diálogo con un número aleatorio e identifica de forma secuencial cada petición.
- Contact: Contiene una (o más) dirección que pueden ser usada para contactar con el usuario.

2.3.3.3.4 Direccionamiento SIP: Una de las funciones de los servidores SIP es la localización de los usuarios y resolución de nombres. Normalmente, el agente de usuario no conoce la dirección IP del destinatario de la llamada, sino su URL (e-mail). Las entidades SIP identifican a un usuario con las SIP URI (Uniform Resource Identifiers) definido en el RFC 2396[14]. Una SIP URI tiene un formato similar al del e-mail, consta de un usuario y un dominio delimitado por una @, como se muestra en los siguientes casos:

- usuario@dominio, donde dominio es un nombre de dominio completo.
- usuario@equipo, donde equipo es el nombre de la máquina.
- usuario@dirección_ip, donde dirección_ip es la dirección IP del dispositivo.
- número_teléfono@gateway, donde el gateway permite acceder al número de teléfono a través de la red telefónica pública.

La solución de identificación de SIP, también puede ser basada en el DNS descrito en el RFC 3263[15], donde se describen los procedimientos DNS utilizados por los clientes para traducir una SIP URI en una dirección IP, puerta y protocolo de

transporte utilizado, o por los servidores para retornar una respuesta al cliente en caso de que la petición falle.

2.3.3.3.5 Llamadas SIP: a continuación se analizará detalladamente una llamada. En una llamada SIP hay varias transacciones SIP. Una transacción SIP se realiza mediante un intercambio de mensajes entre un cliente y un servidor. Consta de varias peticiones y respuestas y para agruparlas en la misma transacción.

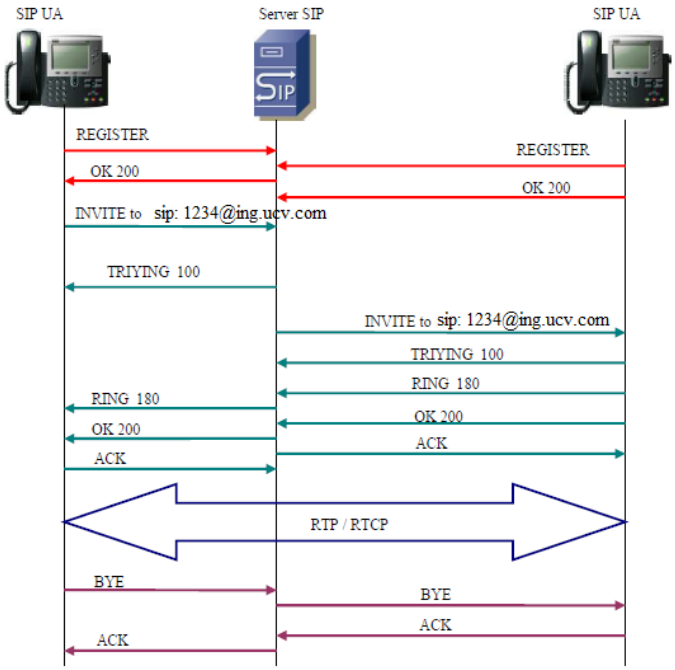


Figura 2.11- Ejemplo de llamada SIP

Fuente: Elaboración propia

En la figura anterior, se muestran cuatro transacciones principales:

- Las dos primeras transacciones corresponden al registro de los usuarios. Los usuarios deben registrarse para poder ser encontrados por otros usuarios. En este caso, los terminales envían una petición REGISTER, donde los campos from y to corresponden al usuario registrado. El servidor Proxy, que actúa

como Register, consulta si el usuario puede ser autenticado y envía un mensaje de OK en caso positivo.

- La siguiente transacción corresponde a un establecimiento de sesión Esta sesión consiste en una petición INVITE del usuario a proxy. Inmediatamente, el proxy envía un TRYING 100 para parar las retransmisiones y reenvía la petición al usuario B. El usuario B envía un Ringing 180 cuando el teléfono empieza a sonar y también es reenviado por el proxy hacia el usuario A. Por último, el OK 200 corresponde a aceptar la llamada (el usuario B descuelga).
- En este momento la llamada está establecida, pasa a funcionar el protocolo de transporte RTP con los parámetros (puertos, direcciones, códecs, etc.) establecidos en la negociación mediante el protocolo SDP.
- La última transacción corresponde a una finalización de sesión. Esta finalización se lleva a cabo con una única petición BYE enviada al Terminal, y posteriormente reenviada al usuario B. Este usuario contesta con un OK 200 para confirmar que se ha recibido el mensaje final correctamente.

2.3.4 Relación y Diferencias entre SIP y H.323

Tanto SIP como H.323 son estándares diseñados para proporcionar el ruteo y la señalización de llamadas, así como intercambio de capacidades, control de medios y servicios adicionales. La fortaleza de H.323 reside en su interoperabilidad con las Redes Telefónicas Conmutadas por Paquetes (PSTN) y la disponibilidad de tener aparatos de videoconferencia más económicos y de excelente calidad desde el escritorio hasta un salón para grupos. SIP es un protocolo desarrollado específicamente para Internet y promete una alta escalabilidad y flexibilidad. H.323 se perfiló como la tecnología predominante de videoconferencia durante los últimos años, sin embargo, con el paso del tiempo este protocolo pierde cada vez más fuerza, siendo sustituido por SIP, protocolo que está creciendo conforme van apareciendo software, unidades multipunto, pasarelas (gateways) y servidores SIP que ya no están en fase de pruebas sino de completo servicio, los cuales además, en su mayoría no son propietarios.

La principal diferencia es la velocidad: SIP hace en una sola transacción lo que H.323 hace en varios intercambios de mensajes. Adicionalmente, SIP usa UDP mientras que H.323 debe usar necesariamente TCP para la señalización (H.225 y H.245), lo que origina que una llamada SIP sea atendida más rápido. Otra diferencia importante es que H.323 define canales lógicos antes de enviar los datos, mientras que una unidad SIP simplemente publicita los códecs que soporta, más no define canales, lo que puede generar saturación de tráfico en casos de muchos usuarios, pues no se separa la tasa de bits necesaria para la comunicación.

H.323 y SIP son dos formas diferentes de resolver un mismo problema. Los dos emplean el protocolo RTP y RTCP para el transporte de medios (audio y vídeo) pero en lo que se diferencian es en cómo desarrollan la señalización y el control de llamadas. Para la interoperabilidad entre entornos SIP y H.323 es factible emplear un gateway que desarrolle el mapping de señalización entre ambas soluciones.

2.4 CODIFICADORES-DECODIFICADORES: CÓDECS

La comunicación de voz es analógica, mientras que la información que circula por una red de datos es digital. Por tanto, es necesaria una transformación analógica-digital de la voz para que esta pueda ser transportada a través de una red de datos. El proceso de convertir ondas analógicas a información digital se realiza mediante un codificador-decodificador, llamado códec. Existen muchas maneras de transformar una señal de voz analógica en digital, todas ellas gobernadas por varios estándares. Además de la ejecución de la conversión de analógico a digital, el códec comprime la secuencia de datos. La compresión de la forma de onda representada puede permitir un ahorro en el ancho de banda. Esto es especialmente interesante en los enlaces de poca capacidad y permite tener un mayor número de conexiones de VoIP simultáneamente. El proceso de la conversión es complejo. Es suficiente decir que la mayoría de las conversiones se basan en la modulación codificada mediante pulsos

(PCM) o variaciones. En la sección de "Anexos" del presente trabajo, se encuentra especificado dicho proceso.

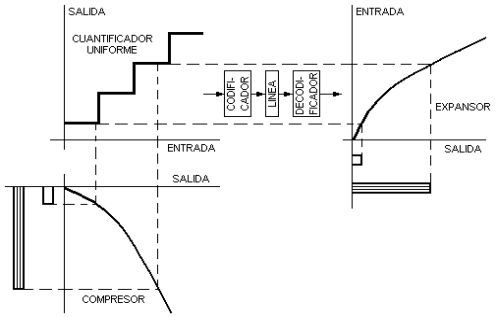


Figura 2.12-Codificación-Decodificación

Fuente: www.voipforo.com

La palabra Códec proviene de Codificador-Decodificador; son aquellos que describen una implementación basada en software o hardware (o su combinación) para la transmisión correcta de un flujo de datos, es decir, un códec es cualquier tecnología para la compresión y descompresión de datos.

2.4.1 Códecs de Audio

II.4.1.1 ITU-G.711: G.711 posee una tasa de transmisión alta de 64 kbps. Desarrollado por la UIT, es el códec nativo de redes digitales modernas de teléfonos. Formalmente estandarizado en 1988, este códec, también llamado PCM, tiene un tasa de muestreo de 8000 muestras por segundo, lo que permite un ancho de banda total para la voz de 4000 Hz. Cada muestra se codifica en 8 bits, luego la tasa de transmisión total es de 64 kbps. Existen dos versiones de este códec: Ley-A (A-law) y Ley-μ (μ-law). La segunda se usa en Estados Unidos y Japón mientras que la primera se usa en el resto del mundo, incluida Latinoamérica. La diferencia entre ellas es la forma como la señal es muestreada. Las ecuaciones de muestreo y sus respectivas gráficas se muestran en la figura a continuación.

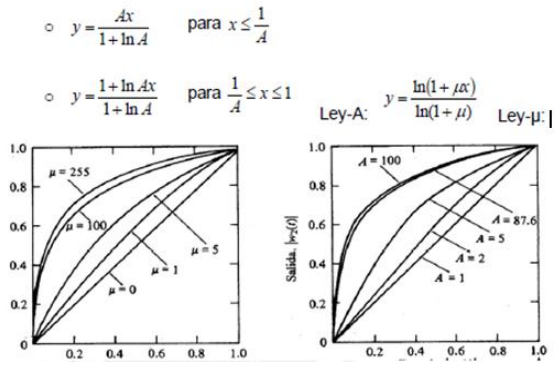


Figura 2.13- Comparación Ley-μ vs. Ley-A

Fuente: "Telecomunicaciones Digitales". Huapaya, J. 2005

Los valores de μ y de A están estandarizados por la UIT (μ=255 para el caso de la ley-μ y de A=100 para el caso de la ley-A). La forma logarítmica refuerza las muestras más pequeñas de la entrada con el fin de protegerlas del ruido. El uso de G.711 para VoIP ofrece la mejor calidad (no realiza compresión en la codificación), por lo que suena igual que un teléfono analógico o RDSI. Esto se comprueba con la medida del MOS. El MOS (Mean Opinion Score) es una medida cualitativa de la calidad de la voz. Un MOS de 5 indica una comunicación con calidad excelente mientras que un MOS de 0 indica una calidad pésima. G.711 tiene el MOS más alto de todos los códecs en condiciones ideales (sin pérdida de paquetes), con un MOS de 4.1. También presenta el menor retardo debido a que no hay un uso extensivo del CPU (no hay compresión de datos). El inconveniente principal es que necesita mayor tasa de bits que otros códecs, aproximadamente 80 Kbps incluyendo toda la cabecera TCP/IP. Sin embargo, con un acceso de alta velocidad, ésto no debería ser mayor problema. Este códec es soportado por la mayoría de compañías de VoIP, tales como proveedores de servicio y fabricantes de equipos, y es uno de los utilizados en el presente trabajo.

2.4.1.2 ITU-G.729: Este códec comprime la señal en períodos de 10 milisegundos. No permite transportar tonos como DTMF o Fáx. G.729 se usa principalmente en aplicaciones VoIP por su poca tasa de bits (8 Kbps). Existen

extensiones de la norma que permiten tasas de 6.4 y 11.8 Kbps para peor y mejor calidad de voz, respectivamente. Idealmente presenta un MOS de 3.8. El uso de aplicaciones usando este códec requiere una licencia. Sin embargo existen implementaciones gratuitas para uso no comercial.

2.4.1.3 GSM (RPE-LTP): Este códec se llama oficialmente RPE-LTP (Regular Pulse Excitation– Long Term Prediction) pero se conoce mundialmente como GSM debido a que es el códec usado en el estándar GSM de comunicaciones móviles. Tiene una tasa de bits de 13 Kbps con un MOS ideal de 3.6 y realiza la codificación generando coeficientes representativos de un intervalo de tiempo determinado. Este intervalo normalmente es de 20 milisegundos de voz.

2.4.1.4 Speex: es un códec libre para voz, está sujeto a la licencia BSD y es usado con el contenedor Ogg de la Fundación Xiph.org. El proyecto Speex se inició debido a la necesidad de un códec de voz que fuera de código libre y libre de patentes de software. También a diferencia de muchos otros códecs de voz, Speex no está diseñado para teléfonos celulares, pero si para Voz sobre IP (VoIP) y compresión basada en archivos. Las metas en el diseño eran permitir buena calidad en la voz y bajo bit-rate. Buena calidad también significaba tener soporte para wideband (frecuencia de muestreo de 16 kHz) además de narrowband (calidad de teléfono, frecuencia de muestreo de 8 kHz). El diseñador de Speex (Jean-Marc Valin) estableció su proyecto como un complemento del proyecto Ogg Vorbis, ya que Vorbis no fue diseñado como códec de voz, sino como códec de audio de propósito general. Speex se basa en CELP y está diseñado para comprimir voz a bit rates desde 2 a 44 kbps y posee características como: Software libre/código libre, libre de patentes y regalías, Integración de narrowband y wideband en el mismo bitstream, Amplio rango de bitrate disponible (desde 2 kbps a 44 kbps), cambio dinámico de bitrate y Variable BitRate (VBR), detección de actividad de voz (VAD en sus siglas en inglés, integrado con VBR), Complejidad variable, Modo Ultra-wideband de 32 kHz, opción de codificación de intensidad estéreo.

Tabla 2.2- Comparación entre Códecs de Audio

Fuente: Elaboración Propia

Nombre	Org.	Descripción	Bit Rate (kbps)	Tamaño de Cuadro (ms)	Obs.	MOS (Ideal)
G.711	UIT	PCM	64	Muestreada	Ley A y Ley u	4.1
G.729	UIT	CS-ACELP	8	10	Bajo retardo (15ms)	3.8
GSM	ETSI	RPE-LTP	13	20	Usado por GSM	3.5-3.7
Speex	Xiph.org	CELP	2 /44	20/30	VBR	4.1

Tabla 2.3- Consumo de Ancho de Banda de los Códecs más utilizados.

Fuente: http://www.informatica-hoy.com

Códec	Ancho de banda	Intervalo de paquete	Bits de voz por paquete	Procesado
G.711	64 Kbps	20ms	1280 bits	Bajo
G.726	32 Kbps	20ms	640 bits	Medio
G.728	16 Kbps	10ms	160 bits	Alto
G.729A	8 Kbps	10ms	160 bits	Alto
GSM	13 Kbps	20ms	160 bits	Bajo

En la sección de "Anexos" del presente Trabajo de Grado, se encuentra una tabla con las especificaciones de los códecs de audio más utilizados en el mercado actual.

2.4.2 Códecs de Video: Un códec de video es un tipo de códec que permite comprimir y descomprimir video digital. Su finalidad es obtener un almacenamiento sustancialmente menor de la información de vídeo. Esta se comprime en el momento de guardar la información hacia un archivo y se descomprime, en tiempo real, durante la visualización. Normalmente los algoritmos de compresión empleados conllevan

una pérdida de información, por tanto, el problema que se pretende acometer con los códec es que la información de video sea fidedigna en comparación a lo que un ordenador normal es capaz de manejar. Es así como un par de segundos de video en una resolución apenas aceptable puede ocupar un lugar respetable en un medio de almacenamiento típico (CD, DVD, etc.) y su manejo (copia, edición, visualización) puede llevar fácilmente a sobrepasar las posibilidades de dicho ordenador o llevarlo a su límite. Se pretende, por otro lado, que el proceso sea transparente para el usuario, es decir, que no intervenga o lo haga lo menos posible. Entre los códecs de video más utilizados se encuentran:

2.4.2.1 ITU-T H.261: El estándar H.261 es parte del grupo de estándares H.320 para comunicaciones audiovisuales. Fue diseñado para una tasa de datos múltiplo de 64 Kbit/s. Lo cual coincide con las tasas de datos ofrecidas por los servicios ISDN. Se pueden usar entre 1 y 30 canales ISDN (64 Kbit/s a 1920 Kbit/s). Aplicaciones que motivaron el diseño de este tipo de estándar son: videoconferencia, vigilancia y monitoreo, telemedicina, y otros servicios audiovisuales. H.261 soporta dos resoluciones CIF (Common Interchange Format, 352x288 pixels) y QCIF (Quarter Common Interchange Format, 176x144 pixels).

2.4.2.2 ITU-T H.263: Esta Recomendación especifica una representación codificada, que se puede usar para comprimir el componente de imagen en movimiento de los servicios audiovisuales a velocidades binarias bajas. La configuración básica del algoritmo de codificación de fuente vídeo se basa en la Recomendación H.261, y es un híbrido de la predicción entre imágenes que utiliza la redundancia temporal y la codificación con transformada de la señal restante para reducir la redundancia espacial. El codificador de fuente puede funcionar con cinco formatos de fuente de vídeo normalizados: sub-cuarto de CIF, cuarto de CIF, CIF, 4 veces CIF y 16 veces CIF, y puede funcionar también utilizando una amplia gama de formatos de vídeo personalizados. El decodificador tiene capacidad de compensación de movimiento, lo que permite la incorporación opcional de esta técnica en el codificador. En la compensación de movimiento se utiliza la precisión de mitad de

píxel, mientras que en la Recomendación H.261 se utiliza la precisión de píxel entero y un filtro de bucle. Se emplea la codificación de longitud variable para la transmisión de los símbolos. Además del algoritmo de codificación de fuente de vídeo básico, se incluyen dieciséis opciones de codificación negociables para mejorar el funcionamiento de la compresión y el soporte de capacidades adicionales.

2.4.2.3 ITU-T H.264: es el resultado de un proyecto conjunto entre el grupo de expertos de codificación de video de ITU-T y el grupo de expertos de imágenes en movimiento de ISO/IEC (MPEG). ITU-T es el sector que coordina los estándares de telecomunicaciones en nombre de la Unión Internacional de Telecomunicaciones. H.264 es el nombre usado por ITU-T, mientras que ISO/IEC utiliza el nombre MPEG-4 Parte 10/AVC, ya que lo presenta como parte de su suite MPEG-4.La suite MPEG-4 incluye, por ejemplo, MPEG-4 Parte 2, que es un estándar que ya ha sido usado por codificadores de video basados en IP y cámaras de red y fue diseñado para solucionar una serie de debilidades de estándares de compresión de video anteriores, H.264 satisface con éxito su objetivo de admitir:

- Implementaciones que ofrezcan una reducción de la frecuencia de bits del 50%, a partir de una calidad de video fija y comparada con otros estándares de video.
- Robustez frente a errores, de forma que se toleren los errores de transmisión a través de varias redes.
- Capacidades de baja latencia y mejor calidad para latencias mayores.
- Especificación de sintaxis directa que simplifique las implementaciones.
- Decodificación de coincidencia exacta, que define cuántos cálculos numéricos debe realizar un codificador y un decodificador para evitar que se acumulen errores.
- H.264 tiene también la flexibilidad suficiente como para admitir una amplia gama de aplicaciones con diferentes requisitos de frecuencia de bits. Por ejemplo, en aplicaciones de video de entretenimiento que incluye retransmisiones, satélite, cable y DVD.

2.5 SOFTWARE LIBRE

2.5.1 Definición: Software libre es el software que, una vez obtenido, puede ser usado, copiado, estudiado, modificado y redistribuido libremente. Suele estar disponible gratuitamente en Internet, o a precio del coste de la distribución a través de otros medios. Existen diversas clasificaciones del software libre: de acuerdo a su filosofía, de acuerdo a su costo, código fuente, protección, de acuerdo a su legalidad.

2.5.2 Clasificación del Software: el software libre, es una pequeña parte de la clasificación total en la que el Software se divide. Éste último, se puede desglosar dependiendo de su naturaleza, su legalidad, su código fuente, etc. A continuación se nombrarán aquellas clases de software concernientes al presente trabajo de grado.

- Propietario**:** es aquel software que refleja el hecho de que su propiedad absoluta permanece en manos de quien tiene sus derechos y no del usuario, quien únicamente puede utilizarlo bajo ciertas condiciones. Su uso, redistribución y/o modificación están prohibidos o restringidos de modo tal que no es posible llevarlos a cabo. Es decir, este tipo de software le da al usuario derechos limitados sobre su funcionamiento, cuyo alcance establece el autor o quien posea ese derecho.
- Libre: es el tipo de software que le da al usuario la libertad de usarlo, estudiarlo, modificarlo, mejorarlo, adaptarlo y redistribuirlo, con la única restricción de no agregar ninguna información adicional al software ya modificado. Vale aclarar que debe permitir el acceso al código fuente, debido a que ello es una condición imprescindible para ejercer las libertades de estudiarlo, modificarlo, mejorarlo y adaptarlo.
- Software de costo cero: también conocido como software gratis o gratuito. Es aquel software cuyo costo de adquisición es nulo, es decir, no hace falta efectuar un desembolso de dinero para poder usarlo.

- De costo mayor a cero: también se conoce como software comercial o de pago. Es el software desarrollado por una entidad que tiene la intención de hacer dinero con su uso.
- De código fuente abierto: también llamado de fuente abierta u Open Source. Es aquel software que permite tener acceso a su código fuente a través de cualquier medio (ya sea acompañado con el programa ejecutable, a través de Internet, a través del abono de una suma de dinero, etc.).
- De código fuente cerrado: también llamado software cerrado. Es el software que no tiene disponible su código fuente por ningún medio, ni siquiera pagando. Generalmente tiene esta característica cuando su creador desea proteger su propiedad intelectual.
- De dominio público: es el software que no está protegido por ningún tipo de licencia. Cualquiera puede tomarlo y luego de modificarlo, podría incluso hacerlo propio.
- Protegido por licencias: es el tipo de software protegido con una licencia de uso. Dentro de este grupo tenemos:
- Protegido con Copyright: es decir, con derechos de autor (o de copia). El usuario no puede adquirirlo para usarlo y luego vender copias (salvo con la autorización de su creador).
- Protegido con Copyleft: es aquel cuyos términos de distribución no permiten a los redistribuidores agregar ninguna restricción adicional. Quiere decir que cada copia del software, aun modificada, sigue siendo como era antes.

2.5.5 Recorrido por el Mercado Actual de la Transmisión de Información a través de Software de Código Abierto

En el mercado actual, existen numerosas soluciones basadas en código abierto, tanto para telefonía como para transmisión de video y datos. Asimismo, se han desarrollado: plataformas, sistemas operativos, distribuciones, servidores, PBXs e inclusive emuladores (de clientes: softphones, de máquinas: VirtualBox, VMWare, de sistemas operativos, etc.), perfectamente válidos y de gran implementación.

Una de las plataformas de mayor estabilidad y utilización (y que se tomó como sistema base para el desarrollo del presente trabajo) es la plataforma basada en Linux. En la actualidad, ésta, ha tomado gran notoriedad gracias a los desarrollos tan acertados por parte de la empresa privada, centros de estudio y la comunidad de colaboradores, todos motivados por la libertad del código y de la fortaleza del mismo para crear sistemas robustos, confiables y con proyección para solucionar estos problemas que cada día son más complicados de manejar. Fundamentadas en Linux, existen implementadas diferentes distribuciones fijas ya desarrolladas como lo son: Ubuntu, Debian, Fedora, Slackware, Centos, entre otras. Igualmente existen distribuciones configurables como lo son: Elastix, Trixbox, Asterisk, etc; que se presentan como soluciones estables y confiables y que además, permiten establecer un ambiente propicio para el enrutamiento y transmisión de información. A continuación se describirán aquellas posibilidades ofrecidas por el mercado que se utilizaron en el presente proyecto.

2.5.5.1 Proyectos OpenH323: El proyecto Open H.323 nace como una iniciativa que aspira crear una implementación de software libre de la torre de protocolos de la recomendación ITU H.323. Al ser un proyecto basado en los principios del software libre, los programadores pueden usar las librerías y el código fuente para fines personales o comerciales. El proyecto Open H.323 nació en septiembre de 1998 por parte de la compañía australiana Equivalente Pty Ltd. y está actualmente coordinado por el operador de telefonía local norteamericano QuickNet Technologies Inc. La iniciativa de Open H.323 de crear una implementación de la recomendación H.323 libre, favorece el uso y el fomento de H.323 por parte de usuarios domésticos y pequeñas empresas, incapaces de pagar las licencias atribuidas a implementaciones comerciales. Actualmente las librerías de Open H.323 implementan la versión 4 de H.323 y constantemente se actualizan debido a mejoras propuestas y errores encontrados por los programadores. Open H.323 dispone diversas aplicaciones que funcionan como elementos de red H.323 como son: Ophone (Terminal H.323 basado en línea de comandos), Open Phone (Terminal H.323 con una interfaz gráfica), Open

GK (Gatekeeper H.323), Open MCU: MCU H.323, PSTN Gateway: Pasarela H.323-RTB. Todas estas aplicaciones están desarrolladas haciendo uso de dos librerías creadas por el proyecto Open H.323; estas librerías son PWLib y OpenH.323. Para comprender mejor el funcionamiento de estas aplicaciones y conocer cómo están desarrolladas es interesante realizar una descripción de ambas librerías.

2.5.5.1.1 La librería PWLib: fue desarrollada años atrás con la finalidad de ofrecer una vía para generar aplicaciones software multiplataforma. PWLib permite ejecutar aplicaciones de forma transparente tanto en sistemas Microsoft Windows como en Unix X-Windows Systems. Desde sus orígenes se ha ido añadiendo código que permite la portabilidad incluso de interfaces gráficos basados en Windows. PWLib incorpora clases para tratar la entrada/salida con la mayor portabilidad posible así como clases que manejan las ejecuciones multi hilo de forma también portable. Incluye al mismo tiempo facilidades para desarrollar los daemons de Unix y proporcionar servicios NT (New Technology). Actualmente también ofrece una implementación de los protocolos de Internet como: TCP, IP y UDP. La librería PWLib está presente en todas las implementaciones del proyecto H.323 y es prácticamente un contenedor de clases que ofrece la portabilidad multiplataforma ofreciendo clases como listas enlazadas, listas ordenadas, tablas hash, sockets, entrada/salida serie, entrada/salida por pantalla, componentes gráficos, procesos, hilos, componentes de sincronización, etc.

2.5.5.1.2 La Librería OpenH323: es la librería que realmente implementa la torre de protocolos H.323, para ello modela cada uno de los elementos necesarios de cada nivel de red que intervienen en la comunicación H.323, así como los parámetros de un punto extremo de red. La clase fundamental de la librería OpenH323 es el endpoint o terminal, entendiendo como terminal la unidad H.323 más genérica posible que funciona como cualquier tipo de elemento de red H.323. OpenH323 está escrita en lenguaje C++. C++ es un lenguaje orientado a objetos y su uso facilita el modelado de los elementos involucrados en una comunicación H.323. Mediante el uso de clases se da forma a las unidades, los elementos y los parámetros necesarios

para establecer y mantener una comunicación. Los objetos pertenecientes a una determinada clase son componentes aislados que cooperan entre sí para dar sentido a una entidad H.323. Las características de estos objetos quedan reflejadas mediante los atributos de las clases; los atributos son variables y, por tanto, los parámetros son configurables. Las acciones que cada objeto puede realizar, o las acciones a las que cada objeto responde, se modelan mediante los métodos de las clases. OpenH323 también aprovecha la herencia entre clases para facilitar una programación más estructurada y evitar la aparición de código redundante. Para mejorar la tarea de los diseñadores se aprovecha el polimorfismo dentro de una misma clase lo que permite redefinir métodos de una clase para reducir, ampliar o modificar la funcionalidad y el comportamiento de una determinada entidad H.323.

Tal y como se ha dicho, la clase fundamental de la librería OpenH323 es la clase EndPoint. Habitualmente una aplicación software implementada sobre OpenH323 sólo tiene un objeto de esta clase, el cual representará un terminal o entidad básica, un Gatekeeper, un Gateway, una MCU, etc. Un objeto EP (End Point) también es el objeto de más alto nivel dentro de la jerarquía de OpenH323; a él se atribuyen funciones genéricas como realizar una llamada, terminar una llamada, localizar un gatekeeper, registrarse en un gatekeeper, añadir información relacionada con el terminal, configurar la tabla de capacidades. Esta última acción sea quizás la más importante a la hora de configurar el EP, ya que permitirá decidir de qué códecs de audio y/o vídeo dispondrá el EP. Dependiendo de los codecs asignados en la tabla de capacidades del EP, éste podrá comunicarse con unos u otros terminales. Existen una gran variedad de Códecs disponibles para seleccionar en una comunicación H.323, sin embargo la ITU tan sólo obliga a los terminales H.323 a disponer de los Códecs de audio G.711 ley A y G.711 ley µ y el códec H.261 para el video (para más información del funcionamiento de esta librería consultar los anexos).

2.5.5.2 Plataformas y Sistemas Operativos basados en Software Libre

2.5.5.2.1 GNU/Linux Ubuntu: Ubuntu es una distribución libre GNU/Linux patrocinado por Mark Shuttleworth y Canónica Ltda. Se centra en la facilidad de uso, soporte de hardware y funcionalidad, es actualmente una de las distribuciones más populares de GNU/Linux con amplia documentación y variadas comunidades en línea. La comunidad se fundamenta en las ideas consagradas en la filosofía Ubuntu: que se basa en que el software debe estar disponible gratuitamente, las herramientas de software deben ser utilizables por la gente en su lengua local, debe ser posible su utilización a pesar de cualquier discapacidad, y que la gente debe tener la libertad de personalizar y modificar de la forma que consideren más adecuada. Ubuntu es rápido y fácil de instalar gracias al Disco Vivo (LiveCD), cuenta con emisiones regulares y previsibles, cada 6 meses con Soporte de Largo Tiempo (LTS). Programas especializados pueden ser agregados fácilmente usando los repositorios y cuenta con un buen apoyo de la comunidad por medio de listas de correo, canales IRC (Internet Relay Chat) y foros web. La interfaz de usuario de Ubuntu (escritorio GNOME) es muy coherente y estética. Adicionales a las aplicaciones estándar de GNOME, se incluyen por defecto algunos paquetes externos de código abierto, como OpenOffice, Firefox y GIMP (GNU Image Manipulation Program, Programa de Manipulación de Imágenes GNU). El sistema detecta automáticamente los dispositivos móviles como, memorias USBs, cámaras digitales y tarjetas de memoria. Su gran capacidad de detección de hardware son especialmente visibles en los equipos portátiles, donde tecnologías como el WiFi, software de suspensión y ahorro de energía que solían causar problemas en sistemas GNU/Linux, ahora son muy fácilmente utilizables. Ubuntu no es sólo de GNOME, otros entornos de escritorio están disponibles también: Ubuntu con KDE (Kubuntu), XFCE (Xubuntu), Fluxbox (Fluxbuntu), etc.

Figura 2.14. Logo de la Distribución Ubuntu
Fuente: *http://www.segmentationfault.es/2009/10/ubuntu-9-10-karmi-koala/*

2.5.5.2.2 Elastix: Elastix es una distribución de "Software Libre" de Servidor de Comunicaciones Unificadas que integra en un solo paquete algunas tecnologías de comunicaciones claves como: VoIP PBX, Fax, Mensajería Instantánea, Email, etc. Al decir distribución nos referimos al concepto de distro, es decir un conjunto de paquetes de software que se distribuyen juntos en un mismo medio, en este caso un CD, incluyendo el instalador y sistema operativo. Al final de la instalación tendremos un Servidor de Comunicaciones Unificadas listo para producción. Elastix implementa gran parte de su funcionalidad sobre 4 programas de software muy importantes como son Asterisk, Hylafax, Openfire y Postfix. Estos brindan las funciones de PBX, Fax, Mensajería Instantánea e Email, respectivamente. La parte de sistema operativo se basa en CentOS, una popular distribución Linux orientada a servidores. A continuación una figura un poco más ordenada donde se pueden observar los componentes de Elastix y su relación entre sí. Elastix es software libre distribuido bajo licencia GPL versión 2. Es decir que puede ser usado, copiado, estudiado, modificado y redistribuido libremente según los lineamientos de esta licencia. Es difícil enlistar todas las características de Elastix en un simple listado, pero las más importantes son según el sitio www.elastix.org: Grabación de llamadas con interfaz vía Web, Voicemails con soporte para notificaciones por email, IVR configurable y bastante flexible, Soporte para sintetización de voz, Herramienta para crear lotes de extensiones lo cual facilita instalaciones nuevas, Cancelador de eco integrado, Provisionador de teléfonos vía Web. Esto permite instalar numerosos teléfonos en muy corto tiempo, Soporte para Video-fonos, Interfaz de detección de hardware de telefonía, Servidor DHCP para asignación dinámica de IPs a IP-Phones, Panel de operador, desde donde el operador puede ver toda la actividad telefónica de manera gráfica y realizar sencillas acciones drag-n-drop como transferencias, parqueos, etc, Reporte de uso de canales por tecnología (SIP, ZAP, IAX, Local, H323), Soporte para colas de llamadas, Centro de conferencias, desde donde se puede programar conferencias estáticas o temporales, Soporta protocolo SIP, IAX, H323, MGCP,

SKINNY entre otros, Codecs soportados: ADPCM, G.711 (A-Law & μ-Law), G.722, G.723.1 (pass through), G.726, G.729 (si se compra licencia comercial), GSM, Ilbc, Troncalización, entre otras

Figura 2.15. Logo de la Distribución Elastix
Fuente: www.elastix.org

2.5.5.2.3 Asterisk: es un software PBX que usa el concepto de software libre (GPL). Digium, empresa que lo promueve, invierte en ambos aspectos, el desenvolvimiento de código fuente y en el desarrollo del hardware de telefonía de bajo costo que funciona con este software. Asterisk corre en plataforma Linux y otras plataformas Unix con o sin hardware conectando a la red pública de telefonía, PSTN (Public Service Telephony Network), FreeBSD, Mac OS, Windows, entre otras; además, permite conectividad en tiempo real entre las redes PSTN y redes Voip. El paquete básico de Asterisk incluye muchas características que antes sólo estaban disponibles en caros sistemas propietarios como por ejemplo: creación de extensiones, envío de mensajes de voz a e-mails, llamadas en conferencia, menú de voz interactivos y distribución automática de llamadas. Además se pueden crear nuevas funcionalidades mediante el propio lenguaje Asterisk o módulos escritos en C o mediante scripts AGI escritos en Perl o en otros lenguajes. Asterisk además, soporta numerosos protocolos como SIP y H.323. Puede operar con muchos teléfonos SIP, actuando como servidor de registro o como Gateway entre los teléfonos IP y la red telefónica convencional. Al soportar una mezla de la telefonía tradicional y los servicios de VoIP, Asterisk permite a los desarrolladores construir nuevos sistemas telefónicos de forma eficiente o migrar de forma gradual los sistemas existentes a las nuevas tecnologías. (para más información acerca de la arquitectura, componentes y canales de Asterisk, véase el anexo)

Terminales VoIP compatibles con Asterisk

Para realizar y recibir llamadas o entablar videoconferencias, los usuarios necesitan de unos dispositivos terminales que proporcionen la funcionalidad de un teléfono. Estos pueden ser ordenadores, teléfonos IP o teléfonos convencionales analógicos. En este último caso será necesario algún tipo de adaptador que convierta las ondas analógicas en digitales.

Softphones: para utilizar un ordenador como terminal VoIP es necesario utilizar una aplicación software que simule un teléfono video llamada Softphone. Entre los modelos más utilizados se encuentran X-Lite de CounterPath Corporation, Yate, Ekiga, entre otros.

- Yate (Yet Another Telephone Engine): es una solución que destaca por su flexibilidad ya que permite implementar un gran número de dispositivos tales como: clientes servidores de VoIP, PBX, H.323 Gatekeeper, etc. Escrita en lenguaje C++, se puede instalar en Linux o Windows, es completamente gratuito y ofrece la posibilidad de extender sus funcionalidades usando para ello lenguajes de programación como PHP, Phyton y Perl.
- X-Lite: se trata de un software que se ejecuta en estaciones de trabajo (PCs) o servidores, permite establecer llamadas de Voz sobre IP basadas en el protocolo de señalización SIP, X-Lite 3.0 de CounterPath es el principal softphone libre SIP del mercado disponible para la transferencia directa. De acuerdo con la arquitectura avanzada del eyeBeam 1.5 (cliente de telefonía de CounterPath), el nuevo X-Lite se diseña para mostrar algunas de las nuevas características disponibles con el softphone comercial tal como audio superior y calidad de video, fácil configuración, IM presencia, y un libro de direcciones personal completo.
- Ekiga: Como H.323 se utilizara Ekiga, el cual es una aplicación de videoconferencia de código abierto; es voz sobre IP, es una aplicación de Telefonía y Videoconferencia sobre IP para Linux, puede correr también

sobre OpenSolaris o MacOSX y WINDOWS. Ekiga es la última evolución de GnomeMeeting, el cual fue escrito por Damien Sandras. Es una aplicación de videoconferencia y telefonía sobre IP compatible con H.323, que te permite realizar llamadas de audio y video a usuarios remotos con hardware o software H.323. La aplicación se distribuye bajo los términos de la licencia GNU/GPL. Es capaz de usar un moderno Protocolo de Voz sobre IP como SIP y H.323, el cual soporta todas las principales características definidas para aquellos protocolos como retención de llamadas, transferencia de llamadas, reenvío de llamadas, también soporta mensajería instantánea, etc. Ekiga soporta los códec libres de audio y video (cuenta con Theora y Speex perteneciente a la organización Xiph.org), y dispone de un respaldo de ancho de banda para una calidad superior de audio, conjuntamente con cancelación de eco. Algunas de sus características son: Permite realizar llamadas PC-teléfono,basada en el estándar H.323 ITU, permite realizar conferencias multiusuarios usando una Unidad de Control Multipunto (MCU), soporta registro en un ILS (Internet Locator Service), entre otros.

2.5.5.2.4 Iperf: es una herramienta que puede ser utilizada para medir, supervisar y calificar el desempeño e eficiencias de sistemas de videoconferencia H323 utilizando una arquitectura distribuida cliente/servidor. Esta herramienta ayuda a los operadores de conferencia a tener una ventana en la cual se puede visualizar el estado de una sesión de videoconferencias H323 y permite así mismo mostrar información necesaria para solucionar problemas de rendimiento en la red. Dentro de este programa, se visualizan datos importantes, los cuales serán definidos a continuación para una mejor comprensión y entendimiento del programa y de lo que sucede en el sistema monitoreado, tales son: ancho de banda, retardo o latencia, jitter y pérdida de paquetes.

a.- Ancho de banda: En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bits

por segundo (BPS), kilobits por segundo (kbps), o megabits por segundo (mps). En la actualidad, aún no se han resuelto los problemas relacionados con el ancho de banda y el cómo crear flujos de cadenas de datos en tiempo real. Lograr transportar voz de alta calidad telefónica sobre IP en tiempo real no es una tarea nada fácil de alcanzar ya que tal labor requiere manejo de las capacidades de la red que permita el control del tráfico, protocolos de tiempo real (TCP/IP no lo son) y anchos de banda dedicados durante el tiempo que tome la realización de la llamada. Como se ha mencionado, la calidad de servicio (QoS), no es una característica ofrecida por las redes de datos IP (redes utilizadas en el presente trabajo). Para el caso de los protocolos involucrados en la videoconferencia, el consumo de ancho de banda utilizado depende directamente de los códecs de audio y de video que serán empleados en la transmisión multimedia.

b.- Retardo de transmisión (latencia): el retardo que no es más que la cantidad de tiempo requerido para transmitir y recibir una señal de audio y video. En los sistemas de videoconferencia esto es un aspecto muy importante ya que si los paquetes tardan en llegar, las personas que participan en una sesión de videoconferencia notaran que se pierde el sincronismo entre lo transmitido y lo recibido perjudicando ésta. Una latencia de 50 ms, su efecto es casi imperceptible, pero arriba de 150 ms ya los usuarios lo detectan y puede notarse la falta de sincronía entre el movimiento de los labios y la voz. En función del retraso se pueden distinguir los siguientes tipos de tráfico: asíncrono (retraso de transmisión sin restricciones), síncrono (el retraso de transmisión está acotado para cada mensaje) e isócrono (el retraso de transmisión es constante para cada mensaje).

c.- Jitter: el jitter no es más que la variación aleatoria de la latencia. Este normalmente es originado por alto tráfico que temporalmente reduce las capacidades de la red o por cambios en el camino de los paquetes. Las redes IP no garantizan la entrega de los paquetes en orden, ni de forma inmediata, mas sin embargo, los paquetes de voz y video pueden ser etiquetados para recibir un trato preferente a la hora de atravesar la red. No obstante, tales medidas no terminan con el jitter, sólo

reducen sus efectos. Un jitter aceptable dentro de una transmisión de audio y video es de máximo 50ms.

d.- Pérdida de paquetes: la pérdida de paquetes significa que los paquetes de datos, no llegan a su destino. Sus efectos son video entrecortado durante la sesión de videoconferencia, fallas de audio, video estático e incluso hasta la misma perdida de la comunicación. La pérdida de paquetes se produce por descartes de paquetes que no llegan a tiempo al receptor. La perdida de paquetes máxima admitida para que no se degrade la comunicación deber ser inferior al 2%. Pero es bastante dependiente del códec que se utiliza. Cuanto mayor sea la compresión del códec más pernicioso es el efecto de la pérdida de paquetes.

2.5.5.2.5 Virtualización: la virtualización se encarga de crear una interfaz externa que esconde una implementación subyacente mediante la combinación de recursos en localizaciones físicas diferentes, o por medio de la simplificación del sistema de control. Ésta se refiere a la abstracción de los recursos de una computadora, llamada Hypervisor o VMM (Virtual Machine Monitor) que crea una capa de abstracción entre el hardware de la máquina física (host) y el sistema operativo de la máquina virtual (virtual machine, guest), siendo un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, un dispositivo de almacenamiento, una red o incluso un sistema operativo, donde se divide el recurso en uno o más entornos de ejecución. Esta capa de software (VMM) maneja, gestiona y arbitra los cuatro recursos principales de una computadora (CPU, Memoria, Red, Almacenamiento) y así podrá repartir dinámicamente dichos recursos entre todas las máquinas virtuales definidas en el computador central. De modo que nos permite tener varios ordenadores virtuales ejecutándose sobre el mismo ordenador físico.

En la sección de “Anexos” del presente trabajo, se explican en detalle las características de cada una de estas plataformas y herramientas; en el caso de los softphones se encuentra un manual con la instalación y configuración paso a paso de dichos programas.

CAPÍTULO IV
3. METODOLOGÍA Y DESARROLLO

En este capítulo, se describirán detalladamente cada una de las fases, junto con los métodos que se llevaron a cabo para lograr el cumplimiento, tanto de los objetivos generales, como de los objetivos específicos fijados en este Trabajo Especial de Grado. El presente trabajo fue dividido en siete fases, a continuación, se describen cada una de ellas.

3. 1 Fase 1. Documentación Inicial: La investigación teórica y documental se basó en la recopilación y estudio de los conceptos involucrados con los sistemas de videoconferencias, protocolos de comunicación, en especial los protocolos H.323 y SIP y su señalización, Gateways y sus implementaciones; así como también se incluye el análisis de lo que es el software libre y proyectos de código abierto enfocados en la videoconferencia y en la traducción de protocolos, verificando que sean de fácil administración, considerando el manejo del lenguaje de programación, bibliotecas y aplicación de los mismos; dando lugar así al Marco Teórico y proporcionando la base conceptual que sustenta el presente Trabajo Especial de Grado.

