ESCUELA POLITECNICA DEL EJÉRCITO

DPTO. DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ANÁLISIS DE DESEMPEÑO Y FUNCIONALIDAD DE UN SISTEMA DE VIDEOCONFERENCIA BAJO LA TECNOLOGÍA DE INTERNET IPV6

Previa a la obtención del título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR:
GABRIEL SANTIAGO VALENZUELA GARZÓN
MARCOS DAVID MEJIA CAMPOVERDE

SANGOLQUÍ, 30 de septiembre de 2008

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por los Srs. Gabriel Santiago Valenzuela Garzón y Marcos David Mejía Campoverde, como requerimiento parcial a la obtención del título de INGENIEROS EN SISTEMAS E INFORMÁTICA.

08 de Agosto de 2008

Ing. Rodrigo Fonseca

DEDICATORIA

A mi hijo Mathías que con su luz llego para iluminar mi vida y darme fuerzas para continuar este largo camino del saber.

A toda mi familia que de una u otra manera supieron apoyarme en todas y cada una de las circunstancias de mi vida académica.

Gabriel Valenzuela G.

A mi madre y padre, quienes me han sabido formar como persona, amigo y profesional, con sus grandes cualidades de trabajo y honradez, cualidades que siempre las llevo presente en todas las etapas de mi vida

A mis hermanos Leo y Paúl, que siempre creyeron en mi y me apoyaron en todo momento.

David Mejía C.

AGRADECIEMIENTO

A todos nuestros amigos y compañeros que supieron poner su granito de arena para el desarrollo y culminación de este proyecto de investigación, a todas las personas que por alguna circunstancia de la vida se cruzaron en nuestras vidas y fueron de gran apoyo en su momento, a nuestras familias por la paciencia, dedicación y apoyo en todo momento.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

En base a la preocupación por el agotamiento inminente del conjunto actual de direcciones de Internet bajo el protocolo de Internet IP versión 4 (IPV4), y la aspiración de proporcionar una funcionalidad adicional para el uso de dispositivos modernos de comunicación, se ha determinado la normalización de la versión actual del protocolo Internet, por la nueva versión de protocolo de Internet IP versión 6 (IPV6).

El valor que aporta una solución de comunicación con la estructura tecnológica actual, no solo depende del canal de comunicación, sino también depende de las necesidades de los usuarios para determinar el tipo de aplicación que se pretenda utilizar, siendo: transferencia de datos, comunicación de voz sobre IP, videoconferencia, etc.

Todo sistema de videoconferencia 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 de sesiones. Al poder implementar este tipo de comunicación sobre una estructura tecnológica innovadora, como lo es el protocolo de Internet versión 6 (IPV6), surge la posibilidad de obtener una mayor calidad de servicios, seguridad integrada, mayor espacio de direcciones, entre otros, frente a las actuales características y propiedades del protocolo de comunicación de Internet versión 4 (IPV4).

CAPITULO I

INTRODUCCIÓN

Uno de los grandes avances dentro de Internet en los últimos años ha sido, sin lugar a dudas, la posibilidad de transmitir imágenes y sonidos en forma combinada en tiempo real entre grupos de usuarios, lo que comúnmente se conoce como videoconferencia.

La Videoconferencia es una herramienta bidireccional de audio y video que permite mantener reuniones con grupos de personas situados en lugares geográficamente distantes, de manera que todos los interlocutores pueden verse y hablar entre si, permitiendo además el uso de varias aplicaciones como: proyectores de documentos, pizarras electrónicas, presentaciones, etc.

La dificultad económica para viajar a hecho que el sistema de videoconferencia vaya tomando fuerza, ya que genera ahorro de tiempo y dinero para poder reunir varias personas a través del sistema de videoconferencia

Este tipo de tecnología surgió a partir de los años 60`s como un prototipo de comunicación para la transmisión de datos analógicos a través de redes digitales, mejorando notablemente en los años 80`s y 90`s debido al incremento de las características tecnológicas de los equipos de comunicación y a la optimización de los métodos de muestreo y conversión de señales analógicas para audio y video, denominado **códecs**.