La recopilación de información se puede dividir en tres etapas fundamentales. En principio, la investigación se basó en el análisis de sistemas de videoconferencias, tipos, componentes, códecs de audio y video utilizados y modo de operación de los mismos; todo esto en el marco de la Red de datos de la Universidad Central de Venezuela (equipos Polycom basados en protocolo H.323 y equipos Cisco y softphones SIP), así como también, se estudiaron los gateways (pasarelas), su funcionamiento, operación y tipos de implementación, recomendaciones ITU e IETF fundamentadas en los protocolos utilizados en el sistema de videoconferencia a instaurar. La segunda etapa se enfocó en el estudio de los dos protocolos principales

involucrados, los cuales son el protocolo H.323 y el Protocolo SIP. Se realizó un estudio minucioso y detallado de las características de ambos protocolos, funcionamiento, llamadas, y en especial la señalización, la cual representa el pilar fundamental para lograr la traducción de información entre ambos.

Por último, la investigación se basó en la búsqueda de proyectos establecidos en software libre, plataformas más utilizadas y distribuciones que una vez instalados, pudieran ofrecer servicios de traducción de protocolos. Tal es el caso de Elastix y Asterisk en concatenación con los proyectos Xiph.org (que incluyen proyectos como OpenH323, Ekiga, Opal, Gnugk Gatekeeper, entre otros). Igualmente, fueron revisados y estudiados distintos tipos de softphones que representan clientes tanto SIP como H.323 (X-Lite y Yate). El criterio principal para realizar la búsqueda, fue que el software libre fuese netamente basado en código abierto, es decir que no requiriera de pagos por licencia.

Otros factores importantes, fueron encontrar un software estable y de buen desempeño, además de proveer un ambiente propicio para realizar funciones de enrutamiento y señalización a fin de conseguir una traducción eficiente. Cabe destacar, que las fuentes utilizadas y de donde se obtuvieron todas las informaciones y conceptos previamente descritos fueron en su mayoría, fuentes electrónicas, documentos encontrados en la web, post informativos de foros VoIP, entre otros; siendo éstos uno de los principales, ya que al tratarse de código abierto existe una constante evolución y mejora de los programas ya existentes y debido a su filosofía estas informaciones siempre son compartidas y publicadas para el uso contínuo de personas alrededor de todo el mundo, así como del enriquecimiento y mejora de los proyectos ya existentes creando la base para nuevos proyectos.

3. 2 Fase 2. Planeamiento del Software: En esta etapa se listan los requerimientos y necesidades de la red. De acuerdo a éstos, se permite trazar una lista de posibles soluciones que permitan comprobar que el proyecto se esté ejecutando de manera adecuada y de acuerdo a los objetivos propuestos. Una vez

aclarado este punto, se define una estrategia funcional y organizada (un diagrama) que describirá cada uno de los elementos que harán posible la implementación del Gateway.

En esta fase, en principio, se realizará una descripción del escenario actual de la red de datos de la Universidad Central de Venezuela. Cabe destacar que dicha descripción está enfocada en el desarrollo e implementación del presente trabajo de grado, el cual fué realizado específicamente en el Laboratorio de Comunicaciones de la Escuela de Eléctrica de la Facultad de Ingeniería de dicha casa de estudios. Acto seguido, serán puntualizados los requerimientos necesarios para llevar a cabo su ejecución; además se presentará de forma general, las soluciones que fueron seleccionadas a fin de brindar la funcionalidad que demanda cada requisito. Por último, se trazará el planeamiento del Gateway en sí, es decir, se describirá un diagrama que indique la arquitectura a implementar.

3.2.1 Análisis Previo: La globalización de la educación superior implica disponer de una infraestructura que permita la interacción de los diferentes actores, tales como estudiantes, profesores y directivos, dado que la población universitaria se encuentra dispersa a lo largo del territorio nacional (debido a la existencia de sedes o núcleos universitarios en otras ciudades o estados). La red de datos actualmente es pilar fundamental de la operación y funcionamiento de las Facultades, Escuelas, Institutos y demás módulos de educación superior, siendo el vehículo de comunicación por excelencia, además del canal de acceso a todos los recursos de información. Las actuales y extendidas ventajas en materia de ancho de banda, calidad de servicio, alta disponibilidad, seguridad y confiabilidad de las redes de datos han conducido, casi naturalmente, a su convergencia con las nuevas tecnologías de comunicación que puedan abastecer estas demandas de información.

3.2.2 Situación Actual. Laboratorio Comunicaciones UCV: Actualmente, la Universidad Central de Venezuela cuenta con una red interna de datos de alta velocidad, la cual es financiada por la propia Institución. Proveé una capacidad de

ancho de banda suficiente para suministrar servicios de intranets, accesos remotos y servicios de internet a altas velocidades a todas y cada una de las facultades y escuelas pertenecientes al recinto universitario.

3.2.2.1 Estructura y Componentes. Laboratorio de Comunicaciones. Escuela de Ingeniería Eléctrica: En el marco de los sistemas de videoconferencias, el Laboratorio de Comunicaciones de la Escuela de Ingeniería Eléctrica cuenta con lo siguiente dentro de su red de datos:

Hardware

- Dos (2) Máquinas PC Intel Pentium IV con 512Mb de Memoria RAM y 80Gb de Disco Duro en cada una (con su monitor, teclado, y mouse correspondiente).
- Una (1) Máquina PC Intel Pentium II con 398Mb de Memoria RAM y 40Gb de Disco Duro (con su monitor, teclado, y mouse correspondiente).
- Una (1) Máquina PC Intel Pentium II con 256Mb de Memoria RAM y 30Gb de Disco Duro (con su monitor, teclado, y mouse correspondiente).
- Equipos Polycom de Videoconferencia (basados en el protocolo H.323): conformado por una cámara, parlantes, micrófono, proyector, equipo (CPU-cócec) de conferencia y un mando. En especial el equipo Polycom MGC-100.
- Teléfonos IP basados en el protocolo SIP y protocolo H.323

Switches y Routers

- Dos (2) Switches Netgear ProSafe Ethernet Gigabit 10/100 Mbps de 16 puertos cada uno.
- Dos (2) Routers Cisco de 150Mbps

Cableado

- Cables de Red UTP de categoría 5 y conectores RJ45
- Cableado convencional perteneciente al Hardware y cableado estructurado existente perteneciente a la Escuela.

Software

- En todas las computadoras se encontraba instalado el sistema operativo Windows XP.

3.2.3 Requerimientos y Soluciones Planteadas para la Plataforma de Videoconferencia: en general los requerimientos para la transmisión de audio y video han sido tratados extensamente en la sección "Marco Teórico" del presente documento, no obstante para el caso práctico se deben especificar en cuanto a hardware, software y demás parámetros como ancho de banda, latencia, etc; aquellos equipos y programas que sean los más adecuados a fin de lograr una implementación adecuada.

3.2.3.1 Software y Hardware: todo el estudio minucioso y detallado expuesto en el capítulo anterior, se realizó con el objetivo de seleccionar la plataforma más adecuada como base para la implementación del software. Fue seleccionada por tanto, la plataforma GNU/Linux, dado que es una de las distribuciones más importantes y posicionadas en el mundo que permite establecer un ambiente propicio, estable y confiable para levantar servicios de enrutamiento. Asimismo, esta plataforma está fundamentada en software de última tecnología capaz de estar listo y acorde con las nuevas tecnologías para redes sin la necesidad de realizar pagos por licencias.

En cuanto a Software se plantea la utilización de la plataforma GNU/Linux Centos para el caso de la implementación del Gateway, ya que en el mismo será instalado una distribución denominada Elastix (distribución basada en plataforma Centos) que a su vez contiene el software Asterisk, el cual posee los soportes

suficientes para la creación del Gateway. Por otra parte, en el caso de los clientes, estos pueden ser softphones gratuitos (X-Lite, Ekiga, Yate) instalados en la plataforma GNU/Linux Ubuntu.

En lo referido al hardware; como se trata del desarrollo de un Gateway basado en código abierto, se debe contar con hardware y equipos periféricos (cámaras, micrófonos, etc.) compatibles con estos software libres. Dada la plataforma de programas escogidas anteriormente, se verificó que el hardware disponible en las instalaciones del laboratorio de la UCV, no es suficiente en cuanto a especificaciones técnicas se refiere (Memoria RAM, Disco Duro), por lo cual se requiere añadir nuevos módulos de memoria RAM (al menos actualizar a 2Gb de Memoria RAM), unidades de Disco Duro (30Gb más al menos) y dispositivos periféricos como cámaras, micrófonos y parlantes compatibles con la plataforma Linux, para lograr la instauración del software necesario en el presente Trabajo de Grado.

No obstante, se cuenta adicionalmente con dos computadoras personales (propiedad de la estudiante) que poseen las siguientes especificaciones:

Laptop HP Intel Core I3-330M 1.8GHz:

- 4GB de Memoria RAM
- 500GB de Disco Duro
- WLAN y Bluetooth con cámara y micrófono integrado

PC Intel Core 2 Dúo 1.8GHz:

- 4GB de Memoria RAM
- 160GB de Disco Duro
- Ethernet 10/100 PCI, LAN y Bluetooth
- Cámara y Micrófono Logibyte Periféricos.

Con estos equipos se solventan los requerimientos de hardware, siendo suficientes para lograr implementar el software que sustentará el presente trabajo.

Por último, otro aspecto importante en la implementación llevada a cabo, es que la distribución Elastix carece de una herramienta que realice la partición del disco; de hecho, este sistema operativo sólo puede funcionar con un almacenamiento dedicado a ella, eliminando durante su instalación cualquier otro sistema contenido en la máquina. Para evitar conflictos de interoperabilidad dentro de la máquina o cualquier otro problema que esta distribución signifique, es necesario realizar una virtualización que soporte dicho sistema operativo. En la sección "Anexos" del presente trabajo se encuentra explicado detalladamente los pasos para realizar una virtualización mediante la herramienta "VirtualBox".

3.2.3.2 Ancho de Banda: Para el caso de los protocolos involucrados, H.323 y SIP (protocolos en el cual se basa la red de videoconferencia de la universidad), el consumo de ancho de banda utilizado depende directamente de los códecs de audio y de video que serán empleados en la transmisión multimedia.

En cuanto al audio, los códecs elegidos fueron: G.711 ley A y ley μ y GSM. La razón de dicha elección, radica en que además de ser de carácter gratuito (casi todos los proyectos de software libre enfocados a la videoconferencia en la actualidad cuentan con librerías que incluyen en su mayoría estos códecs), son soportados y aprobados por las normativas de los protocolos mencionados (en especial por la arquitectura H.323) y brindan alta calidad. Otro aspecto importante que se debe tener presente al momento de calcular el ancho de banda consumido por una llamada, es que éste está compuesto de dos valores: Ancho de Banda Entrante y Ancho de Banda Saliente (por ejemplo, para una llamada utilizando el códec G.711 cuyo ancho de banda es de 64kbps, el ancho de banda total consumido será (64Kbps + 16Kbps) x 2, ya que se incluye el canal entrante y el canal saliente de la llamada más la cabecera del datagrama TCP/IP). A continuación de muestra una tabla en la que se muestra el Ancho de Banda Nominal y el Ancho de Banda Total Consumido correspondiente a cada códec seleccionado:

Tabla 3.1- Características de los Códecs de Audio seleccionados incluyendo el Ancho de Banda Nominal y el Ancho de Banda Consumido
Fuente: Elaboración Propia

Códec	Ancho Banda (Kbps)	Período de Muestra (ms)	Carga Útil (bytes)	Ancho Banda Nominal (Kbps)	Ancho Banda Consumido* (Kbps)
G.711	64	20	160	80	160
GSM	13	20	32.5	29	58
G.729	8	20	20	16	32

**Ancho de Banda Consumido para una (1) llamada (canal bidireccional)*
Los cálculos de las cifras mostradas en esta y la siguiente tabla se encuentran en la sección de Anexos del presente TEG

En lo referente al video, como se mencionó en el capítulo anterior, la información actualmente se trata casi exclusivamente de forma comprimida. El ancho de banda dependerá por tanto del tipo de compresión y de la calidad con que se quiera transmitir. Se eligieron tres de los estándares más difundidos para compresión de vídeo: ITU H.261, ITU H.263 y MPEG; éstos requieren un ancho de banda de 1.2 a 40 Mbps para el MPEG, MPEG-2 y MPEG-4 (también llamado H.264) de 0.064 a 1.2 Mbps para el H.261 y de 1.2 a 1.8 Mbps para el H.263 respectivamente. La tabla a continuación resume lo anterior.

Tabla 3.2- Características de los Códecs de Video seleccionados incluyendo el Ancho de Banda Nominal y el Ancho de Banda Consumido
Fuente: Elaboración Propia

Códec	Ancho Banda Nominal (Mbps)	Ancho Banda Consumido* (Mbps)
H.261	0.064 – 2	0.128 – 4
H.263	1.2 – 1.8	2.4 – 3.6
H.264 (MPEG-1…4)	1.2 – 40	2.4 - 80

**Ancho de Banda Consumido para una (1) llamada (canal bidireccional)*

En la práctica (lo que se requerirá en el Laboratorio para el desarrollo del Gateway) la transmisión multimedia demanda un ancho de banda de 0.4 Mbps a 8Mbps aproximadamente, sí se tratase de una comunicación unidireccional (una sola llamada). Por otro lado, en el caso de los códec de video, para realizar la traducción de un protocolo a otro se utilizará únicamente el códec H.261, ya que es el de menor capacidad de comprensión (la red H.323 obliga a usar únicamente el códec H.261 para el video). Si se realiza una videoconferencia, el ancho de banda consumido aumentará conforme aumenten los participantes, y aún más si todos se encuentran interconectados simultáneamente. A pesar de que el ancho de banda disponible en la red de datos de la UCV parece suficiente, dispositivos como switches y routers, jugarán un papel importante al momento de establecer una comunicación multiusuario, ya que, ofrece una distribución equitativa del mismo, proporcionando la capacidad necesaria para establecer todas las conversaciones, por tanto se requiere que dichos dispositivos sean de gran desempeño y de alta velocidad.

3.2.3.3 Retraso de Transmisión (Latencia) y Fiabilidad: Estos requerimientos son más estrictos que los de ancho de banda. La experiencia con los sistemas de conferencia multimedia y los estándares ITU sugieren un retraso máximo de 150 ms en las aplicaciones de vídeo interactivas (véase "Marco Teórico"). Para el caso particular de este trabajo, en la red de la universidad, la isocronía no tiene que ser mantenida durante todo el camino de un mensaje, ya que puede ser recuperada en el destino mediante un almacenamiento para visualización, lo cual no representa problema, dado el tipo de implementación utilizada. Otro tema son los tiempos de compresión y descompresión de las imágenes de vídeo. Siguiendo los requerimientos del CCITT de un máximo de 150 ms de fuente a destino, se pueden identificar las siguientes componentes en el retraso: retraso en la compresión y descomposición en paquetes en la fuente, retraso de transmisión en la red, almacenamiento en el destino, retraso de sincronización y retraso por la composición de los paquetes y la descompresión en el destino. La imagen debe tener de 25 a 30 tramas por segundo.

Esto deja un tiempo máximo de compresión/descompresión de 30 a 40 ms (aunque puede ser menor). Restando a 150 ms deja un retraso máximo de 70 a 90 ms para la transmisión en la red. Asumiendo que la red posee una topología básica, y teniendo en cuenta que los elementos de enlace (switches, routers, etc.), también contribuyen al retraso, resta un retraso máximo aceptable de 10 a 15 ms por salto. Aunque estos cálculos son aproximados y dependerían de muchos otros factores, aportan una idea de los problemas de la transmisión que puedan presentarse. Para controlar estos problemas en la comunicación, se procurará la utilización de la menor cantidad de dispositivos que puedan contribuir al retraso, adicionalmente la compresión con que se está trabajando, permite acotar los niveles de latencia dentro del sistema. Por otra parte, tanto el audio como el video serán transmitidos por el mismo canal, ésto a fin de evitar problemas tanto de sincronización de canales como de retardo a causa de esta sincronización.

3.2.3.4 Jitter: Un margen requerido por todo sistema de videoconferencia debe ser un jitter menor a 50ms (véase "Marco Teórico"). En este caso, por los protocolos utilizados y la señalización (etiquetas dentro de paquetes) involucrada, el jitter no debería sobrepasar los límites estipulados en la normativa.

3.2.3.5 Pérdida de Paquetes: para una videoconferencia aceptable se deben tomar en cuenta:

- Una pérdida de paquetes de 1% puede producir congelamiento en el video y/o pérdida del audio.
- Una pérdida de paquetes de 2% puede hacer que el video sea malo, aunque el audio puede sonar algo aceptable.
- Una pérdida de paquetes por arriba del 2% es inaceptable.

3.2.4 Diagrama General: En base a lo anterior, para lograr el desarrollo del Gateway se procura implementar lo siguiente:

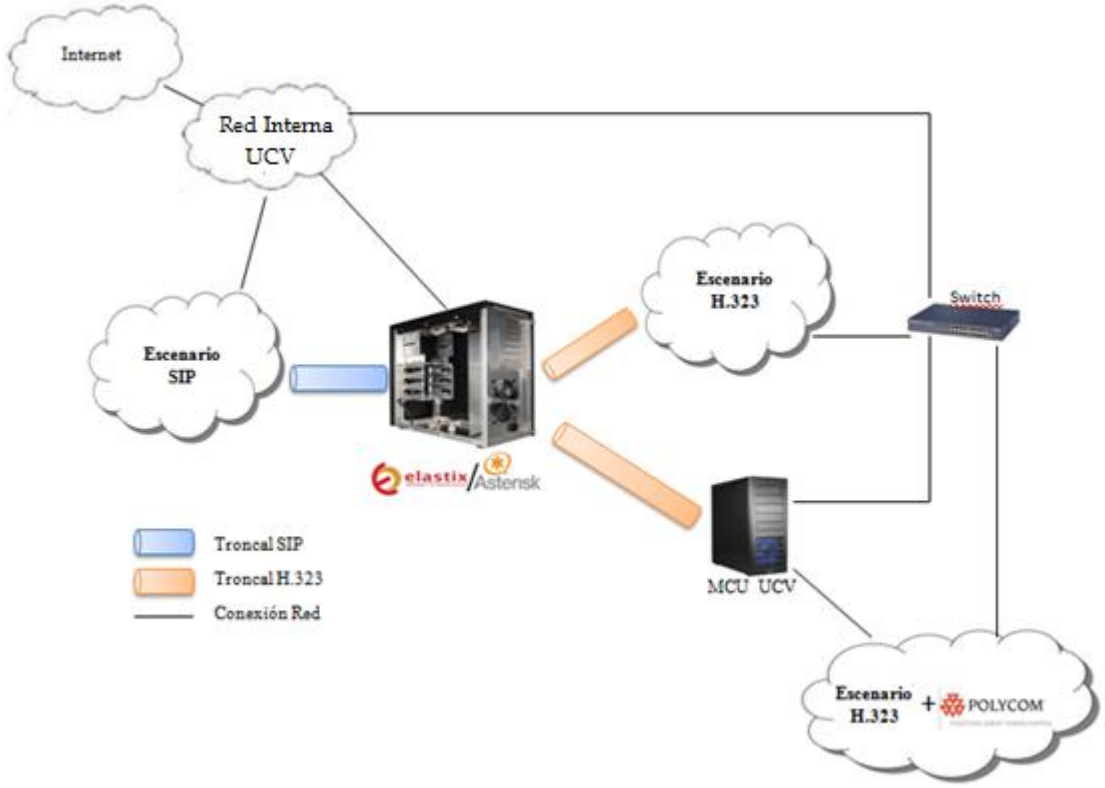


Figura 3.1- Diagrama General de la Arquitectura a Implementar

Fuente: Elaboración Propia

3.3 Fase 3. Diseño del Software: se realizaron diseños pequeños simples, adaptándolos a los protocolos utilizados con la finalidad de concatenarlos y conformar la arquitectura total requerida; es decir; se realizó el diseño de cada escenario tanto SIP como H.323, para luego realizar la interconexión entre ellos. Paralelamente en esta etapa, se consideraron las necesidades que deben cumplirse en la interacción de los protocolos, así como de los mecanismos de control y la señalización que permitirá la traducción de los mismos.

III.3.1 Interconexión SIP/H.323. Problemática Asociada a la señalización de redes heterogéneas: Después del análisis realizado en el capítulo anterior, la problemática asociada a la señalización dentro del sistema de videoconferencia que se quiere implementar en la red de datos UCV, radica fundamentalmente en la

traducción de protocolos SIP a H.323. Por tanto, del estudio anteriormente realizado, se puede deducir que una llamada de VoIP se divide en diferentes fases (véase "Llamada H.323" y Llamada SIP" en la sección "Marco Teórico"), las cuales son principalmente:

- Registro de usuarios: Los usuarios se registran en un servidor de registro (para usuarios SIP) o en un Gatekepeer (para usuarios H.323). El problema que se desprende de esta fase es la identificación de usuarios, puesto que una red H.323 no tiene constancia de los usuarios de una red SIP, ni viceversa. Por lo cual, para solucionar esta problemática, se proponen dos soluciones: una es implementar un ENUM mediante la aplicación Bind 9 en Elastix (más adelante se explicará con detalle) y crear un canal dedicado (troncal) que soporte la traducción de los protocolos; la segunda es implementar Elastix interconectado a un Gatekeeper, por ejemplo el OpenGatekeeper o GnuGK como es más comúnmente conocido.
- Establecimiento de la conexión: En esta fase, uno de los participantes inicia la llamada mediante mensajes de INVITE, TRYING y RINGING (para SIP) o CALLPROCEEDING y ALERTING (para H.323).
- Negociación de parámetros: Los participantes anuncian sus características (para SIP) o negocian las características (para H.323). La fase de negociación es la más crítica, ya que la conversación puede llegar a ser rechazada, en caso de no llegar a un acuerdo de parámetros.
- Comunicación: Una vez establecida la comunicación y acordados los parámetros, se inicia la transmisión de información mediante el protocolo RTP/RTCP. En esta fase no se necesitará una traducción del protocolo por que tanto SIP como H.323 utilizan RTP y el RTCP para la transmisión multimedia sobre IP.
- Finalización de la llamada: Uno de los participantes inicia esta fase con un mensaje de BYE (para SIP) o ENDSESSIONCOMMAND, RELEASECOMPLETE (para el H.323).

En las fases de establecimiento de la conexión, negociación de parámetros y finalización se necesita un mapeo de mensajes SIP a H.323, que será analizado a continuación.

3.3.1.1 Identificación de Usuarios: En una red de VoIP, cada usuario puede disponer de múltiples direcciones a través de las cuales puede ser localizado. Para resolver esta problemática se propone ENUM. El protocolo ENUM (Electronic Number/Telephone Mapping), fue desarrollado por IETF (Internet Engineering Task Force) para definir una arquitectura y un protocolo basado en DNS (Domain Name System). ENUM traduce los números telefónicos de la recomendación ITU-T E.164 a una o más URI (Uniform Resource Identifiers) utilizando una arquitectura DNS con TLD (Top Level Domain) e164.arpa. Esta traducción está descrita en el RFC 2916. Utiliza los llamados registros de recursos NAPTR, definidos en el RFC 2915. Estos registros identifican un número telefónico E.164 a diferentes métodos o servicios disponibles para contactar con el usuario final. ENUM utiliza un tipo específico de registro de servicio NAPTR para la resolución de E.164 a URI ("E2U").

En definitiva ENUM proporciona identificación de usuarios tanto para interconectar una red IP a redes de telefonía convencionales, como para interconectar diferentes protocolos como SIP o H.323. En lo que respecta al Gateway, se debe contener un servicio de resolución de numeración centralizada. Así pues, será asignado un rango de numeración para cada uno de los terminales, los cuales quedarán almacenados en una base de datos dentro de Elastix (Asterisk cuenta con MySQL que proporciona estos servicios) para poder ser consultados y actualizados periódicamente contra el Gateway. Algunas aplicaciones que soportan ENUM son Bind 9 y PowerDNS. Se decidió implementarlo mediante BIND 9 por su fácil configuración y la gran utilización que este servidor posee en la web, además del hecho de que en nuevas distribuciones de Elastix, dicha aplicación ya está incluida dentro de sus directorios constitutivos y archivos de configuración.

Adicionalmente con esta configuración, será necesaria la creación de un troncal con el soporte preciso para suministrar el mapeo de los mensajes entre los protocolos y la señalización necesaria. Al ser agregado este canal, se podrá configurar el direccionamiento de las llamadas entre cada uno de los terminales, ya que, uno o varios troncales, podrán ser modificados asignándoles un rango de posibles números (números de identificación de cada cliente) en base al destino de la comunicación que se desee establecer. El sistema configurado de esta manera, no sólo facilita y flexibiliza el registro de usuarios, sino que además provee servicios de seguridad, ya que las conexiones se realizarán mediante enlaces dedicados (troncales configurables) previamente establecidos en base a los requerimientos de cada red.

Por otra parte, la segunda solución propuesta se basa en interconectar Elastix junto con el OpenGatekeeper GnuGK. Tanto Asterisk como GnuGK, poseen servicios de almacenamiento de datos y control de base de datos en general. Para el caso de Elastix, éste cuenta con MySQL el cual es un sistema de gestión de base de datos relacional y multiusuario; dicho sistema se encargará del registro de los usuarios SIP y el direccionamiento dentro de los mismos. GnuGK también provee servicios de registros de usuarios y en este caso, permitirá el direccionamiento de las llamadas entre los elementos H.323 y el reconocimiento, tanto de los terminales H.323, como del propio Asterisk. Existen modos de operación del GnuGK que permite el registro automático de todos los End Points y el enrutamiento directo de los paquetes a dichos usuarios registrados.

3.3.1.2 Mapeo de Mensajes: Para un correcto funcionamiento de la interconexión de redes SIP y H.323 se necesita un ente que nos garantice la traducción de los mensajes de señalización de SIP a H.323. Este ente se denomina Signalling Gateway (SGW) y en este caso, estará representado por un soporte añadido a un canal (canal H.323) perteneciente a Asterisk, el cual portará la señalización y el mapeo. El SGW, según el RFC 4123[16] debe presentar las siguientes características:

- Mapeo del establecimiento y finalización de una llamada.
- Mantener el registro de los usuarios.
- Resolución de direcciones SIP y H.323.
- Mantener los estados de las redes SIP y H.323.
- Negociar parámetros de las capacidades de los terminales.
- Apertura y cierre de canales lógicos.
- Mapear algoritmos de codificación para la red SIP y H.323.
- Capacidad para resolver y administrar los recursos de la llamada y los posibles cambios producidos en una llamada.

En algunos casos la traducción de los mensajes SIP y H.323 se realiza uno a uno, es decir, un mensaje SIP corresponde a un mensaje H.323 o viceversa. En la siguiente tabla se presentan los mensajes más significativos:

Tabla 3.3- Tabla de mapeo de métodos SIP a mensajes H.323 (uno a uno)
Fuente: Elaboración Propia

Métodos SIP	Mensaje H.323
INVITE	SETUP
INVITE	ARQ
OPTIONS	H.245
INFO	H.245 UserInputIndication
BYE	H.245 ReleaseComplete (envía el cierre a los canales de señalización)

Tabla 3.4- Tabla de mapeo de códigos de respuesta SIP a mensajes H.323 (uno a uno)

Fuente: Elaboración Propia

Respuestas SIP	Mensaje H.323
180 Ringing	H.225 Alerting
183 Session Progress	H.225 Alerting/Progress
400 Bad Request	H.225 ReleaseComplete Razón (undefinedReason)
404 Not Found	H.225 ReleaseComplete Razón (unreachableReason)
405 Method Not Allowed	H.225 ReleaseComplete Razón (undefinedReason)
408 Request Timeout	H.225 ReleaseComplete Razón (adaptativeBusy)
420 Bad Extension	H.225 ReleaseComplete Razón (badFormatAddress)
500 Server Internal Error	H.225 ReleaseComplete Razón (undefinedReason)
501 Not Implemented	H.225 ReleaseComplete Razón (invalidRevision)
600 Decline	H.225 ReleaseComplete Razón (destinationRejection)
606 Not Acceptable	H.225 ReleaseComplete Razón (undefinedReason)

Tabla 3.5- Mapeo de Mensajes SIP-H.323 (uno a uno).

Fuente: Elaboración Propia

Mensaje SIP	Mensaje H.323
OPTIONS	H.245 sendTerminalCapabilitySet
BYE	H.245 EndSesionComand
CANCEL o BYE (si la llamada está establecida)	H.225 Release Complete
CANCEL o BYE (si la llamada está establecida)	RAS DRQ

En cambio, en otros casos se requiere la traducción de un mensaje SIP a una secuencia de mensajes H.323 o viceversa. La siguiente tabla muestra esos casos:

Tabla 3.6- Mapeo de Mensajes SIP-H.323 (uno a N).

Fuente: Elaboración Propia

Mensaje SIP	Mensaje H.323
BYE	H.245 EndSesionComand H.225 Release Complete RAS DRQ
CANCEL	H.245 EndSesionComand H.225 Release Completeras RAS DRQ
4XX BYE o CANCEL	DRQ

Para poder señalizar una llamada de SIP a H.323 o viceversa, no sólo se realizan un mapeo de mensajes, sino también el SGW debe guardar el estado de la llamada y producir una serie de mensajes (tanto SIP como H.323) para una correcta transferencia de mensajes. En las figuras siguientes se detallan un ejemplo sencillo de

una llamada SIP a H.323 y de H.323 a SIP para poder ver el funcionamiento global del SGW (Asterisk):

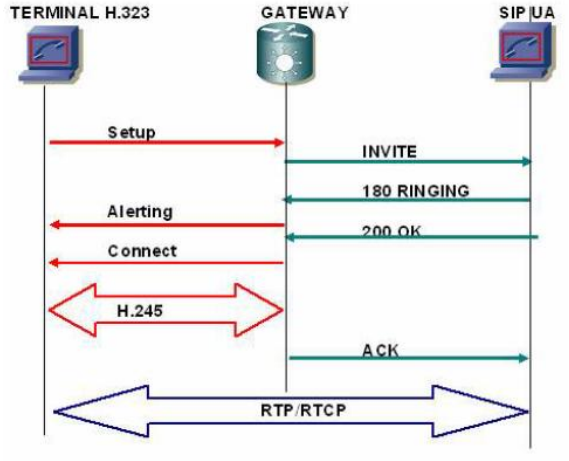


Figura 3.3- Llamada de Interconexión H.323-SIP

Fuente: Elaboración Propia

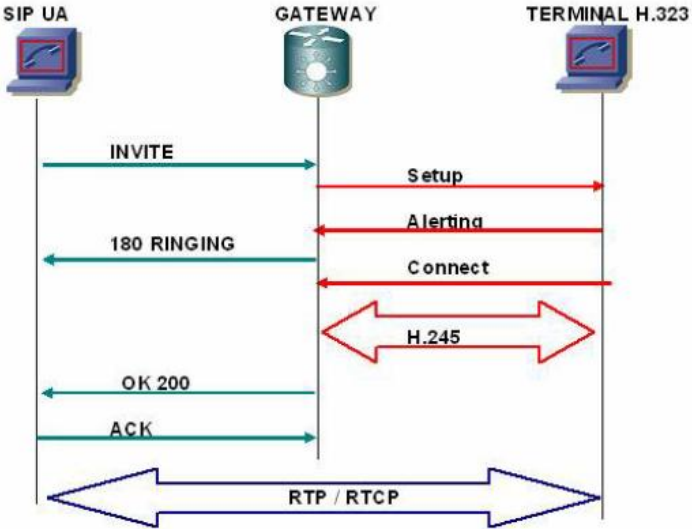


Figura 3.4- Llamada de Interconexión SIP-H.323

Fuente: Elaboración Propia

3.3.2 Escenarios Propuestos: Después del análisis anterior sobre la interconexión de las redes heterogéneas y las soluciones propuestas, se plantean dos escenarios:

3.3.2.1 Escenario A: en este se implementa lo siguiente:

- Una computadora que consta de: una máquina virtual (VirtualBox) con la distribución Elastix (basada en la plataforma GNU/Linux Centos), la cual posea lo siguiente: Asterisk (última versión estable existente 1.6.2.20) con la configuración del protocolo ENUM, activación del servidor MySQL, aplicación Bind 9 ya la adición del soporte H.323 mediante un canal que incluirá las librerías PwLib, Openh323 y todos los plugins necesarios para soportar audio y video.
- Una PC que consta de: un Gatekeper OpenH323 GnuGK instalado en la distribución GNU/Linux Ubuntu 10.04.3
- Dos (2) PC que constan de: un softphone SIP (puede ser X-Lite o Ekiga) y un softphone H.323 (Ekiga o Yate). Ambos instalados en la distribución GNU/Linux Ubuntu 10.04.3.

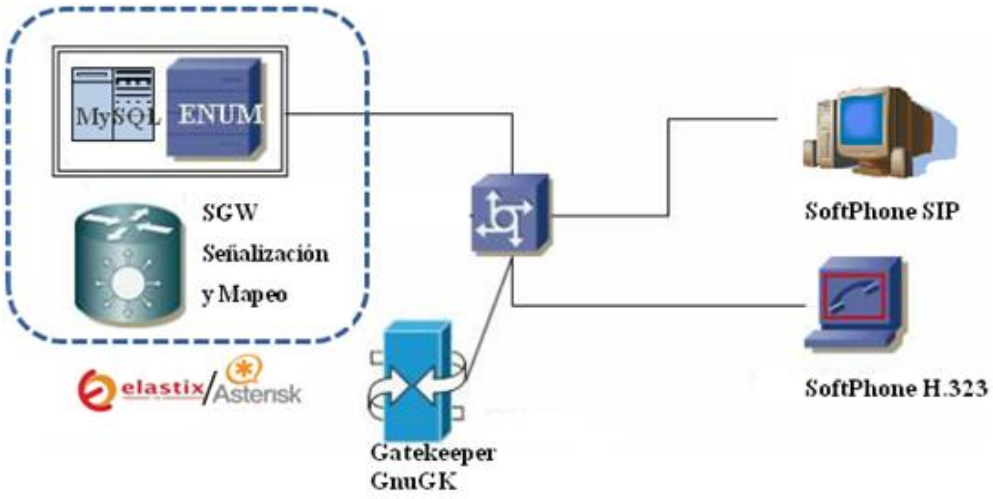


Figura 3.5- Escenario Propuesto A. Gateway incluyendo un Gatekeeper GnuGK

Fuente: Elaboración Propia

3.3.2.2 Escenario B: en este se implementa lo siguiente:

- Una computadora que consta de: una máquina virtual (VirtualBox) con la distribución Elastix (basada en la plataforma GNU/Linux Centos), la cual poseea lo siguiente: Asterisk (última versión estable existente 1.6.2.20) con la configuración del protocolo ENUM, activación del servidor MySQL, aplicación Bind 9 y la adición del soporte H.323 mediante un canal que incluirá las librerías PwLib, Openh323 y todos los plugins necesarios para soportar audio y video.
- Dos (2) PC que constan de: un softphone SIP (puede ser X-Lite o Ekiga) y un softphone H.323 (Ekiga o Yate). Ambos instalados en la distribución GNU/Linux Ubuntu 10.04.3.

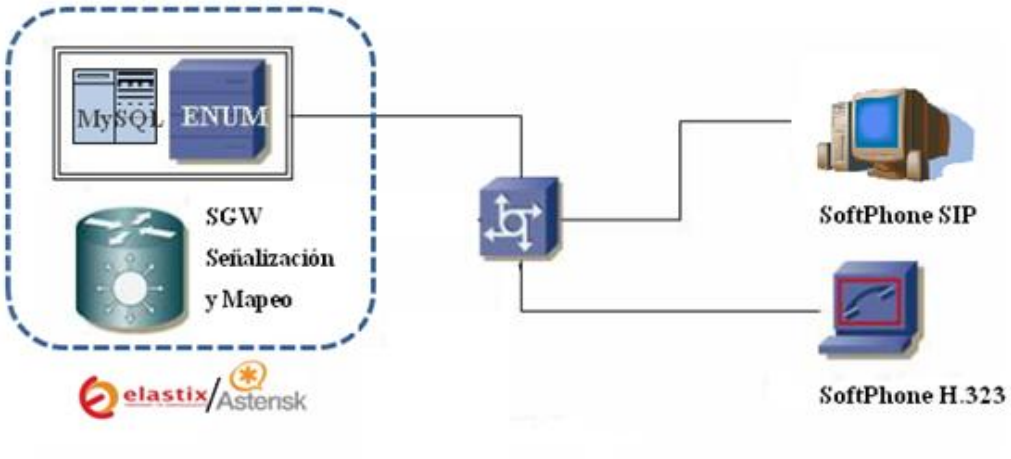


Figura 3.6- Escenario Propuesto B. Gateway sin la inclusión del GnuGK

Fuente: Elaboración Propia

III.3.3 Ejemplo de Llamadas: Después de realizar el montaje de los diferentes servidores del Gateway, se realizan las pruebas para comprobar el correcto funcionamiento de la interconexión.

3.3.3.1 Llamada SIP a SIP

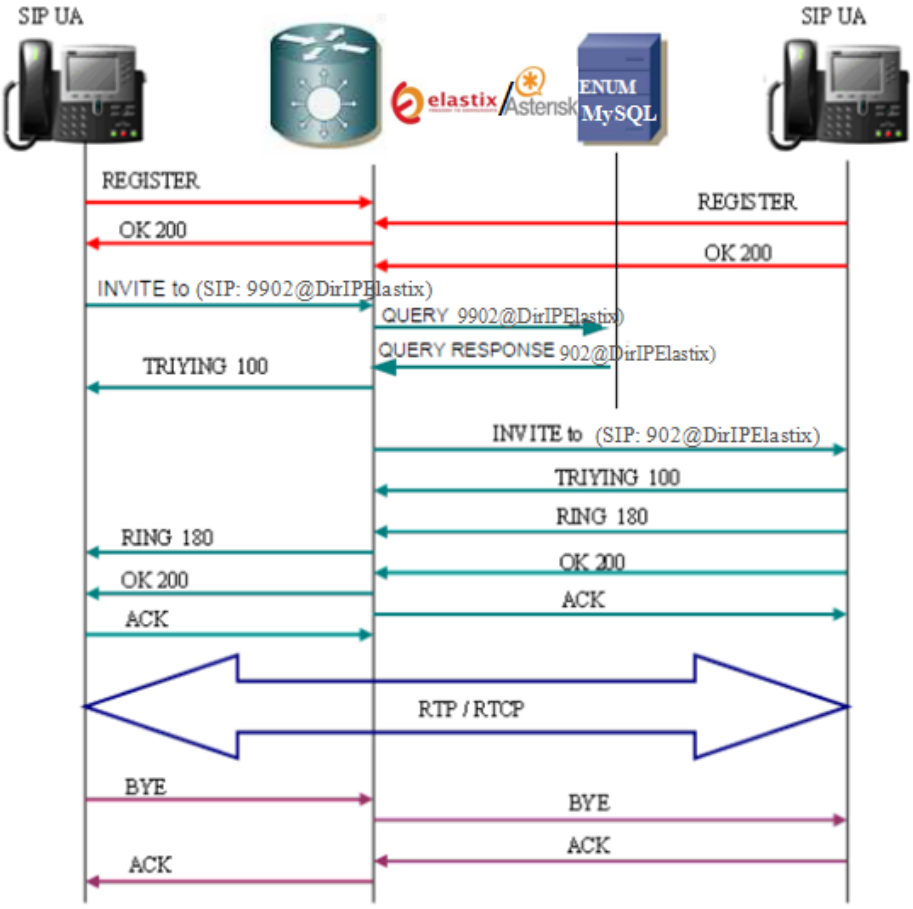


Figura 3.7- Ejemplo de llamada SIP-SIP utilizando el Gateway implementado

Fuente: Elaboración Propia

Como se puede observar en la figura anterior y comparándola con el ejemplo de llamada SIP a SIP (véase "Marco Teórico"), la única diferencia se produce cuando el servidor Elastix recibe un INVITE. Asterisk consulta a la base de datos ENUM y de MySQL extrayendo el prefijo correspondiente a una llamada proveniente de un terminal SIP y devolviendo el número llamado.

3.3.3.2 Llamada H.323 a H.323

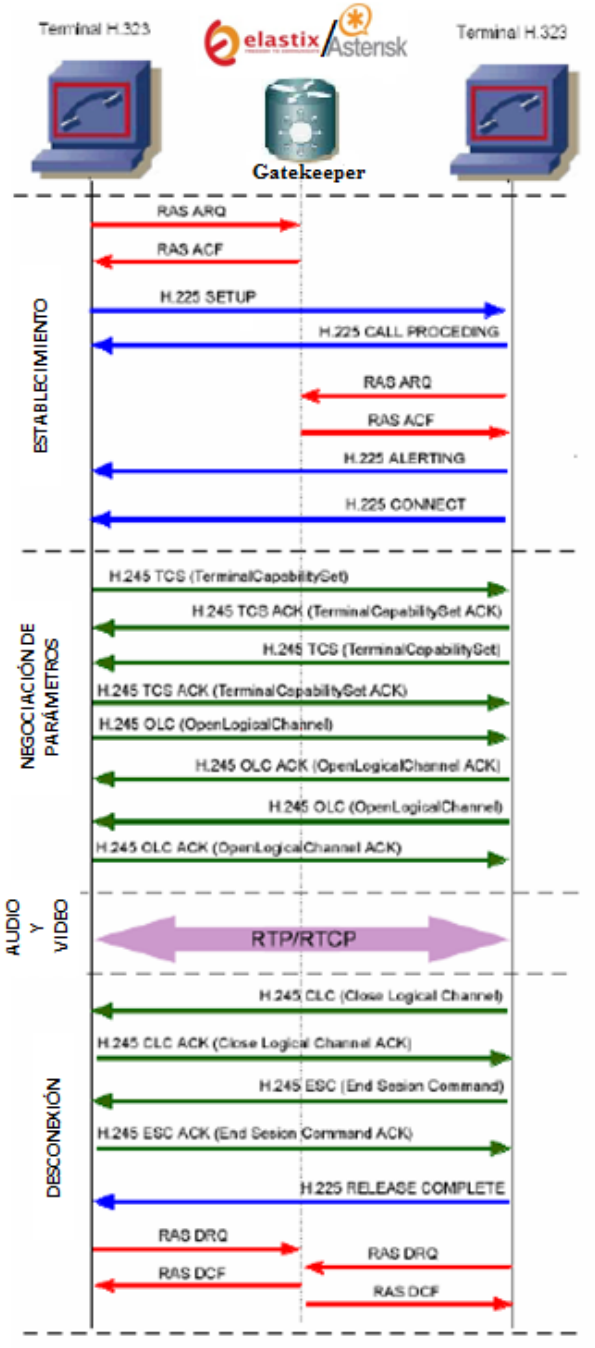


Figura 3.8- Ejemplo de llamada H.323-H.323 utilizando el Gatekeeper junto con Gateway Implementado.

Fuente: Elaboración Propia

3.3.3.3 Llamada H.323 a SIP

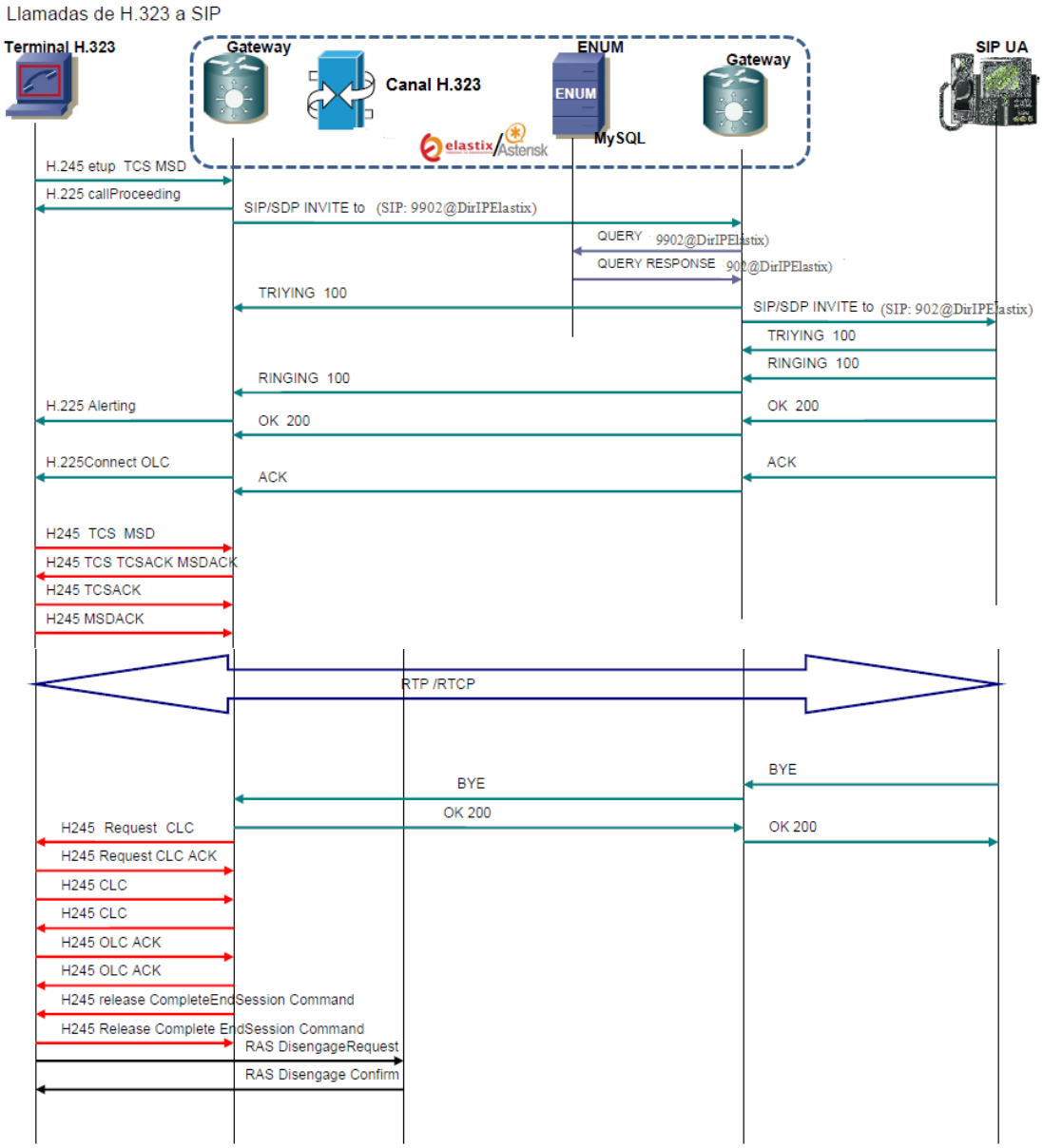


Figura 3.9- Ejemplo de llamada H.323-SIP utilizando el Gateway Implementado (en este caso en base al Escenario B propuesto)

Fuente: Elaboración Propia

3.3.3.4 Llamada SIP-H.323

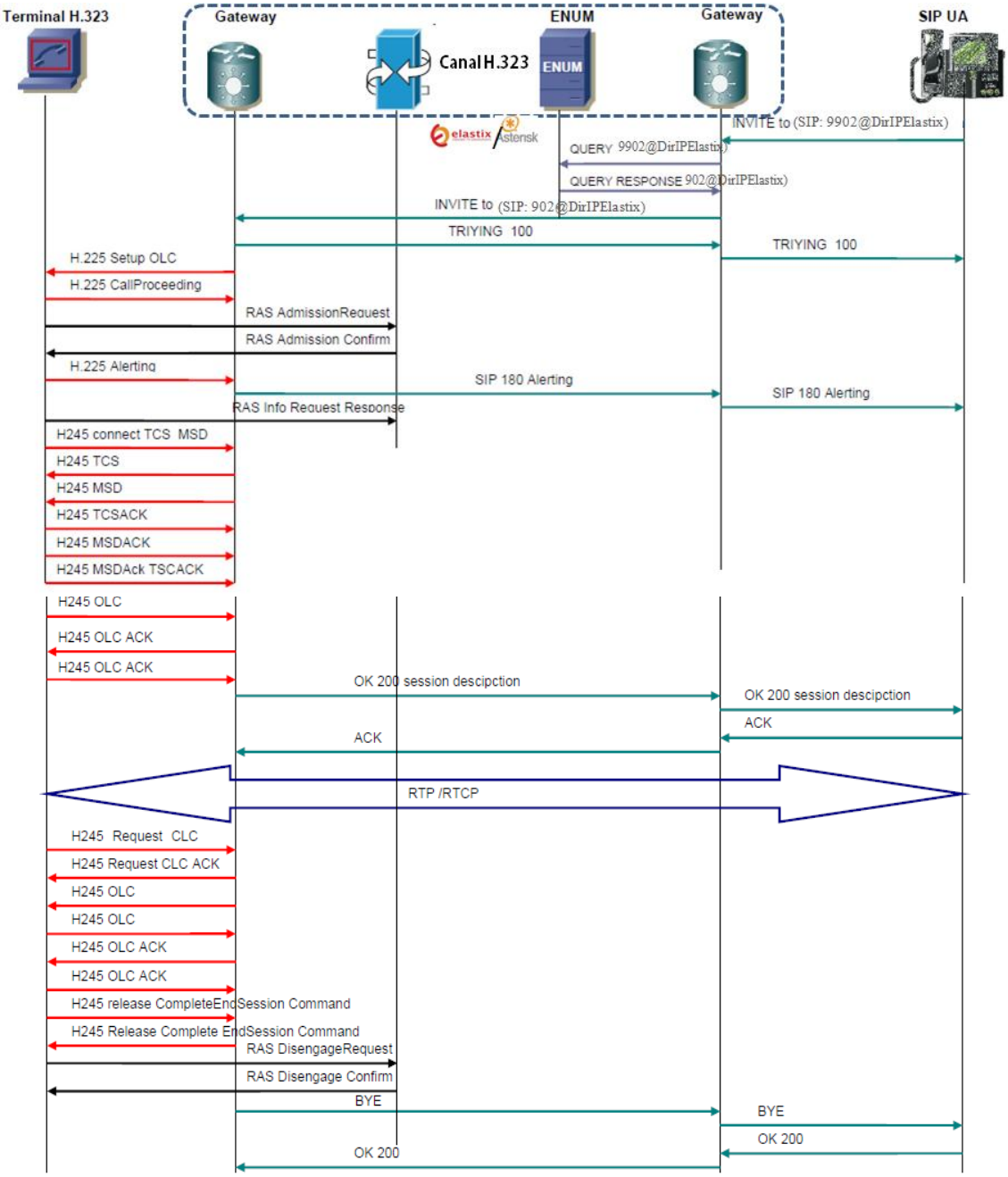


Figura 3.10- Ejemplo de llamada SIP-H.323 utilizando el Gateway Implementado (en este caso en base al Escenario B propuesto)

Fuente: Elaboración Propia

3.4 Fase 4. Desarrollo y Codificación del Software: Esta etapa se basa en la construcción del Gateway planteado en la etapa de diseño y se divide en dos desarrollos principales de acuerdo a los escenarios trazados anteriormente, por tanto cada uno se explicará separadamente.

3.1 Escenario A

3.1.1 Ambiente SIP: en una máquina, que poseía Windows XP como sistema operativo se procedió a descargar e instalar el software X-Lite, este proceso está descrito en detalle en la sección "Anexos" sin embargo la configuración utilizada se muestra en la siguiente figura:

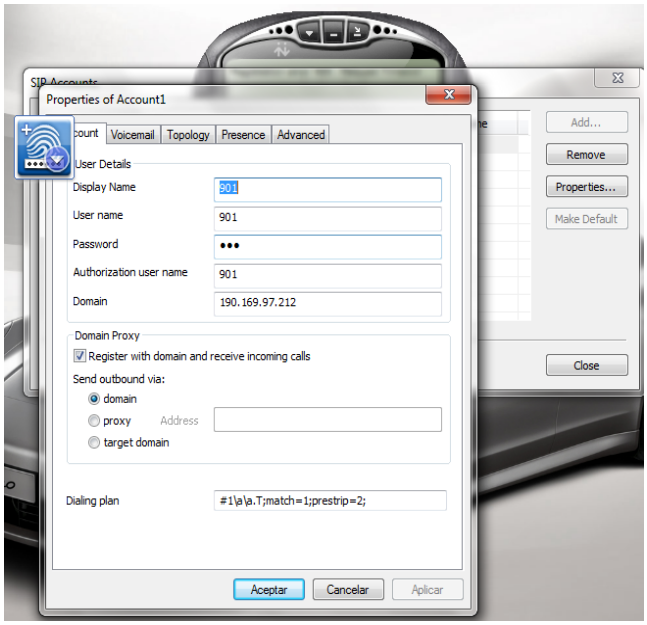


Figura 3.11- Configuración Softphone X-Lite

Fuente: Elaboración Propia

Los campos configurados fueron:

- *Display Name:* Nombre a mostrar en la pantalla para el terminal, es útil para conocer a quién pertenece el número de extensión. En este caso para los End Points SIP se tomó la numeración que comienza con los números 9XX (901 para este primer terminal)

- *User Name:* corresponde a la extensión del usuario. Se utiliza el mismo Display Name para evitar confusiones.
- *Password:* contraseña a adoptar por la extensión. En este caso se colocó el mismo número de extensión (es opcional)
- *Authorization User Name:* el número de autorización de la extensión. Se utiliza el mismo número de extensión
- *Domain:* aquí se coloca la dirección IP del Elastix.
- *Register with domain and receive incoming calls:* se activa esta casilla para que la extensión se registre en la dirección IP colocada en el campo domain.

3.1.2 Ambiente H.323: En este caso, se realizaron dos tipos de ambiente H.323. El primero se construyó instalando el softphone Yate en una máquina que poseía Windows XP como sistema operativo, para que cumpliera las funciones de terminal H.323; sin embargo dicho softphone tiene la desventaja de sólo proporcionar llamadas H.323 en audio, por lo que se utilizó únicamente en las primeras pruebas del Gateway a fin de verificar el correcto funcionamiento del mismo en cuanto a la transmisión del audio. Posteriormente éste fue suplantado por el software Ekiga instalado en una máquina con GNU/Linux Ubuntu 10.04LT; el cual si permite tanto transmisión de audio como de video y fue el que finalmente se tomó como terminal H.323. La instalación y configuración de ambos softphones se encuentran explicados en la sección “Anexos” del presente trabajo; no obstante a continuación se describirán los parámetros de configuración utilizados:

Para Yate:

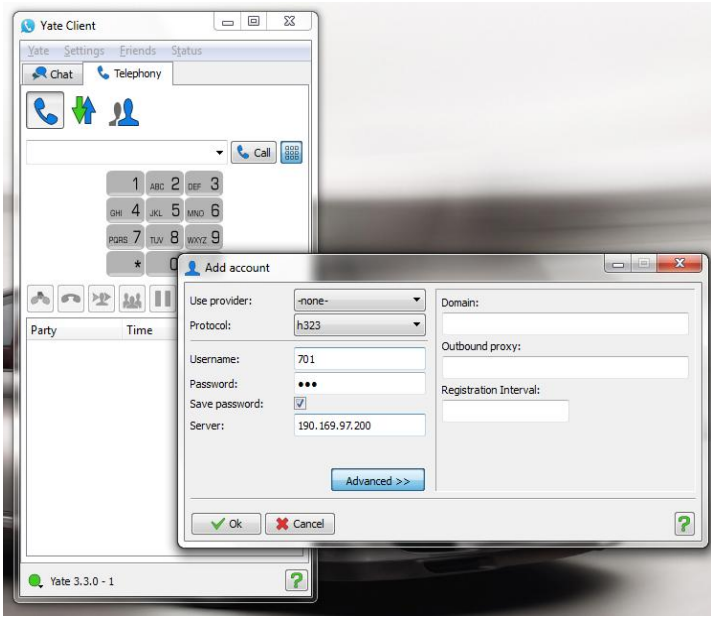


Figura 3.12- Configuración Softphone Yate

Fuente: Elaboración Propia

- *Protocol:* Tipo de protocolo utilizado por el softphone, en este caso como Yate va a representar el terminal H.323, por lo tanto se coloca el protocolo H.323.
- *User Name:* corresponde a la extensión del usuario. En este caso para los End Points H.323 se tomó la numeración del rango 7XX (701 para este primer terminal). Este campo es importante, ya que contiene la identificación que posee el terminal y con el cual se registrará bien sea en Elastix o en el Gatekeeper según sea el caso.
- *Password:* contraseña a adoptar por la extensión. En este caso se colocó el mismo número de extensión (es opcional)
- *Server:* aquí se coloca la dirección IP del Servidor que se utilice, es decir, puede ser la dirección IP del Gatekeeper para el Escenario A o la dirección IP del Gateway (Elastix) para el caso del Escenario B.

Para Ekiga

En cuanto a la configuración de Ekiga, solamente se modificó en el Menú del software en la sección "Editar" se selecciona "Preferencias" y se desplegará las dos pantallas anteriormente mostradas en las cuales se pueden configurar que tipos de códecs de audio y video se desea emplear en la comunicación así como la configuración de los dispositivos periféricos como la cámara, micrófono y parlantes o auriculares. Para las pruebas iniciales sólo fueron activados los códecs G.711 Ley A y Ley u, GSM y Speex para el audio, y el códec H.261 para el video (para las demás configuraciones e instalación del software Ekiga véase el anexo).

IV.1.3 Gatekeeper GnuGK: Para la implementación del Gatekeeper se procedió a instalar en una máquina con GNU/Linux Ubuntu 10.04LT el OpenGatekeeper GnuGK, para mayor información acerca del comportamiento del GnuGK se puede consultar directamente en la página http://www.gnugk.org. Éste fue descargado e instalado directamente desde el gestor de paquetes "Synaptic".

Una vez instalado el GnuGK en el sistema se procedió a realizar su configuración pertinente; dicha configuración se encuentra en la sección de "Anexos", no obstante para este caso se utilizó el Gnugk en modo "Enrutado" para permitir el direccionamiento de las llamadas entre los terminales H.323 y el Gateway (Elastix) y se modificó el archivo gatekeeper.ini de la siguiente manera:

```
$sudo su (contraseña) ; ingreso como super usuario
$cd etc; ingreso al directorio de configuración
$ gedit gatekeeper.ini; se ingresa al archivo gatekeeper.ini para su posterior
                        modificación
```

Archivo gatekeeper.ini

```
;Sección principal del archivo
[Gatekeeper::Main]
;Parámetro obligatorio para encabezar esta sección. Se usa para pruebas
Fortytwo=42
;Nombre del gatekeeper. De gran importancia, sobre todo cuando hay
;más de un gatekeeper
Name=GatekeeperH323
;Configuración del modo enrutado por gatekeeper
[RoutedMode]
;Se habilita en el enrutado del canal Q.931
GKRouted=1
;Se habilita el enrutado del canal H.245
H245Routed=1
;Al igual que con la configuración inicial, el gatekeeper aceptará
;llamadas no registradas
AcceptUnregisteredCalls=1
;Sección de autenticación del gatekeeper
[GkStatus::Auth]
;Con este regla se permitirá cualquier conexión no autentificada
rule=allow
;Ahora se configura el endpoint cuyo H.323ID es ELASTIX323 (Asterisk)
;es decir aquí se configura al gateway Asterisk
[EP::ELASTIX323]
;Prioridad del gateway, como solo hay un gateway, se le asignará
;prioridad máxima (1)
GatewayPriority=1
;Prefijos del gateway
;Cualquier llamada a un número que comience con 9 será
;automáticamente transmitida hacia Asterisk
GatewayPrefixes=9
```

Por último, se reinicia toda instancia del gnugk y se reinicia la computadora, luego se ingresa nuevamente al terminal y se inicia el gnugk de la forma:

```
$ gnugk – c /etc/gatekeeper.ini
$gnugk –rr -ttt
```

3.1.4 Elastix y Asterisk: Ésta es la configuración más importante, ya que, toda la compilación y el desarrollo del Gateway se basa en la instalación de dichos programas, y son éstos, los que permiten su correcto funcionamiento. Para poder utilizar la distribución Elastix, se procedió a realizar una máquina virtual (véase "virtualización" en la sección de "Anexos") que contuviese dicho sistema operativo.

Una vez configurada la máquina virtual, se procedió a descargar el archivo imagen ISO de la versión más reciente de Elastix (2.0.3 en este caso) desde la página fuente www.elastix.org, para luego almacenarla en un CD. Posteriormente se realizó la instalación tanto de Elastix como de ENUM (BIND9) y la Activación de MySQL, tal y como se indica en la sección de "Anexos" del presente trabajo de grado.

Una vez instalado Elastix junto con ENUM, BIND9 y MySQL; se procedió a agregar el soporte H.323 y a configurar el canal H.323 de Asterisk que portará la traducción de los protocolos SIP y H.323. Para ello, desde la cónsola de Elastix, se descargaron, configuraron e instalaron los paquetes de Pwlib, Openh323 y los Plugins necesarios, de la siguiente forma:

$yum install flex bison // se instalan las dependencias
touch /usr/include/linux/compiler.h // se crea un archivo vacío que permite la compilación del canal H.323 dentro de Asterisk

Instalando PWLIB

cd /usr/src
wget http://ufpr.dl.sourceforge.net/sourceforge/openh323/pwlib-v1_10_3-src-tar.gz
tar zxvf pwlib-v1_10_3-src-tar.gz
cd pwlib_v1_10_3/
./configure
make
make install
make opt
PWLIBDIR=/usr/src/pwlib_v1_10_3
export PWLIBDIR

Instalando Openh323 y Plugins

cd /usr/src
wget http://ufpr.dl.sourceforge.net/sourceforge/openh323/openh323-v1_18_0

-src-tar.gz

tar zxvf openh323-v1_18_0-src-tar.gz

cd openh323_v1_18_0/

wget http://www.h323plus.org/source/download/plugins-v1_21_0.tar.gz

tar zxvf plugins-v1_21_0.tar.gz

cd plugins_v1_21_0

. /configure

make opt

PLUGINDIR=/usr/src/openh323-v1_18_0/plugins/video/H.261-vic:/usr/src/openh323-v1_18_0/plugins/audio

export PLUGINDIR

cd /usr/src/openh323_v1_18_0

./configure

Make

make opt

make install

OPENH323DIR=/usr/src/openh323_v1_18_0/

export OPENH323DIR

Posteriormente se debe compilar una nueva versión de Asterisk dentro de Elastix, a fin de que éste se cargue con el nuevo soporte H.323. Para activar el canal dentro de Asterisk y compilar de nuevo éste último se realizó lo siguiente:

Compilación de Asterisk. Activación canal H.323

cd /usr/src/

wget http://downloads.asterisk.org/pub/telephony/asterisk/releases/asterisk-1.6.2.20.tar.gz

cd asterisk-1.6.2.20

./configure

cd /usr/src/asterisk/channels/h323/

```
make
make opt
cd /usr/src/asterisk
./configure
make
make install
echo "/usr/local/lib" >> /etc/ld.so.conf
ldconfig
```

Finalmente, se necesita configurar el canal de Asterisk con la dirección del portal web de Elastix, para lograr cargar el canal dentro de éste último.

```
nano /etc/asterisk/h323.conf // el archivo de configuración se modifica
[general]
port = 1720
bindaddr = 0.0.0.0 // aquí se coloca la dirección ip de Elastix
asterisk –rvvvv
module load chan_h323.so
```

Luego de culminada la codificación anterior, se reinicia la máquina virtual y se ingresa al portal web de Elastix para comprobar que se ha agregado correctamente el canal. Pare ello, se ingresa en la pestaña de “PBX” y en la barra de “Tools” se selecciona el editor “CLI”. En la barra del editor se escribe “core show channeltypes” y se presiona “execute”. Si se realizó correctamente todo el proceso anterior, Elastix mostrará en pantalla la existencia del canal H.323; tal cual se muestra en la siguiente figura:

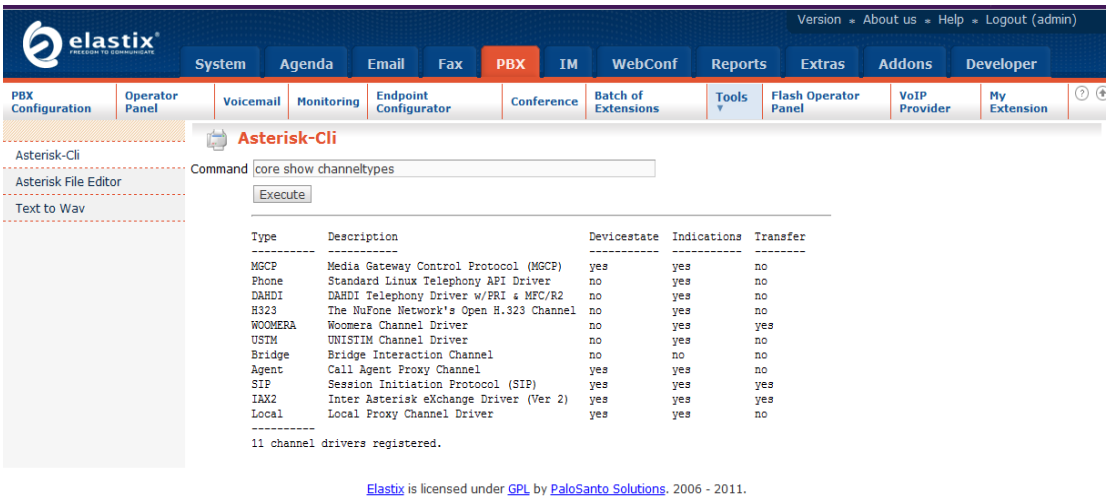


Figura 3.13- Canal H.323 instalado en Elastix

Fuente: Elaboración Propia

3.1.4.1 Configuración Canal H.323: Para realizar esta tarea, es necesario editar el archivo h323.conf localizado en Asterisk, el cual se puede ingresar mediante el Editor de Archivos de Asterisk, que se encuentra en la pestaña de "tools" en la interfaz web de Elastix. Las instrucciones para configurar este archivo se encuentran en el mismo archivo, pero dado, que es un poco complejo, se colocarán a continuación únicamente las modificaciones que fueron realizadas para lograr configurar el Escenario "A".

Archivo h323.conf

;Sección general, usada para configurar parámetros globales **[general]**
;Puerto que asterisk debe escuchar para llamadas H323 entrantes **port=1720**
;Dirección IP que asterisk debe escuchar para llamadas H323 entrantes
;0.0.0.0 intenta encontrar la dirección por si solo o se coloca la dirección de Elastix
bindaddr=0.0.0.0
;H.323ID para el servidor (gateway) asterisk
h323id=ELA323
;ID para llamadas generadas por asterisk
callerid=asterisk
;Este parámetro indica si asterisk se debe registrar con el gatekeeper como
;gateway (yes) o como endpoint (no)
gateway=yes
;Dirección del gatekeeper (GNU Gatekeeper)
gatekeeper = <dirección ip gatekeeper>
;Admitir el modo ruteado por gatekeeper
AllowGKRouted = yes
;Usar protocolo H.245 en la configuración de llamadas
h245inSetup=yes
;Ubicación del archivo de registro (log)
logfile=/var/log/asterisk/h323_log
;Contexto en el cual serán ubicados por defecto los terminales
context=default
;Alias para el cual se aplican las opciones siguientes
alias=asterisk
;Prefijo del gateway, con ésta configuración Asterisk se hará cargo siempre
;que el número marcado comience con 7 o 9
gwprefix=7
gwprefix=9
;Timeout del protocolo de transporte (RTP) para todos los clientes
;Con esta configuración la llamada se abortará si no hay actividad
;en el protocolo de transporte durante 60 segundos
rtptimeout=60
;Codecs utilizados. Los únicos codecs soportados son GSM, G.711 ulaw
; G.711 alaw, y h261 por lo cual se debe inicializar esta parte deshabilitando
;todos los codecs, y luego activando solo los que serán usados
disallow=all
allow=gsm
allow=ulaw
allow=alaw
allow=h261
; definición del terminal h323
[701]
type=user
e164=701
context=default
ip = <dirección ip del terminal h323>
callerid = 701
port = 1719
videosupport=yes
disallow=all
allow=alaw
allow=ulaw
allow=gsm
allow=h261

Cabe destacar que en el archivo anteriormente descrito, sólo se especifica un End Point H.323 (701), ya que para el caso de las pruebas iniciales, únicamente se tomó un solo End Point H.323; sin embargo; si se requiere de la existencia de varios, se deben especificar cada uno de los terminales H.323 conformantes del sistema, a fin de que éstos queden registrados respectivamente en el canal.

IV.1.4.2 Configuración de los Terminales SIP y H.323 dentro de Elastix: A fin de completar la construcción del Gateway, se requiere del registro de los terminales dentro de Elastix. Cada uno de los terminales, pueden ser agregados y modificados a partir de la interfaz web de Elastix; una vez incluidos allí, automáticamente quedarán registrados en la base de datos de Asterisk. Para registrar cualquier terminal dentro de Elastix, se debe ingresar a la sección "Extensions" en la interfaz web, localizada en el panel de configuración de "PBX". Allí se escoge que tipo de terminal se desea agregar; para este caso extensiones SIP para los terminales SIP y extensiones Custom para los teminales H.323 respectivamente.

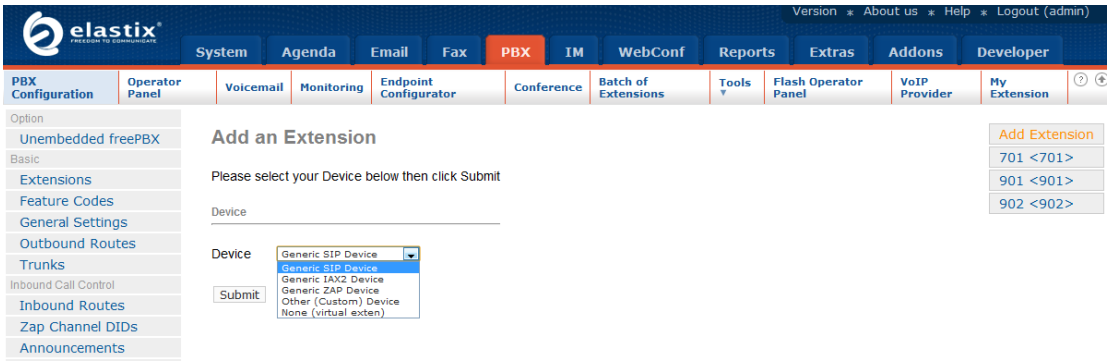


Figura 3.14- Añadiendo terminales en Elastix

Fuente: Elaboración Propia

Para el caso de los terminales SIP, los campos a configurar son los siguientes:

- User Extension: es el número de extensión correspondiente al terminal SIP. En este caso a todos los terminales SIP se les asignó la numeración 9XX.

- Display Name: contiene el nombre de la extensión que se mostrará en pantalla. Se colocó el mismo número de extensión para evitar confusiones.
- SIP Alias: Contiene el nombre con el cual los demás terminales SIP reconocen a la extensión. Para efectos de síntesis se coloca el mismo número de extensión.
- Secret: es la contraseña del terminal. Es opcional y para este caso se usó el mismo número de extensión.
- Language: para efectos del software se coloca ES para que opere en idioma español

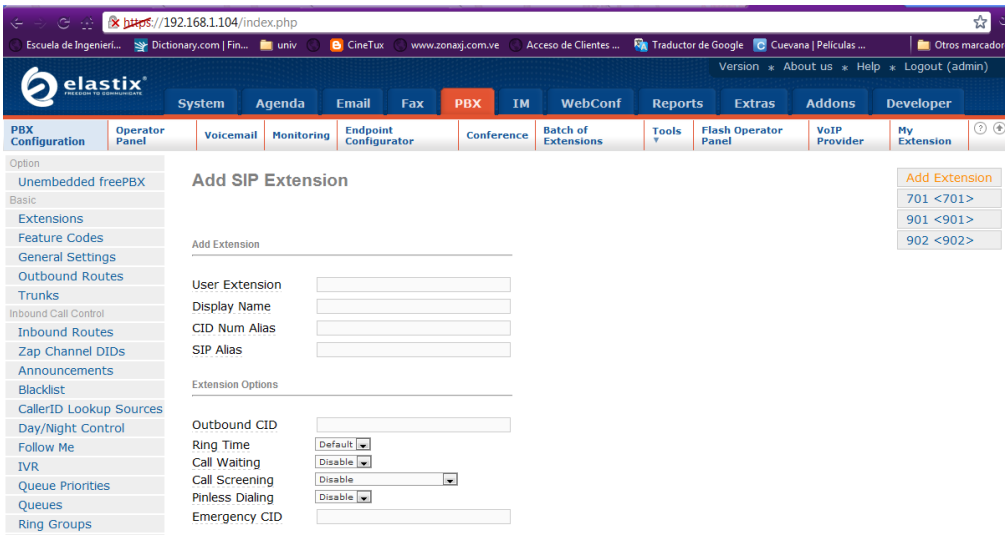


Figura 3.15- Añadiendo terminal SIP en Elastix

Fuente: Elaboración Propia

Adicionalmente, para permitir que entre los terminales exista soporte para video, se debe modificar el archivo sip.conf en el Editor de Asterisk CLI, agregándole las siguientes líneas de comandos:

Videosupport=yes ; permite soporte de video en la llamada

Disallow=all ; desactiva todos los códecs instalados para posteriormente activar aquellos que se deseen

```
Allow=alaw    ;activa el códec G.711 Ley A
Allow=ulaw    ;activa el códec G.711 Ley µ
Allow=h261    ;activa el códec de video H.261
```

Para añadir un terminal H.323 se debe elegir una extensión "Custom" y se procede de igual manera que para un terminal SIP, pero en este caso, se rellenarán los campos respectivos con la información correspondiente al terminal H.323; recordando que para las extensiones H.323 se utilizó el rango de numeración 7XX. La única diferencia es que se le agregará dentro de la configuración del terminal, que éste operará mediante el canal H.323 agregado a Elastix; para ello en la sección "Device Options" dentro de la casilla "Dial" que especifica la tecnología utilizada por el dispositivo será añadida la sintáxis: H323/extensión terminal h323 @ ip del Gatekeeper. Tal como muestra la figura a continuación.

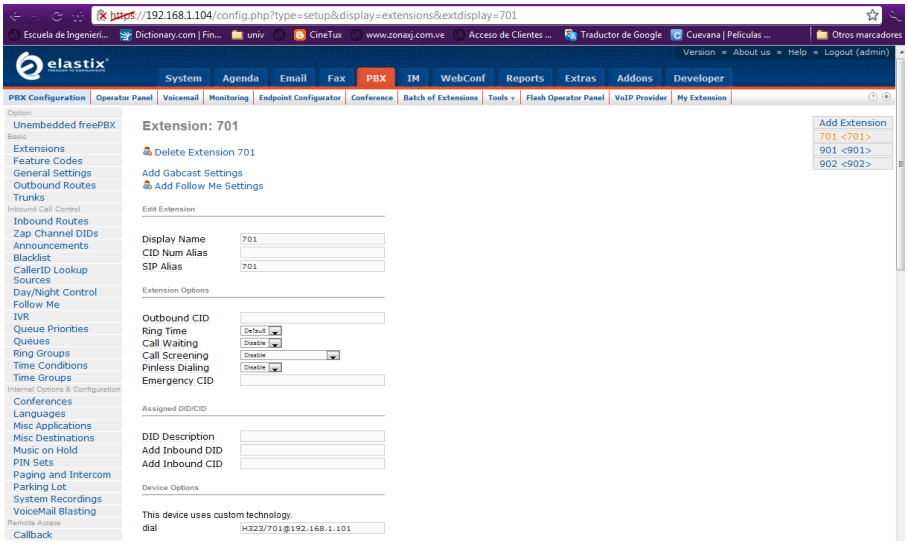


Figura 3.16- Añadiendo un Terminal H.323 en Elastix

Fuente: Elaboración Propia

Finalmente, para que Elastix reconozca los terminales añadidos, se debe hacer click en el link superior “Apply Configurations Changes Here” que permite guardar los cambios cambios aplicados.

IV.2 Escenario B: Para la construcción del Escenario B, se ejecutó un procedimiento muy similar al realizado en el Escenario A, con ciertas modificaciones, las cuales son las siguientes:

- Se elimina la Máquina que contiene el Gatekeeper GnuGK
- Se conservan las configuraciones predispuestas en el Escenario A para los Softphones tanto SIP como H.323; a excepción de los campos referidos al servidor, que serán reemplazados con la dirección IP correspondiente a Elastix
- Dentro del archivo de configuración h323.conf se comentaron las líneas de códigos referidas al Gatekeeper a fin de desactivarlas.
- Se conservó el mismo procedimiento aplicado al registro de terminales SIP y H.323 dentro de Elastix, a excepción de los campos referidos a la tecnología utilizada por los terminales H.323, donde la dirección del gatekeeper se sustituyó por la dirección IP de la máquina donde se encuentra cada terminal H.323 respectivamente (para el caso de la conexión con una MCU, se sustituirá, en consecuencia, por la dirección donde se encuentre la MCU)
- Dada la eliminación del GnuGK, para lograr la transmisión de audio y video entre los terminales H.323 y SIP (y viceversa), es necesaria la creación de un troncal que porte el canal H.323 contenido en Asterisk y que a su vez sea independiente de los demás medios contenidos en el software, posibilitando así, el direccionamiento y la comunicación dentro de los terminales a los cuales se desea conectar.

3.2.1 Configuración del Troncal y las Rutas de Entrada/Salida: En primer lugar se debe configurar el troncal H.323, accediendo a la sección “Trunks” dentro de la configuración de la “PBX”. Una vez allí se elige que tipo de troncal que se desea añadir, para este caso será un troncal “custom” H.323.

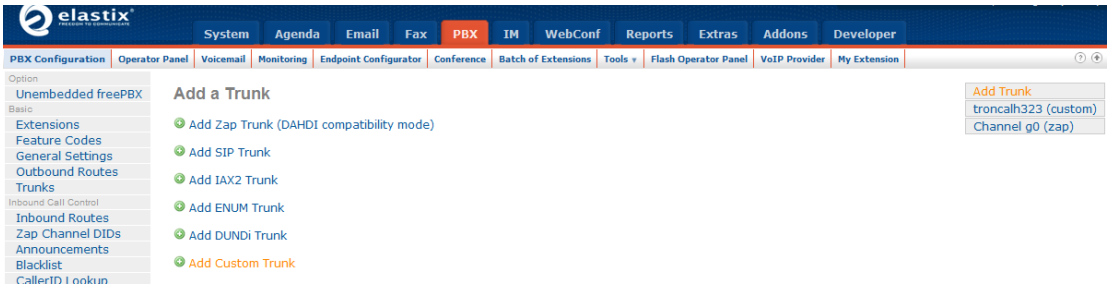


Figura 3.17- Añadiendo un Troncal H.323 en Elastix

Fuente: Elaboración Propia

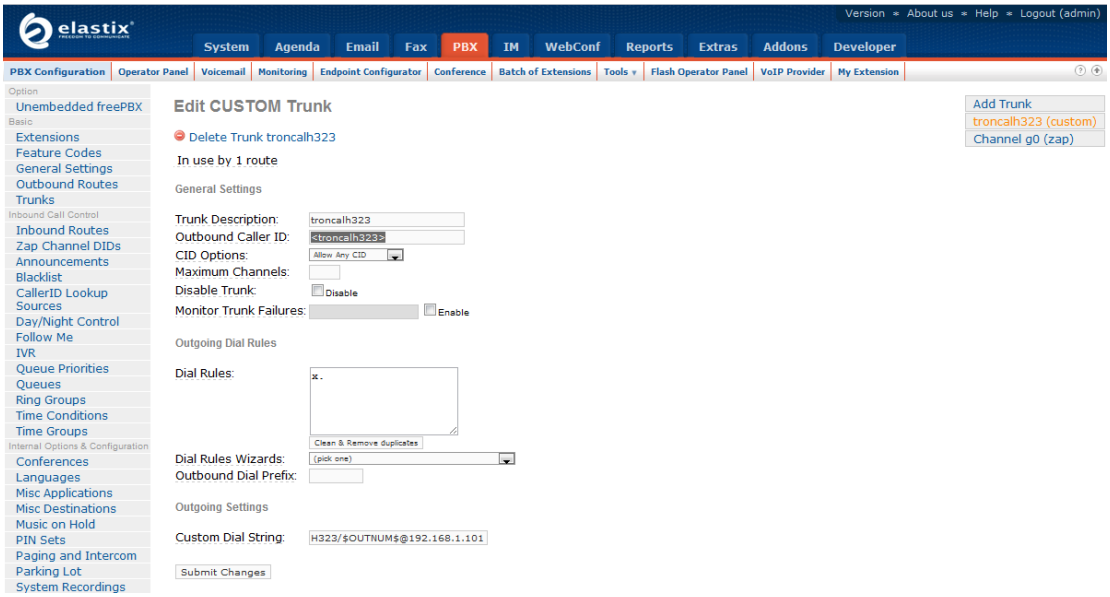


Figura 3.18- Configuración de un Troncal H.323 en Elastix

Fuente: Elaboración Propia

Los campos a configurar dentro del troncal son los siguientes:

- Trunk Description: en este campo se coloca la descripción y nombre del troncal. Se utilizó troncalh323 para este caso
- Outbound Caller ID: contiene la identificación de la ruta de salida utilizada por el troncal. Se utilizó el mismo nombre de descripción del troncal <troncalh323>

- Dial rules: en este campo se especifica como las llamadas serán direccionadas dentro del troncal; es decir; se describe las reglas de marcación utilizadas por el mismo. Se coloca X. que indica que uno o más dígitos del 0 al 9 están incluidos dentro del troncal. (para mayor información acerca de la configuración, la misma página posee una guía automática bien detallada de cada campo específico, en cualquier caso se puede visitar la documentación incluida en la página oficial www.elastix.org)
- Custom Dial String: este campo especifica que el troncal utilizará el canal H.323 como medio de transmisión y el usuario final. La sintáxis es: H323/$OUTNUM$@ dirección ip del usuario final.

Para finalizar la configuración de la ruta se deben guardar los cambios y hacer click en el link de aplicar cambios, para que Elastix admita las nuevas configuraciones. Por último, para lograr conectar cualquier terminal SIP o H.323 previamente registrado, con otro terminal SIP o H.323, se deben asignar las rutas salientes y entrantes de Elastix. En la sección de configuración se debe acceder a la pestaña de "Outbound Routes" y se procede a abrir la ruta "0_9 outside" que tiene incluida por defecto Elastix. En ella se modifica lo siguiente:

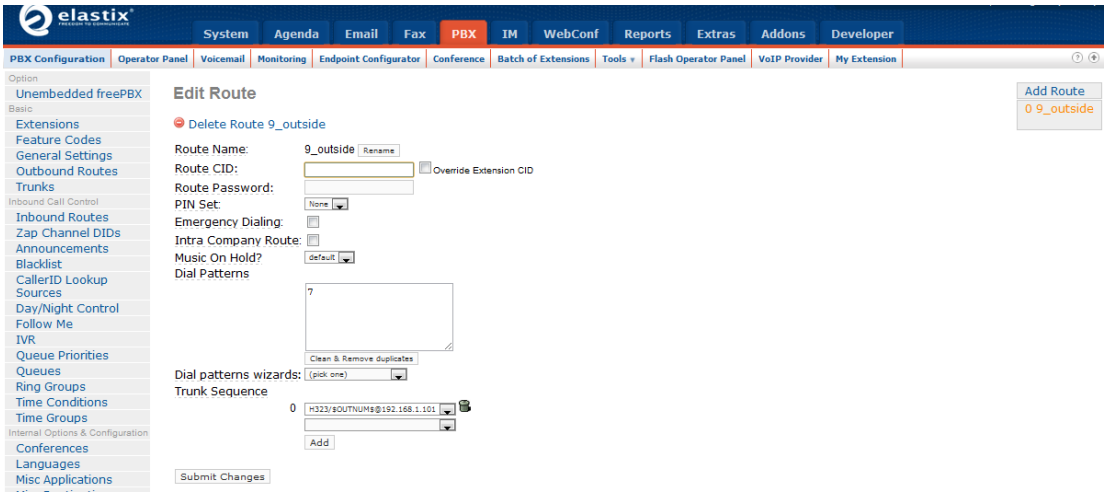


Figura 3.19- Configuración de una Ruta Saliente H.323 en Elastix

Fuente: Elaboración Propia

- Dial Pattern: este campo especifica la marcación que caracteriza la ruta. Como se quiere que el troncal sea H.323, la ruta saliente deberá especificar a todos aquellos terminales involucrados en el ambiente H.323, los cuales se especificaron con la numeración 7XX. Por tanto la sintáxis en este caso será 7. El cual le indica a Elastix que una vez marcado el dial 7, se deberá tomar la ruta saliente que contiene el troncal H.323
- Trunk Sequence: define el troncal que debe tomar la ruta. En este caso se selecciona la pestaña con el troncal definido en la sección anterior.

En el caso de las rutas entrantes, éstas definirán la comunicación hacia los terminales SIP; para configurar una ruta de entrada en el panel de configuración en la pestaña de "Inbound Routes" se modifican los campos siguientes:

- Description: descripción de la ruta. Se coloca el nombre correspondiente a la ruta entrante que identificará las llamadas de los terminales H.323 hacia los terminales SIP
- Caller ID number: define la identificación de la ruta entrante. Es el nombre de la ruta entrante que se mostrará en pantalla.
- Language: ES para el idioma español
- Set destination: aquí se indica el destino de las llamadas que tomen esta ruta. En este caso se selecciona las pestañas con las extensiones SIP.

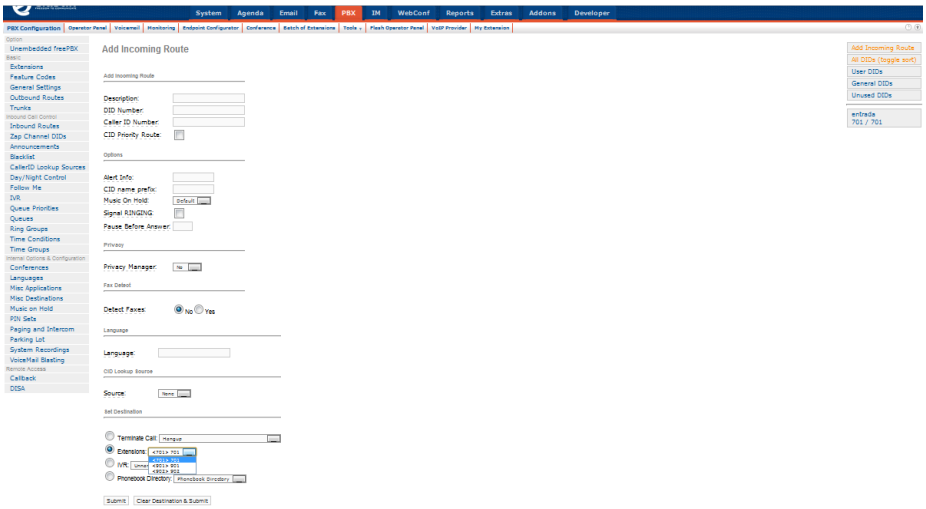


Figura 3.20- Configuración de una Ruta Entrante SIP en Elastix

Fuente: Elaboración Propia

Para finalizar, al igual que los casos anteriores, se deben guardar los cambios y posteriormente actualizarlos haciendo click en el link "apply configurations changes here" para así Elástix los logre admitir dentro de su configuración.

3.5 Fase 5. Implementación del Software: Se realizaron los ensamblajes finales así como también se implementaron los esquemas y especificaciones tanto de la interfaz creada como del software y del sistema en su totalidad para ambos escenarios propuestos y descritos en detalle en las fases anteriores.