En la actualidad la relación costo beneficio de una videoconferencia, está dada por el nivel de calidad de compresión de audio y video que se puede transmitir a través de una red de datos utilizando el protocolo IP.

Actualmente el protocolo de Internet que se utiliza para todo tipo de comunicación de datos a nivel mundial, es la versión 4 denominada IPv4, y debido al actual agotamiento de direcciones bajo esta versión de protocolo, surgió la necesidad de crear una nueva versión de protocolo de Internet denominado IPv6, el mismo que incorpora en su estructura, mayor compatibilidad con servicios de calidad, seguridad integrada, gran espacio de direcciones, capacidad de ampliación, movilidad, entre otros.

1.1 Hipótesis

La transferencia de datos, voz y video, de forma bidireccional por un canal de comunicación, que utilice el protocolo IPv6, tendrá mejores características de rendimiento y funcionalidad, frente al actual protocolo IPv4.

1.2 Justificación

En el presente proyecto de tesis se pretende analizar el desempeño y funcionalidad de una estructura de red dual bajo los protocolos de red IPv4 e IPv6 en tiempo real, con el fin de demostrar las ventajas, desventajas y mejoras en la transmisión de datos y paquetes que existen entre estas dos tecnologías.

1.3 Objetivos

1.3.1 Objetivo General:

Implementar un sistema de Videoconferencia a través de un prototipo de red que utilice independientemente los protocolos de Internet tanto versión 4 (IPv4) como versión 6 (IPv6), el cual permita denotar las principales diferencias y características de funcionamiento en tiempo real de estas tecnologías de red.

1.3.2 Objetivos Específicos:

- Diseñar e implementar un prototipo de red dual que utilice independientemente los protocolos de Internet tanto versión 4 (IPv4) y versión 6 (IPv6) para la simulación de un sistema de videoconferencia en una red WAN.
- Controlar y supervisar el canal de comunicación de datos en el prototipo de red WAN a ser implementado.
- Analizar el desempeño y funcionalidad en tiempo real de un sistema de video conferencia.
- Obtener y medir los datos estadísticos generados por la implementación del proyecto para determinar las conclusiones de esta investigación.

1.4 Alcance

El presente trabajo tiene como finalidad establecer el análisis de desempeño y funcionalidad de un prototipo de red dual en una aplicación de Videoconferencia mediante el uso de la tecnología de red IPv4 e IPv6, en el mismo que se determinará las características técnico-funcionales con la asignación y control del ancho de banda en un prototipo de simulación de red WAN en base a la aplicación de una herramienta GNU GPL.

Para el estudio del proyecto, se establecerá el diseño e implementación de un prototipo de comunicaciones de videoconferencia tanto para la tecnología de Internet versión 6 como para la tecnología versión 4, integrado por un ruteador (configurado bajo linux) y 2 servidores (también configurados bajo linux) que puedan soportar los dos tipos de tecnología de Internet, en los cuales se estructurará una simulación de enlace de red WAN, determinando una velocidad específica para los dos casos de estudio, con la finalidad de establecer los análisis de comparación propuestos en los objetivos anteriores.

Además a esto se incorporará todos los elementos y equipos necesarios para realizar el sistema de videoconferencia propuesto a través del enlace de red WAN, los cuales deberán tener soporte para ser configurados bajo los dos tipos de tecnología de Internet.

1.5 Metología

Para el desarrollo del proyecto, se analizará y pondrá en práctica los conocimientos teóricos prácticos de redes y tecnologías de comunicación para la transferencia de datos, con el fin de estructurar el análisis y diseño de un prototipo de sistema de videoconferencia sobre los protocolos de Internet versión 6 y versión 4, en laboratorios estructurados y compatibles para el caso de estudio presente.

Para determinar el prototipo de comunicaciones del presente proyecto, se determina una metodología de **PROTOTIPO** con análisis **deductivo**, la cual, establece una serie de procedimientos para establecer secuencialmente el análisis de desempeño y funcionamiento de un Sistema de videoconferencia bajo la tecnología de Internet versión 6, integrando:

- **Análisis** de la estructura de funcionamiento de los protocolos de Internet versión 6 frente a las características y funcionalidad del protocolo de Internet versión 4.