A fin de lograr el modo más adecuado de acondicionar el Gateway a la red de datos de la Universidad Central de Venezuela, se decidió que el Escenario B, era el más apropiado a ser implementado, ya que posee todas las características necesarias de estabilidad, flexibilidad y seguridad requeridas, atendiendo a todas las particularidades de la red. El porqué de esta decisión, radica en tres puntos importantes: en principio, se suprime el Gatekeeper, lo cual lo convierte en una implementación más eficiente y compacta, ya que se está eliminando un punto de posible error dentro de la arquitectura. En segundo lugar, al implementar el Escenario A, el GnuGK presentó en muchas ocasiones fallas e intermitencias en la transmisión introduciendo inestabilidad al sistema, en contraste al Escenario B, que se caracteriza por un diseño más robusto y estable. Por último, también influye el tema de seguridad y la practicidad, el hecho de

que el Escenario B, posea troncales dedicadas a la transmisión entre los terminales, posibilita la configuración del registro de las extensiones asignándole códigos (rangos de números) destinados a los terminales que se deseen conectar, controlando así, la capacidad del canal de información y discriminando el ingreso de usuarios a la red. No obstante, vale la pena mencionar que la universidad cuenta también con un administrador de red que también puede prestar las funciones de seguridad y control nombradas anteriormente, tal es el caso de Cisco Call Manager.

Otro punto importante, es que al realizar las pruebas iniciales de audio y video utilizando a Elastix como Gateway y como clientes: X-Lite para SIP y Ekiga para H.323, se observó que los códec de video no eran compatibles entre sí, esto debido a que el softphone X-Lite únicamente trabaja con los códecs H.263 y no con el códec H.261, el cual es el único que logra portar el canal H.323 instalado en Elastix para la transmisión de video. Por tanto, se procedió a utilizar a Ekiga (instalado en un ordenador con Ubuntu como sistema operativo) tanto como cliente H.323 como cliente SIP, ya que éste programa posibilita el manejo de los códecs requeridos.

Finalmente, al ser implementado el escenario elegido, se realizaron pruebas pilotos de llamadas entre los terminales involucrados a fin de comprobar el correcto funcionamiento del software. Dichas pruebas se especifican en una fase más adelante.

3.6 Fase 6. Adaptación a la Red de Datos de la UCV: Una vez elegido el escenario más propicio para la transmisión, de su posterior implementación y de haber comprobado el correcto funcionamiento del Gateway; se realizaron las adaptaciones externas necesarias en el Laboratorio de la Escuela de Ingeniería Eléctrica, con la finalidad de cubrir todos los requerimientos trazados, permitiendo orientar el código al alcance y disposición de la comunidad universitaria.

Para ello, fue necesario el acondicionamiento de los equipos del Laboratorio, en particular, la computadora con mayor capacidad de memoria y de mayor velocidad de procesamiento, proporcionada por la universidad (véase “Situación Actual de la Red de Datos” en la “Fase 2” del presente trabajo), donde se realizó la instalación de

las librerías, dependencias y el software que sustenta al Gateway en sí, tal como se describió en las fase de implementación. Como se mencionó en apartados anteriores, los equipos existentes en el Laboratorio, no cumplen con los requerimientos necesarios para el correcto funcionamiento del Gateway; por tanto se procedió a acondicionar la máquina en cuestión, añadiéndole equipos periféricos como auriculares, micrófonos y parlantes de bajo costo que fueran compatibles con el software libre involucrado; a fin de proporcionar al menos los servicios de transmisión de audio entre los equipos telefónicos SIP existentes en el Laboratorio, los softphone previamente instalados, y el resto de los equipos de conferencia basados en protocolo H.323.

Asimismo, se configuraron otras dos computadoras adicionales con los programas pertinentes, para que trabajaran como clientes SIP y H.323 respectivamente, y de esta forma recrear el Escenario B planteado anteriormente dentro del entorno universitario. Cabe destacar que fueron tomados en cuenta, todos y cada uno de los equipos necesarios para la conexión; es decir, fue preparado todo el cableado de red necesario para la conexión entre las computadoras y el servidor de la Universidad; además, se dispuso un Switch de 16 puertos para abastecer a cada uno de los elementos conformantes del sistema, asegurando así la interconexión entre los ordenadores.

Adicionalmente, se realizó una implementación del Gateway junto con la MCU realizada por otro estudiante de la Escuela. Esto, con la finalidad de establecer una sesión simultánea entre los diversos equipos de videoconferencia existentes en la universidad; tanto los Polycom como los softphone instalados previamente; comprobando así, la compatibilidad del software y la interoperabilidad del mismo en la red de datos. Es importante mencionar, que para este caso donde se interconectan el Gateway con la MCU, debido a la insuficiencia de equipos en el laboratorio (un ordenador para el Gateway uno para la MCU más los ordenadores requeridos por los clientes y terminales junto con los equipos de videoconferencia) y el conflicto por no contar con un hardware con suficiente capacidad para soportar la implementación, sólo se pudo comprobar el funcionamiento del audio en las conexiones entre los equipos SIP y los terminales H.323 a través del MCU.

3.7 Fase 7. Validación y Pruebas: En esta fase, se efectuaron las pruebas requeridas y necesarias de validación del software a fin de verificar la interoperabilidad del mismo con el código abierto y con la plataforma de videoconferencia de la red de datos. Dentro de estas pruebas se incluyen: pruebas iniciales de cada ambiente de forma independiente (Ambiente SIP y Ambiente H.323), pruebas de desempeño del Gateway en audio y video y por último las pruebas de interconexión del Gateway con la MCU de la universidad.

Adicionalmente, se realizó un análisis del servicio proporcionado por el Gateway instalado, mediante el uso de las herramientas Iperf y Jperf, las cuales permiten realizar una medición en la calidad de videoconferencias y además cuentan con una interfaz gráfica. Las mismas fueron instaladas en los extremos de la red donde se encontraban tanto los terminales SIP como los H.323 así como también en el ordenador donde se encontraba el Gateway. Los resultados arrojados por el programa, como son ancho de banda, tasa de transmisión, etc; se muestran y analizan en el capítulo siguiente. El proceso de instalación de esta herramienta y su configuración y manejo se encuentra descrito en la sección de anexos.

3.8. Fase 8. Elaboración del Informe Final: En esta etapa, el software fue correctamente documentado, con sus respectivos fragmentos constitutivos. Se describieron los diversos escenarios de implementación, así como paso a paso, cada uno de los procedimientos del desarrollo de los módulos del software, organizados por etapas con sus respectivos reportes, incluyendo las contribuciones del proyecto. Así mismo, se realizó la redacción del informe final bajo todos los lineamientos y estatutos que rigen la elaboración de un Trabajo de Grado en la Escuela de Ingeniería Eléctrica, dando como resultado el presente Trabajo Especial de Grado.

CAPÍTULO IV

4. RESULTADOS

En este capítulo se muestran los resultados obtenidos luego de haber desarrollado cada una de las etapas y procesos definidos y explicados en los capítulos anteriores. Las pruebas se ejecutaron de acuerdo al orden de implementación desarrollado en el marco metodológico y se muestran en detalle a continuación.

4.1.- Pruebas Iniciales: En una primera fase de implementación de los Escenarios descritos anteriormente, se comenzaron probando cada ambiente de forma independiente, para comprobar su correcto funcionamiento.

4.1.1 Pruebas Ambiente SIP: En este ambiente fueron conectados dos softphones X-Lite a través de Elastix, añadiendo en la configuración de los softphones el soporte de video. Los resultados fueron exitosos y se muestran en la figura a continuación.

Figura 4.1.- Prueba de Llamada Ambiente SIP-SIP a través de Elastix con softphone X-Lite.

Fuente: Elaboración Propia

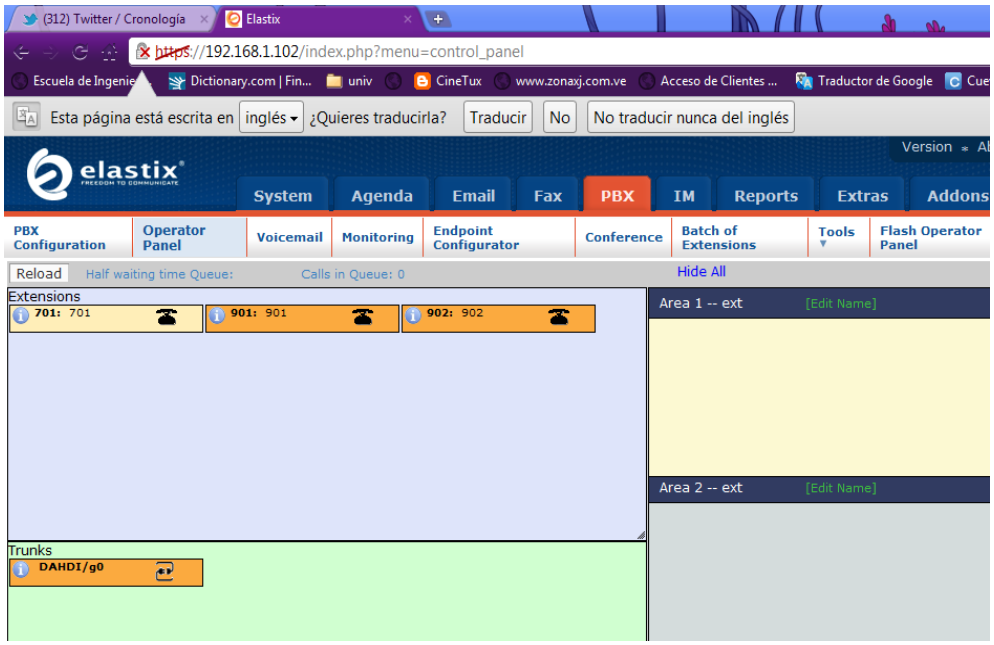


Figura 4.2.- Prueba de Llamada Ambiente SIP-SIP. Pantalla de visualización de Elastix durante la comunicación.

Fuente: Elaboración Propia

No obstante, se pudo constatar con esta prueba que el softphone X-Lite únicamente transmite video a través del códec H.263, por lo cual, dicho softphone sólo se utilizó para las prueba de traducción SIP/H.323 de audio y no de video, dado que el canal H.323 construido en Elastix sólo posee soporte en video para el códec H.261. En consecuencia a lo anterior, para las pruebas de traducción SIP/H.323 con video, se sustituyó por el software Ekiga, el cual si soporta el códec H.261.

4.1.2 Pruebas Ambiente H.323: Para la construcción de este ambiente se utilizaron como terminales H.323, en principio dos computadores con el softphone Yate y se enrutaba la llamada a través de un Gatekeeper GnuGK instalado en otro ordenador; ésto a fin de comprobar el correcto funcionamiento de una llamada H.323 mediante la implementación de un GnuGK. En segundo lugar, se tomaron dos computadores con el software Ekiga instalado, y se realizó una llamada directa H.323 entre los dos terminales. Ambos escenarios funcionaron a la perfección y los resultados se muestran a continuación.

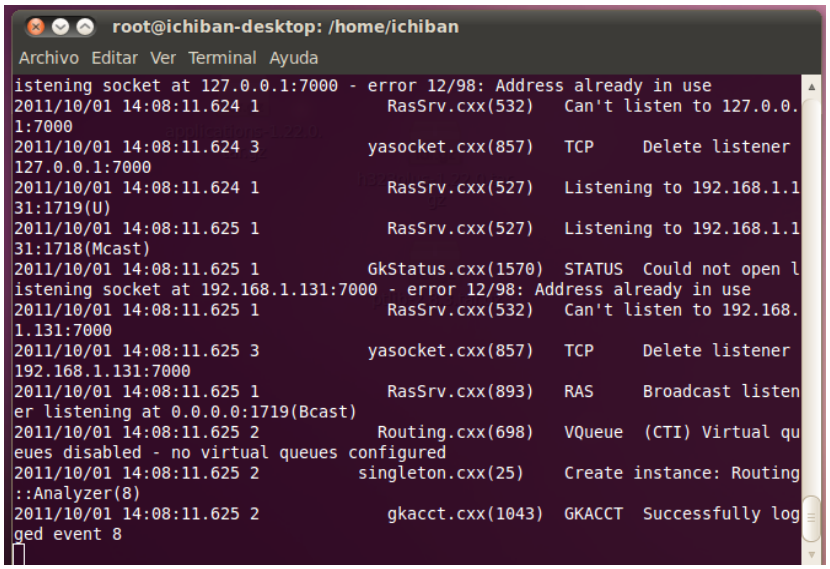


Figura 4.3.- Prueba de Llamada Ambiente H.323-H.323. Pantalla de visualización del GnuGK durante la comunicación.

Fuente: Elaboración Propia

Figura 4.4.- Prueba de Llamada Ambiente H.323-H.323 entre softphone Ekiga enrutado con un Gatekeeper

Fuente: Elaboración Propia

4.2.- Pruebas de Escenarios Propuestos: Una vez comprobado el funcionamiento de los ambientes de forma independiente, se procedió a testear cada uno de los escenarios implementados en el marco metodológico.

4.2.1 Pruebas Escenario A: En principio, se realizó el montaje del Escenario A para realizar pruebas de audio, el cual contenía: un cliente H.323 (softphone Yate), un cliente SIP (softphone X-Lite), un Gatekeeper (GnuGK) y el Gateway (Elastix). Los resultados no fueron muy satisfactorios, ya que a pesar que se establecía la comunicación, el Gatekeeper operaba de forma intermitente y en muchas ocasiones colgaba la llamada, de hecho al momento de realizar las pruebas de video para este escenario (con ambos Softphone Ekiga, uno configurado para SIP y otro configurado para H.323), la comunicación entre el Gateway Elastix y el Gatekeeper se interrumpió, dejando de funcionar repentinamente, obligando a compilar e instalar de nuevo ambos software para poder probar el video a través de los clientes Ekiga/SIP y Ekiga/H.323. De allí, que este escenario fuera descartado como solución de implementación final. Los resultados se muestran a continuación.

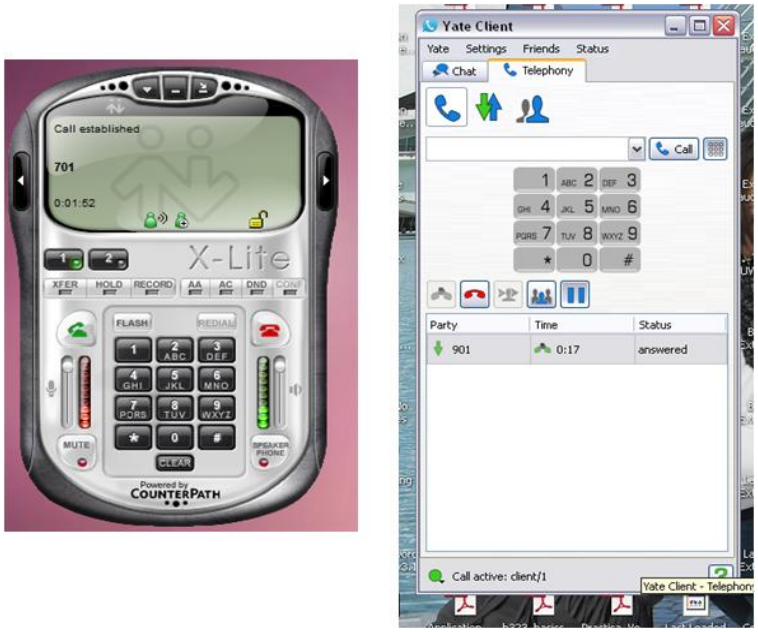


Figura 4.5.- Prueba de Escenario A en Audio

Fuente: Elaboración Propia

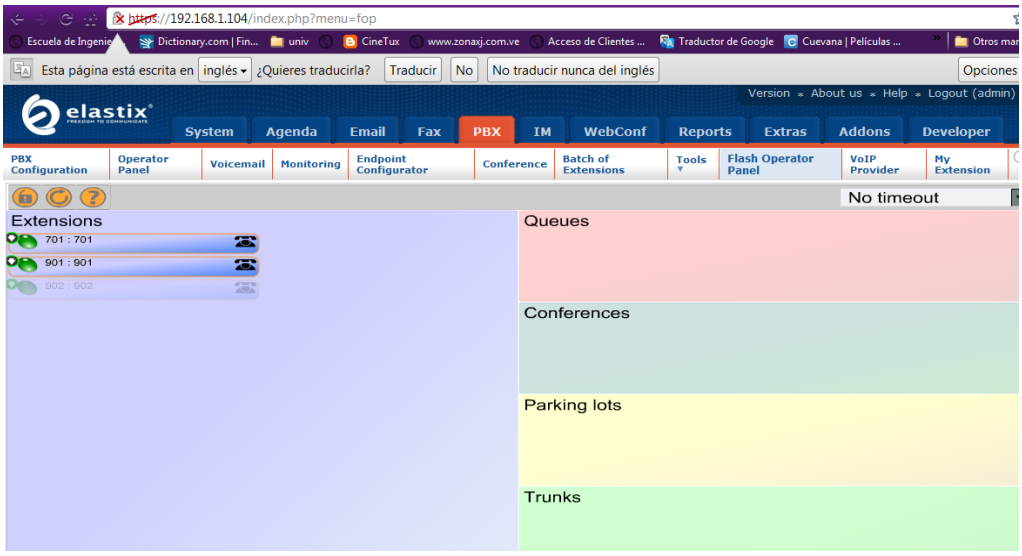


Figura 4.6.- Prueba de Escenario A en Audio Pantalla de Visualización de Elastix durante la comunicación

Fuente: Elaboración Propia

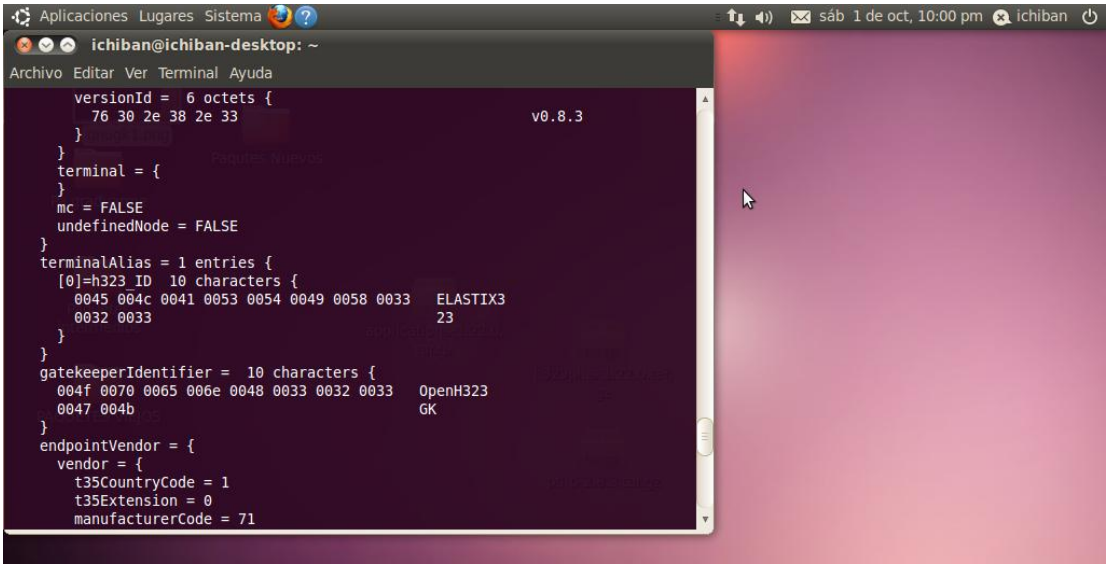


Figura 4.7.- Prueba de Escenario A en Audio Pantalla de Visualización del Gatekeeper durante la comunicación. Registro de Elastix dentro del GnuGK

Fuente: Elaboración Propia

4.2.2 Pruebas Escenario B: Este se presentó como una implementación más estable, robusta y segura, además proporcionó un ambiente propicio para el enrutamiento y la señalización en la traducción de ambos protocolos. Recordando, el Escenario B lo constituyen: un ordenador con Elastix instalado, con la inclusión de un Troncal H.323; dos computadoras cliente: terminal H.323 y terminal SIP. Del mismo modo que en pruebas anteriores, se comenzó por el testeo del Gateway en audio, utilizando X-Lite y Yate para conformar la arquitectura. Los resultados fueron exitosos y en contraste con el Escenario A, la aplicación se mantuvo estable durante toda la comunicación, y en las comunicaciones sucesivas realizadas a modo de prueba. Adicionalmente, a través de la interfaz web de Elastix, mediante su panel de operación, se pudo apreciar, el funcionamiento de cada elemento en la red, bien sea, el troncal, la ruta de salida o entrada y los softphone registrados.

Figura 4.8.- Equipo Servidor de 4GB de Memoria RAM donde fue implementado el Gateway

Fuente: Elaboración Propia

Figura 4.9.- Prueba de Escenario B en Audio.

Fuente: Elaboración Propia

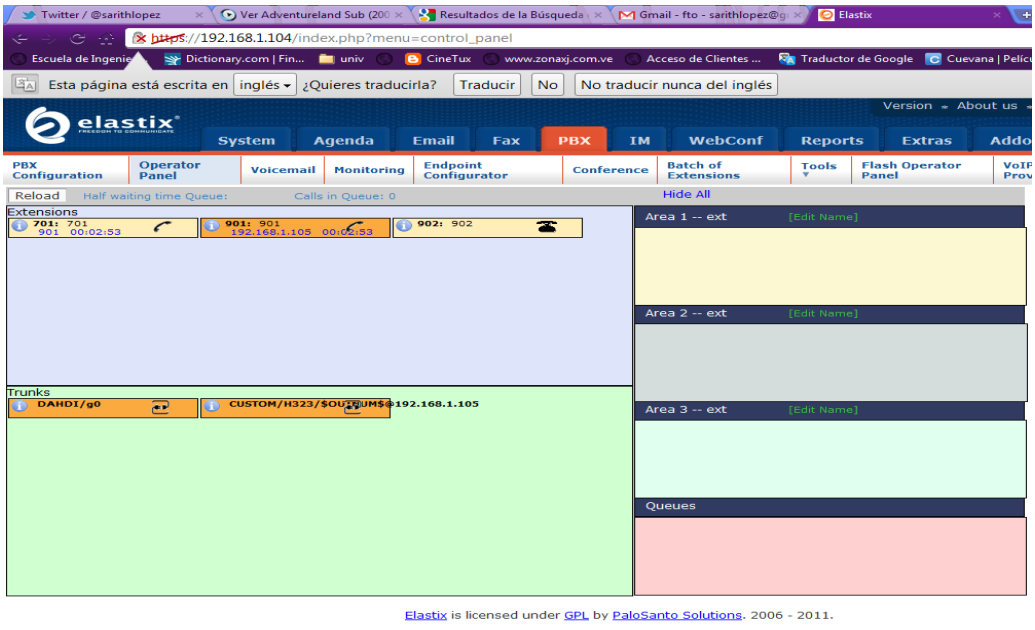


Figura 4.10.- Prueba de Escenario B en Audio. Interfaz Gáfica de Elástix durante la comunicación.

Fuente: Elaboración Propia

Posteriormente, se sustituyeron ambos clientes por el software Ekiga para poder transmitir video y audio en la comunicación. Los resultados fueron igualmente exitosos. Sin embargo, en esta prueba se verificó que cuando se realizaban los ensayos de audio y video a través de una máquina virtual con una memoria RAM inferior a 2GB, se imposibilitaba la transmisión de video, y la comunicación se interrumpía, por lo cual, se decidió, cambiar el Elastix a una máquina con 4GB de RAM e incrementar la memoria de la máquina virtual, para lograr la conexión adecuada.

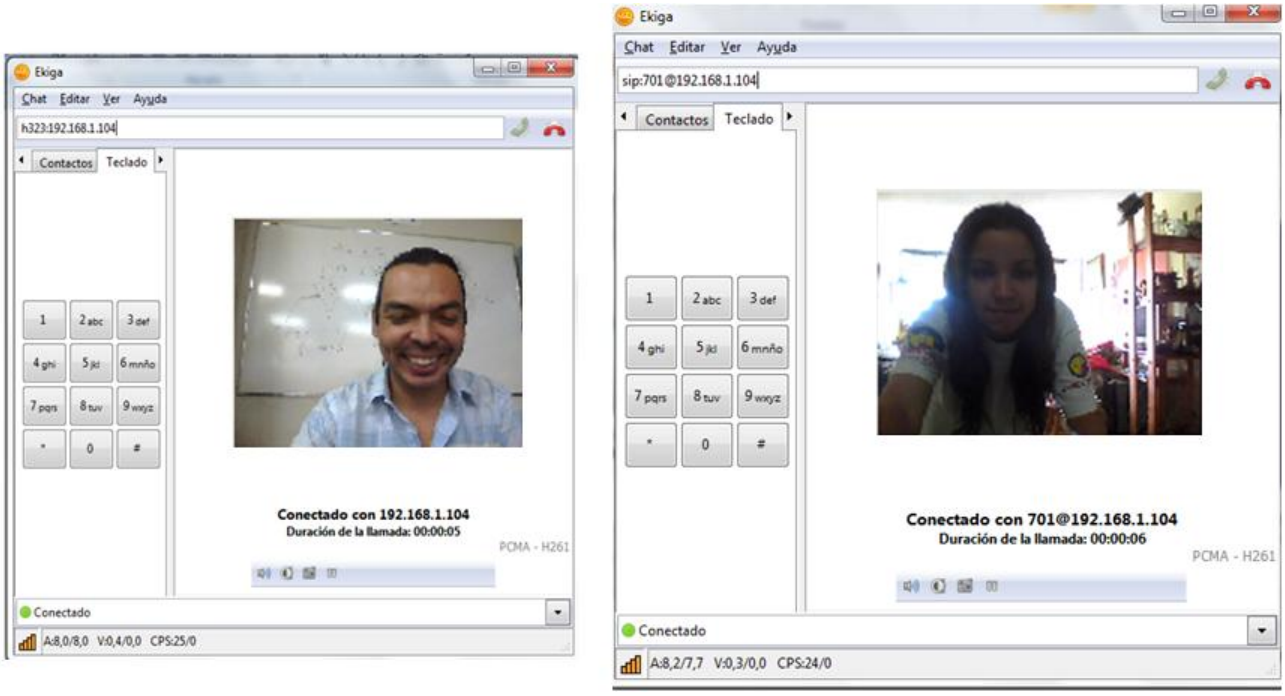


Figura 4.11.- Prueba de Escenario B en Audio y Video.

Fuente: Elaboración Propia

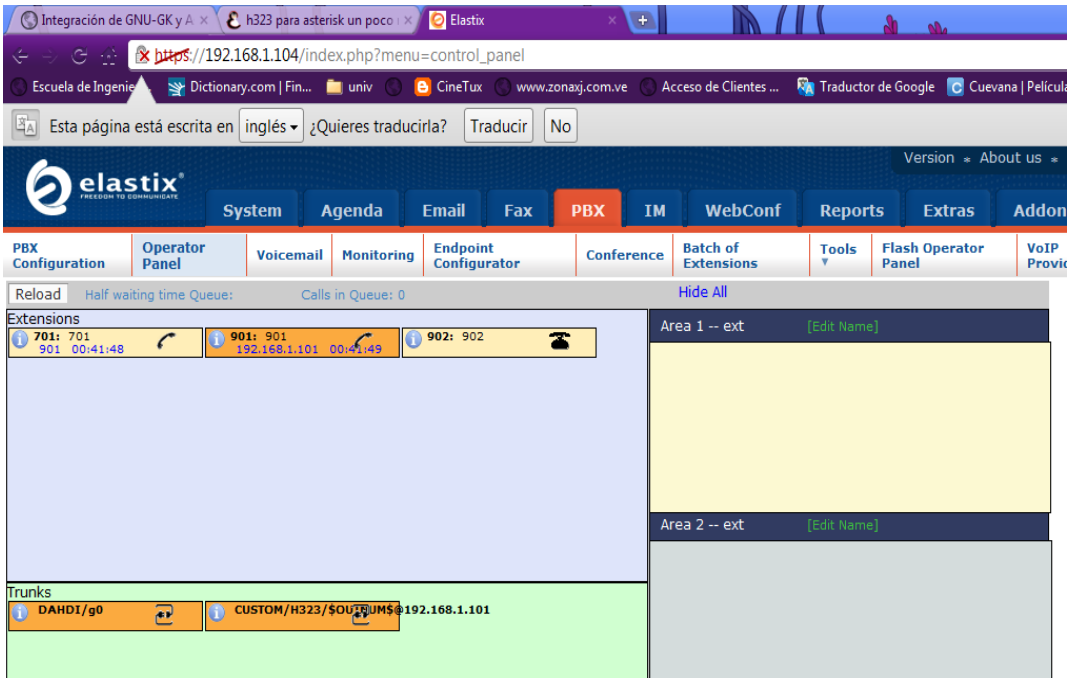


Figura 4.12.- Prueba de Escenario B en Audio y Video. Interfaz Gáfica de Elástix durante la comunicación.

Fuente: Elaboración Propia

4.3.- Pruebas de Adaptación a la Red de Datos de la UCV: En este apartado se especifican las pruebas realizadas con los equipos proporcionados por el Laboratorio de Ingeniería Eléctrica. Mientras se efectuaba la implementación de los equipos, al realizar la interconexión entre ellos y el servidor de internet de la universidad, se presentaron diversos conflictos de enrutamiento, ya que al conectar más de dos ordenadores, las direcciones IP asignadas a las computadoras variaban, convirtiéndose en direcciones privadas (172.xxx.xxx.xxx), lo que ocasionaba un impedimento en la comunicación. Para solucionar ésto, en principio fueron configuradas cada una de las máquinas con una IP estática; no obstante, dado lo engorroso de este proceso, se dispuso de un Router Cisco (proporcionado por el Laboratorio de Comunicaciones de la Universidad), el cual suministró las direcciones IP a cada una de las computadoras involucradas, asegurando la interconexión entre ellas.

Figura 4.13- Adaptación a la Red de Datos de la UCV. Equipos Existentes utilizados en la Implementación

Fuente: Elaboración Propia

Luego de ejecutados los pasos de configuración pertinentes, y de haber instalado el Gateway, recreando el Escenario B en el entorno universitario, se procedió a realizar las llamadas de prueba entre el softphone X-Lite SIP y el softphone Ekiga H.323. Los resultados arrojados por estos ensayos fueron positivos, del mismo modo que en casos anteriores, sin embargo, como se mencionó anteriormente, debido a la baja capacidad de procesamiento de las computadoras existentes en el Laboratorio de la UCV, sólo fue posible realizar llamadas de voz de SIP a H.323 y viceversa. La presencia de este conflicto se debe principalmente a la complejidad de las redes H.323; éstas aunque no obligan el uso de códecs de audio y video de menor compresión; contienen por defecto dentro de las librerías y archivos constitutivos del paquete OpenH323 como único códec de video incluido, el códec H.261 (códec instaurado sobre el canal H.323 de Elastix), de hecho, para lograr activar dicho códec dentro del canal, éste tuvo que ser exportado hacia la carpeta donde estaban contenido los códecs de audio.

El códec H.261, aunque sea de menor compresión, está diseñado con librerías que son muy densas y requieren de una compilación más compleja y eficiente, a diferencia del códec H.263, el cual contiene pocas librerías dentro de sus archivos de configuración y es más práctico y flexible en cuanto a compilación se refiere, ofreciendo además una alta y mejorada calidad de video; de hecho, éste puede ser descargado como pluggin adicional desde las páginas de los proyectos Xiph.org (de allí que sea el códec de video más utilizado en la actualidad). Lo anterior se traduce en que para lograr implementar el video mediante el Gateway en el Laboratorio de la universidad, las computadoras dispuestas para este fin, deben estar provistas de gran cantidad de memoria RAM y procesadores más veloces. No obstante, la voz (audio) no necesita de tanto trabajo por parte de las máquinas, de allí que se haya podido lograr la traducción del audio entre terminales SIP y H.323 dentro de este entorno.

Figura 4.14.- Adaptación a la Red de Datos de la UCV. Pruebas de llamada SIP-H.323 (Audio) sobre el Gateway implementado en los Equipos de la UCV

Fuente: Elaboración Propia

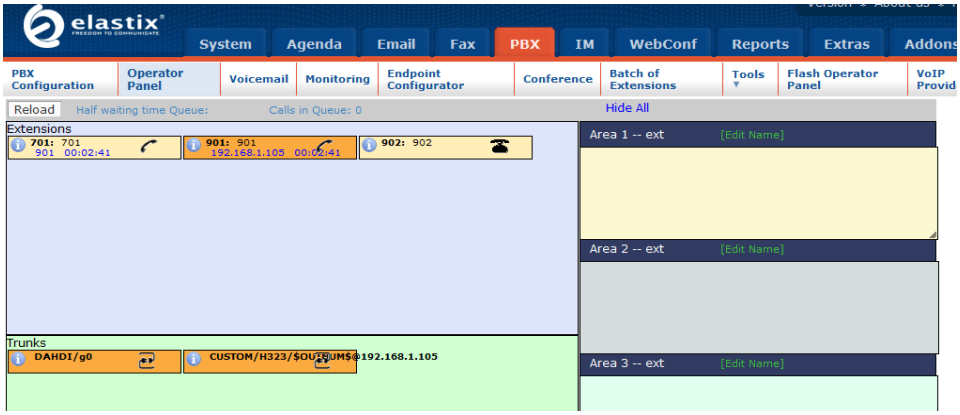


Figura 4.15.- Adaptación a la Red de Datos de la UCV. Pantalla de Visualización de Elastix durante la comunicación implementado en los Equipos de la UCV
Fuente: Elaboración Propia

4.4.- Pruebas con la MCU implementado en la UCV: Por último, se interconectó el Gateway desarrollado junto con la MCU implementada en la universidad. Con este ensayo, se comprueba la interoperabilidad del software desarrollado junto con todos los Equipos tanto SIP (softphone y Teléfonos SIP IP) como H.323 (equipos de videoconferencia Polycom) existentes en el entorno universitario; evidenciando la compatibilidad proporcionada por el Gateway diseñado.

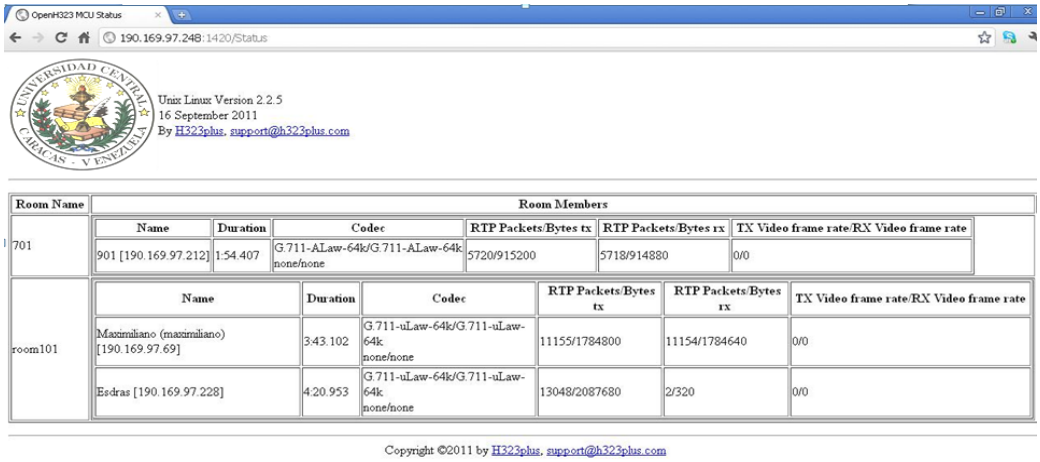


Figura 4.16.- Estatus de la MCU durante la comunicación entre equipos SIP y terminales H.323 (Audio) interconectando el Gateway con la MCU implementada en la UCV.Fuente: Elaboración Propia

Cabe destacar, que en la primera llamada realizada, el equipo SIP se conecta al MCU en una sala diferente (véase figura 4.15), esto ocurre debido a que por defecto, el troncal del Gateway está direccionado al MCU con el nombre de 701, lo cual posteriormente se corrigió, cambiándole el nombre por la sala de conferencia correspondiente.

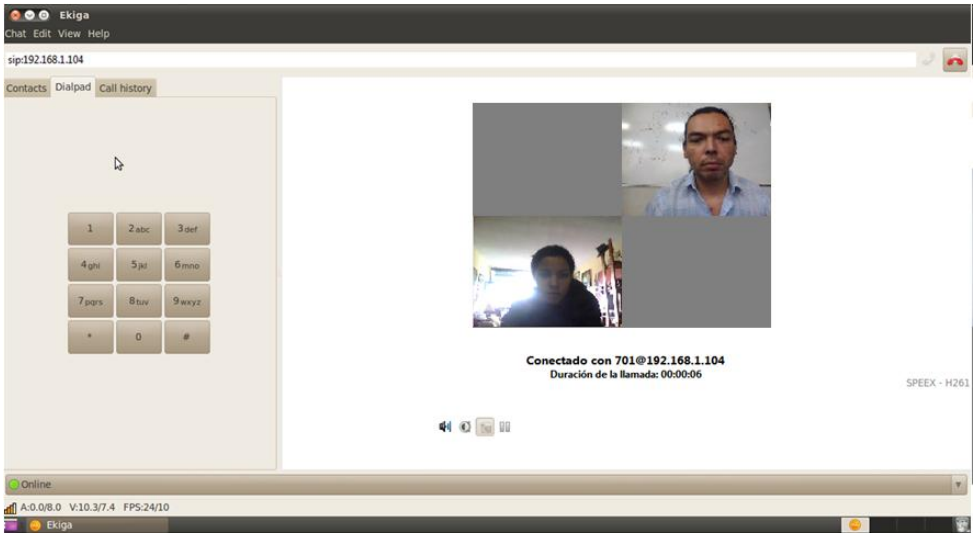


Figura 4.17.- Prueba de llamada entre equipos SIP y terminales H.323 (Audio y Video) interconectando el Gateway con la MCU implementada en la UCV con 2 participantes. Fuente: Elaboración Propia

Figura 4.18.- Estatus de la MCU durante la comunicación entre equipos SIP y terminales H.323 interconectando el Gateway con la MCU implementada en la UCV.

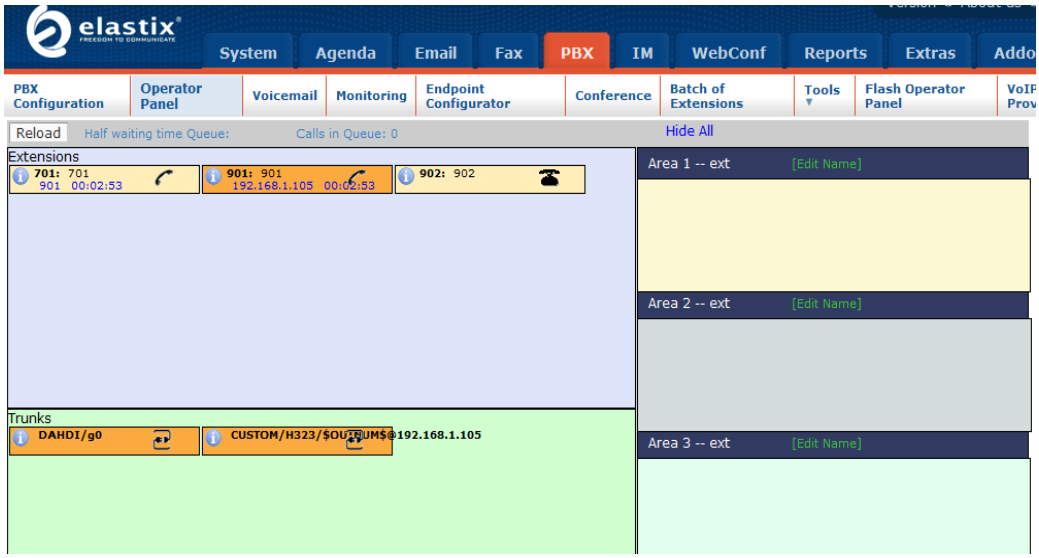


Figura 4.19.- Estatus del Gateway durante la comunicación entre equipos SIP y terminales H.323 (Audio y Video) interconectando el Gateway con la MCU implementada en la UCV.Fuente: Elaboración Propia

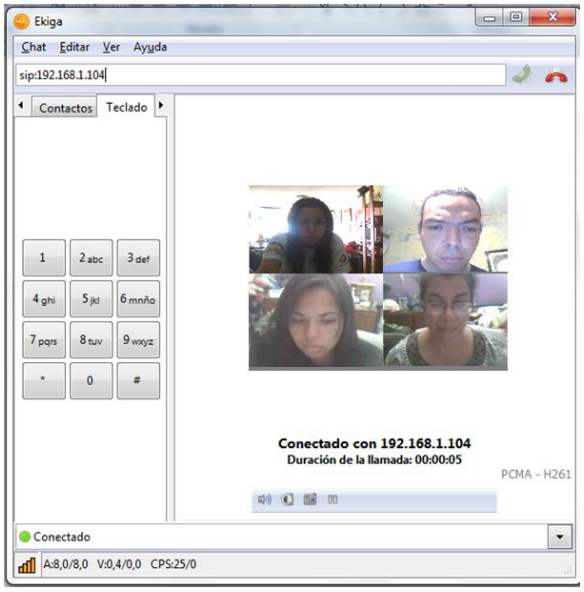


Figura 4.20.- Prueba de llamada entre equipos SIP y terminales H.323 (Audio y Video) interconectando el Gateway con la MCU implementada en la UCV con 4 participantes. Fuente: Elaboración Propia

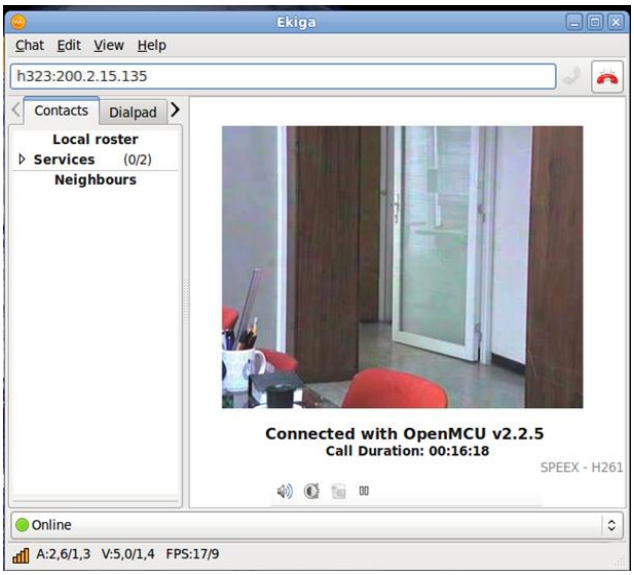


Figura 4.21.- Prueba de llamada entre equipos SIP y Equipo Polycom (Audio y Video) interconectando el Gateway con la MCU implementada en la UCV. Fuente: Elaboración Propia

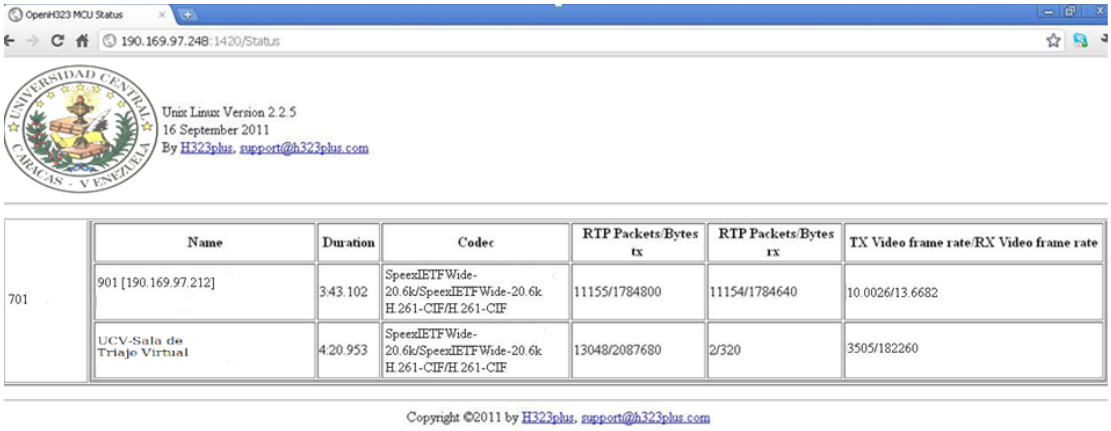


Figura 4.22.- Estatus del MCU durante la comunicación entre equipos SIP y Equipo Polycom (Audio y Video) interconectando el Gateway con la MCU de la UCV. Fuente: Elaboración Propia

4.5.- Validación y Pruebas de Desempeño: Durante la ejecución de todas y cada una de las pruebas anteriores, se realizó un monitoreo de las llamadas mediante la instalación en cada uno de los terminales SIP y H.323 involucrados de las herramientas Jperf e Iperf. Mediante estas herramientas se pudo constatar con precisión, el establecimiento y la transmisión en detalle de cada una de las llamadas. El monitoreo abarcó desde los paquetes perdidos, hasta la calidad de transmisión de las comunicaciones; y se dividió en dos sondeos principales: un testeo de las comunicaciones a través del Gateway con audio únicamente y un testeo de transmisión bajo soporte de audio y video. Los resultados arrojados por ambos sondeos, fueron tabulados respectivamente y se muestran a continuación.