- **Diseño** de la estructura tecnológica para el prototipo del sistema de Videoconferencia Punto a Punto a través de la simulación una red WAN con el uso de Internet.

- **Implementación** del prototipo de comunicación con la ayuda de los equipos necesarios para establecer el sistema de videoconferencia,

- **Pruebas** de calidad de servicios, tasa de transferencia de datos, escalabilidad y seguridad del funcionamiento del sistema de videoconferencia a través de diferentes herramientas de análisis de paquetes de datos para evaluar la comunicación de datos entre las dos tecnologías de Internet, versión 6 y versión 4 respectivamente.

1.6 Herramientas

Las herramientas a utilizar en el desarrollo del proyecto de tesis son los equipos que soporten las mencionadas tecnologías en conjunto para su respectivo análisis.

1.6.1 Descripción del Hardware que se utilizará como herramientas para el presente proyecto

- 1 Router con soporte para tecnología de Internet versión 4 y versión 6.
- 2 servidores.
- 2 Switch con soporte de red 10/100 Mbps.
- 2 Estaciones de trabajo.
- 2 Cámaras de video.
- 2 Micrófonos.

CAPITULO II

MARCO TEORICO

2.1 La Videoconferencia

La videoconferencia es un sistema de comunicación que permite enlazar dos o más puntos ubicados en localidades separadas y admite la interacción visual, auditiva y verbal entre personas de cualquier parte del mundo.

Con este tipo de tecnología se pueden compartir aplicaciones, intercambiar puntos de vista, mostrar y ver todo tipo de documentos, dibujos, gráficas, fotografías, imágenes de computadora y videos en tiempo real; con el fin de crear, visualizar y modificar archivos de forma simultánea; sin necesidad de que él o los participantes tengan que trasladarse al lugar en el cual se esté realizando el evento.

2.2 Funcionamiento de una Videoconferencia

El funcionamiento de una sala de videoconferencia requiere de los elementos que se mencionan a continuación.

2.2.1 Codec

Es una abreviatura de Codificador-Decodificador. Sirve para codificar el flujo de una señal y recuperarla o cifrarla.

2.2.2 Sistema de audio

Se compone de audio de entrada y audio de salida. Con el sistema de audio, se puede lograr cancelación de eco y supresión de ruidos adaptándose a las características acústicas de la sala.

2.2.3 Sistema de video

El sistema de video permite observar la imagen del sitio remoto y del sitio local.

2.2.4 Iluminación

La iluminación debe tener una tonalidad neutra (ni muy clara, ni muy obscura), para la correcta visualización de las imágenes.

2.2.5 Enlace

El enlace de comunicación sirve para establecer la videoconferencia, entre mayor sea el ancho de banda, mejor será la calidad de la videoconferencia.

2.2.6 Velocidad de Transmisión

La velocidad estándar de transmisión en una videoconferencia es de 384 kbps. A esta velocidad se cuenta con una calidad de video óptima para todo tipo de presentaciones.

2.3 Modalidades de Videoconferencia.

Las modalidades que existen en videoconferencia se clasifican por: el tipo de dimensión espacial, el tipo de dimensión temporal, el tipo de datos que se transmiten, el tipo de equipamiento, el tipo de participación de los asistentes.

2.3.1 Tipo de Dimensión Espacial:

Dependiendo del número de lugares las videoconferencias se clasifican en:

2.3.1.1 Videoconferencia Punto a Punto.-

Este tipo de videoconferencia es la que se realiza entre dos puntos remotos.

2.3.1.2 Videoconferencia Multipunto.-

Es cuando las personas participantes de la videoconferencia se encuentran en tres o más lugares distintos.

2.3.2 Tipo de Dimensión Temporal:

Se clasifican en:

2.3.2.1 Videoconferencia Síncrona o en Línea.-

Se realiza en tiempo real, es decir existe coincidencia de tiempo

2.3.2.2 Videoconferencia Asíncrona.-

No se realiza en tiempo real, es decir se presenta con una prórroga de tiempo.

2.3.3 Tipo de Datos que se Transmite:

Se clasifican en:

2.3.3.1 Audio Conferencia.-

Se mantiene activa una conversación entre dos o varios sitios sin imagen.

2.3.3.2 Conferencia Audio Gráfica:

Este tipo de conferencia se caracteriza por hacer uso de audio y de elementos que puedan ilustrar gráficamente lo que se está emitiendo.

2.3.4 Tipo de Equipamiento:

Se clasifican en:

2.3.4.1 Videoconferencia de Escritorio:

Este sistema usa un ordenador personal y un software especializado. Es de uso personalizado o para grupos pequeños máximo de 4 personas.

2.3.4.2 Videoconferencia para Auditorios Pequeños:

Este sistema está diseñado para grupos entre 4 y 12 personas, situados todos alrededor de una mesa.

2.3.4.3 Videoconferencia de Salas:

Este sistema se caracteriza por que los participantes se encuentran en una sala equipada con todos los equipos necesarios para realizar una videoconferencia. La cantidad de asistentes depende del espacio físico con que cuente la sala.

2.3.5 Tipo de Participación de los Asistentes:

Se clasifican en:

2.3.5.1 Videoconferencias Abiertas.-

En este tipo de videoconferencias los participantes pueden intervenir libremente.

2.3.5.2 Videoconferencias Cerradas.-

Este tipo de videoconferencias no permite que los participantes intervengan libremente. Para poder hacerlo existen una serie

de restricciones, las cuales son impuestas por los organizadores de la videoconferencia.

2.4 Videoconferencia sobre IP

La videoconferencia sobre IP (Protocolo de Internet) está diseñada para organizaciones que cuentan con redes corporativas, sus principales ventajas son: mayor calidad de imagen, mayor compatibilidad de compartición de datos, mayor disponibilidad de puntos de conexión, etc.

Este tipo de videoconferencia está definido por el estándar H.323, el cual define la forma cómo los puntos de la red transmiten y reciben llamadas, compartiendo las capacidades de transmisión de audio, vídeo y datos.

2.5 Estándares para Sistemas de Videoconferencia:

Los estándares para sistemas de videoconferencia permiten conexiones entre diversas marcas de fabricantes de equipos de videoconferencia, siempre y cuando cumplan con las normas internacionales propuestas por la Unión Internacional de Telecomunicaciones.

A continuación se describen varios estándares propuestos por la **ITU** para la aplicación de sistemas de Videoconferencias.

2.5.1 H.320.-

Este estándar establece los conceptos básicos para el intercambio de audio y vídeo en un sistema de videoconferencia punto a punto o multipunto sobre redes que utilizan un canal con ancho de banda garantizado como **RDSI**.

2.5.2 H.321.-

Es la adaptación del estándar H.320 para ATM, garantiza la interoperabilidad entre ambas redes (RDSI y ATM), aprovechando toda la infraestructura de H.320 como son los estándares H.261, H.221 y H.242.

Sin embargo, H.321 no aprovecha todas las ventajas que proporciona ATM por las siguientes razones:

- Al usar el estándar H.261 la transmisión de vídeo queda limitada a 2 Mbps mientras que usando otros estándares de vídeo podría aprovechar mejor el ancho de banda que ofrece ATM.

- Al usar AAL1 (ATM Adaptation Layer 1) con una tasa de bits constante no puede obtener las ventajas que ofrecería el servicio VBR de una tasa de transmisión variable.

2.5.3 H.322.-

Es una extensión del estándar H.320 a redes de área local que garantizan el ancho de banda combinando las capacidades de RDSI (WAN) y 10BaseT (LAN).

Proporciona una calidad de video equivalente a la basada en RDSI y es necesario que los terminales dispongan de los mecanismos de sincronización de la RDSI.

2.5.4 H.323.-

Es considerado por la ITU más que como un estándar como una recomendación de forma que queda abierta para que los distintos fabricantes se adapten a ella según sus necesidades, permitiendo así que los usuarios se comuniquen sin tener que preocuparse de la compatibilidad entre sus sistemas.