Tabla 4.1.- Resultados del programa Iperf y Jperf sobre comunicaciones SIP/H.323 en Audio.

Fuente: Elaboración Propia

Intervalos Datagramas	Bandwidth (Mbits/s)	Latencia (ms)	Jitter (ms)	Paquetes Perdidos	Paquetes Totales	Pérdida de paquetes (%)
0.0-1.0sec	7.78	1.11	0.113	12	944	1.27
1.0-2.0sec	8.00	1.11	0.177	0	770	0.00
2.0-3.0sec	10.00	1.12	1.249	0	769	0.00
3.0-4.0sec	8.98	1.11	1.188	44	851	5.17
4.0-5.0sec	8.00	1.12	0.032	17	870	1.95
Promedio	8.55	1.11	0,551	14.16	840.80	1.67

Tabla 4.2.- Resultados del programa Iperf y Jperf sobre comunicaciones SIP/H.323 en Audio y Video.

Fuente: Elaboración Propia

Intervalos Datagramas	Bandwidth (Mbits/s)	Latencia (ms)	Jitter (ms)	Paquetes Perdidos	Paquetes Totales	Pérdida de paquetes (%)
0.0-1.0sec	7.78	1.12	0.141	0	944	0.00
1.0-2.0sec	7.78	1.23	0.147	0	770	0.00
2.0-3.0sec	8.00	1.18	2.249	14	770	1.81
3.0-4.0sec	10.00	1.17	1.788	6	850	0.70
4.0-5.0sec	10.00	1.18	0.113	11	851	1.29
Promedio	8.71	1.17	0.887	6.20	837	0.76

Analizando los resultados obtenidos en las tablas 4.1 y 4.2 de las mediciones con el Gateway, se puede verificar lo siguiente:

- El porcentaje de pérdidas de paquetes tanto para la comunicación de audio como la comunicación multimedia se mantuvo por debajo del 2%, lo cual es un promedio aceptable y cumple con la normativa referente a la pérdida de paquetes sobre sistema de videoconferencia señalada en el capítulo anterior. No obstante, se aprecia en la tabla 4.1 que a pesar de que el porcentaje esté por debajo de ese valor, la cantidad de paquetes perdidos es bastante alto, ésto se debe a que al no existir un hardware con capacidad para soportar este tipo de software, se genera inestabilidad en la transmisión, produciendo en consecuencia que muchos de los paquetes ni siquiera sean transmitidos. En contraste con lo anterior, la tabla 4.2, es evidencia de que el hardware está asegurando una transmisión fidedigna, de allí que se pueda proporcionar servicios multimedia.
- Como es sabido, debido a su naturaleza, las redes IP no garantizan calidad de servicio; es decir no aseguran la entrega de los paquetes en orden, ni de forma inmediata. Mas sin embargo, al observar los resultados obtenidos en las tablas anteriores, en lo que al Jitter se refiere, se obtuvo en promedio 0.88ms y 0.55ms respectivamente, los cuales son valores bastante bajos, tomando en cuenta que los valores aceptables para las transmisiones de VoIP deben mantenerse por debajo de los 50ms.
- En lo referente al ancho de banda, tal como se estimó en capítulos anteriores, se esperaba un consumo de al menos de 2 a 4Mbps por llamada multimedia unidireccional, y se obtuvo un consumo promedio de 8.7Mbps para el caso de las llamadas multimedia, lo que indica la presencia de códecs como lo son H.261 que implican transmisión de video.
- Por último, en cuanto a los niveles de latencia y retardo obtenidos, éstos se encontraron alrededor de los 1.15ms; dichos valores están por debajo de la norma y son evidencia del sincronismo que existe en la comunicación.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

Tras el desarrollo del presente trabajo, la implementación del Gateway, el estudio de los protocolos involucrados en el mismo y la elaboración de las pruebas descritas en el capítulo anterior, se extraen las siguientes conclusiones:

- Luego de la experiencia adquirida, se puede decir que con la elaboración de este proyecto, se ha cumplido con el objetivo principal de interconectar diversos dispositivos y equipos de protocolos y características diferentes, proporcionando la compatibilidad necesaria para unificar las comunicaciones dentro de la Red de Datos de la UCV.
- Con este trabajo no solo se logra una completa interoperabilidad en la red; sino que además, la unificación entre las telecomunicaciones y el software libre permite que los costos de hardware; y más propiamente en cuanto a transmisión multimedia se refiera; se reduzcan al máximo posible, pues se puede aprovechar al máximo, la disponibilidad de procesamiento cada vez más potente de los servidores y computadoras de hoy en día, eliminando así, gastos inherentes a equipos de traducción de protocolos, de videoconferencia y los no menos importantes costos de licencias y software propietarios que en su mayoría son bastante altos.
- El Gateway desarrollado provee a los usuarios de una conexión con servicios de telefonía IP estable y flexible, ya que, al estar basado en un software libre de código abierto, su utilización no requiere de licencias costosas, sino que está enmarcado en un ámbito muy configurable que se presta a modificaciones y nuevas implementaciones que día a día no sólo evolucionan en calidad, sino que logran satisfacer y adaptarse a los requerimientos de cualquier red.
- La implementación del Gateway permite la traducción de protocolos de redes de diversa índole, en específico, los protocolos H.323 y SIP. Este software ha sido examinado satisfactoriamente mediante la realización de diferentes llamadas de video y audio con varios clientes H.323 y SIP, tanto en hardware

como en software, como es el caso de los equipos Polycom de videoconferencia, los equipos de telefonía IP SIP y los softphone instalados en la universidad, lo que evidencia la compatibilidad adquirida en la red.

- La convergencia de diversas redes de paquetes provoca la aparición de problemas de interoperabilidad. Un primer punto crítico reside, como se ha visto, en la conversión de los diferentes protocolos de señalización empleados por redes heterogéneas, solucionado mediante la integración de un canal dentro de Elastix que soporte este mapeo. Sin embargo, no menos importante es la problemática asociada a la interconexión de redes que utilizan identificadores de usuario diferentes. La manera de identificar a los usuarios en la red H.323 (alias H.323) y SIP (SIP-URI) deriva en escenarios completamente incompatibles y por lo tanto no sería posible la comunicación entre clientes que perteneciesen a éstos. Es necesario, pues, establecer un mecanismo que permita identificar a un usuario con independencia del soporte tecnológico del servicio de VoIP; tales pueden ser los bloques de aplicaciones de manejo de base de datos insertados en Elastix como son MySQL y ENUM, que proporcionan una solución alternativa a la problemática de registro presentada
- Al basarse el Gateway en protocolos y estándares internacionales y comerciales, se posibilita la interacción con gran variedad de tecnologías de software y hardware, así como también con otros protocolos de comunicación y codificación.
- El elemento central en la arquitectura del Gateway es el software Elastix con el servidor Asterisk, que realiza las principales funciones como registro de usuarios y mapeos de mensajes, además, es el que porta la señalización necesaria para la traducción de los protocolos; en otras palabras, Elastix es el que permite establecer las sesiones de traducción y comunicación SIP/H.323.
- El conocimiento del funcionamiento de las comunicaciones sobre software libre, las bases teóricas en cuanto a los protocolos, su transmisión y codificación; así como, la utilización de los códec de audio y video; y más

importante aún, el manejo de diversos lenguajes de computación (como son: C++, perl, php, java entre otros), jugaron un papel importante a la hora de realizar todas las implementaciones necesarias en el presente trabajo.

- La complejidad de la redes H.323 fue la causa de la mayoría de los conflictos de compatibilidad existentes en el presente trabajo. Uno de los más importantes es que este tipo de red contiene bibliotecas y librerías de compilaciones más densas en audio como en video, lo que implica una mayor capacidad de procesamiento por parte de los ordenadores y por ende, requerirá que éstos sean más veloces y de mayor rendimiento. Adicionalmente, el único códec de video incluido por defecto dentro de las librerías de compilación es el códec H.261, dejando de lado otros códecs como el H.263 que poseen mejor calidad de video requiriendo menos trabajo por parte de los ordenadores.
- En el presente ya son pocos los usuarios de H.323, SIP le ha arrebatado dignamente una gran parte del mercado y se ha convertido rápidamente en el protocolo más usado a nivel mundial. Sin embargo, H.323 sigue siendo usado por grandes empresas, que, fieles a su inversión en equipos compatibles con H.323, continúan utilizándolo a pesar de la tendencia a migrar a SIP. En este proyecto se realizó una tarea de gran importancia, que consistió en comunicar ambos protocolos, lo cual puede permitir no sólo a la universidad sino a cualquier empresa que desea migrar a SIP, hacerlo de forma paulatina y sin dejar de lado sus equipos H.323.
- A pesar de que la política no privativa del software libre y la filosofía del código abierto, proporciona la integración del Gateway con otros servicios y proyectos; hoy en día existen innumerables restricciones, al menos en nuestro país, en cuanto a la disponibilidad de equipos periféricos de audio y video, como lo son: cámaras, micrófonos y parlantes; que sean compatibles con plataformas como GNU/Linux. Éstos en su mayoría, son diseñados para sistemas operativos más comerciales y populares (como son las nuevas versiones de Windows), y aunque algunos posean la versatilidad de

interactuar sobre otros sistemas operativos (los de software libre), en muchas ocasiones, éstos, o presentan fallas de operación y la calidad brindada es muy baja, o simplemente la instalación de los drivers correspondientes (o hasta la búsqueda de los mismos en la web) se convierte en un proceso aún más engorroso, lo que imposibilita cada vez más el uso de dichas plataformas.

- Lo anterior, aunado a la inestabilidad de algunos de los programas y los largos y tediosos códigos que se requieren en la mayoría de los casos para instalar e inclusive disfrutar de aquellas aplicaciones y sistemas basados en software libre, representan las razones principales del por qué hoy en día, los usuarios en su mayoría, opten por sistemas propietarios que contienen aplicaciones mucho más amigables y fáciles de instalar y utilizar.
- Los sistemas de Firewall y corta fuegos brindan protección frente a cualquier tráfico previamente autorizado, y aunque éstos originen una labor más ardua de manejo y administración cuando se requiera implementar algún nuevo servicio como es el VoIP; representan la forma más segura de proteger la red de datos de la UCV. Sin embargo, éstos, no podrán hacer nada con respecto al tráfico autorizado de paquetes. Por esta razón, la creación y establecimiento de troncales de comunicación en la red, se presenta como una solución práctica y confiable en cuanto a seguridad se refiera, ya que, logra controlar la capacidad del canal y discriminar entre los que hacen uso de la misma.
- El desempeño del Gateway se estableció con la medición de parámetros que fueron evaluados con la ayuda de las herramientas Iperf y Jperf para la medición de la calidad en el servicio. Demostrándose que el Gateway puesto en funcionamiento, provoca niveles de latencia y una pérdida de paquetes inferior al 2%, lo cual resulta bastante aceptable para cualquier sistema de este tipo.
- Por último, es importante mencionar que, si bien el software libre abarata los costos en equipos y licencias propietarias; éstos requieren de un hardware con características y dispositivos que sustenten los programas instaurados dentro de ellos. Por tanto, la carencia de servidores y computadores de envergadura que soporten software como el Gateway diseñado en este trabajo, fue la mayor

limitación presentada al implementar el mismo dentro del entorno universitario. De hecho, ésta fue la razón fundamental por la que únicamente se pudo implementar una comunicación bidireccional en audio y no en audio y video, como sí se pudo realizar con otros equipos fuera de la universidad.

En toda comunicación debe existir un elemento que se encargue de la traducción de la información transmitida y recibida, y que además sea capaz de proporcionar compatibilidad entre los elementos del sistema; ya que de nada vale transmitir cualquier cantidad o tipo de información, si ésta, luego de ser recibida, no puede ni ser entendida, ni ser utilizada. Hablar de comunicación sin la presencia de una coexistencia entre los elementos involucrados, no tiene ningún sentido. Por tanto, la compatibilidad, es el pilar fundamental que hace posible las comunicaciones.

RECOMENDACIONES

- Actualizar y potenciar la plataforma de hardware existente en la universidad. En especial, acondicionar los equipos y computadores, cuyos dispositivos y elementos conformantes ya están bastante obsoletos, añadiéndoles módulos nuevos de memorias RAM, nuevas unidades de almacenamiento como lo son: Discos Duros, lectores y quemadoras de CD y DVD y equipos periféricos de multimedia; o en el mejor de los casos, sustituir dichos equipos por unos nuevos de mayor velocidad, capacidad y procesamiento.
- Implementar el Gateway en una PC con alto poder de procesamiento así como velocidades de memoria RAM bastante elevadas para que el mismo pueda desempeñar su procesamiento, traducción y distribución de audio y video a los distintos terminales de manera eficiente dentro del entorno universitario. Adicionalmente, realizar la interconexión con la MCU de la Universidad a fin de conformar una plataforma de videoconferencia más robusta.
- Proporcionar un ancho de banda dedicado o una conexión de internet sólo para la plataforma de videoconferencia (Gateway y MCU) implementado en la PC

proporcionada por el Laboratorio de Comunicaciones, con el fin de independizar éste de la red hostil de la UCV.

- Desarrollar un Trabajo Especial de Grado, en donde sea modificado el código fuente de Elastix, para lograr incluir en las transmisiones de video sobre H.323 los códec H.263 y H.264, a fin de prestar un servicio más amplio y de mayor calidad de videoconferencia, ya que dichos códecs son soportados por softphone como X-Lite, entre otros y la calidad de video brindada es mejorada.
- Se aconseja el desarrollo de un Gateway utilizando Asterisk y su protocolo IAX el cual es mucho más manejable en entornos en los que los dispositivitos clientes están detrás de elementos que empleen NAT como son los router y mecanismos de filtrado de tráfico como los son los Firewall, debido a que el trafico de audio, video y señalización son enviados a un mismo puerto. Adicionalmente, este protocolo es manejado en la actualidad, por una gran variedad de dispositivos y equipos, por tales razones se recomienda dicha migración.
- Realizar una investigación con el fin de desarrollar un Gateway que permita proporcionar garantías de QoS, ya que a medio plazo se prevé la sustitución de la telefonía tradicional por la Telefonía de voz sobre IP. Al tratarse de conmutación de paquetes, la QoS no está garantizada en sentido estricto (como sí lo estaba en conmutación de circuitos). Por esta razón es necesario el uso de protocolos que permitan diferenciar los tráficos presentes en la red (DiffServ, MPLS,...) y que permitan minimizar el retardo extremo-extremo (factor crítico en la transmisión multimedia).
- Otro aspecto importante a tratar es la integración del Gateway con la telefonía tradicional. La arquitectura del mismo, debería implementar una función adicional para la interconexión de las redes IP con la red PSTN. Se recomienda integrar los proyectos OpenSource como son el PSTNGateway de la fundación Xpih.org dentro del software ya desarrollado. Quedan por lo tanto como desafíos, integrar a este proyecto estas funcionalidades de modo de convertirlo en una experiencia útil y lo suficiente rentable como para ser implementada para fines no académicos.

- La confidencialidad y seguridad de los datos de los usuarios debe ser primordial en un sistema de VoIP, se propone por tanto realizar un estudio sobre los diferentes software que existen en el mercado, a fin de desarrollar un modelo de encriptación y codificación confiable que aseguren la privacidad dentro de las transmisiones
- Se sugiere explotar el estudio del software libre y de los distintos proyectos en la actualidad Open Source, mediante la elaboración de un grupo de investigación con estudiantes así como la dotación de un laboratorio VoIP con el fin de facilitar e incentivar este campo tan importante por parte de la Universidad Central de Venezuela. Otra recomendación sería conformar fundaciones de investigación sobre este campo, patrocinadas por la universidad, para contar así con la colaboración de la mayor cantidad de personas que manejen el tema y por ende lograr desarrollar proyectos de este tipo más allá del entorno universitario.

REFERENCIAS BIBLIOGRÁFICAS

- [1] Kundan Sign; Henning Schulzrinne. *Interworking Between SIP/SDP and H.323.* Dept. of Computer Science Columbia University. Nueva York. EEUU. (2005)
- [2] M. Jeffries, W.D. Tucker. *An Interoperale Signaling Solution between SIP an H.323*. Broadband Applications and Networking Group Computer Science Department, University of the Western Cape Private. Sur África.
- [3] Janus Friis; Niklas Zendstrom. Skype Technologies. *Skype.*. Recuperado el 15 de Noviembre de 2010 de la World Wide Web: http://www.skype.com/.
- [4] Robert F. Ryan. Dialcom Inc. *Spontania.* Recuperado el 16 de Noviembre de 2010 de la World Wide Web: http://www.dialcom.com/.
- [5] Fundación para Software Libre.Licencia pública General GNU. *Ekiga.* Recuperado el 16 de Noviembre de 2010 de la World Wide Web: http://www.ekiga.org/.
- [6] Clayton L. Mathile. ooVoo LLC. *ooVoo.* Recuperado el 17 de Noviembre de 2010 de la World Wide Web: http://www.oovoo.com/.
- [7] Christopher Montgomery. *Fundación Proyectos Xiph.org.* Recuperado el 15 de Noviembre de 2010 de la World Wide Web: http://www.xiph.org/.
- [8] Craig Southeren, Robert Jongbloed. Equivalence Pty Ltd. *OpenH323.*Recuperado el 18 de Noviembre de 2010 de la World Wide Web: http://openh323.sourceforge.net/
- [9] Aggio, Santiago. *Implementación de una MCU por software Ariu*, Jornadas Técnicas de Ariu, UTN. Uruguay. (Mayo 2010).
- [10] Espinoza Pinzon, Antonio. *Desarrollo de una MCU H.323 con asignación dinámica de salas para Videoconferencia*, tesis en Ingeniería, UMA. Málaga. España (s.f).
- [11] TANDBERG-Fabricante que ofrece equipos especialmente diseñados para la industria de la salud. www.tandbergvision.com

- [12] RFC 2822 - Internet Message Format. The Internet Engineering Task Force (IETF). 1998. www.ietf.org/rfc/rfc2822.txt
- [13] RFC 2543 - Internet Message Format. The Internet Engineering Task Force (IETF). 2002. www.ietf.org/rfc/rfc2543.txt
- [14] RFC 2396-Uniform Resources Identifiers: Generis Sintax. The Internet Engineering Task Force (IETF). 2001. www.ietf.org/rfc/rfc2396.txt
- [15] RFC 3263 – Session Initiation Protocol (SIP): Locating SIP Servers. The Internet Engineering Task Force (IETF). 2002. www.ietf.org/rfc/rfc3263.txt
- [16] RFC 4123 - Session Initiation Protocol (SIP)-H.323 Internetworking Requirements. The Internet Engineering Task Force (IETF). 2002. www.ietf.org/rfc/rfc4123.txt

BIBLIOGRAFÍA

- Gomilion D, Dempster B. Building Telephony Systems with Asterisk, Pack Publishing. (2005)
- Goncalvez F. Configuration Guide for Asterisk PBX, Booksurge Llc. (2007)
- Wallingford T. Switching to VoIP, O'Reilly. (2005)
- Álvarez M, F. A. Diseño de una red telefónica IP interna entre los colegios San José – La Salle de Guayaquil y Hno Miguel – La Salle de Quito e implementación de un prototipo, usando como central telefónica servidores con Sistema Operativo libre y Software libre. Guayaquil, Ecuador. (2006)
- Estrada J, J. A. Diseño e implementación del prototipo de un sistema de seguridad para la red de voz y datos de la Corporación Machangarasoft, utilizando el sistema operativo Linux. Quito, Ecuador: Escuela Politécnica Nacional. (2007)
- Fernández, L. Difusión Multimedia. Caracas. 6 de Septiembre 2008
- Ferreira, P. (Septiembre de 2005). Recuperado en Diciembre de 2010, de http://www.fccn.pt/files/documents/D2.05.2.PDF?947cda2253a1dc58fe23dc95ac31cbed=e3fbccc61614de6343e90171d1d8d1c8
- http://www.voip-info.org/. (s.f). Recuperado Enero 2011, de http://www.voip-info.org/.
- http://www.voipforo.org/. (s.f). Recuperado Enero 2011, de http://www.voipforo.org/
- http://www.elastix.org/. (s.f). Recuperado Enero 2011, de http://www.elastix.org/
- http://www.asterisk.org/. (s.f). Recuperado Enero 2011, de http://www.asterisk.org/
- http://openh323.sourceforge.net/. (s.f.). Recuperado en Diciembre de 2010, de http://openh323.sourceforge.net/: http://openh323.sourceforge.net/
- http://www.gnu.org/home.es.html. (s.f.). Recuperado en Enero de 2011, de http://www.gnu.org/home.es.html: http://www.gnu.org/home.es.html

- Villacrés S, W. H. Estudio Comparativo de plataformas alternativas de videoconferencia basadas en software en el Backbone de la ESPOCH. Tesis de Grado. Escuela Superior Politécnica de Chimborazo. (2010)
- Kundan Sign; Henning Schulzrinne. Interworking Between SIP/SDP and H.323. Dept. of Computer Science Columbia University. Nueva York. EEUU. (2005)

ANEXOS

ANEXO 1. CÁLCULO DE MEMORIA RAM Y PROCESAMIENTO. PROBLEMÁTICA CON CÓDEC H.261

Cálculo de memoria= velocidad de reloj efectiva x 8bits x 2 (doble tasa de transferencia)

Módulos [editar]

Para usar en PC, las DDR2 SDRAM son suministradas en tarjetas de memoria DIMM con 240 pines y una localización con una sola ranura. Las tarjetas DIMM son identificadas por su máxima capacidad de transferencia, llamado ancho de banda.

Nombre estándar	Velocidad del reloj	Tiempo entre señales	Velocidad del reloj de E/S	Datos transferidos por segundo	Nombre del módulo	Máxima capacidad de transferencia
DDR2-400	100 MHz	10 ns	200 MHz	400 millones	PC2-3200	3200 MB/s
DDR2-533	133 MHz	7,5 ns	266 MHz	533 millones	PC2-4200	4264 MB/s
DDR2-600	150 MHz	6,7 ns	300 MHz	600 millones	PC2-4800	4800 MB/s
DDR2-667	166 MHz	6 ns	333 MHz	667 Millones	PC2-5300	5336 MB/s
DDR2-800	200 MHz	5 ns	400 MHz	800 Millones	PC2-6400	6400 MB/s
DDR2-1000	250 MHz	3,75 ns	500 MHz	1000 Millones	PC2-8000	8000 MB/s
DDR2-1066	266 MHz	3,75 ns	533 MHz	1066 Millones	PC2-8500	8530 MB/s
DDR2-1150	286 MHz	3,5 ns	575 MHz	1150 Millones	PC2-9200	9200 MB/s
DDR2-1200	300 MHz	3,3 ns	600 MHz	1200 Millones	PC2-9600	9600 MB/s

Nota: DDR2-xxx indica la velocidad de reloj efectiva, mientras que PC2-xxxx indica el ancho de banda teórico (aunque suele estar redondeado). El ancho de banda se calcula multiplicando la velocidad de reloj efectiva por ocho, ya que la DDR2 (como la DDR) es una memoria de 64 bits, hay 8 bits en un byte, y 64 es 8 por 8 y por último por 2 (doble tasa de transferencia), esto se empezó a usar para mostrar la velocidad de transferencia frente a las memorias "Rambus" que eran mas rápidas en sus ciclos de reloj operación, pero solo eran de 16 bits

[1] *Algunos fabricantes etiquetan sus memorias DDR2-667 como PC2-5400 en vez de PC2-5300. Al menos un fabricante ha reportado que esto refleja pruebas satisfactorias a una velocidad más rápida que la normal.*

- ✓ Para el caso de la computadora Servidor: DDR2800 PC6400 = 400x2x8=6400Mbits por segundo y contiene un módulo ECC(Puede ser de cualquier tipo, aunque sobre todo EDO-ECC o SDRAM-ECC. Detecta errores de datos y los corrige; para aplicaciones realmente críticas. Usada en servidores y mainframes.) que se encarga de detectar y corregir posibles errores que se presenten en la memoria.
- ✓ Para el caso de las computadoras UCV: DDR266 = 266x2x8=3192Mbits por segundo
- ✓ Para el códec de video H.261. según la recomendación H.261, en lo referente la codificación de transmisión, la velocidad de transmisión dependerá de la velocidad del reloj externo de la interfaz física (véase http://neutron.ing.ucv.ve/comunicaciones/Asignaturas/DifusionMultimedia/T-REC-H.261-199303-I!!PDF-S.pdf) en este caso la interfaz física que

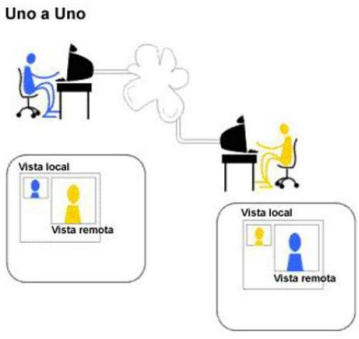
proporciona los procesamientos de transmisión, son los bloques de Memoria RAM, por lo tanto, la calidad de la codificación de transmisión del códec dependerá directamente de la velocidad del reloj efectivo que posea el dispositivo de memoria. Lo anterior indica que códecs con menor capacidad de compresión, requieren de mayor procesamiento externo, a diferencia de los códecs de mayor capacidad de compresión como lo es el códec H.263, que aunque abarca mayor ancho de banda, posee una codificación de transmisión independiente del procesamiento externo, y por ende contiene una velocidad de transmisión fija.

ANEXO 2. USOS DE LA VIDEOCONFERENCIA

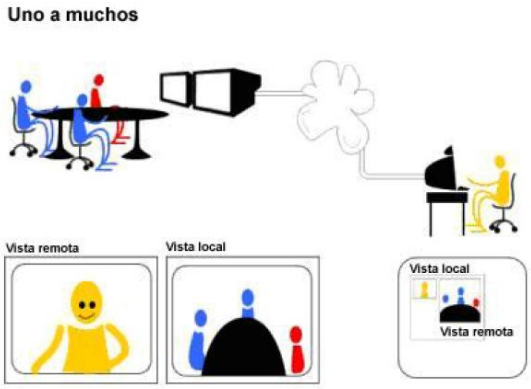
II.2.4 Usos de la Videoconferencia

Los sistemas de videoconferencia están siendo utilizados en diferentes áreas y aplicaciones, diferentes tipos de reuniones o para aplicaciones específicas, como lo son las conferencias utilizadas en el área de la medicina, la judicial, entre otras.

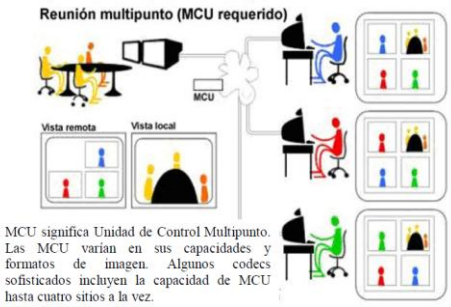
II.2.4.1 Reuniones: facilitar la participación en reuniones es una de las formas más simples y populares de usar la videoconferencia. Para reuniones que regularmente se llevan a cabo y necesitan de comunicación cara a cara, la videoconferencia puede sustituir la actual presencia física por la participación de personas en sitios remotos. Esto reduce los costos de viaje así como el tiempo invertido en ello y hace la asistencia más fácil. Además puede propiciar la realización de más reuniones de las que originalmente se tenían. Las reuniones frecuentes que podrían no haberse efectuado por los costos de viaje o los tiempos, son más sencillas de implementar por videoconferencia incrementando la sensación de trabajo en equipo entre los participantes de los diversos lugares que colaboran en el mismo proyecto. En cada uno de los casos citados, es crítica la calidad del audio y del video para el éxito de la participación remota. Ambos afectarán o no la sensación de los participantes remotos de si son realmente parte de la reunión. En el caso de las reuniones, el audio es probablemente el mayor factor, comparado con el video. Pequeñas fallas en el video (congelamientos, baja resolución, imagen en cuadrícula) son generalmente toleradas por los usuarios.



Otro factor que puede influir en la calidad de la videoconferencia es la velocidad a la que están conectados los participantes, mayores velocidades resultan en mejor calidad. 384 Kbps. es el estándar para muchas de las conferencias. Esto funciona bien en reuniones estáticas donde la mayor actividad se limita a los rostros. Si la videoconferencia involucra movimientos de algunos participantes o la captura de un evento en vivo, conectarse a mayor velocidad puede ser innegable. En el caso específico de una reunión multipunto, donde participan más de dos usuarios, existen factores adicionales que afectan el éxito de una participación remota. Estos incluyen la imagen que cada participante tiene de los demás, qué tan bien escuchan a otros y pueden ser escuchados por los demás y cómo los participantes determinan quién encabeza la reunión en un momento dado.



II.2.4.2 Salón de Clases. Los participantes remotos pueden ser estudiantes adicionales a los que el instructor debe integrar a los participantes locales, haciendo un solo grupo. En otros casos, éstos podrían ser adiciones a la instrucción misma, como catedráticos o instructores. Como en toda enseñanza en equipo, se requiere un balance cooperativo en las labores, pero esto puede ser más complicado si la presencia en video no puede competir con la presencia física. Por ende, la accesibilidad del instructor en el salón físico puede sobrepasar rápidamente la presencia y control del instructor remoto, fomentando conversaciones paralelas y poca atención a la instrucción remota.



II.2.4.3 Específicos. La videoconferencia hoy en día se está orientando por diferentes caminos, los cuales ayudan a la sociedad en diferentes campos como lo es la telemedicina, aplicaciones jurídicas, entre otros.

- **Telemedicina***:* El diagnóstico clínico remoto por videoconferencia se usa frecuentemente en áreas rurales. Un médico rural o practicante de la enfermería puede consultar con un médico localizado en un hospital. Por medio de la videoconferencia y algunos instrumentos médicos adaptados, el médico remoto puede ver al paciente, hablar con el responsable médico local, escuchar el ritmo cardíaco con un estetoscopio remoto, observar las imágenes de sus análisis de oído, nariz y garganta o examinar el estado de la piel. El sistema HealthCare III (véase figura más abajo) creado por Tandberg[11], es una solución interesante que combina una estación de videoconferencia H.323 con herramientas para exámenes médicos que se pueden leer a distancia, permitiendo al doctor ver tanto al paciente como a la transmisión auxiliar, que incluye radiografías o imágenes generadas por computadora.

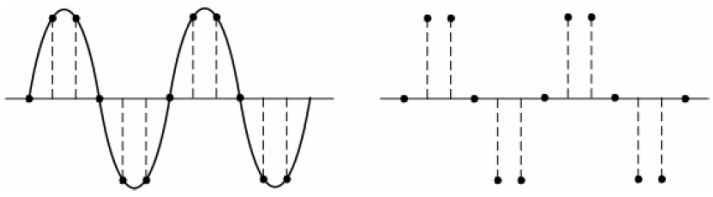
- **Aplicaciones Judiciales:** El sistema judicial encuentra en la videoconferencia una herramienta de bajo costo, alto beneficio y muy productiva. Esto tiene muchos beneficios para el sistema de justicia, ya que reduce el número de inculpados que se deben transportar de las cárceles hacia los juzgados, baja el índice de asistentes a los juzgados y limita los riesgos asociados con la transportación de los prisioneros, ahorrando tiempo y dinero. Muchos de estos sistemas usan actualmente redes privadas con tecnologías propietarias, pero podrían diseñarse para usar la tecnología H.323 dentro de una Intranet segura.
- **Vigilancia y Seguridad:** La videoconferencia puede usarse como una tecnología de monitoreo en un sentido al apagar el micrófono y la cámara de uno de los lados. La conferencia H.323 se puede adaptar como una herramienta de vigilancia y seguridad, sólo se necesita ver situaciones donde el video ya esté siendo usado con esos propósitos.

ANEXO 3. PCM. DIGITALIZACIÓN

Proceso de Conversión Analógico-Digital

Este proceso se puede dividir en tres fases resaltantes:

- Muestreo: consiste en tomar valores instantáneos de una señal analógica a intervalos de tiempo iguales. A los valores obtenidos se les denomina muestras. El muestreo se efectúa siempre a un ritmo uniforme, que viene dado por la frecuencia de muestreo (sampling rate). La condición que debe cumplir la frecuencia de muestreo viene dada por el teorema de Nyquist: si una señal contiene únicamente frecuencias inferiores a f, queda completamente determinada por muestras si estas son tomadas a una velocidad igual o superior a 2f. De acuerdo al teorema de muestreo, las señales telefónicas de frecuencia vocal (que ocupa la banda de 300 a 3400 Hz), se han de muestrear a una frecuencia igual o superior a 6.800 Hz (2*3.400); sin embargo en la práctica, se suele tomar una frecuencia de muestreo de fm=8.000Hz (2*4.000), es decir, se toman 8.000 muestras por segundo (o lo que es igual una muestra cada 125µs).



Proceso de Muestreo

- *Cuantificación: es el proceso mediante el cual se asignan valores discretos a las amplitudes de las muestras obtenidas en el proceso de muestreo. Este valor es elegido por aproximación dentro de un margen de niveles previamente fijado. El proceso de cuantificación introduce necesariamente un error ya que se sustituye la amplitud real de la muestra por un valor*

aproximado. A este error se le llama error de cuantificación. Las distintas técnicas de cuantificación son: uniforme, no uniforme, logarítmica y vectorial.

- *Uniforme: es el más simple. Toda la gama de amplitudes que pueden tomar las muestras se divide en intervalos iguales y a todas las muestras cuya amplitud cae dentro de un intervalo, se les da el mismo valor.*
- *No Uniforme: en este caso, se realiza un estudio del comportamiento de una señal y se le asignan niveles de cuantificación no uniformes de acuerdo a los rangos de amplitudes que más frecuentemente se dan en la señal.*
- *Logarítmica: como paso previo a la propia cuantificación, se hace pasar la señal por un compresor logarítmico. Con esto se consigue que la distancia entre los niveles de cuantificación aumente a medida que crece la amplitud de la señal. Así, se consigue tener más niveles para las amplitudes más pequeñas y menos niveles con aquellas con poca frecuencia de aparición; con lo que se proporciona mayor resolución en señales débiles. Para llevar a cabo la compresión, existen dos funciones muy utilizadas: Ley-A (utilizada principalmente en Europa) y la ley-μ (utilizada en EEUU); más adelante serán explicados con mayor detalle.*
- *Vectorial: es una extensión de los procesos anteriormente descritos. El bloque de N muestras se trata como un vector N-dimensional, esta cuantificación ofrece mejores resultados que la cuantificación escalar, sin embargo, es más sensible a los errores de transmisión y lleva consiga una mayor complejidad computacional.*

- *Codificación: es el proceso mediante el cual se representa una muestra cuantificada, mediante una sucesión de ceros y unos (número binario ejemplo: 1000111010100111001). El dispositivo que realiza la cuantificación y codificación se denomina codificador; el dispositivo que hace la operación inversa (decodifica) se le denomina decodificador.*

ANEXO 4. Protocolo TCP/IP

II.3.1 *Protocolo TCP*

TCP proporciona un servicio de dúplex completo, reconocido y de flujo controlado a los protocolos de capa superior. Mueve los datos en una corriente de bytes continua no estructurada donde los bytes se identifican mediante números de secuencia. Para maximizar el rendimiento o tasa de transferencia, TCP permite que cada estación envié múltiples paquetes antes de que llegue un acuse de recibo. Cuando el remitente ha recibido un acuse de recibo para un paquete saliente, el remitente desliza la ventana de paquetes por la corriente de bytes y envía otro paquete. Este mecanismo de control del flujo se conoce como sliding window (ventana deslizante). TCP puede soportar numerosas conversaciones de capa superior simultáneas. Los números de puerto de una cabecera TCP identifican una conversación de capa superior. Muchos puertos TCP bien conocidos están reservados para el Protocolo de transferencia de archivos (FTP, File Transfer Protocol), World Wide Web (WWW), Telnet, etc. Dentro de la porción de señalización de VoIP, TCP se utiliza para asegurar la fiabilidad de la configuración de una llamada. Debido a la manera de operar de TCP, actualmente no es posible utilizar TCP como el mecanismo para transportar la voz en una llamada VoIP. Con VoIP, la pérdida de paquetes es menos importante que la latencia.

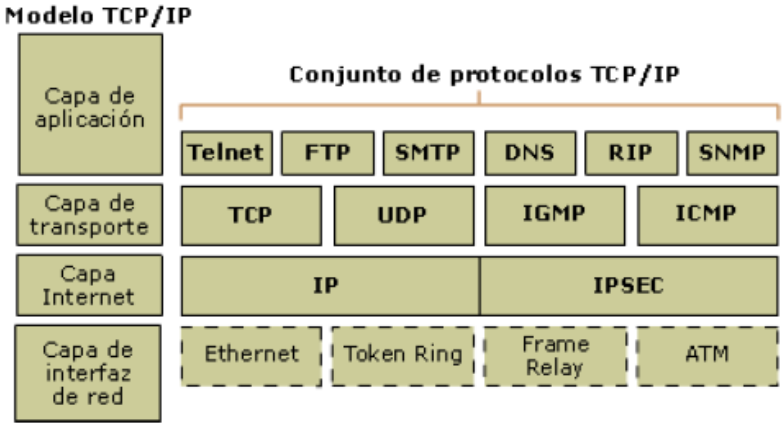


Figura 2.14. Protocolos del Modelo de Referencia TCP/IP

Fuente: http://securenet2002.tripod.com/tcp.html

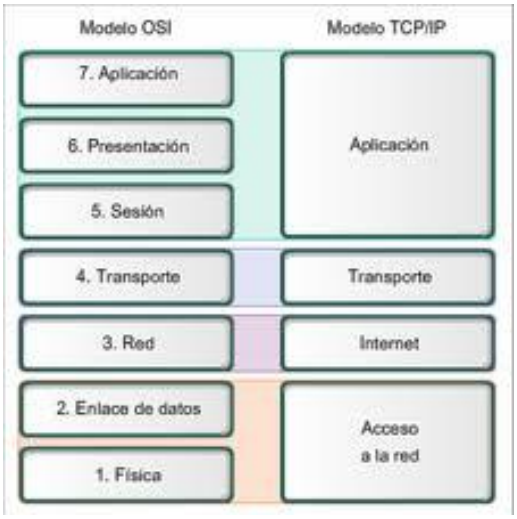


Figura 2.14. Capas Modelo TCP/IP vs Capas Modelo OSI

Fuente: http://securenet2002.tripod.com/tcp.html

En la tabla siguiente se describen las características de cada una de las capas del modelo TCP/IP.

Tabla 2.1.- Descripción capas Modelo TCP/IP

Referencia: www.microsoft.com/technet

Capa	Descripción	Protocolos
Aplicación	Define los protocolos de aplicación TCP/IP y cómo se conectan los programas de host a los servicios del nivel de transporte para utilizar la red.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows
Transporte	Permite administrar las sesiones de comunicación entre equipos host. Define el nivel de servicio y el estado de la conexión utilizada al transportar datos.	TCP, UDP, RTP
Interred	Empaqueta los datos en datagramas IP, que contienen información de las direcciones de origen y destino utilizada para reenviar los datagramas entre hosts y a través de redes. Realiza el enrutamiento de los datagramas IP.	IP, ICMP, ARP, RARP
Host a red	Especifica información detallada de cómo se envían físicamente los datos a través de la red, que incluye cómo se realiza la señalización eléctrica de los bits mediante los dispositivos de hardware que conectan directamente con un medio de red, como un cable coaxial, un cable de fibra óptica o un cable de cobre de par trenzado.	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35

II.3.1.1.4 Direccionamiento: es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo dentro de una red. Existen dos tipos de direcciones IP, una dinámica y una estática. Un usuario que se conecta desde su hogar a internet, utiliza una dirección IP, la cual puede cambiar al reconectar; y a esta forma de asignación se le denomina IP dinámica; por el contrario los sitios de internet que necesitan estar permanentemente conectados, tienen una dirección IP fija o estática, no cambian con el tiempo.

II.3.1.1.5 Clases de direcciones: cada nodo de una red IP tiene una dirección numérica de 4 byte (32 bits). Esa dirección se suele representar por cuatro números entre 0 y 255 separados por puntos, y tiene dos partes; la primera representa la red, y la segunda representa al nodo en ella. Existen dos direcciones especiales, el que tiene todos los bits a 0 en el campo de Host (representa a la red), y el que tiene todos los bits a 1 en el mismo campo (que representa a todos los nodos).

- *Clase A: tiene una longitud de 8 bits y se caracterizan por tener en 0 el primer bit del campo de red. Las direcciones correspondientes van de la 1.0.0.0 a la 126.0.0.0 con 128 redes de clase A; la red 0 (bits con valores 000000) no existe y el número 127 está reservado para indicar el propio equipo.*
- *Clase B: se caracterizan por tener los dos primeros bits del campo de red con la secuencia 1 0 y una longitud de 16 bits. Las direcciones van de la 128.0.0. a la 191.255.0.0.*
- *Clase C: tienen un campo de red de 24 bits que comienzan con 1 1 0. Las direcciones correspondientes van de la 192.0.0. a la 223.255.255.0. Existen 2.097.152 redes de clase C.*
- *Clase D: se caracterizan porque su dirección comienza con la secuencia de bit 1 1 1 0 y corresponden a las direcciones desde la 224.0.0. a la 255.255.255.255. Son direcciones especiales y sólo está asignada la 255.255.255.255. que corresponde a todas las máquinas conectadas a un soporte físico.*

II.3.1.1.6 Enrutamiento: el encaminamiento es una función implantada en la capa 3 (capa de red) del modelo de referencia OSI; es el mecanismo por el que en una red, los paquetes de información llegan desde su origen a su destino final, siguiendo un camino o ruta, cuyo ideal es conseguir caminos óptimos.