Se centra en la descripción de las comunicaciones multimedia entre terminales, equipos de redes y servicios en redes LAN, de forma que es el estándar utilizado para el establecimiento de videoconferencias sobre redes que no tienen garantizado el ancho de banda y no tienen un retardo fijo, como son Ethernet, Token Ring o Internet. Se caracteriza por utilizar las ventajas que aportan las redes de conmutación de paquetes para el tráfico en tiempo real.

Se ocupa además de gestionar el ancho de banda disponible para evitar que la LAN se colapse con la transmisión de audio y vídeo limitando el número de conexiones simultáneas.

Los componentes definidos dentro de H.323 son:

2.5.4.1 Terminal:

Es un extremo de la red que proporciona comunicaciones bidireccionales (como señales de control, audio, vídeo o datos) en tiempo real con otro terminal H.323, Gateway o unidad de control multipunto (MCU).

2.5.4.2 Gate Keeper:

Realiza la traducción de direcciones y el control de acceso a la red de los terminales H.323, Gateways y MCUs, además puede gestionar el ancho de banda y la localización de los gateways o pasarelas.

2.5.4.3 Gateway:

Proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. Es una pasarela entre el

entorno de vídeo sobre IP H.323 y el entorno vídeo sobre RDSI H.320.

2.5.4.4 MCU:

Permite que tres o más terminales y gateways participen en una conferencia multipunto.

Estos componentes interoperan con otros estándares en el otro extremo de la comunicación como se representada en la figura 2.1.

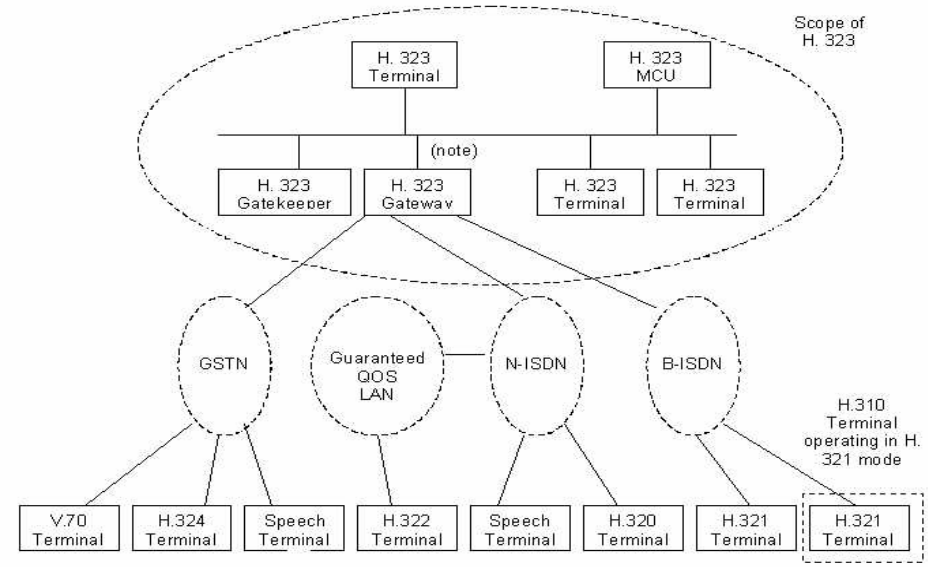


Figura 2.1.- Interoperabilidad de estándares de comunicación para videoconferencia.

H323 utiliza H.261 y H.263 para la codificación de vídeo. Para audio usa los estándares G.711 y G.723. Y T.120 para conferencias con datos.

H.323 usa la norma H.245 para llevar a cabo tareas tales como fijar el establecimiento de llamadas, el intercambio de la información, la terminación de las llamadas y la forma de codificar y decodificar.

Las ventajas que aporta H.323 respecto a H.320 son:

- Reducción de los costes de implantación: mientras que H.320 requiere doble cableado para transportar audio y vídeo, H.323 puede utilizar conexiones WAN.