- *Estático: una red con un número mínimo de enrutadores o con un solo Gateway, puede ser configurada con enrutamiento estático. Una tabla de enrutamiento estático es construida manualmente por el administrador de la red: Estas tablas no se ajustan a los cambios de la red, ellos trabajan mejor cuando las rutas no cambian.*
- *Dinámico: una ruta dinámica es construida mediante información intercambiada por los protocolos de enrutamiento. Esta información permite ajustar las rutas reflejadas en las condiciones de la red y manejar complejas situaciones de enrutamiento más rápido de lo que un administrador del sistema podría hacer.*

II.3.1.2 *Aplicaciones del Protocolo de Internet. Redes sobre IP*

Hasta hoy ha habido una clara división entre dos tipos de redes:

- *Redes de Voz: están basadas en conmutación de circuitos. En ellas los equipos de conmutación deben establecer un camino físico entre los medios de comunicación, previo a la conexión entre los usuarios. Este camino permanece activo durante la comunicación entre los usuarios, liberándose al terminar la comunicación. Un ejemplo claro de este tipo de red es la Red Telefónica Conmutada.*
- *Redes de Datos: basadas en conmutación de paquetes, los datos que se van a transmitir se dividen en paquetes y se envían por separado a través de la red. Los nodos de la red determinan libremente la ruta de cada paquete de manera individual, según su tabla de enrutamiento. Los paquetes que se envían de esta manera pueden tomar varias rutas y se vuelven a montar una vez que lleguen al receptor. Un ejemplo de este tipo de redes es Internet.*

Entre las ventajas y deventajas de la redes IP se encuentran:

- *A pesar de que mediante la conmutación de circuitos, se realice la transmisión en tiempo real (siendo adecuado para la comunicación de voz y video) y que una vez conectado el circuito, éste no da lugar a congestión; el problema con esta radica en que requiere una significativa cantidad de ancho de banda y el circuito no es empleado eficientemente ya que emplea un canal durante toda la duración de la llamada no teniendo en cuenta por ejemplo los abundantes silencios que se producen durante una conversación. Además, necesita tiempo para realizar la conexión, lo que conlleva a un retraso en la transmisión de la información. Por el contrario, las redes de datos, sólo transmiten información cuando es necesario, aprovechando al máximo el ancho de banda y en el cual el retardo, la alteración del orden de llegada o la pérdida de paquetes no son inconvenientes (lo que proporciona gran flexibilidad y en rentabilidad en las líneas), ya que el sistema al final dispone de una serie de procedimientos de recuperación de la información original (reenvío de los paquetes necesarios, asignación de prioridades, enrutamiento optimizado). Pero para la voz y el video, estos factores son altamente influyentes. Se considera que la señal transmitida debe llegar al destino con un retardo no superior a 150ms para que no exista una degradación de la comunicación. Por consiguiente, a la hora de transmitir voz y video, es necesario disponer de unos protocolos especiales que nos garanticen un servicio confiable.*
- *Voz sobre IP (VoIP) define los sistemas de enrutamiento y los protocolos necesarios para la transmisión de conversaciones a través de internet, lo cual lo convierte en una red de conmutación de paquetes para el envío de información. Actualmente existen, principalmente, dos arquitecturas o protocolos más sobresalientes de VoIP para la transmisión de voz y video por internet: H.323 y SIP.*

II.3.1.3 *Tipos de Redes IP*

- *Internet:* Se ofrece el servicio de telefonía sobre ésta estructura
- Red IP pública: Los operadores ofrecen a las empresas la conectividad necesaria para interconectar sus redes de área local en lo que al tráfico IP se refiere. Se puede considerar como algo similar a Internet.
- Intranet: La red IP implementada por la propia empresa. Suele constar de varias redes LAN (Ethernet conmutada, ATM, etc.) que se interconectan mediante redes WAN tipo Frame-Relay/ATM, líneas punto a punto, RDSI para el acceso remoto, etc. En este caso la empresa tiene bajo su control prácticamente todos los parámetros de la red, por lo que resulta ideal para su uso en el transporte de la voz.

ANEXO 5. TABLA DE COMPARACIÓN DE LOS CÓDECS DE AUDIO MÁS UTILIZADOS EN EL MERCADO ACTUAL.

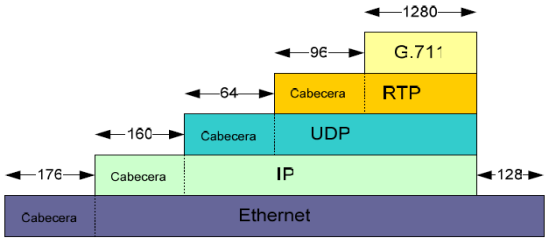
Nombre	Estandarizado	Descripción	Bit rate (kb/s)	Sampling rate (kHz)	Frame size (ms)	Observaciones	MOS (Mean Opinion Score)
G.711 *	ITU-T	Pulse code modulation (PCM)	64	8	Muestreada	Tiene dos versiones u-law (US, Japan) y a-law (Europa) para muestrear la señal	4.1
G.721	ITU-T	Adaptive differential pulse code modulation (ADPCM)	32	8	Muestreada	Obsoleta. S e ha transformado en la G.726.	
G.722	ITU-T	7 kHz audio-coding within 64 kbit/s	64	16	Muestreada	Divide los 16 Khz en dos bandas cada una usando ADPCM	
G.722.1	ITU-T	Codificación a 24 y 32 kbit/s para sistemas sin manos con baja perdida de paquetes	24/32	16	20		
G.723	ITU-T	Extensión de la norma G.721 a 24 y 40 kbit/s para aplicaciones en circuitos digitales.	24/40	8	Muestreada	Obsoleta por G.726. Es totalmente diferente de G.723.1.	
G.723.1	ITU-T	Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s	5.6/6.3	8	30	Parte de H.324 video conferencing. Codifica la señal usando linear predictive analysis-by-synthesis coding. Para el codificador de high rate utiliza Multipulse Maximum Likelihood Quantization (MP-MLQ) y para el de low-rate usa Algebraic-Code-Excited Linear-Prediction (ACELP).	3.8-3.9
G.726	ITU-T	40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM)	16/24/32/40	8	Muestreada	ADPCM; reemplaza a G.721 y G.723.	3.85
G.727	ITU-T	5-, 4-, 3- and 2-bit/sample embedded adaptive differential pulse code modulation (ADPCM)	var.		Muestreada	ADPCM. Relacionada con G.726.	
G.728	ITU-T	Coding of speech at 16 kbit/s using low-delay code excited linear prediction	16	8	2.5	CELP.	3.61

G.729 **	ITU-T	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)	8	8	10	Bajo retardo (15 ms)	3.92
GSM 06.10	ETSI	RegularPulse Excitation Long-Term Predictor (RPE-LTP)	13	8	22.5	Usado por la tecnología celular GSM	
LPC10	Gobierno de USA	Linear-predictive codec	2.4	8	22.5	10 coeficientes.La voz suena un poco "robotica"	
Speex			8, 16, 32	2.15-24.6 (NB) 4-44.2 (WB)	30 (NB) 34 (WB)		
iLBC			8	13.3	30		
DoD CELP	American Department of Defense (DoD) Gobierno de USA		4.8		30		
EVRC	3GPP2	Enhanced Variable Rate CODEC	9.6/4.8/1.2	8	20	Se usa en redes CDMA	
DVI	Interactive Multimedia Association (IMA)	DVI4 uses an adaptive delta pulse code modulation (ADPCM)	32	Variable	Muestreada		
		(ADPCM)					
L16		Uncompressed audio data samples	128	Variable	Muestreada		

* El codec g711 tiene dos versiones conocidas como alaw (usado en Europa) y ulaw (usado en USA y Japón). U-law se corresponde con el estandar T1 usado en Estados Unidos y A-law con el estandar E1 usado en el resto del mundo. La diferencia es el método que se utiliza para muestrear la señal. La señal no se muestrea de forma lineal sino de forma logaritmica. A-law tiene un mayor rango. Para mas información de las diferencias ver G.711 Ley A vs Ley u

** existen varias versiones del codec g729 que es interesante explicar por su extendido uso
G729: es el códec original
G729A o anexo A: es una simplificación de G729 y es compatible con G729. Es menos complejo pero tiene algo menos de calidad.
G729B o anexo B: Es G729 pero con supresion de silencios y no es compatible con las anteriores.
G729AB: Es g729A con supresión de silencios y sería compatible solo con G729B.
Aparte de esto G729 (todas las versiones) en general tienen un bit rate de 8Kbps pero existen versiones de 6.4 kbps (anexo D) y 11.4 Kbps (anexo E).

ANEXO 6. GENERALIDADES. CÓDEC DE AUDIO Y VIDEO



Longitud total de bits de un paquete IP sobre Ethernet utilizando códec G-711.

Tabla de resolución del códec h.263

	Sub-QCIF	QCIF	CIF	4CIF	16CIF
Pixels de luminancia	128	176	352	704	1408
Líneas de luminancia	96	144	288	576	1152
Pixels de crominancia	64	88	176	352	288
Líneas de crominancia	48	72	144	288	576

Resolución espacial del formato de video H.263

Fuente: www.ing.ucv.ve/Revista/JRozada

Códec de Video MPEG

- MPEG: Moving Picture Experts Group (Grupo de Expertos en Imágenes Móviles), referido comúnmente como MPEG, es un grupo de trabajo del ISO/IEC encargado de desarrollar estándares de codificación de audio y vídeo. Desde 1988, el MPEG ha crecido hasta incluir 350 miembros de distintas industrias y universidades. La designación oficial del MPEG es ISO/IEC JTC1/SC29 WG11. El MPEG utiliza códecs (codificadores-

decodificadores) de compresión con bajas pérdidas de información usando códecs de transformación. En los códecs de transformación con bajas pérdidas, las muestras tomadas de imagen y sonido son troceadas en pequeños fragmentos y solamente las diferencias con estas imágenes reconstruidas y algún extra necesario para llevar a cabo la predicción es almacenado. MPEG solamente normaliza el formato del flujo binario y el descodificador. El codificador no está normalizado en ningún sentido, pero hay implementaciones de referencia, para los miembros, que producen flujos binarios válidos.

MPEG ha normalizado los siguientes formatos de compresión y normas auxiliares:

- MPEG-1: estándar inicial de compresión de audio y vídeo. Usado después como la norma para CD de vídeo, incluye el popular formato de compresión de audio Capa 3 (MP3).
- MPEG-2: normas para audio y vídeo para difusión de calidad de televisión. Utilizado para servicios de TV por satélite como DirecTV , señales de televisión digital por cable y (con ligeras modificaciones) para los discos de vídeo DVD.
- MPEG-3: diseñado originalmente para HDTV (Televisión de Alta Definición), pero abandonado posteriormente en favor de MPEG-2.
- MPEG-4: expande MPEG-1 para soportar audio/vídeo, contenido 3D, codificación de baja velocidad binaria y soporte para gestión de derechos digitales(protección de copyright) actualmente se emplea como códec HDTV en detrimento de MPEG-2.
- MPEG-7: sistema formal para la descripción de contenido multimedia
- MPEG-21: MPEG describe esta norma futura como un marco multimedia.
- MPEG-A (ISO/IEC 23000)
- MPEG-B (ISO/IEC 23001)
- MPEG-C (ISO/IEC 23002)

- MPEG-D (ISO/IEC 23003)
- MPEG-E (ISO/IEC 23004)

ANEXO 7. SOFTWARE LIBRE. VENTAJAS Y DESVENTAJAS

Ventajas: el software libre presenta un gran número de ventajas que no tienen otros tipos de software, algunas se nombran a continuación.

- Escrutinio Público: Al ser muchas las personas que tienen acceso al código fuente, eso lleva a un proceso de corrección de errores muy dinámico, es decir, no hace falta esperar que el proveedor del software saque una nueva versión, los propios usuarios están constantemente actualizando y modificando el software y ya que los términos de las libertades del software libre implican la publicación de estas mejoras, siempre será sencillo para otros usuarios poder tener acceso a ellas. Muchas veces el proveedor hace también las veces de mediador y administrador de estas mejoras, revisándolas e incorporándolas en futuras versiones del software.
- Independencia del proveedor: Al disponer del código fuente, cualquier persona puede continuar ofreciendo soporte, desarrollo u otro tipo de servicios para el software.
- Mayor seguridad y privacidad: Los sistemas de almacenamiento y recuperación de la información son públicos. Cualquier persona puede ver y entender cómo se almacenan los datos en un determinado formato o sistema.
- Existe una mayor dificultad para introducir código malicioso como puede ser: virus, espías, etc. Es prácticamente imposible ser vulnerables a este tipo de ataques. 4. Garantía de continuidad: el software libre puede seguir siendo usado aun después de que haya desaparecido la persona que lo elaboro, dado que cualquier técnico informático puede continuar desarrollándolo, mejorándolo o adaptándolo.
- Ahorro en costos: en cuanto a este tópico debemos distinguir cuatro grandes costos: de adquisición, de implantación (este a su vez se compone de costos de migración y de instalación), de soporte o mantenimiento, y de

interoperabilidad. El software libre principalmente disminuye o elimina el costo de adquisición ya que al otorgar la libertad de distribuir copias se puede ejercer con la compra de una sola licencia y no tantas como computadoras posean (como sucede en la mayoría de los casos de software propietario) o en muchos casos este ya es gratuito. Cabe aclarar que también hay una disminución significativa en el costo de soporte, no ocurriendo lo mismo con los costos de implantación y de interoperatividad.

- Documentación: por lo general, el software libre siempre está bien documentado, no solo en su código fuente, sino también en los archivos auxiliares de configuración que este usa, haciéndolo de esta manera más sencillo al usuario en cuanto a su estudio, ejecución, configuración, mejoras y modificación.

Desventajas

- Dificultad en el intercambio de archivos: esto se da mayormente en los documentos de texto (generalmente creados con Microsoft Word), ya que si los se desean abrir con un Software Libre (como lo son: Open Office o LaTeX) nos arrojan errores o se pierden datos.
- Mayores costos de implantación e interoperabilidad: dado que el software constituye una novedad, ello supone afrontar un costo de aprendizaje, de instalación, de migración, de interoperabilidad, etc., cuya cuantía puede verse disminuida por: mayor facilidad en las instalaciones y/o en el uso, uso de emuladores. Vale aclarar que el costo de migración está referido al software, ya que en lo que respecta a Hardware; generalmente el Software Libre no posee mayores requerimientos que el Software Propietario.

ANEXO 8. SOFTWARE LIBRE. PLATAFORMAS Y SISTEMAS OPERATIVOS

Características Técnicas de la Distribución GNU-Linux Ubuntu

Ítem	*Características*	*Detalles*	*Valoración Comparativa*[1]
1	**Arquitecturas Soportadas**	I386, IA64, AMD64.	3
2	**Requisitos de Hardware Mínimos**	Modo texto: *Procesador: 400 MHz Pentium,* *Memoria: 192MB,* *Disco Duro: 450MB.* Modo gráfico: *Procesador: 800 MHz Pentium,* *Memoria: 256MB,* *Disco Duro: 2GB.*	4
3	**Licencia**	El Software básico es libre GNU GPL pero incluye paquetes con software propietario.	5
INSTALACIÓN			
4	**Instalador Global**	El programa de instalación es rápido y realiza muy pocas preguntas. Únicamente se añaden unas pocas pantallas para el modo experto, y elimina algunas en modo principiante, por lo que limita la posibilidad de personalización.	3
5	**Selección de Paquetes**	La selección de paquetes es muy deficiente, pues no está disponible. Sin embargo, se puede instalar paquetes adicionales usando apt-get.	1

6	Grupo de paquetes predefinidos	Únicamente se puede seleccionar entre opciones de escritorio o servidor. No se puede realizar la selección por grupos de paquetes.	2
7	Instalación en Modo Experto	Posee dos opciones de instalación: Modo Experto (núcleo 2.4) y Principiante (núcleo 2.6).	3
8	Instalación Gráfica	Los cuadros de diálogo del instalador son bastante simples de entender y es muy amigable para usuarios novatos. Las instalaciones personalizadas no cuentan con facilidades.	3
9	Velocidad de Instalación	El Live-CD de instalación es bastante rápido, realiza pocas consultas y luego copia todo el Live-CD en el disco, configura el hardware e inicia el menú de arranque, proceso que lleva alrededor de 30 minutos.	9
	CONFIGURACIÓN		
10	Manejo del Sistema Basado en Modo Gráfico	Ubuntu no proporciona un panel de control específico para su distribución. Aún así cuenta una gran cantidad de herramientas específicas agregadas por defecto como: notificador de actualizaciones, gestor de instalación y actualizaciones, gestor de red para wifi y gestores de búsqueda.	10
11	Manejo del Sistema Basado en Consola	Este paquete de herramientas de configuración llamado debconf, es muy útil, proviene del proyecto Debian y está disponible en las herramientas de configuración estándar de Debian.	10
	SISTEMA DE PAQUETES		
12	Cantidad de Paquetes	Existen repositorios oficiales, con más de 10000 paquetes específicos para Ubuntu, construido y soportado por su equipo de desarrollo.	8
13	Gestión de Paquetes y Resolución Automática de Dependencias	Smart es un gestor de paquetes utilizado en Ubuntu es el único gestor que se considera superior a APT por su rapidez. Permite encontrar los paquetes certificados y no certificados desde los repositorios de la distribución en internet y resolver automáticamente las dependencias.	10
14	Herramientas Gráficas de Manejo de Paquetes	Sináptica es una interfaz gráfica para Smart y es una herramienta de actualización muy útil si los usuarios prefieren hacer clic rápidamente.	10

EFICIENCIA			
15	**Velocidad del Sistema de Arranque**	Considerando la selección de los servicios y la configuración por defecto el arranque de Ubuntu lleva en promedio un tiempo de 1 minuto.	8
16	**Velocidad de Respuesta del Sistema**	Cuenta con configuraciones especiales de optimización habilitadas manualmente para utilización especialmente como estaciones de trabajo.	5
ESTABILIDAD Y DISPONIBILIDAD			
17	**Centro de Seguridad**	Todos los paquetes de seguridad importante incluyendo los paquetes de protección de memoria y núcleo que se actualizan a diario, sin embargo, no existen cortafuegos y casi ninguna herramienta de seguridad acceso a recursos de red en la instalación por defecto.	8
18	**Estabilidad y Madurez**	Ubuntu está basado en Debian, que es una de las distribuciones más estables y maduras disponibles actualmente. Sin embargo, Ubuntu incluye software adicional y las situaciones de inestabilidad pueden ocurrir.	5
19	**Documentación**	Permite obtener fácilmente la documentación necesaria, desde varias fuentes, como: la página oficial del proyecto, las comunidades y los manuales del sistema.	7

Características Técnicas de GNU-Linux CentOS

Ítem	Características	Detalles	Valoración Comparativa(*)
1	**Arquitecturas Soportadas**	I386, IA64, AMD64, SPARC, HPPA, S390, POWERPC, ALPHA.	7
2	**Requisitos de Hardware Mínimos**	Modo texto: Procesador: 200 MHz Pentium, Memoria: 128MB, Disco Duro: 1 GB. Modo gráfico: Procesador: 400 MHz Pentium, Memoria: 512 MB, Disco Duro: 1 GB.	10
3	**Licencia**	Software GNU GPL en su totalidad.	10
		INSTALACIÓN	
4	**Instalador Global**	El instalador es muy desarrollado, pues es similar a Red Hat utiliza Anaconda para realizar el proceso de instalación, ofrece funciones tanto para principiantes como para usuarios expertos. Contiene numerosas características que permiten personalizar la instalación del sistema operativo.	7
5	**Selección de Paquetes**	Los paquetes pueden ser seleccionados fácilmente e incluyen todas las dependencias, pero no describe muy claramente la utilidad de cada paquete.	7
6	**Grupo de paquetes predefinidos**	Esta característica es muy buena, pues, se realizó pensando en el perfil de uso del sistema operativo. Todos los grupos de paquetes incluyen paquetes instalados por defecto y opcionales. La instalación por defecto es un sistema de escritorio con GNOME, podrá elegir entre 4 modalidades: Escritorio Personal, Estación de Trabajo, Servidor o Personalizada.	4
7	**Instalación en Modo Experto**	Durante la instalación frecuentemente se puede ingresar a opciones de configuración avanzada, para realizar instalaciones no comunes.	7
8	**Instalación Gráfica**	La instalación gráfica utiliza Anaconda aunque se puede seleccionar la instalación basada en consola, ya que la instalación gráfica requiere de una elevada cantidad de memoria.	10

9	**Velocidad de Instalación**	El tiempo de instalación es algo extenso, aunque eso depende del perfil seleccionado, la instalación que demora más tiempo es el perfil de servidor, un sistema básico lleva alrededor de 2 horas y media.	4
CONFIGURACIÓN			
10	**Manejo del Sistema Basado en Modo Gráfico**	Existen muchas herramientas que permiten la configuración en modo gráfico en su mayoría basado en GNOME. La mayor parte de configuración del sistema de operaciones se puede realizar sin necesidad de abrir la ventana del terminal.	5
11	**Manejo del Sistema Basado en Consola**	Centos contiene algunas herramientas de consola que permiten la gestión del equipo de manera integral, incluyen la configuración de la tarjeta de red, audio, video, servicios, etc.	10
SISTEMA DE PAQUETES			
12	**Cantidad de Paquetes**	El número de paquetes incluidos en los discos de instalación es muy completo aunque los repositorios no son tan extensos como los de sus competidores. Cuenta con repositorios activados: kbs-CentOS-Extras, update, rpmforge, base, contrib, addons, extras. El número de paquetes reportados por un listado con yum es 5785.	6
13	**Gestión de Paquetes y Resolución Automática de Dependencias**	Posee un gestor de paquetes por defecto llamado yum, heredado de su fuente como es Red Hat Linux.	6
14	**Herramientas Gráficas de Manejo de Paquetes**	Centos 5 cuenta con herramientas gráficas basadas en yum como son: Pirut para realizar el manejo de paquetes y Pup para realizar las actualizaciones.	6
EFICIENCIA			
15	**Velocidad del Sistema de Arranque**	El tiempo de arranque de Centos depende en gran parte de su configuración y de los servicios activados, si se configura adecuadamente se puede lograr un sistema de arranque muy rápido en promedio lleva de 1 a 2 minutos en una instalación por defecto.	7
16	**Velocidad de Respuesta del Sistema**	La velocidad de respuesta es bastante buena, aunque cuenta con configuraciones especiales para optimizaciones ya sea para uso de escritorio o de servidor que deben ser configuradas manualmente.	5

ESTABILIDAD Y DISPONIBILIDAD			
17	Centro de Seguridad	Ofrece una gran cantidad de características de seguridad similares a Red Hat, partiendo de las aplicaciones más seguras como: permitir el acceso a nuevas herramientas de seguridad a nivel chip y memoria. La desventaja es que lleva un tipo considerable los parches oficiales para vulnerabilidades detectadas.	10
18	Estabilidad y Madurez	La estabilidad es una de las características más importantes de esta distribución, ya que se basa en paquetes de software bien probado y conservador que aseguran que su funcionamiento sea adecuado para ambientes empresariales.	10
19	Documentación	Existe disponible documentación muy variada, especialmente proveniente del proyecto Red Hat, y complementada por la comunidad de desarrolladores.	8

II.5.5.2.2 GNU/Linux Centos: CentOS (Community ENTerprise Operating System - Sistema Operativo de la Comunidad Empresarial) es una distribución Linux de clase empresarial derivada de los archivos fuentes provistos libremente al público por Red Hat. CentOS cumple completamente la política de redistribución y apunta a ser 100% compatible a nivel binario (programas) con Red Hat Enterprise Linux. En CentOS los principales cambios con respecto a RHEL(Ret Hat Enterprise Linux), es la eliminación de las ilustraciones y marcas de Red Hat de los paquetes. CentOS es gratuito, y está orientado a los usuarios que necesiten un sistema operativo de nivel empresarial, pero sin pagar los costos de certificación y soporte de Red Hat. CentOS es desarrollado por un creciente grupo de programadores. Los que son ayudados por una activa comunidad de usuarios, que incluye administradores de sistema, administradores de red, empresas, administradores, contribuidores del núcleo Linux y

entusiastas de Linux de todo el mundo. CentOS tiene algunas ventajas con respecto a proyectos similares: una activa y creciente comunidad de usuarios, desarrollo rápido, probado y corregido, una extendida red de réplicas, múltiples y gratuitas vías de soporte, foros, etc. CentOS es un sistema estable que puede ser usado, ya sea como un servidor o como un sistema de escritorio de un usuario normal. Esto último requiere algunas modificaciones en la instalación por defecto.

Arquitectura de Asterisk

La figura a continuación, muestra los diferentes subsistemas que conforman Asterisk

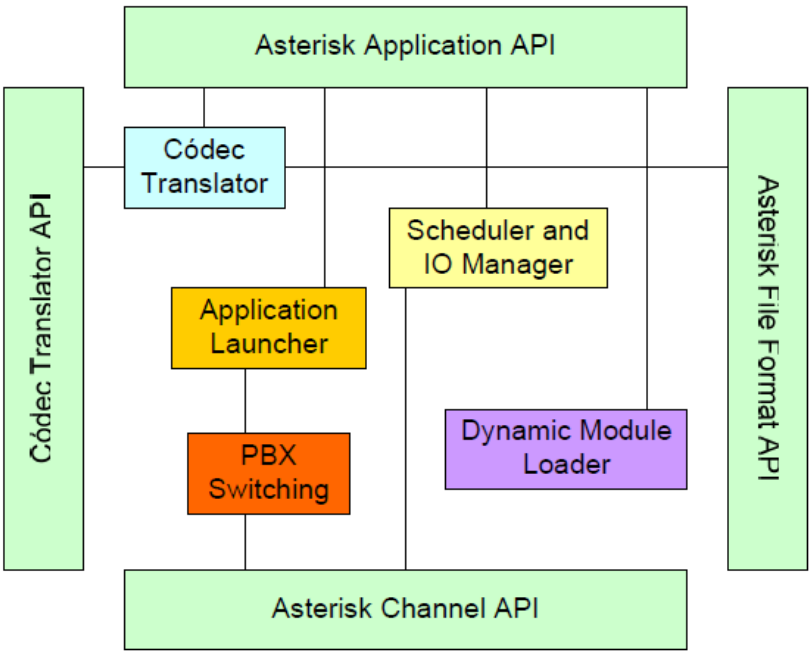


Figura 2.35- Arquitectura y Subsistemas de Asterisk.

Fuente: www.asterisk.org

Cada uno de ellos realiza una función diferente:

- *Dinamic Module Loader: cuando se inicia Asterisk, es el encargado de cargar e inicializar los drivers necesarios*
- *PBX Switching: es el encargado de aceptar y conectar las llamadas que recibe por las interfaces. Actúa según lo definido en el plan de numeración*
- *Application Launcher: el PBX Switching utiliza este subsistema para lanzar las aplicaciones que sean necesarias como por ejemplo hacer sonar un teléfono, hacer saltar el buzón de voz de un usuario, etc.*
- *Codec Translator: codifica y decodifica los formatos de audio en el caso de que dos canales usen un códec diferente*
- *Scheduler and I/= Manager: es el encargado de organizar las tareas de bajo nivel y de gestionar la entrada/salida para conseguir un óptimo rendimiento en todo tipo de situaciones de carga de trabajo.*

Hay cuatro APIs (Application Programming Interface) definidas para proporcionar funcionalidad de forma independiente al tipo de hardware y al protocolo que usen.

- *Channel API: esta API provee mecanismos para manejar el tipo de conexión que se está utilizando en una llamada (VoIP, ISDN, etc.)*
- *Application API: proporciona la funcionalidad para ejecutar aplicaciones tales como el buzón de voz, directorio de llamadas, etc.*
- *Codec Translator API: contiene los módulos de diferentes códecs para dar soporte a los diferentes formatos de audio y video*
- *File Format API: proporciona la funcionalidad necesaria para la lectura y escritura de diferentes formatos de archivo que se almacenan en el sistema.*

Canales en Asterisk

El concepto de canal en Asterisk es de suma importancia. Asterisk utiliza un canal para comunicarse con los clientes que utilicen un protocolo o una tecnología determinada. Los nombres de estos canales coinciden con los nombres de los protocolos y tecnologías que se emplean para la comunicación. Así, se pueden identificar los siguientes canales:

- *Canal SIP: será el canal que se utilice para las comunicaciones que se envíen o reciban de clientes SIP*
- *Canal H.323: es el canal que se usará en las comunicaciones de los clientes que utilicen el protocolo H.323*
- *Canal IAX2: lo mismo pero para clientes que utilicen el protocolo IAX2*
- *Canal Dahdi: es el canal que utiliza Asterisk para comunicarse con las líneas provenientes de la RTB tanto analógicas como digitales.*

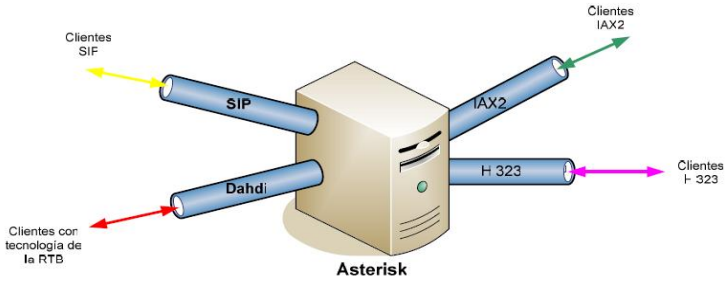


Figura 2.36- Canales de Asterisk.

Fuente: www.asterisk.org

ANEXO 9. LIBRERÍA OPENH323.

En el objeto EP se configura la tabla de capacidades disponibles y el orden de preferencia en cuanto a uso se refiere. El EP también puede proponer conjuntos de capacidades o Códecs informando así a otros terminales de posibles modos de funcionamiento incluyendo o excluyendo el uso de Códecs de forma simultánea. El intercambio de primitivas para la selección de Códecs corre a cargo de la negociación basada en la norma UIT-T H.245. Esta negociación se conoce como "Intercambio de capacidades". Como métodos o funciones de más bajo nivel, la clase EP también ofrece el manejo de canales lógicos, determinación del tipo de terminal, configuración de temporizadores y contadores.

Como clase que desciende directamente de la clase EP, se tiene la clase H323Listener. Esta clase representa un punto de escucha para la recepción de primitivas entrantes. El tipo de listener depende del tipo de protocolo. Por ejemplo, para el caso de una comunicación VoIP basada en H.323 se empleará un listenerIP que equivale a tener un hilo testeando cualquier petición de llamada entrante. Una vez que la petición llega al listener, éste creará un objeto perteneciente a la clase H323Transport. Un objeto de tipo H323Transport representa a una entidad equivalente al nivel de transporte del modelo OSI. El objeto del nivel de transporte recibirá y enviará las PDU (Packet Data Unit) relacionadas con la llamada H.323. Una vez que una llamada es aceptada, a la llamada se le asigna un identificador único, lo que equivale identificar la conexión H.323 realizada. La conexión H.323 se modela mediante objetos de la clase H323Connection; al crearse un objeto de esta clase se crea un canal ITU-T Q.931 sobre el que comienza el intercambio de señalización ITU-T H.225.0. Con la finalización de la señalización H.225.0 se habrá establecido un canal de control por el que se llevará a cabo la señalización de llamada. (http://openh323.sourceforge.net/).

Evolución OpenH323

El proyecto OpenH323 y su evolución hasta la actualidad:

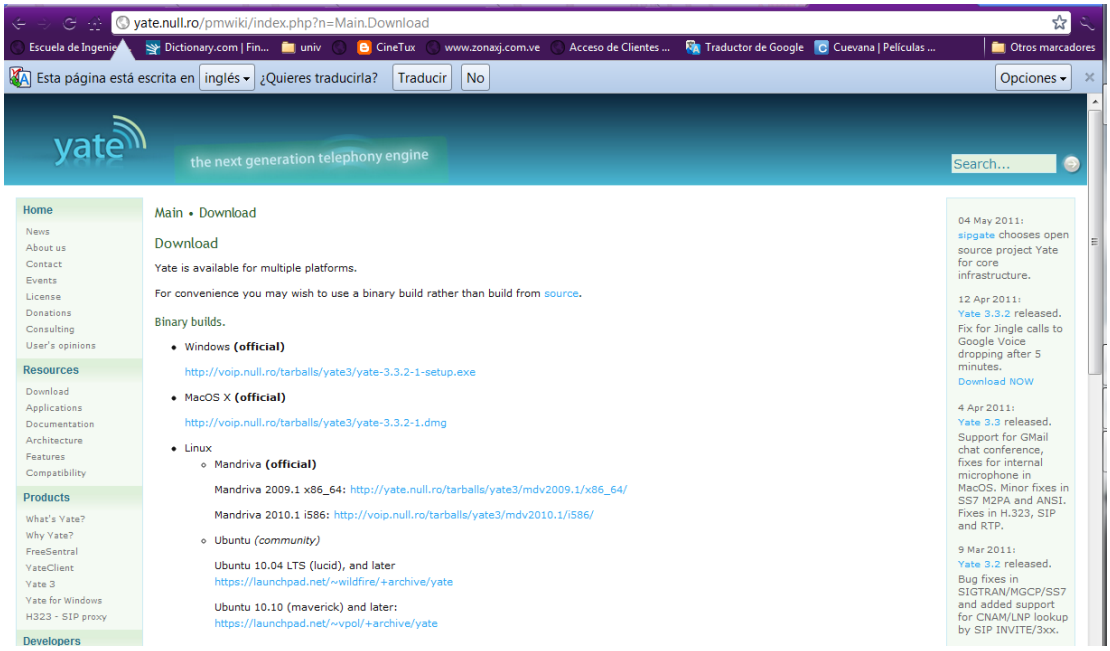
- 1998 openh323.org.
- Pwlib (1992).
- Codigo Abierto bajo MPL.
- 1999 Open Phone Abstraction Library OPAL.
- 2003 openh323 fue incorporado al repositorio SourceForge.
- 2007 Pwlib es renombrada Ptlib.
- 2007 Una rama de Openh323 es llamada h323plus y es incorporado al repositorio SourceForge.
- 2009 Pasa a manos de Voxgratia y se une al proyecto OPAL y es incorporado al repositorio SourceForge.

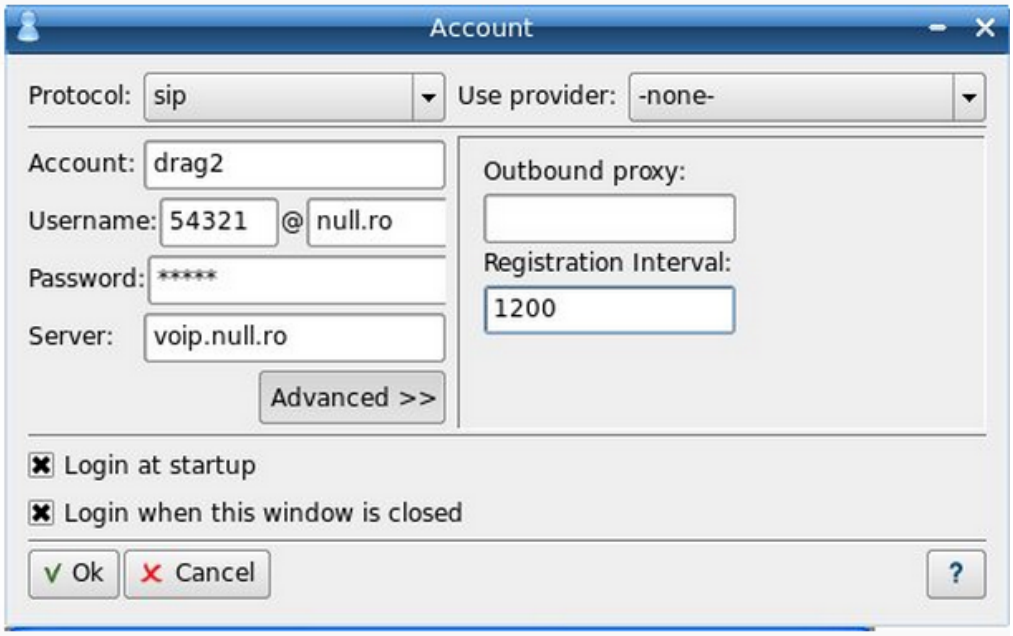
ANEXO 10. SOFTPHONES. INSTALACIÓN Y CONFIGURACIÓN

Configuración Cliente Yate

Para la instalación del Cliente Yate, en principio se puede acceder a la página www.yate.null.ro y descargar el programa de acuerdo al sistema operativo con que se cuente; posteriormente se seguirán los pasos de instalación encontrados en el asistente de instalación propio de Yate.

Para la configuración de un cliente Yate es necesario asignar crear una cuenta con un número de marcación indistinto ya que lo único que se necesita es crear la cuenta para que se puedan comunicar sin necesidad de registrar previamente una cuenta. (Hay que tener a la mano la IP del ordenador donde se encuentre el Gatekeeper, en caso de contar con uno y la IP del Gateway).


yate.null.ro/pmwiki/index.php?n=Main.Download
Esta página está escrita en inglés ¿Quieres traducirla? Traducir No Opciones
yate
the next generation telephony engine
Search...
Home
News
About us
Contact
Events
License
Donations
Consulting
User's opinions
Resources
Download
Applications
Documentation
Architecture
Features
Compatibility
Products
What's Yate?
Why Yate?
FreeSentral
YateClient
Yate 3
Yate for Windows
H323 - SIP proxy
Developers
Main • Download
Download
Yate is available for multiple platforms.
For convenience you may wish to use a binary build rather than build from source.
Binary builds.
Windows (official)
http://voip.null.ro/tarballs/yate3/yate-3.3.2-1-setup.exe
MacOS X (official)
http://voip.null.ro/tarballs/yate3/yate-3.3.2-1.dmg
Linux
Mandriva (official)
Mandriva 2009.1 x86_64: http://yate.null.ro/tarballs/yate3/mdv2009.1/x86_64/
Mandriva 2010.1 i586: http://voip.null.ro/tarballs/yate3/mdv2010.1/i586/
Ubuntu (community)
Ubuntu 10.04 LTS (lucid), and later
https://launchpad.net/~wildfire/+archive/yate
Ubuntu 10.10 (maverick) and later:
https://launchpad.net/~vpol/+archive/yate
04 May 2011:
sipgate chooses open source project Yate for core infrastructure.
12 Apr 2011:
Yate 3.3.2 released.
Fix for Jingle calls to Google Voice dropping after 5 minutes.
Download NOW
4 Apr 2011:
Yate 3.3 released.
Support for GMail chat conference, fixes for internal microphone in MacOS. Minor fixes in SS7 M2PA and ANSI. Fixes in H.323, SIP and RTP.
9 Mar 2011:
Yate 3.2 released.
Bug fixes in SIGTRAN/MGCP/SS7 and added support for CNAM/LNP lookup by SIP INVITE/3xx.

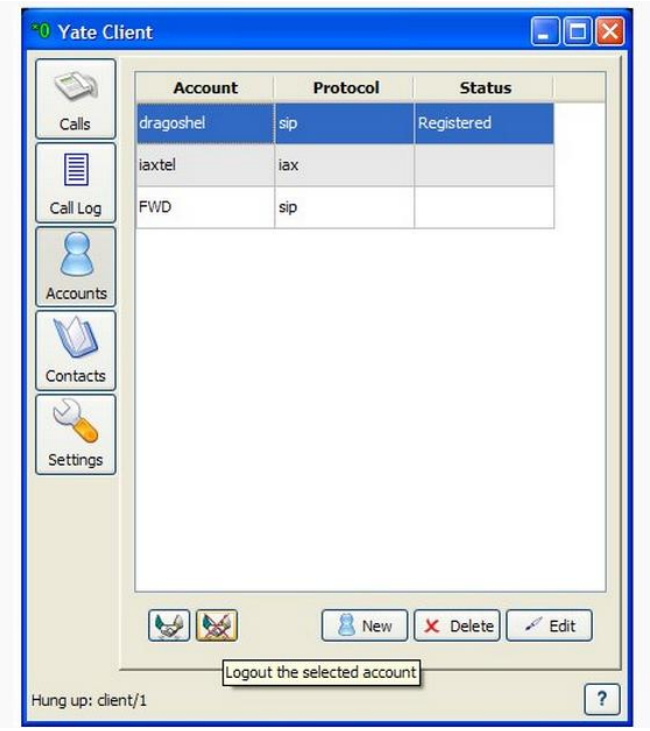

Account
Protocol: sip
Use provider: -none-
Account: drag2
Username: 54321 @ null.ro
Password: *****
Server: voip.null.ro
Advanced >>
Outbound proxy:
Registration Interval:
1200
Login at startup
Login when this window is closed
Ok
Cancel
?

Zonas a Configurar:

- Se selecciona el protocolo para este fin seleccionaremos H.323. Este cliente cuenta con opciones para manejar otros protocolos, como SIP, en el caso de que se quiera tomar como cliente SIP.
- Accounting (cuenta). Se escoge un nombre cualquiera. O en su defecto puede ser el mismo número, en este caso como los clientes H.323 se le asignaron los números con extensiones 7XX, se colocó el número 701.
- Username (nombre de usuario). En este campo se coloca el número que escogimos. seguido del @servidor, en caso de contar con un servidor se especifica en este apartado pero para este caso, no se usará ninguno.
- Password (contraseña). Se coloca la contraseña deseada o se puede omitir. Para este caso se colocó el mismo número de la extensión 701.
- Server (para este caso será Elastix o el Gateway). Se coloca la IP donde está el Gateway (Gatekeeper); para este caso la IP será la IP donde se encuentre el Gateway o Elastix.
- Para finalizar se selecciona OK

Finalmente para realizar una llamada, bse disca dependiendo del cliente con que se esté trabajando

- Se verifica que la cuenta esté activa y el softphone registrado

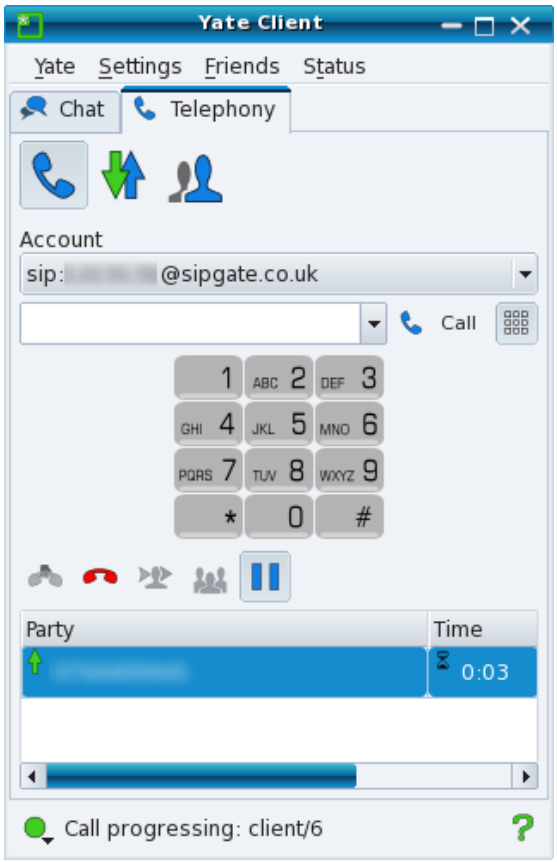


- En caso de llamar a través de una cuenta SIP, una vez posicionado en la cuenta, se disca el número de la extensión a la cual se desea llamar. (se recuerda que en la cuenta debe colocarse la dirección IP del servidor, en este caso Elastix) y posteriormente la tecla de llamada (teléfono verde).
- En caso de llamar a través de una cuenta H.323: existen diferentes formas:
    - Si se cuenta con un Gatekeeper, se debe colocar la dirección del Gatekeeper en la cuenta y para realizar la llamada se debe discar h323:ext@ip…..Donde ext: es el número o nombre de la extensión h.323 que se desea llamar e ip: es una dirección IP válida donde se encuentra el gatekeeper y luego presionar la tecla de llamada.
    - Si se cuenta con un servidor, MCU, Gateway (Elastix en este caso): se realiza igual a la llamada con Gatekeeper, sin incluir el nombre de la extensión y se sustituye la dirección IP donde se encuentra el Gatekeeper, por la dirección IP donde se encuentre el Servidor, MCU o Gateway (Elastix) según sea el caso (para el caso del MCU, se debe

especificar el puerto, la sintaxis de la llamada sería: h323: 192.168…<ip MCU>:1420<puerto MCU>).

- Si se desea llamar a otro cliente H.323, simplemente basta con escribir h323: dirección IP del otro cliente H.323 y posteriormente presionar la tecla de llamada.

Para finalizar una llamada en cualquiera de los casos anteriores, sólo basta con presionar el botón de finalización de llamada (teléfono rojo)



Configuración e Instalación del Softphone X-Lite

Primero debe de tener instalado el Programa X Lite, para posteriormente pasar a configurar su Extensión y Nombre del usuario de la misma. El programa lo puede descargar sin costo alguno de: http://www.counterpath.com/x-lite.html

Es importante que descargue la aplicación que va acorde con su Sistema Operativo.

La siguiente tabla es muy parecida a la que aparece en la dirección que se proporcionó arriba.