- H.320 es un estándar orientado a terminal mientras que H.323 tiene sus capacidades distribuidas a través de la red lo que le permite disponer de funciones de comunicación complementarias.

2.5.5 H.324.-

Este estándar define una terminal multimedia para la comunicación de voz, datos y vídeo sobre la red telefónica conmutada pública. Para ello utiliza módems sin detección ni corrección de errores para evitar los retrasos debidos a retransmisiones.

Utiliza el estándar G.723 para la codificación de voz, H.263 para la codificación de vídeo, H.245 para el control y H.223 para multiplexación.

La calidad de audio y vídeo es peor que la ofrecida por H.320 pero tiene los beneficios de ser una tecnología de bajo coste y que aprovecha red telefónica.

2.5.6 H.310.-

Es la adaptación de los estándares de audio y vídeo sobre ATM. Contempla, además de H.261 y G.711, el uso del método de compresión MPEG.

Permite soportar aplicaciones simétricas como la videoconferencia y asimétricas como el vídeo bajo demanda, servicios de mensajería y servicios de distribución como la TV broadcast.

Este estándar incluye H.321 para la interconexión con otras redes. Y tiene la particularidad de definir distintos tipos de terminales según la capa de adaptación ATM en la que esté soportada la videoconferencia.

2.6 Estándares de Control para Videoconferencia

2.6.1 H.221.-

Define la estructura de la trama audiovisual en uno o en múltiples canales B (*figura 2.2*) de redes RDSI agrupados, utilizando así un ancho de banda de 64Kbps a 2Mbps.

En la figura 2.2 se muestra la trama H.221 que permite multiplexar en los canales B información diversa como: audio y vídeo codificados, o señales de control del sistema que son transportados

en un canal de señalización permanentemente abierto que dispone esta trama.

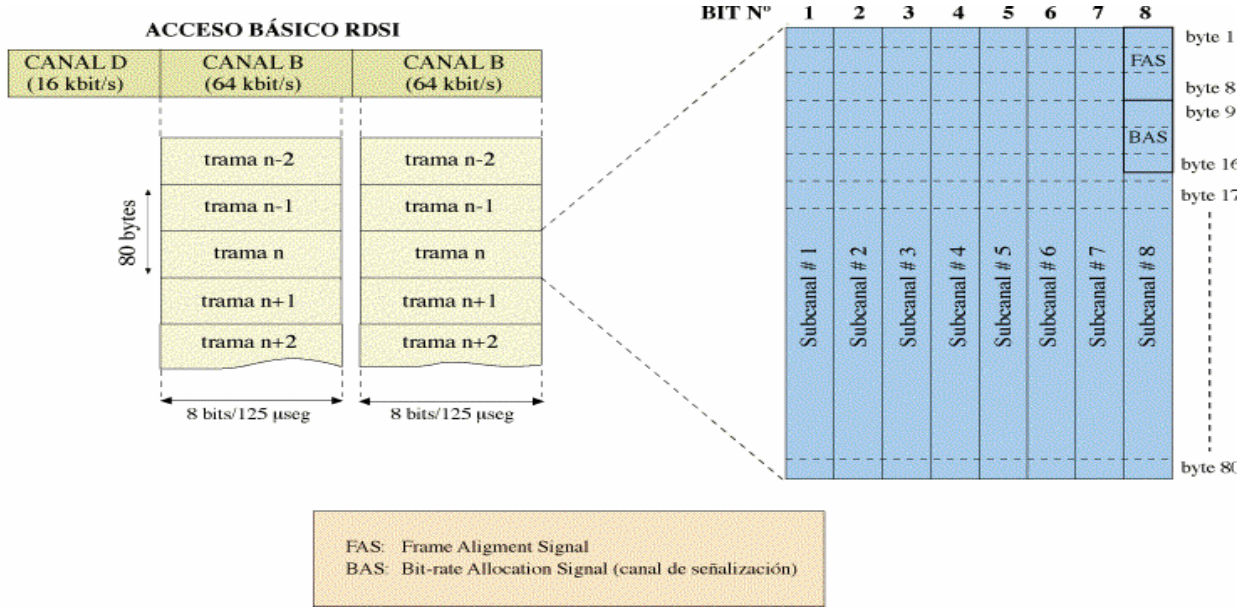


Figura 2.2.- Estructura de trama H.221 sobre un acceso básico RDSI

2.6.2 H.225.-

Estándar utilizado para dar formato a las tramas de vídeo, audio, datos y control para lanzarlos y recuperarlos de la red. Sus tareas son:

- Definir la forma de empaquetar el vídeo, el audio y los datos en bits o paquetes para su transmisión por la red.
- Determinar el orden de los paquetes.
- Detectar errores que puedan producirse en la transmisión.

Además, lleva a cabo las tareas de registro, admisión y control del canal de señalización RAS que realiza las conexiones entre el gatekeeper y los demás componentes.

2.6.3 H.230.-

Establece el modo de realizar el refresco de las imágenes y la conmutación entre audio y vídeo en una multivideoconferencia.

Define las señales de control y de indicación relacionadas con el vídeo, audio, gestión y el multipunto de una conferencia, y especifica, además, una tabla de códigos con las circunstancias bajo las cuales los códigos de control y de indicación son obligatorios u opcionales.

2.6.4 H.242.-

Define los protocolos para la negociación y establecimiento de videoconferencias entre terminales a través de canales digitales de hasta 2 Mbps.

Se encarga de negociar las mejores características para mantener la videoconferencia.

2.6.5 H.245.-

Estándar de control y señalización de llamada que permite a las terminales compatibles H.323 conectarse unas con otras.

Se encarga de negociar parámetros como la razón de bits, razón de tramas y el formato de imagen, así como de la apertura y cierre de

canales lógicos, peticiones de preferencia y mensajes de control de flujo.

2.7 Protocolos para Transmisión de Voz y Video

Un protocolo es un conjunto de reglas de comunicación entre dispositivos, como es el caso de computadoras, teléfonos, ruteadores, switches, por mencionar algunos. Los protocolos establecen el formato, sincronización, secuencia y control de errores. Sin estas reglas, los dispositivos no podrían detectar la llegada de bits.

2.7.1 Protocolo S.I.P.

SIP o Protocolo de Inicio de Sesiones, es un protocolo desarrollado por el IETF MMUSIC Working Group con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos online y realidad virtual. SIP es uno de los protocolos de señalización para voz sobre IP, acompañado por H.323.

2.7.2 Protocolo R.T.P.

RTP o Protocolo de Transporte de Tiempo real. Es un protocolo de nivel de transporte utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una videoconferencia.

Los servicios prestados por RTP incluyen:

- **Payload-type identification -** Indicación de qué tipo de contenido se lleva
- **Sequence numbering -** Secuencia de
- **Time stamping Sellado de tiempo** - permite la sincronización y cálculos de jitter
- **Delivery monitoring -** Entrega de vigilancia

2.7.3 Protocolo I.A.X.2

El protocolo IAX ahora se refiere generalmente al IAX2. AX2 permite manejar una gran cantidad de códecs y un gran número de streams, por lo que puede ser utilizado para transportar virtualmente cualquier tipo de dato. Esta capacidad lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas.

IAX2 utiliza un único puerto UDP, generalmente el 4569, para comunicaciones entre puntos finales (terminales VoIP) para señalización y datos.

2.8 Códecs de Audio y Video para Videoconferencia

2.8.1 Códecs de Audio.

Es un tipo de codec específicamente diseñado para la compresión y descompresión de señales de sonido.

2.8.2 Estándares de codificación de Audio.-

Los estándares especificados por la ITU-T para la codificación de audio son: G.711, G.722, G.723, G.728 y G.729.

2.8.2.1 G.711.-

Se basa en codificar muestras de la señal de audio a 8 KHz y asignar a esas muestras un código de 8 bits con el que se consigue tener 256 posibles valores de la muestra con flujos de 64 Kbps.