Nombre	Sistema Operativo	Logotipo Representativo.
X-Lite v3.0 for Windows	Microsoft Windows XP	
X-Lite v2.0 Build 1106q for MAC OS X [X-Lite_Install.dmg]	Mac OS X	
X-Lite v2.0 Build 1105d for Linux [X-Lite_Install.tar.gz]	Linux	

Posteriormente ya descargado el archivo, ejecútelo y seguirá los siguientes pasos.

Tras instalar, la pantalla principal de X-Lite es la siguiente:

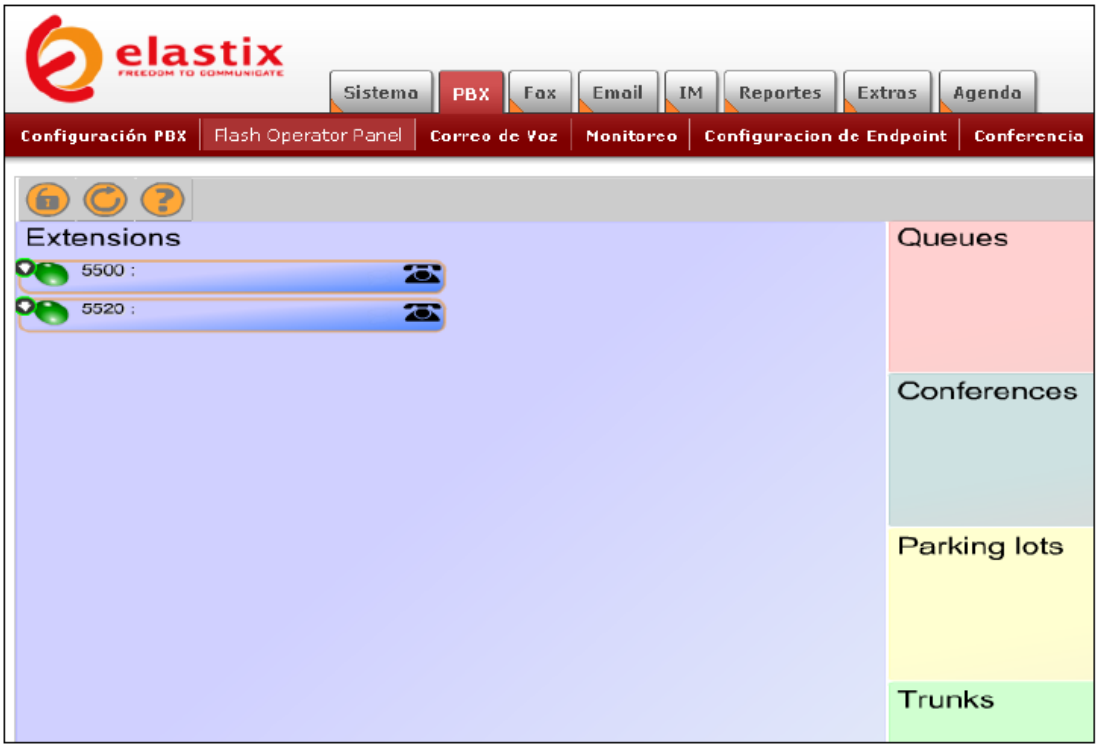
Para configurarlo se debe acceder a la opción SIP Account Settings… en el menú principal. Aparecerá un listado de cuentas (en este momento vacío), al lado derecho se debe pulsar Add… y luego, en la primera pestaña, Account, se deben ingresar los datos:

- Display Name: en este caso el nombre o número de la extensión sip (para este trabajo las extensiones SIP utilizan el prefijo 9XX)
- User Name: corresponde a User Extension, la cual es el número de la extensión (para este caso 901)
- Password (secret): es una contraseña que se añade si se quiere se puede omitir, en este caso se le colocó el mismo número de extensión.
- Domain: dominio o dirección IP del Gateway, Gatekeeper o servidor SIP; cualquiera sea su caso. Para este trabajo, se utilizó la dirección del Gateway, que en este caso es la máquina que contiene Elastix.

Todos los datos deben coincidir con los que se usaron al momento de crear la extensión dentro de Elastix (o Asterisk). Posteriormente se debe pulsar Accept, y luego en el listado de cuentas marcar la casilla Enabled junto a la cuenta que se acaba de crear. Después de unos segundos, y si todo se ha hecho correctamente, el estado del teléfono cambiará a conectado.

Para realizar una llamada, basta con discar el número de la extensión a la cual se quiere contactar y posteriormente la tecla de llamada (teléfono verde). Para finalizar una llamada, se disca la tecla de finalización de llamada (teléfono rojo).

Además mediante la interfaz web de Elastix se podrá apreciar qué teléfonos están conectados, además de mostrar su actividad en el Flash Operator Panel (FOP) al cual se accede recorriendo los menús PBX -> Flash Operator Panel, la contraseña por defecto se encuentra en el archivo /etc/amportal.conf y por defecto es „eLaStIx.2oo7“ .


elastix
FREEDOM TO COMMUNICATE
Sistema
PBX
Fax
Email
IM
Reportes
Extras
Agenda
Configuración PBX
Flash Operator Panel
Correo de Voz
Monitoreo
Configuracion de Endpoint
Conferencia
Extensions
5500 :
5520 :
Queues
Conferences
Parking lots
Trunks

Configuración del Software Ekiga en ambiente Linux (método más estable)

Instalación de las librerías:

Accediendo al terminal en modo súper usuario se escribieron los siguientes comandos:

apt-get install autoconf2.59 cpp cpp-4.4 dpkg-dev gcc gcc-4.4 gcc-4.4-base gcc-4.4-doc gcc-4.4-multilib gcc-4.4-plugin-dev gcc-4.4-source gcc-doc gcc-multilib gccxml gcj gcj-4.4-base gcj-4.4-jdk gcj-4.4-jre-lib gcj-jdk gfortran-doc gfortran gfortran-4.4-doc gfortran-4.4 gfortran-4.4-multilib gfortran-multilib gobjc gobjc-4.4 hardening-wrapper lib64gcc1 lib64gcc1-dbg lib64gomp1 lib64gomp1-dbg libeigen2-dev libgcc1 libgcc1-dbg libgcj10 libgcj10-dbg libgcj10-dev libgomp1 libgomp1-dbg llvm uno-libs3 uno-libs3-dbg.

apt-get install gnome-common libsasl2-dev gettext libgnome2-dev libldap2-dev libgconf2-dev autoconf libgnomeui-dev libxv-dev intltool scrollkeeper libxml-parser-perl evolution-data-server-dev libavahi-common-dev libavahi-client-dev libavahi-glib-dev gnome-doc-utils libsigc++-2.0-dev libdbus-glib-1-dev libebook1.2-dev.

Luego de ser instaladas se descargaron las siguientes carpetas comprimidas: *opal-3.6.8.tar.gz, ekiga.tar.gz, ptlib-2.6.7.tar.gz* de la pagina: http://www.voxgratia.org/ específicamente del proyecto *opal* y fueron guardadas en el escritorio para su fácil ubicación.

Posteriormente se procedió a la compilación escribiendo los siguientes comandos en el terminal:

*aptitude install libspeex-dev libx264-dev libtheora-dev libavcodec-dev libavformat-dev //*librerías de *codecs* de video necesarias para el proyecto *Ekiga*

aptitude install flex bison

apt-get install libdv4-dev libv4l-dev libasound2-dev //proyecto *Open Source* video para *Linux* el cual reconoce los drivers de las cámaras y micrófonos del PC.

cp opal-3.6.8.tar.gz /usr/src

cp ptlib-2.6.7.tar.gz /usr/src

cp ekiga.tar.gz /usr/src

cd /usr/src

ls //verificando que las librerías se ubican en el directorio /usr/src

Para instalar PTLIB:
cd /usr/src
tar zxvf ptlib-2.6.7.tar.gz
cd ptlib-2.6.7
./configure --enable-sunaudio=no --enable-oss=yes --prefix=/usr --disable-sdl --enable-v4l
make
make install
Para instalar OPAL:
cd /usr/src
tar zxvf opal-3.6.8.tar.gz
cd opal-3.6.8
./configure
make
make install

Para instalar Ekiga:
cd /usr/src
tar zxvf ekiga.tar.gz
cd ekiga
./autogen.sh

make
make install
cd /usr/src/opal-3.6.8/lib_linux_x86
cp libopal.so.3.6.8 /usr/local/lib
cd /usr/local/bin
/sbin/ldconfig

Una vez completada la instalación se procedió a reiniciar la computadora y se ubicó el programa en el menú de Aplicaciones → Internet →*Softphone Ekiga*. Para realizar las pruebas necesarias, se utilizó la dirección IP de la computadora donde se encontraba instalado el Elastix (Gateway), con esto se realizó el proceso de establecimiento de sesión

de videoconferencia, luego se verificó en cada uno de los programas cliente los códec de video y audio disponibles y activados, esto se verificó entrando en el menú, luego en la sección de Editar → Preferencias, al realizar esto se abrió una ventana donde se encontraba el menú de audio y video especificando los códec disponibles y se activo el códec de audio PCMA y el códec h261 de video para las pruebas iniciales. Asimismo se pueden elegir otros códecs de audio como lo son Speex, PCMU, GSM, entre otros.

Para realizar la llamada en cada una de las computadoras, este procede a escribir la dirección IP de la máquina con el Gateway (Elastix) previamente instalado, en la barra de llamada del programa *Ekiga* precedido por la especificación del protocolo a usar en este caso H323 (si es el caso del protocolo SIP se colocará SIP seguido de la siguiente sintaxis: SIP: extensión SIP @ dirección ip de la extensión o en su defecto del servidor SIP utilizado) y luego se presionó el botón de llamada representado por un teléfono verde. Existe una forma más sencilla de instalar Ekiga en Ubuntu, la cual es por medio del administrador de descargas de paquetes Synaptic, buscando y seleccionando para instalar el software Ekiga, éste se encontrará listo para usarse, sin embargo, de esta manera el software muchas veces presenta fallas en su operación.

Configuración del Software Ekiga en ambiente Windows

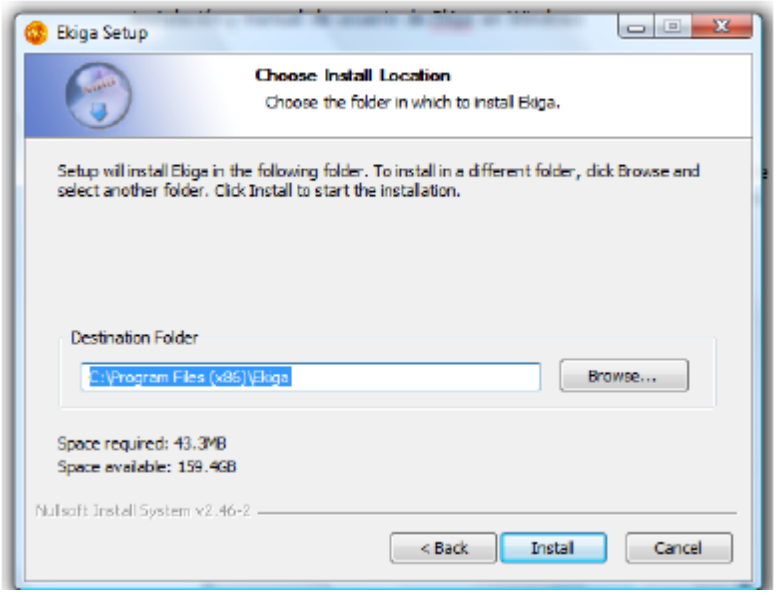
NOTA: antes de realizar los pasos de instalación verificar que tanto su cámara como el micrófono y parlantes funcionan correctamente.

Pasos a seguir:

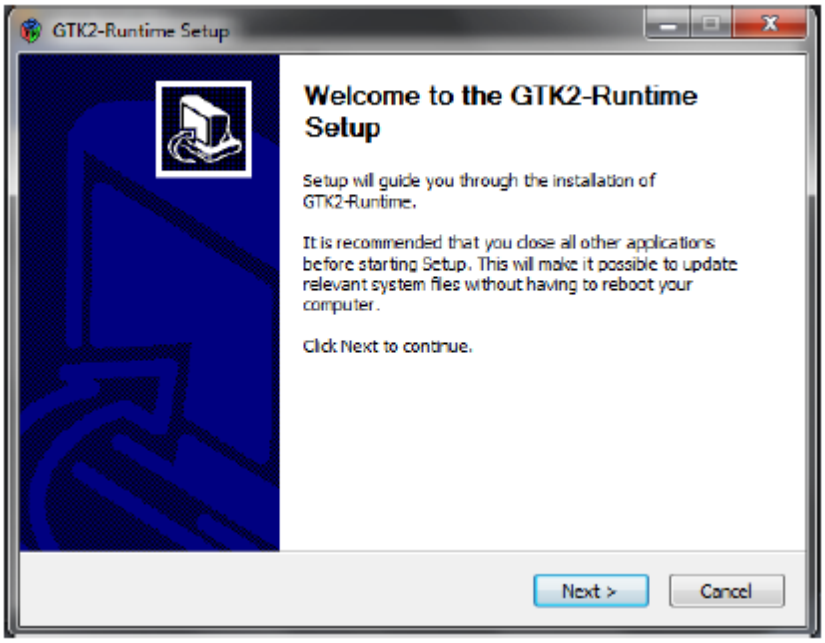
1) Ingresar en la página http://ekiga.org/

2) Descargar la versión 3.2.

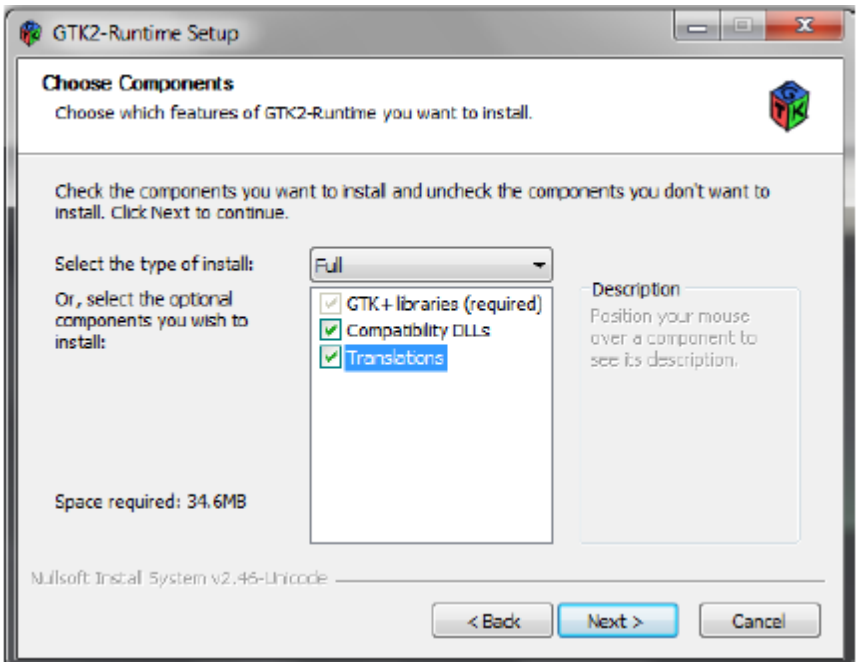
3) Al terminar la descarga ejecutar el *Setup*, aparecerá el asistente de instalación, hacer click en "Next" hasta llegar a la ventana de elección de ubicación para la instalación y hacer click en "Install".



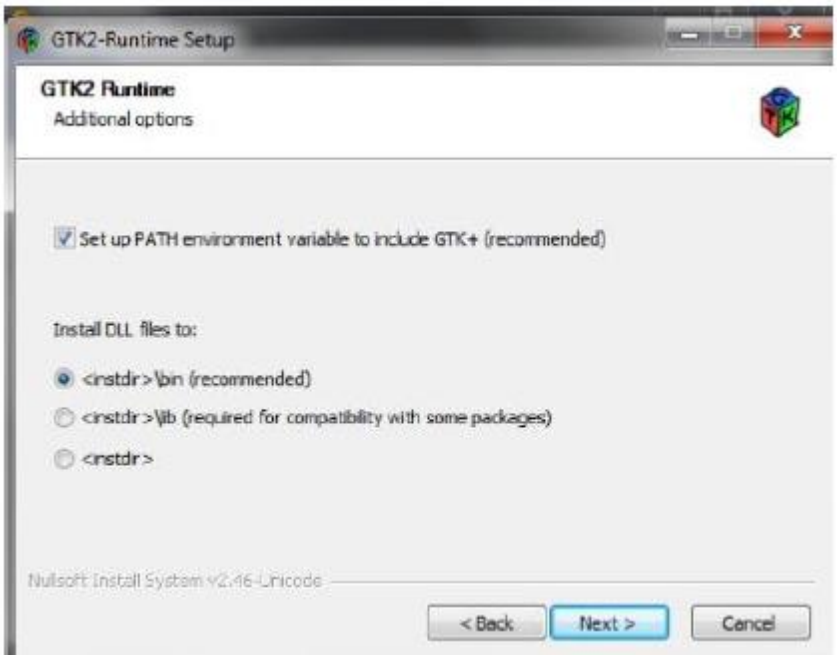
4) Probablemente mientras se realiza la instalación aparezca una ventana para instalar GTK-2, hacer click en “Next”, en la siguiente ventana aceptar los acuerdos y términos de licencia.



5) En la siguiente ventana se deberán elegir los componentes a instalar seleccionar “Compatibilidad DLLs” y “Traducciones”, hacer click en “Next”.



6) La siguiente ventana verificar que tenga seleccionado lo mismo que la imagen y hacer click en ”Next” y finalmente en la siguiente ventana hacer click en “Instalar”.



7) Una vez completado el proceso hacer click en “Next” y “Finish” para Salir del asistente de GTK-2.

8) Luego se abrirá otra ventana, hacer click en “Finalizar”.

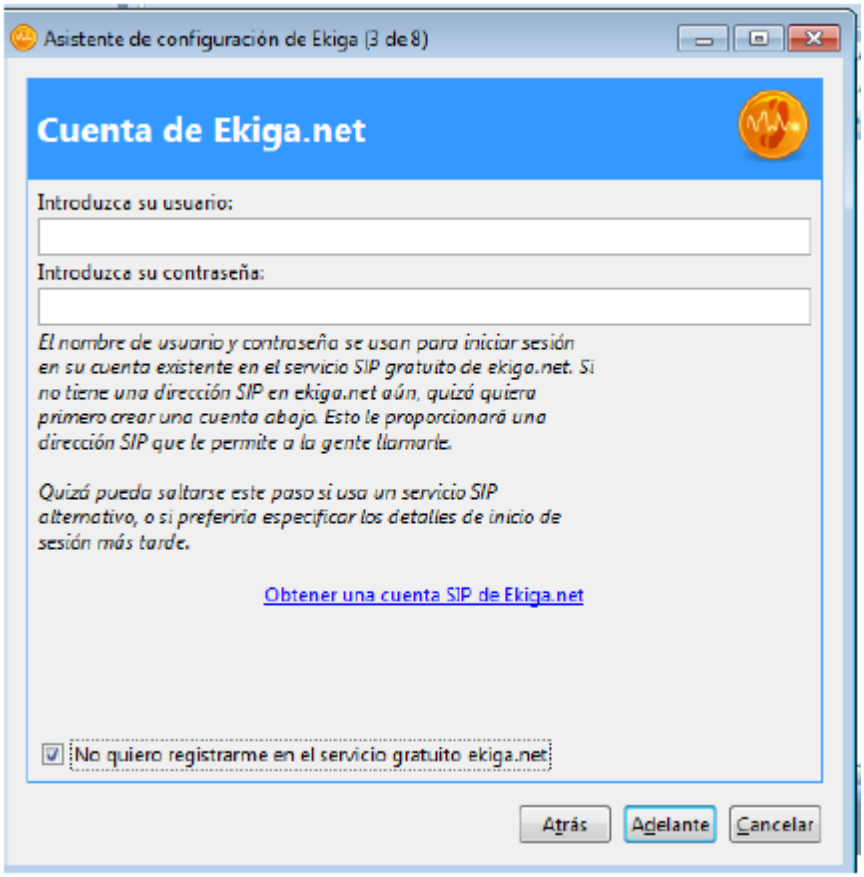
9) Una vez instalado el programa aparecerá el asistente de configuración de *Ekiga* el cual consta de 8 sencillos pasos:

1- Bienvenido, hacer click en “Adelante”.

2- Configuración de nombre de usuario, colocar el nombre y hacer click en “Adelante”.

3- Configuración cuenta de *Ekiga* aquí solo se debe seleccionar la casilla que dice: “No quiero registrarme en el servicio gratuito ekiga.net” y hacer click en “Adelante”.

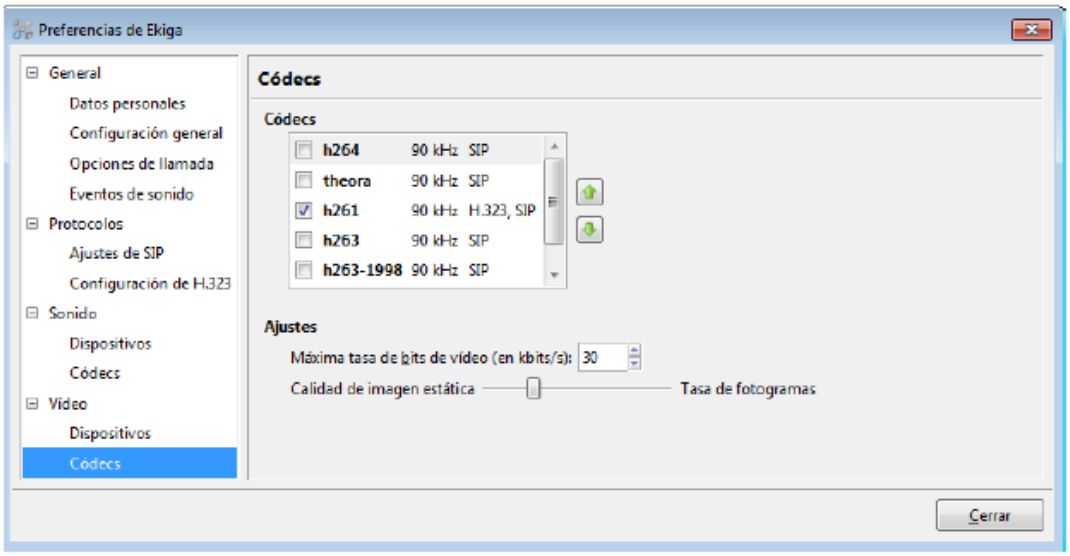
4- Configuración de cuenta de *Ekiga Call out* solo se debe seleccionar la casilla que dice: “No quiero registrarme en el servicio Ekiga call out” y hacer click en “Adelante”.

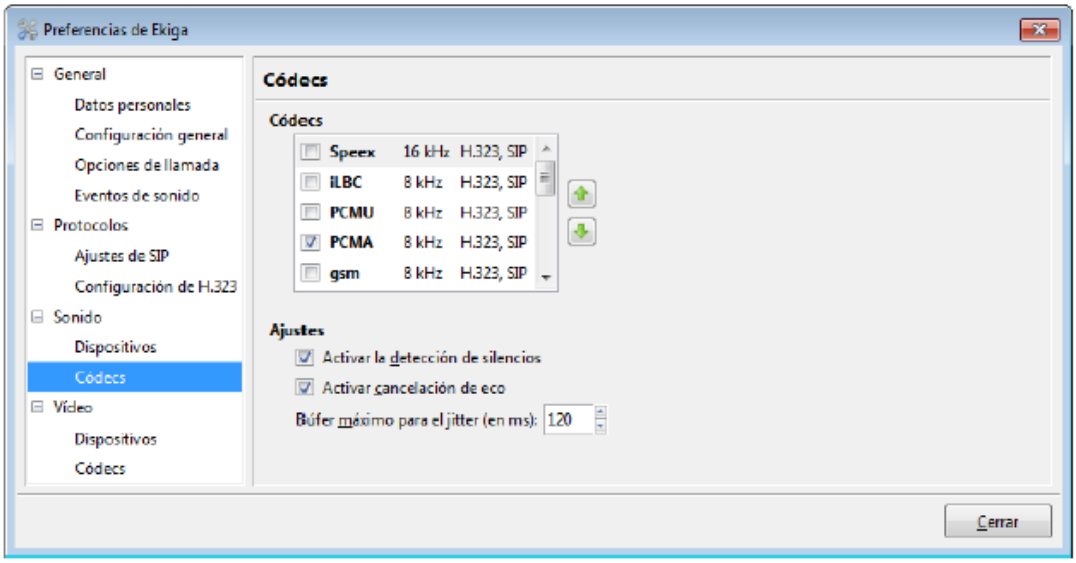


5- Luego los siguientes pasos especifican los dispositivos de conexión de sonido y de entrada de video, dejar lo que sale establecido y hacer click en “Adelante” en las 3 ventanas.

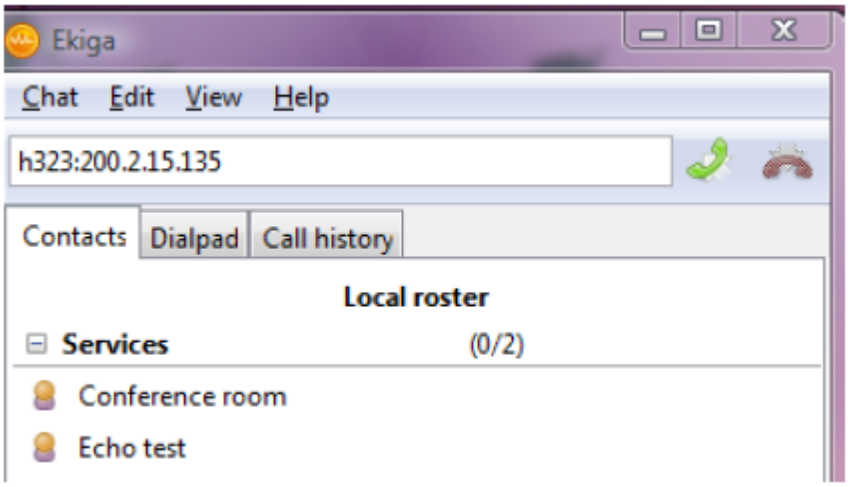
6- Finalmente el último paso es verificar todas las configuraciones hechas anteriormente y hacer click en “Aceptar” para terminar los pasos de configuración.

10) Al hacer esto aparecerá la interfaz grafica de *Ekiga*, se deben ajustar algunas cosas para ello accedemos al menú de Editar -> Preferencias -> Video -> Códec habilitar el h261 y en audio habilitar el códec PCMA hacer esto y cerrar la ventana. Y colocar los valores que se muestran en las imágenes, con respecto a la calidad de imagen estática sólo es necesario bajar un poco la tasa de fotogramas no se requiere ningún valor exacto.





11) Finalmente para establecer la comunicación en la barra de llamada escribir **h323:<dirección ip (Gateway, servidor, MCU, cliente)>** y presionar enter o el símbolo de llamada el cual está representado por un teléfono verde a la derecha de la barra.



12) El programa iniciará la conexión.

13) Para terminar la comunicación presionar el botón de pausar que se encuentra justamente bajo la imagen y luego finalizar haciendo click en el botón de terminar representado por un teléfono rojo en la parte superior derecha al final de la barra de llamada.

ANEXO 11. VIRTUALIZACIÓN

Instalación y Configuración de VirtualBox

VirtualBox es un programa de virtualización capaz de instalar y manejar en nuestro ordenador varios sistemas operativos virtuales en el mismo equipo. El programa ha sido creado por la empresa alemana Innotek y se puede descargar de la web desde el sitio oficial de virtualbox: www.virtualbox.org. Vale decir que este programa es completamente gratuito y está traducido al español.

Instalación de VirtualBox

Para el caso de sistemas operativos basados en Windows, basta descargar la aplicación desde la dirección mencionada e instalarla en la máquina en cuestión. Posteriormente se seguirán los pasos del asistente de instalación.

Para el caso de sistemas basados en plataforma Linux, (dependiendo de la distribución ast-get install, yum install, etc) se puede instalar VirtualBox de dos formas (en este caso sólo se especifica para la distribución GNU/Linux):

1. Descargar VirtualBox de la web oficial. Se trata de un .deb. Una vez descargado se puede instalar:

a.) Desde Terminal: Hay que ir a la carpeta dónde está el fichero descargado e instalarlo con el comando dpkg mediante los siguientes comandos:

```
cd Desktop  dpkg  -i nombredelarchivo.deb
```

b.) Mediante APT (Aptitude, Apt-Get, Synaptic): Ésta es la mejor forma y la más sencilla. Sólo hay que añadir en sources.list el repositorio correspondiente a la versión de Ubuntu con la que se cuente. En el terminal primero se edita el archivo sources.list:

```
sudo gedit /etc/apt/sources.list
```

y se actualiza la lista de repositorios y de la distribución.

sudo apt-get update sudo apt-get dist-upgrade

Se puede instalar VirtualBox desde Synaptic, con apt-get o con aptitude. La ventaja es que con este sistema se resuelven dependencias, cosa que no ocurre con el método anterior. Con cualquiera de estos métodos ya estará instalado VirtualBox en el sistema.

Para abrir el programa hemos de ir a:

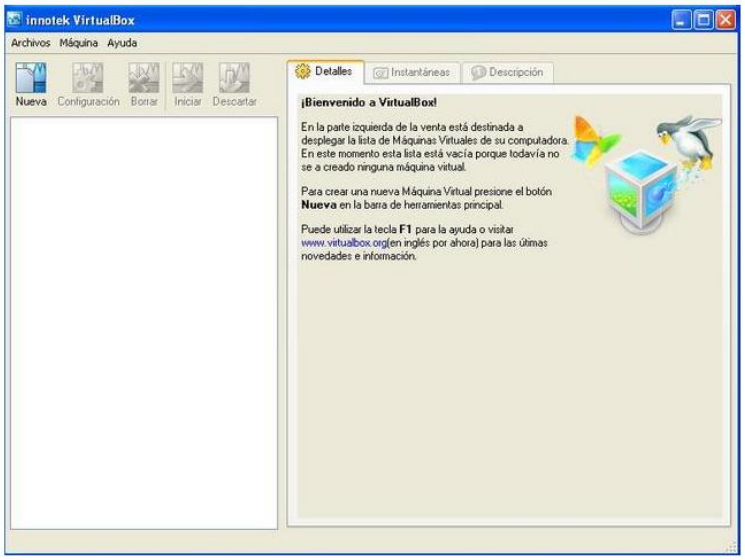
Aplicaciones -> Herramientas del Sistema -> Innotek VirtualBox

con lo que se seguirán los pasos del asistente de configuración.

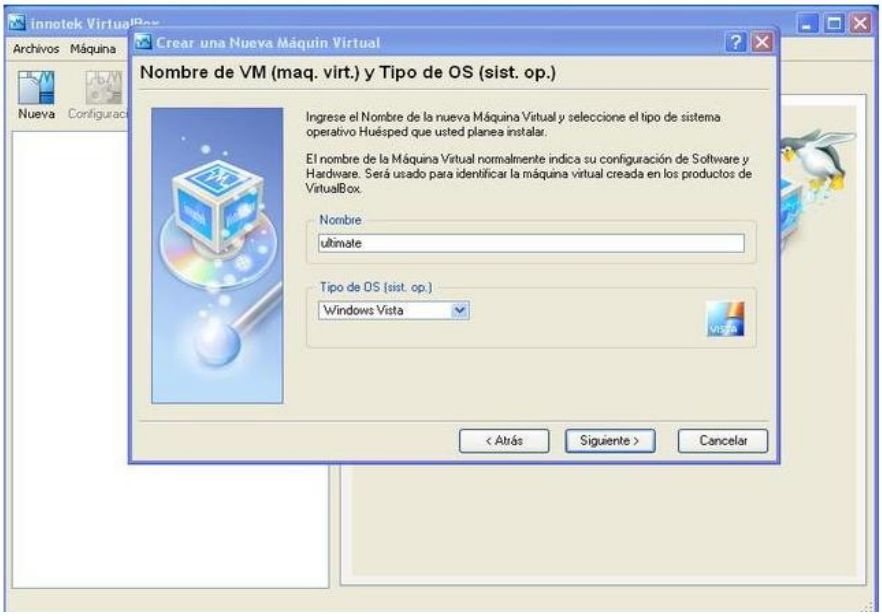
Creación de una Máquina Virtual

Una vez instalado VirtualBox en el sistema (sea Windows, Ubuntu, etc), el siguiente paso es crear una máquina virtual, ésta puede contener cualquier sistema operativo, sólo se debe contar de una unidad de almacenamiento con la imagen correspondiente al sistema operativo a instalar. Los pasos a continuación son iguales para cualquier distribución.

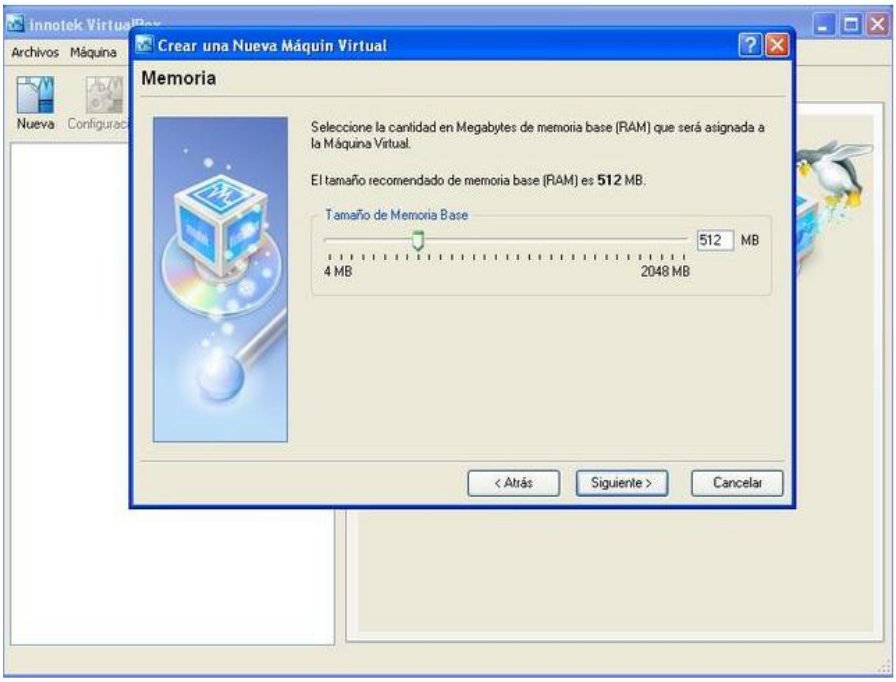
Al ejecutar el programa aparecerá la siguiente ventana de bienvenida, se pulsará en "Nueva" y posteriormente se hará click en "Siguiente"



Luego, se le debe asignar un nombre a la máquina virtual, y seleccionar el sistema operativo correspondiente al que será instalado

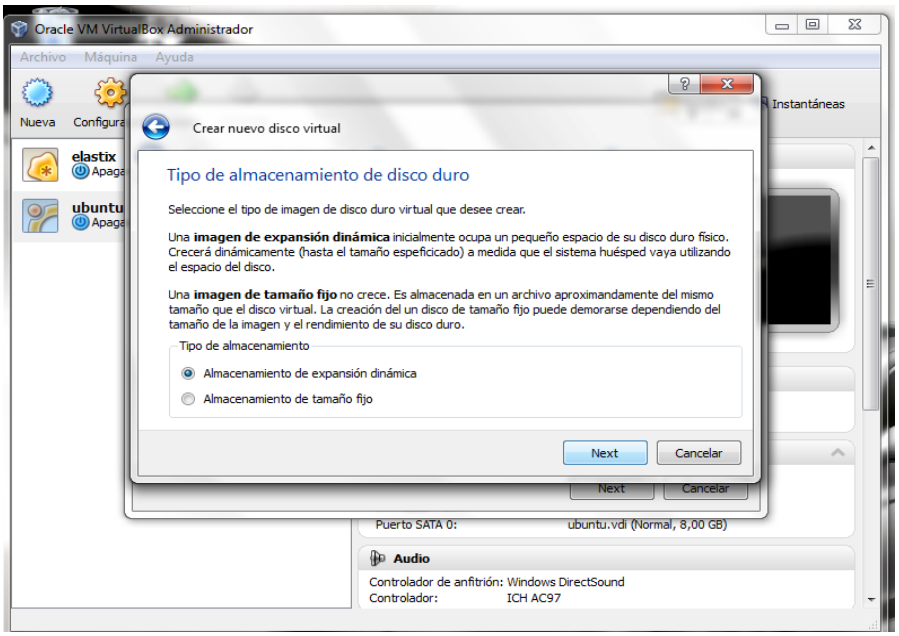


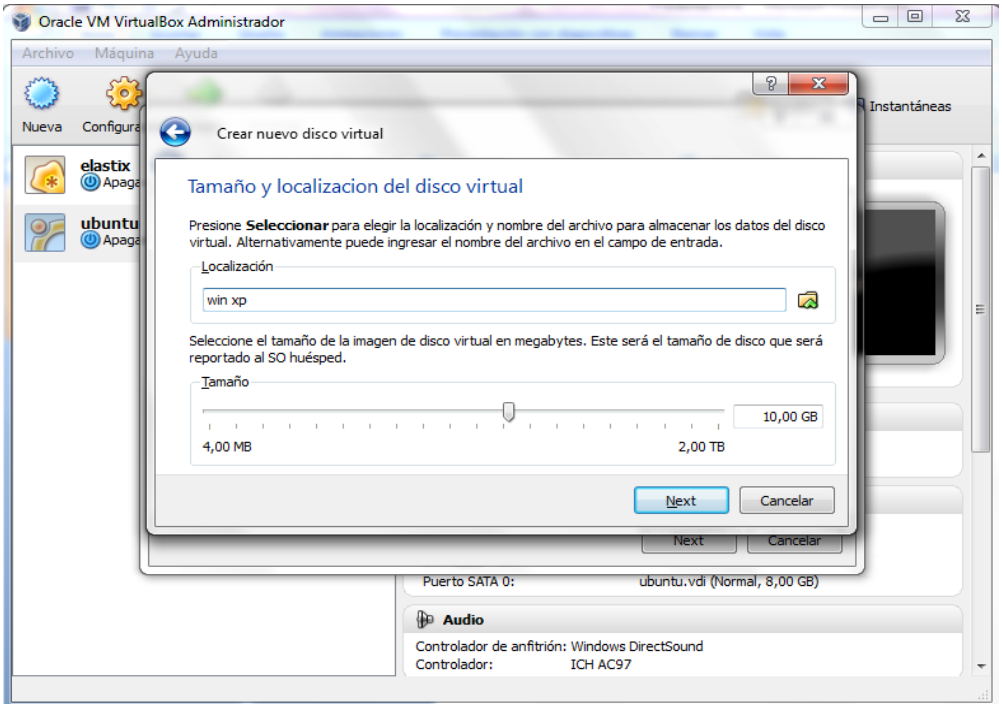
En la siguiente pantalla, se asignará la memoria deseada para la nueva máquina, luego se pulsa “siguiente”



Ahora, se creará un disco duro virtual, se creará uno nuevo como lo muestran las siguientes imágenes:

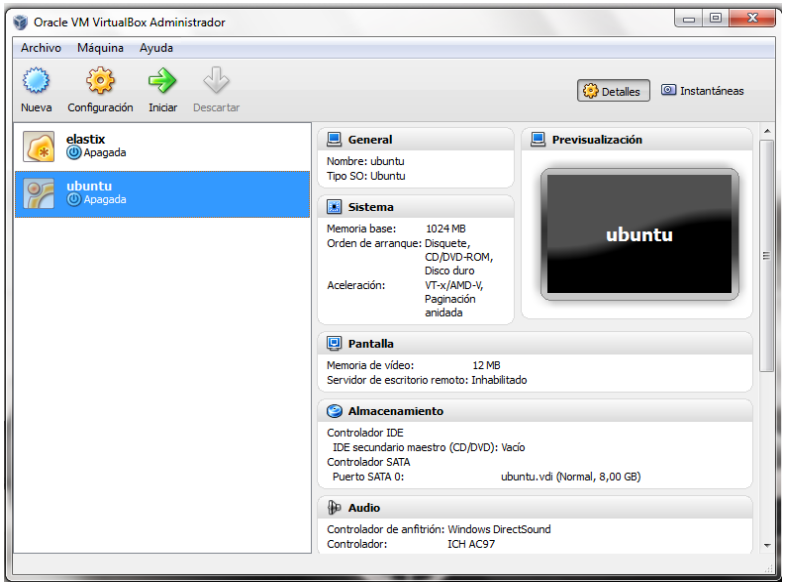
Se debe seleccionar en la siguiente pantalla el tipo de disco duro que sea de expansión dinámica, se le asignará posteriormente el tamaño deseado y el nombre y se presiona "Next"





Para finalizar, se selecciona terminar y el asistente mostrará un resumen de la instalación, a partir de aquí, para instalar el sistema operativo deseado sólo debe hacerse doble click en la máquina instalada y automáticamente VirtualBox

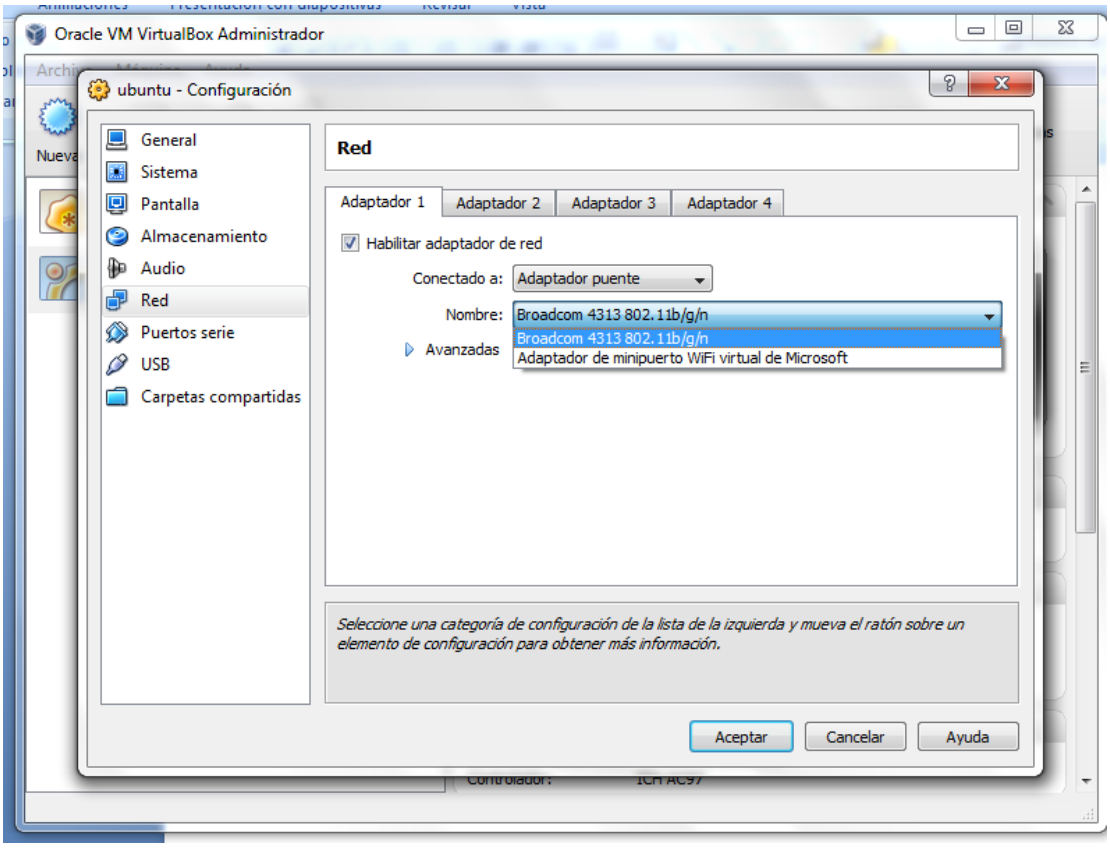
reconocerá la unidad de almacenamiento donde se encuentra la imagen con el sistema operativo a instalar. Luego se procederá a instalar el sistema operativo en cuestión.



Configuración de la Máquina Virtual

En cuanto al presente trabajo especial de grado se refiere, únicamente los parámetros de red, del menú de configuración de VirtualBox serán modificados.

Para que la máquina pueda acceder a los servicios de internet, y además pueda estar en red en conjunto con otras máquinas, se debe seleccionar en el menúa de configuración, en la sección red: la forma de Adaptador Puente, y seleccionar el tipo de red a la que se está conectada (bien sea, mediante WIFI o directamente por tarjeta de red y Ethernet. La siguiente pantalla muestra dicha configuración:


Oracle VM VirtualBox Administrador
ubuntu - Configuración
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Red
Adaptador 1
Adaptador 2
Adaptador 3
Adaptador 4
Habilitar adaptador de red
Conectado a:
Adaptador puente
Nombre:
Broadcom 4313 802.11b/g/n
Broadcom 4313 802.11b/g/n
Adaptador de minipuerto WiFi virtual de Microsoft
Avanzadas
Seleccione una categoría de configuración de la lista de la izquierda y mueva el ratón sobre un elemento de configuración para obtener más información.
Aceptar
Cancelar
Ayuda

ANEXO 12. CONFIGURACIÓN DEL GNUGK GATEKEEPER

Para realizar la instalación del GnuGK, se procede en primer lugar a descargar desde el administrador de paquetes "Synaptic" el software libre gnugk. Una vez instalado el paquete en el sistema, el gatekeeper puede ser configurado para operar conde dos formas diferentes:

- Para que el gatekeeper use el modo de llamada directa, debe ejecutarse de la siguiente forma:

  $gnugk –tt

  Con esta configuración el gatekeeper aceptará el registro de cualquier endpoint. El parámetro `-tt` indica al gatekeeper que debe escribir un registro en la consola cuando recibe y envía paquetes. Si solo se usa `-t`, el gatekeeper indicará solo los paquetes recibidos, pero no los que envía. Si se omite el parámetro, el gatekeeper solo mostrará el número de endpoints registrados. Por lo tanto, la finalidad de este parámetro en el ejemplo práctico es la de monitorear al gatekeeper.

- Para ejecutar el gatekeeper en modo enrutado, deben usarse los parámetros:

  $gnugk –rr –tt

  Usando `-rr`, se le dice al gatekeeper que debe enrutar los canales **Q.931** y **H.245**, lo cual corresponde al modo enrutado teórico. Es posible enrutar solamente el canal **Q.931** usando `-r` en lugar de `-rr`. Se añade –tt para que se pueda visualizar cada mensaje dentro de la comunicación.

  Configuración del archivo Gatekeeper.ini para permitir la comunicación con Elastix:

Archivo gatekeeper.ini

```
;Sección principal del archivo
[Gatekeeper::Main]
;Parámetro obligatorio para encabezar esta sección. Se usa para pruebas
Fortytwo=42
;Nombre del gatekeeper. De gran importancia, sobre todo cuando hay
;más de un gatekeeper
Name=GatekeeperH323
;Configuración del modo enrutado por gatekeeper
[RoutedMode]
;Se habilita en el enrutado del canal Q.931
GKRouted=1
;Se habilita el enrutado del canal H.245
H245Routed=1
;Al igual que con la configuración inicial, el gatekeeper aceptará
;llamadas no registradas
AcceptUnregisteredCalls=1
;Sección de autenticación del gatekeeper
[GkStatus::Auth]
;Con este regla se permitirá cualquier conexión no autentificada
rule=allow
;Ahora se configura el endpoint cuyo H.323ID es ELASTIX323 (Asterisk)
;es decir aquí se configura al gateway Asterisk
[EP::ELASTIX323]
;Prioridad del gateway, como solo hay un gateway, se le asignará
;prioridad máxima (1)
GatewayPriority=1
;Prefijos del gateway
;Cualquier llamada a un número que comience con 9 será
;automáticamente transmitida hacia Asterisk
GatewayPrefixes=9
```

Para configuraciones avanzadas:

Tal y como se explicó en su momento, el comportamiento del gatekeeper está completamente determinado por los parámetros de la línea de comandos y del archivo de configuración. Un manual completo acerca de los parámetros y las opciones del archivo de configuración puede ser encontrada en la página oficial http://www.gnugk.org/gnugk-manual-es.html. A continuación, un resumen de lo más importante.

Parámetros.

Casi todas las opciones del gatekeeper a las que se tienen acceso mediante parámetros, poseen una forma corta y una larga, por ejemplo, `-c` es lo mismo que `--config`.

Parámetro		Acción
-h	--help	Muestra todas las opciones disponibles y sale del programa.
-c	--config filename	Especifica el archivo de configuración a usar.
-s	--section section	Especifica cual sección del archivo de configuración será utilizada como principal. Por defecto es [Gatekeeper::Main].
-i	--interface IP	Especifica la interfaz (número IP) por el que el gatekeeper escuchará. Si se omite será el gatekeeper quien determine cual dirección escuchar.
-l	--timetolive n	Especifica el tiempo de vida (en segundos) para el registro de los endpoints. Este prevalece sobre el atributo TimeToLive del archivo de configuración.
-b	--bandwidth n	Especifica el total de ancho de banda disponible para el gatekeeper. Si no se especifica esta opción, la administración de ancho de banda se desactiva por defecto.
-d	--direct	Utiliza señalización de llamadas directamente entre endpoints.
-r	--routed	Utiliza señalización de llamadas enrutadas a través del gatekeeper. (Solo Q.931).
-rr	--h245routed	Utiliza señalización de llamadas y canal de control H.245 enrutadas a través del gatekeeper. (Q.931 y H.245)
-o	--output filename	Escribe anotaciones de trazado hacia un archivo específico.
-t	--trace	Ver trazado detallado (verbosity). Cuantas más -t se añadan, más detallada será la salida. Por ejemplo, utilice -ttttt para configurar el nivel de detalle al 5.

ANEXO 13. ELASTIX

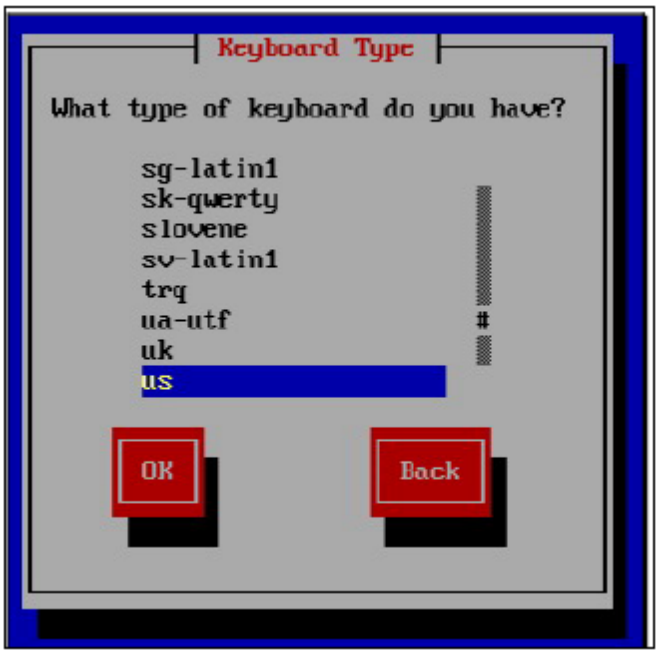
Instalación y Configuración de Elastix, ENUM y MySQL

los siguientes pasos:

- Instalación de Elastix

En principio se creó una máquina virtual con las siguientes características: 2GB de Memoria Ram, 128MB de Memoria para video y un procesador Intel Córe de tres núcleos y de velocidad 1.8GHz. Tras montar la imagen en la unidad de la máquina virtual y arrancar el sistema desde el CD se mostrará una pantalla como la siguiente:

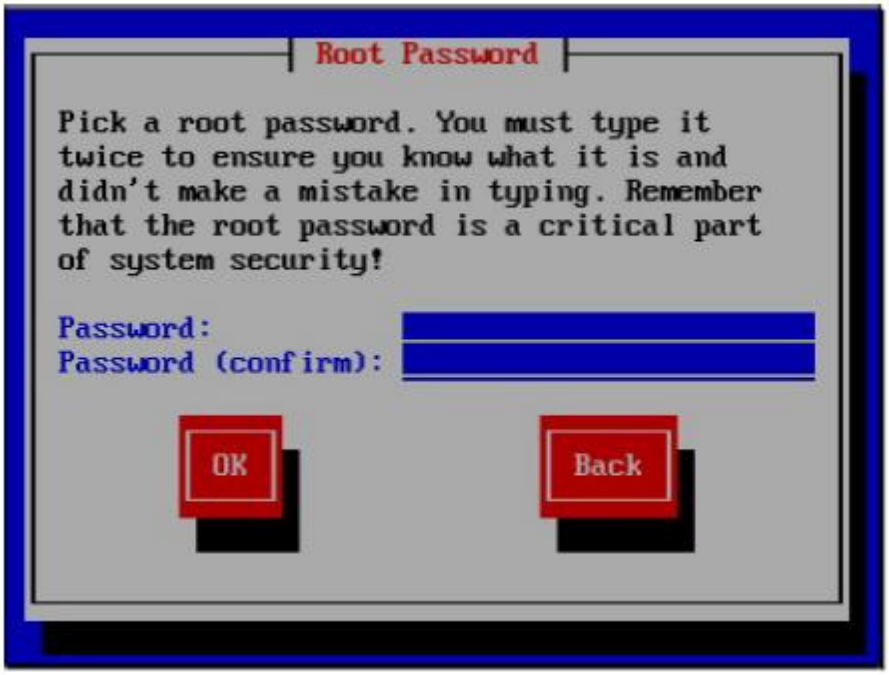
A continuación se debe pulsar ENTER para proceder con la instalación. Tras unos segundos el sistema solicitará seleccionar el tipo de teclado:



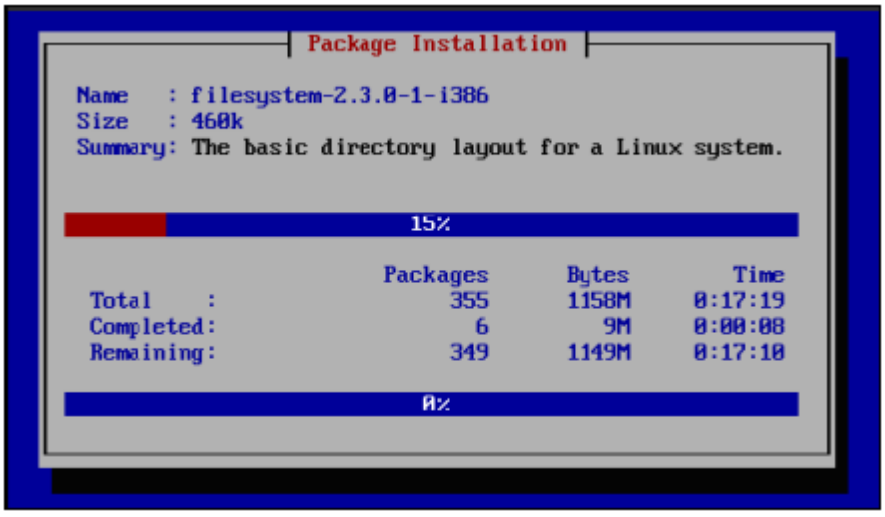
En donde se debe seleccionar el tipo de teclado que el equipo usa (normalmente *es* o *latin*) y seleccionar luego la opción OK (pulsando la tecla TAB) y luego ENTER para continuar.

Del mismo modo se debe seleccionar la zona horaria:

A continuación se debe introducir la contraseña del root (recordar esta contraseña):



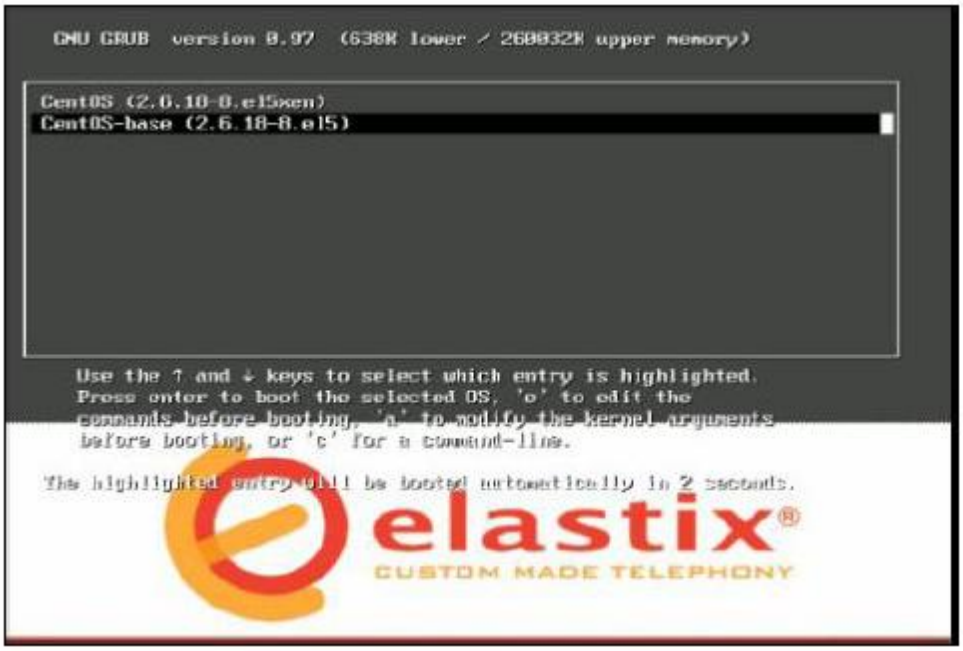
Una vez ingresada y confirmada la contraseña del root, se iniciará la instalación del sistema, comenzando con el formateo de los discos, para luego proceder con la instalación de paquetes:



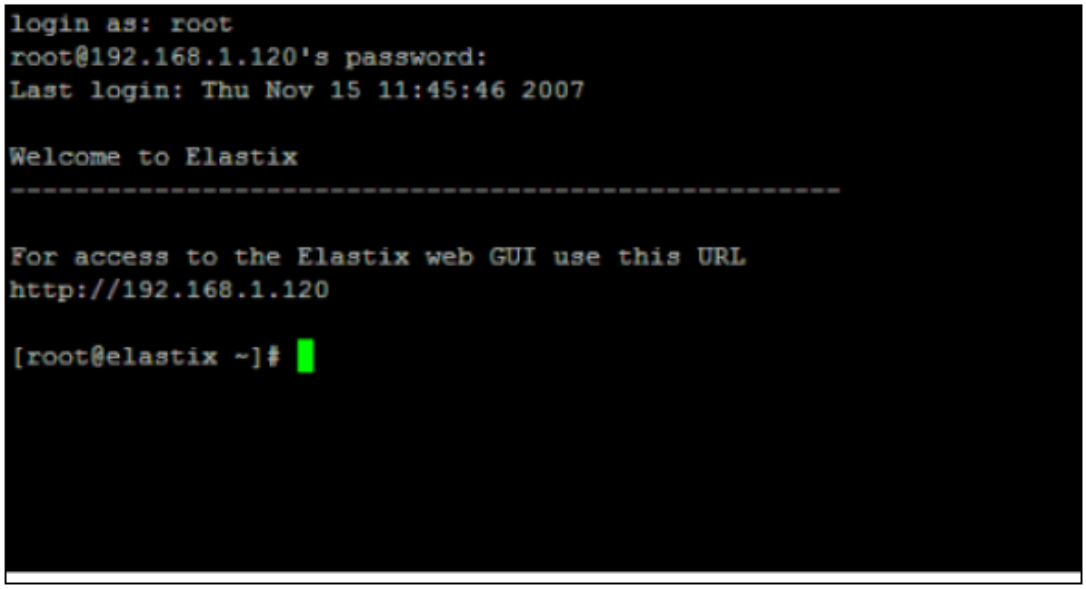
Cuando la instalación termine, se debe reiniciar el sistema, cuando el programa de instalación lo indique. Dado que se trata de una máquina virtual, puede ser necesario apagarla, para desmontar la imagen de CD.

Tras reiniciarse, pueden verse en el arranque muchas líneas de código, esto porque se debe construir Asterisk. Cuando este proceso termine, nuevamente se debe reiniciar la máquina.

Una vez que la máquina se ha reiniciado nuevamente, aparecerá la pantalla del gestor de arranque, en la cual se debe seleccionar la segunda opción (por defecto) como muestra la siguiente imagen:



Ahora el sistema debe estar en condiciones de ser usado, solo falta iniciar sesión como root usando la contraseña configurada anteriormente para acceder a la consola.



Existen algunas tareas adicionales que pueden ser necesarias en este punto. La primera es cambiar el idioma del teclado a español o latino en el caso que no se reconozcan adecuadamente algunos caracteres.

Para ello se debe usar el comando:

```
$system-config-keyboard
```

Si no funciona, porque no está instalada la aplicación. Se puede instalar con:

```
$yum install system-config-keyboard
```

Algo similar puede ocurrir con la red. Para configurar la dirección IP, se debe usar:

```
$system-config-network
```

Y para instalar esta herramienta:

```
$yum install system-config-network
```

Tras cambiar la dirección IP, es importante reiniciar el servicio network usando:

```
$service network restart
```

Por último, se debe chequear la configuración IP usando:

$ifconfig

La dirección IP de esta máquina corresponde también a la dirección web para acceder a la interfaz gráfica del sistema. Para esto basta abrir cualquier navegador en una máquina dentro de la misma red que la máquina **Elastix**, e ingresar:

http://<direccion-IP-de-Elastix>

Configuración e Instalación de MySQL

En esta parte, para instalar MySQL serán necesarios los paquetes del lenguaje de programación PHP y los propios archivos de configuración de MySQL. Para ello desde la consola de Elastix se descargan los paquetes con los siguientes comandos:

$yum install php5-cli php5-mysql mysql-server-5.0 mysql-client-5.0 libmysqlclient15-dev libmysqlclient15-off

Seguidamente, el servidor pedirá una contraseña para el usuario, el cual será la misma utilizada en root y con esto quedará activo el servidor MySQL dentro de Elastix

Configuración e Instalación de ENUM y Servidor BIND9

Como se observa en el ejemplo la consulta ENUM puede constar de uno o más URI con el orden y la preferencia que indican los registros NAPTR. En este caso si llamamos al número al +58 93 444 22 11 el procedimiento a seguir será el siguiente:

- Comprobar que el número sea escrito de manera completa: +58-93- 4442211.
- Borrar todos los caracteres no-dígitos a excepción de "+": +58934442211.
- Borrar todos los caracteres a excepción de los dígitos: 58934442211.
- Colocar puntos (".") entre los dígitos: 5.8.9.3.4.4.4.2.2.1.1.
- Invertir el orden de los dígitos: 1.1.2.2.4.4.4.3.9.8.5.

- Añadir el string ".e164.arpa": 1.1.2.2.4.4.4.3.9.8.5.e164.arpa.

En este momento realizará la consulta a 1.1.2.2.4.4.4.3.9.8.5.e164.arpa DNS, escogerá la URI sip:usuarioSIP@operadorA.com puesto que es el primero en la lista y todos tienen la misma preferencia.

El servidor BIND es el servidor de nombres DNS más popular en Internet y está desplegado en millones de máquinas. Las últimas versiones (9.1 en adelante) soportan ENUM. El servidor de nombres es el responsable de proporcionar dirección IP a partir del nombre de la maquina o viceversa, en nuestro caso, proporciona una dirección URI a partir de un número telefónico. Existen otros servidores DNS pero se decidió utilizar este por su sencilla instalación y configuración. Este servidor se puede instalar utilizando

$yum install bind9

Luego se procede a configurar:

Configuración:

```
*.4.3.4.1.2.1.e164.i2cat.arpa. IN NAPTR 100 10 "u" "E2U+sip"
 "!^\\+1214(.*)$!sip:\\1@operadorA.com!" .
```

```
*.4.3.5.1.2.1.e164.i2cat.arpa. IN NAPTR 100 10 "u" "E2U+sip"
 "!^\\+1215(.*)$!sip:\\1@operadorB.com!" .
```

En segundo lugar, para instalar ENUM dentro de Elastix, se procede a cargar los módulos con los siguientes comandos dentro de la cónsola de Elastix:

Modificando el archivo mysql.so con el comando nano mysql.so en la ruta /usr/local/lib/modules/ se configuró lo siguiente:

```
# ------------------ module loading ----------------------------------

# Uncomment this if you want to use SQL database
loadmodule "/usr/local/ser/lib/ser/modules/mysql.so"

loadmodule "/usr/local/ser/lib/ser/modules/sl.so"
loadmodule "/usr/local/ser/lib/ser/modules/tm.so"
```

```
loadmodule "/usr/local/ser/lib/ser/modules/rr.so"
loadmodule "/usr/local/ser/lib/ser/modules/maxfwd.so"
loadmodule "/usr/local/ser/lib/ser/modules/usrloc.so"
loadmodule "/usr/local/ser/lib/ser/modules/registrar.so"
loadmodule "/usr/local/ser/lib/ser/modules/textops.so"
loadmodule "/usr/local/ser/lib/ser/modules/xlog.so"
loadmodule "/usr/local/ser/lib/ser/modules/enum.so"

# Uncomment this if you want digest authentication
# mysql.so must be loaded !
loadmodule "/usr/local/ser/lib/ser/modules/auth.so"
loadmodule "/usr/local/ser/lib/ser/modules/auth_db.so"

# accounting
loadmodule "/usr/local/ser/lib/ser/modules/acc.so"
```

- ✓ auth, auth_db, auth_radius : digest autenticación.
- ✓ ENUM: Resolución de números de teléfono E.164 usando ENUM.
- ✓ maxfwd: Chequea el campo max-forwards.
- ✓ mysq : Base de datos mysql.
- ✓ registrar, usrloc: Localización de los usuarios en la base de datos.
- ✓ rr: Record Routing .
- ✓ sl: Servidor stateless.
- ✓ textops: Base de datos de texto.
- ✓ tm : Habilita los procesos stateful.
- ✓ Xlog: Imprime los log de los scrips de SER.
- ✓ Acc : Accounting

Por último se reinicia Elastix y se accede al portal verificando que todo esté en correcto funcionamiento.

ANEXO 14. Instalación de la herramienta Jperf e Iperf

Para instalar esta herramienta, desde la terminal de Ubuntu, se ingresa como super usuario, posteriormente se escribe:

$aptitude install iperf

Una vez instalado el programa, se indicó que computadora actuaba como cliente y cual actuaba como servidor con los comandos *iperf –s* (servidor) e *iperf –c dirección IP del Servidor* (cliente).

Con lo anterior, se da inicio al funcionamiento de la herramienta, la cual comenzará a mostrar en pantalla, los datos y la información referente a: ancho de banda, tasa de transmisión, paquetes enviados, etc; de la transmisión monitoreada.

ANEXO 15. CALIDAD DE SERVICIO EN REDES IP

Calidad de Servicio en Redes IP

Dos son los mitos que involucran a la Telefonía-IP. Uno se refiere a la baja calidad de Internet. Se confunden las prestaciones de los accesos dial-up con el uso de canales de transporte punto-a-punto con calidad contratada. Otro se refiere al medio de transportar a los paquetes IP (sólo ATM está en condiciones de garantizar la calidad de servicio). Nuevamente se ignora la serie de herramientas que posee una red IP y Gigabit-Ethernet para garantizar una calidad de servicio.

Los problemas que son evidentes en una red de VoIP, son la Latencia, el Jitter, el Eco y la pérdida de paquetes. En Telefonía-IP estos problemas son resueltos mediante diversas técnicas.

Latencia. Se define así al gap en la conversación debido a los retardos acumulados. El primer retardo es en la matriz de switch (el retardo producido por el proceso store-and-forward) y el retardo de procesamiento (cambio de encabezado de paquetes, por ejemplo). A esto se suman los retardos propios del proceso de compresión vocal (insignificante en codificación G.711 y más elevado en aplicaciones con G.729).

Los retardos en la red pueden ser reducidos mediante el protocolo de reservación RSVP. El retardo debido a la compresión vocal se puede eliminar usando la velocidad de 64 kbps sin compresión (G.711). Este último aspecto es muy interesante. Inicialmente VoIP se desarrolló para reducir costos con menor velocidad y usando la infraestructura de Internet. Actualmente, con el modelo de una red IP de alta velocidad, la compresión vocal no es obligatoria en una red local. En este caso, Telefonía-IP se desarrolla para brindar una red de servicios integrados soportada en protocolo IP, sin límites de ancho de banda.

Cuando se trabaja con señales en Internet en cambio, el ancho de banda es limitado y por ello se requiere compresión vocal. Por ejemplo, el tamaño de un paquete RTP incluye 66 Bytes de encabezado (26 de MAC, 20 de IP, 8 de UDP y 12 de RTP) y 71

de carga útil. El overhead puede ser comprimido. La información vocal puede ser reducida. Por ejemplo: para G.723 trabajando a 6,3 kbps (trama de 30 mseg) sin supresión de silencios se requieren 11 paquetes/seg y 71 Bytes/paquete. Si integramos la supresión de silencios (técnica VAD) esta velocidad se reduce sustancialmente.

Causas: A la latencia también se la llama retardo. No es un problema específico de las redes no orientadas a conexión y por tanto de la VoIP. Es un problema general de las redes de telecomunicación. Por ejemplo, la latencia en los enlaces via satelite es muy elevada por las distancias que debe recorrer la información. La latencia se define técnicamente en VoIP **como el tiempo que tarda un paquete en llegar desde la fuente al destino.** Las comunicaciones en tiempo real (como VoIP) y full-duplex son sensibles a este efecto. Es el problema de "pisarnos". Al igual que el jitter, es un problema frecuente en enlaces lentos o congestionados.

Valores Recomendados: La latencia o retardo entre el punto inicial y final de la comunicación **debiera ser inferior a 150 ms**. El oído humano es capaz de detectar latencias de unos 250 ms, 200 ms en el caso de personas bastante sensibles. Si se supera ese umbral la comunicación se vuelve molesta.

Posibles Soluciones: No hay una solución que se pueda implementar de manera sencilla. Muchas veces depende de los equipos por los que pasan los paquetes, es decir, de la red misma. Se puede intentar **reservar un ancho de banda de origen a destino** o **señalizar los paquetes con valores de** TOS para intentar que los equipos sepan que se trata de tráfico en tiempo real y lo traten con mayor prioridad pero actualmente no suelen ser medidas muy eficaces ya que no disponemos del control de la red. Si el problema de la latencia está en nuestra propia red interna podemos aumentar el ancho de banda o velocidad del enlace o priorizar esos paquetes en la red.

Jitter. Es el efecto por el cual el retardo entre paquetes no es constante. Se trata de una latencia variable producida por la congestión de tráfico en el backbone de red, por distinto tiempo de tránsito de paquetes debido al connectionless, etc. Se puede utilizar un buffer para distribuir los paquetes y reducir el jitter, pero introduce un retardo adicional. Lo correcto es incrementar el ancho de banda del enlace; solución posible en un backbone pero de menor posibilidad en los enlaces WAN. Otra posibilidad es la formación de colas para prioridad de tráfico de telefonía sobre los de datos.

Causas: El jitter es un efecto de las redes de datos no orientadas a conexión y basadas en conmutación de paquetes. Como la información se discretiza en paquetes cada uno de los paquetes puede seguir una ruta distinta para llegar al destino. Se define, como **la variación en el tiempo en la llegada de los paquetes, causada por congestión de red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes.**
Las comunicaciones en tiempo real (como VoIP) son especialmente sensibles a este efecto. En general, es un problema frecuente en enlaces lentos o congestionados. Se espera que el aumento de mecanismos de QoS (calidad del servicio) como prioridad en las colas, reserva de ancho de banda o enlaces de mayor velocidad (100Mb Ethernet, E3/T3, SDH) puedan reducir los problemas del jitter en el futuro.

Valores Recomendados: El jitter entre el punto inicial y final de la comunicación **debiera ser inferior a 100 ms**. Si el valor es menor a 100 ms el jitter puede ser compensado de manera apropiada. En caso contrario debiera ser minimizado.

Posibles Soluciones: La solución más ampliamente adoptada es la utilización del **jitter buffer.** El jitter buffer consiste básicamente en asignar una pequeña cola o almacen para ir recibiendo los paquetes y sirviéndolos con un pequeño retraso. Si alguno paquete no está en el buffer (se perdió o no ha llegado todavía) cuando sea

necesario se descarta. Normalmente en los teléfonos IP (hardware y software) se pueden modificar los buffers. Un aumento del buffer implica menos perdida de paquetes pero más retraso. Una disminución implica menos retardo pero más perdida de paquetes.

Eco. Las características anteriores (latencia y jitter) pueden producir eco sobre la señal telefónica, lo cual hace necesario el uso de canceladores de eco (ITU G.168). Se tienen 2 tipos de eco. Uno tiene alto nivel y poco retardo y se produce en el circuito híbrido de 2 a 4 hilos local; mientras que otro es de bajo nivel y gran retardo y se produce en el circuito separador híbrido remoto. El cancelador de eco se construye mediante la técnica de ecualización transversal autoadaptativa. Consiste en usar una parte de la señal de transmisión para cancelar el eco producido por la desadaptación de impedancias en el circuito híbrido que convierte de 4 a 2 hilos.

Packet Loss. Es la tasa de pérdida de paquetes. Representa el porcentaje de paquetes transmitidos que se descartan en la red. Estos descartes pueden ser producto de alta tasa de error en alguno de los medios de enlace o por sobrepasarse la capacidad de un buffer de una interfaz en momentos de congestión. Los paquetes perdidos son retransmitidos en aplicaciones que no son de Tiempo Real; en cambio para telefonía, no pueden ser recuperados y se produce una distorsión vocal. El delay afecta a la performance de aplicaciones interactivas (por ejemplo, Telnet). El throughput afecta a la performance de aplicaciones que mueven grandes volúmenes de información (por ejemplo, Mail y FTP). El packet loss afecta a ambos tipos de aplicaciones. El jitter afecta a aplicaciones de tiempo real como la voz y el video por IP.

***Causas*:** Las comunicaciones en tiempo real están basadas en el protocolo UDP. Este protocolo no está orientado a conexión y si se produce una pérdida de paquetes no se reenvían. Además la perdida de paquetes también se produce por descartes de paquetes que no llegan a tiempo al receptor. Sin embargo la voz es bastante predictiva y si se pierden paquetes aislados se puede recomponer la voz de una manera bastante

óptima. El problema es mayor cuando se producen pérdidas de paquetes en ráfagas.

Valores Recomendados: La perdida de paquetes máxima admitida para que no se degrade la comunicación deber ser **inferior al 1%.** Pero es bastante dependiente del códec que se utiliza. Cuanto mayor sea la compresión del códec más pernicioso es el efecto de la pérdida de paquetes.

Posibles soluciones: Para evitar la pérdida de paquetes una técnica muy eficaz en redes con congestión o de baja velocidad **es no transmitir los silencios.** Gran parte de las conversaciones están llenas de momentos de silencio. Si solo transmitimos cuando haya información audible liberamos bastante los enlaces y evitamos fenomenos de congestión.De todos modos este fenomeno puede estar también bastante relacionado con el jitter y el jitter buffer.

Throughput. Es la capacidad de un enlace de transportar información útil. Representa a la cantidad de información útil que puede transmitirse por unidad de tiempo. No tiene relación directa con el delay. (por ejemplo, se puede tener un enlace de alto throughput y alto delay o viceversa, como sería por ejemplo un enlace satelital de 2Mbps y 500 mseg de delay).

ANEXO 16. TABLA COMPARATIVA H323-SIP

H323 es el protocolo más definido pero adolece de cierta falta de flexibilidad . SIP está menos definido pero es más fácil de integrar, ¿Que protocolo ganará al final?. Es difícil de decir pero dependera de la aplicación que cada uno quiera desarrollar. (SIP es más facil de implementar aunque los conceptos de H.323 son mejores).

	H.323	SIP
Arquitectura	H.323 cubre casi todos los servicios como capacidad de intercambio,control de conferencia , señalización basica, calidad de servicio, registro, servicio de descubrimiento y más.	SIP es modular y cubre la señalización básica, la localización de usuarios y el registro. Otras carcterísticas se implementan en protocolos separados.
Componentes	Terminal/Gateway	UA
	Gatekeeper	Servidores
Protocolos	RAS/Q.931	SI
	H.245	SDP
Funcionalidades de control de llamada		
Transferencia de llamada (Call Transfer)	Si	Si
Expedición de llamada (Call Forwarding)	Si	Si
Tenencia de llamada (Call Holding)	Si	Si
Llamada estacionada/recogida (Call Parking/Pickup)	Si	Si
LLamada en espera (Call Waiting)	Si	Si
Indicación de mensaje en espera (Message Waiting Indication)	Si	No
Identificación de nombre (Name Identification)	Si	No

Terminación de llamada con subscriptor ocupado (Call Completion on Busy Subscriber)	Si	Si
Ofrecimiento de llamada (Call Offer)	Si	No
Intrusión de llamada (Call Intrusion)	Si	No
	H.323 las divide en los protocolos H.450, RAS, H.245 y Q.931	
Características Avanzadas		
Senalización multicast (Multicast Signaling)	Si, requiere localización (LRQ) y descubrimiento automático del gatekeeper (GRQ).	Si, ejemplo, a través de mensajes de grupo INVITEs.
Control de la llamada de un tercero (Third-party Call Contro)l	Si, a través de pausa de la tercera parte y re-enrutando según esta definido en H.323. Un control más sofisticado se define en el standard de las series H.450.x .	Si, según se describe en los borradores (Drafts) del protocolo.
Conferencia	Si	Si
Pinchar para llamar (Click for Dial)	Si	Si

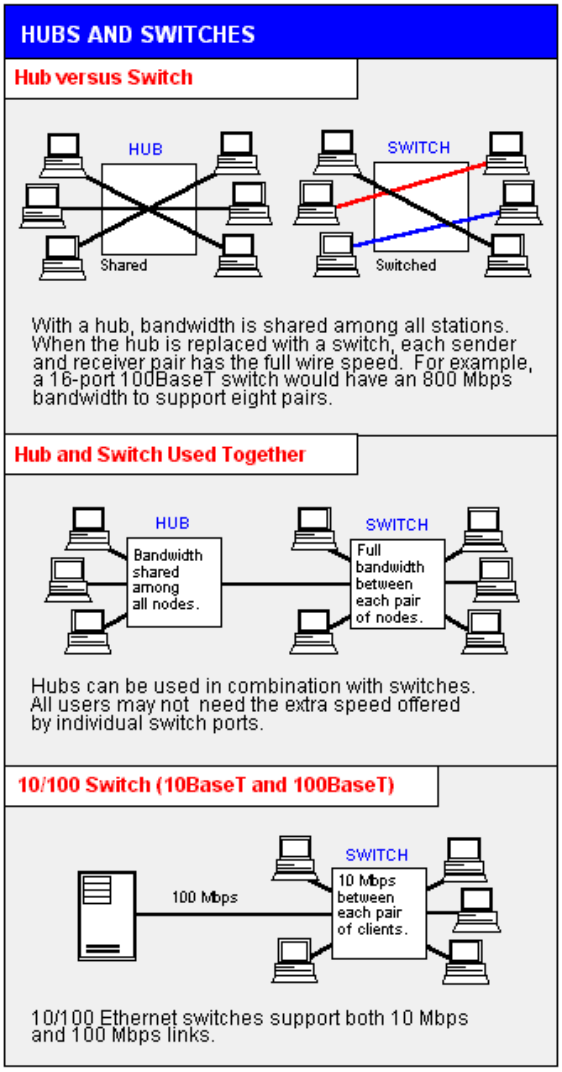
Escalabilidad		
Número amplio de dominios (Large Number of Domains)	La intención inicial de H.323 fue el soporte de LANs, por lo que está pensado para el direccionamiento de redes amplias. El concepto de zona fue añadido para acomodar este direccionamiento amplio. Los procedimientos son definidos por localización de usuarios a través de nombres de email. El anexo G define la comunicación entre dominios administrativos, describiendo los metodos para resolución de direcciones, autorización de acceso y el reporte entre dominios administrativos. En las busquedas multidominio no hay formas sencillas de detectar bucles. La detección de bucles se puede realizar a través del campo "PathValue" pero introduce problemas relativos a la escalabilidad.	SIP soporta de manera inherente direccionamientos de áreas. Cuando muchos servidores están implicados en una llamada SIP usa un algoritmo similar a BGP que puede ser usado en una manera sin estado evitando problemas de escalabilidad. Los SIP Registrar y servidores de redirección fueron diseñados para soportar localización de usuarios.
Gran cantidad de llamadas (Large Number of Calls)	El control de llamadas en se implementa de una manera sin estado. Un gateway usa los mensajes definidos en H.225 para ayudar al gatekeeper en el balanceo de carga de los gateways implicados.	El control de llamadas en se implementa de una manera sin estado. SIP soporta escalabilidad n a n entre UAs y servidores. SIP necesita menos ciclos de CPU para generar mensajes de señalización Por lo tanto, teoricamente un servidor puede manejar más transacciones. SIP ha especificado un método de balanceado de carga basado en el mecanismo de traslación DNS SRV.
Estado de la conexión	Con estado o sin estado.	Con estado o sin estado. Una llamada SIP es independiente de la existencia de una conexión en la capa de transporte, pero sin embargo la señalización de llamadas tiene que ser terminada explicitamente.
Internationalización	Si, H.323 usa Unicode (BMPString con ASN.1) para alguna información textual (h323-id), pero generalmente tiene pocos parametros textuales	Si, SIP usa Unicode (ISO 10646-1), codificado como UTF-8, para todas las cadenas de texto, permitiendo todos los caracteres para nombres, mensajes y parametros. SIP provee metodos para la indicación del idioma y preferencias del idioma.

Seguridad	Define mecanismos de seguridad y facilidades de negociación mediante H.235, puede usar SSL para seguridad en la capa de transporte.	SIP soporta autentificación de llamante y llamado mediante mecanismos HTTP. Autenticación criptográfica y encriptación son soportados salto a salto por SSL/TSL pero SIP puede usar cualquier capa de transporte o cualquier mecanismo de seguridad de HTTP, como SSH o S-HTTP. Claves para encriptación multimedia se ofrecen usando SDP. SSL soporta autenticación simétrica y asimétrica. SIP también define autenticación y encriptación final usando PGP o S/MIME.
Interoperabilidad entre versiones	La compatibilidad hacia atás de H.323 permite que todas las implementaciones basadas en diferentes versiones de H.323 sean fácilmente integrables.	En SIP, una nueva versión puede descartar características que no van a ser soportadas más. Esto consigue reducir el tamaño del código y la complejidad del protocolo , pero hace perder cierta compatibilidad entre versiones.
Implementación de la Interoperabilidad	H.323 provee una guía de implementación, que clarifica el standard y ayuda a la interoperabilidad entre diferentes implementaciones.	SIP no prevee ninguna guía de interoperabilidad
Facturación	Incluso con el modelo de llamada directa H.323, la posibilidad de facturar la llamada no se pierde porque los puntos finales reportan al gatekeeper el tiempo de inicio y finalización de la llamada mediante el protocolo RAS.	Si un proxy SIP quiere recoger información de facturación no tiene otra opción que revisar el canal de señalización de manera constante para detectar cuando se completa la llamada. Incluso así, las estadísticas están sesgadas porque la señalización de la llamada puede tener retardos.
Codecs	H.323 suporta cualquier codec, estandarizado o propietario, no sólo codecs ITU-T, por ejemplo codecs MPEG o GSM. Muchos fabricaantes soportan codecs propietarios a través de ASN.1 que es equivalente en SIP a "códigos privados de mutuo acuerdo" Cualquier codec puede ser señalizado a través de la característica GenericCapability añadida en H.323v3.	SIP soporta cualquier codec IANA-registered (es una característica hererada) o cualquier codec cuyo nombre sea de mutuo acuerdo.
Bifurcación de llamadas (Call Forking)	Un gatekeeper H.323 puede controlar la señalización de la llamada y puede bifurcar a cualquier número de dispositivos simultaneamente.	Un proxy SIP puede controlar la señalización de la llamada y puede bifurcar a cualquier número de dispositivos simultaneamente.

Bifurcación de llamadas (Call Forking)	Un gatekeeper H.323 puede controlar la señalización de la llamada y puede bifurcar a cualquier número de dispositivos simultaneamente.	Un proxy SIP puede controlar la señalización de la llamada y puede bifurcar a cualquier número de dispositivos simultaneamente.
Protocolo de transporte	Fiable (Reliable) o no fiable (unreliable), ej., TCP o UDP. La mayoría de las entidades H.323 usan transporte fiable (TCP) para señalización.	Fiable (Reliable) o no fiable (unreliable), ej., TCP o UDP. La mayoría de las entidades SIP usan transporte no fiable (UDP) para señalización.
Codificación de mensajes (Message Encoding)	H.323 codifica los mensajes en un formato binario compacto adecuado para conexiones de gran ancho de banda.	SIP codifica los mensajes en formato ASCII, adecuado para que lo puedan leer los humanos.
Direccionamiento (Addressing)	Mecanismos de señalización flexibles, incluyendo URLs y números E.164.	SIP sólo entiende direcciones del estilo URL.
Interconexión Red Telefónica Pública (PSTN Interworking)	H.323 toma prestado de la red telefónica pública protocolos como Q.931 y está por tanto bien adecuada para la integración. Sin embargo, H.323 no emplea la analogía a tecnología de conmutación de circuitos de red telefónica pública de SIP. H.323 es totalmente una red de conmutación de paquetes. El como los controles deben implementarse en la arquitectura H.323 está bien recogido en el estándar.	SIP no tiene nada en común con la red telefónica pública y esa señalización debe ser "simulada" en SIP. SIP no tiene ninguna arquitectura que describa cómo deben implementarse los controles.
Detección de bucles (Loop Detection)	Si, los gatekeepers pueden detectar bucles mirando los campos "CallIdentifier" y "destinationAddress" en los mensajes de procesamiento de la llamada. Combinando ambos se pueden detectar bucles	Si, el campo "Via" de la cabecera de los mensajes SIP facilita el proceso. Sin embargo, este campo "Via" puede generar complejidad en los algoritmos de detección de bucles y se prefiere usar la cabecera "Max-Forwards" para limitar el número de saltos y por tanto los bucles.
Puertos mínimos para una llamada VoIP	5 (Señalización de llamada, 2 RTP, and 2 RTCP.)	5 (Señalización de llamada, 2 RTP, and 2 RTCP.)
Conferencias de vídeo y datos	H.323 suporta todo tipo de conferencia de vídeo y datos. Los procedimientos permiten control de la conferencia y sincronización de los streams de audio y vídeo,	SIP no soporta protocolos de vídeo como T.120 y no tiene ningún protocolo para control de la conferencia.

ANEXO 17. SWITCHED-ETHERNET

Un switch proveé de un canal dedicado a cada par de usuarios (transmisor receptor), asignándole a cada uno la totalidad del ancho de banda disponible; en donde un Hub comparte el ancho de banda total entre cada uno de los usuarios.



ANEXO 18. CÁLCULO DE ANCHO DE BANDA DE CÓDECS DE AUDIO Y VIDEO UTILIZADOS

Las cifras calculadas en el presente TEG acerca del Ancho de banda de los códecs utilizados se basaron en los siguientes cálculos:

Codec G.711 sobre Ethernet

➔ Tamaño del paquete de voz

TPV = L2 + (IP + UDP + RTP) + VPS

TPV = 18 + (20+8+12) + 160 = 218 Bytes

➔ Paquetes de voz por segundo

PPS = Codec bit rate / VPS

PPS = **64 Kbps** / (160 * 8) = 50 pps

➔ Ancho de banda

AB = TPV * PPS

AB = 218 * 50 = 10900 = **87.2 Kbps 36% + de Ancho de Banda**

TPV: Tamaño de Paquete de Voz
PPS: Paquetes de Voz por Segundo
AB: Ancho de Banda