2.8.2.2 G.722.-

Este estándar utiliza la técnica ADCPM, es decir, no codifica el valor de la muestra sino la diferencia con el valor anterior de la muestra que se puede codificar con menos bits al ser una diferencia muy pequeña. En este estándar se muestrea la señal a 16 KHz y se asignan códigos de 4 bits consiguiendo tener 16 posibles valores de la señal y obteniendo así mayor calidad que con el estándar G.711.

2.8.2.3 G.723.-

Al igual que G.722 comprime frecuencias comprendidas entre 50 Hz y 7KHz pero lo hace a canales de 48, 56 y 64 Kbps, consiguiendo así mayor disponibilidad y mayor calidad en la transmisión y recepción.

2.8.2.4 G.728.-

Este estándar se basa en fórmulas matemáticas para reproducir la señal y lo que codifica son los parámetros predictores utilizados en esas fórmulas para los que sólo son necesarios 2 bits con los que se consigue sólo 4 niveles de cuantificación para la señal con 16 Kbps.

2.8.2.5 G.729.-

Estándar equivalente a G.728 pero se reduce el régimen binario de 16 Kbps a 8 Kbps permitiendo comprimir así los 64 Kbps.

2.8.3 Códecs de Video.-

Es un programa que permite comprimir y descomprimir video digital. Su funcionalidad se basa en obtener un almacenamiento substancialmente menor de la información de video, esta se

comprime en el momento de guardar la información hacia un archivo y se descomprime en tiempo real al momento de la visualización.

La codificación de vídeo viene especificada en los estándares H.261 y H.263.

2.8.3.1 H.261.-

Se encarga de definir el algoritmo de codificación de vídeo, el formato de las imágenes y la corrección de errores.

La técnica empleada por este estándar para comprimir la información de cada fotograma es la redundancia espacial, es decir, asegura que la información correspondiente a un punto del fotograma será la misma para los puntos de alrededor, con lo que transmitiendo sólo la información de ese punto central se ahorra la de los demás.

2.8.3.2 H.263.-

Este estándar ofrece mejoras respecto a H.261 desde dos aspectos:

- Soporta más formatos de imagen, como son: 16CIF, 4CIF, CIF, QCIF y Sub-QCIF (para transmisiones en Internet de baja velocidad como módems de 28.8 Kbps).

- Mejora la técnica de redundancia temporal, ya que tiene en cuenta no sólo los fotogramas pasados sino también los siguientes esperados, y además ofrece mayor calidad al ampliar la zona en la que busca el macrobloque en la imagen siguiente a 32 puntos en lugar de los 16 que usa H.261.

2.9 Protocolo de Internet Versión 4 (IPv4)

La versión 4 del protocolo para Internet, denominada (IPV4), fue la primera versión de protocolo de uso masivo, y en la actualidad se utiliza en la mayoría del tráfico actual de Internet en todo el mundo.

Existen algo más de 4000 millones de direcciones IPv4 distribuidas en todo el mundo cubriendo las actuales necesidades pero no toda la demanda que las telecomunicaciones de hoy en día requieren.

IPv4 trabaja con un mecanismo de control de errores, el cual es controlado por el Internet Control Message Protocol (ICMP), por ejemplo, si a un ruteador le falla un enlace por el cual estaba transmitiendo los datos, elimina el datagrama y manda un mensaje de ICMP al equipo que está enviando los datos y se olvida del datagrama, no trata de retransmitirlo, el equipo que estaba transmitiendo, retransmite el datagrama, no teniendo la información de cual enlace está activo o no.

Cuando el datagrama llega al ruteador él verá la manera de hacerlo llegar a su destino por otro enlace, lo que nos refleja éste tipo de servicio es que no implica fiabilidad (unreliable) y no conexión (conectionless) por un camino específico.

2.9.1 Estructura del Datagrama IPv4

La estructura de un datagrama IPv4, se divide en bloques de 32 bits (4 bytes), comenzando de izquierda a derecha y de arriba hacia abajo, el primer bit es el bit 0, el orden es importante ya que dependiendo del equipo al que se está comunicando es su manera de guardar los bits en memoria, (figura 2.3). A ésta manera de transmitir los bits se le denomina network byte order.

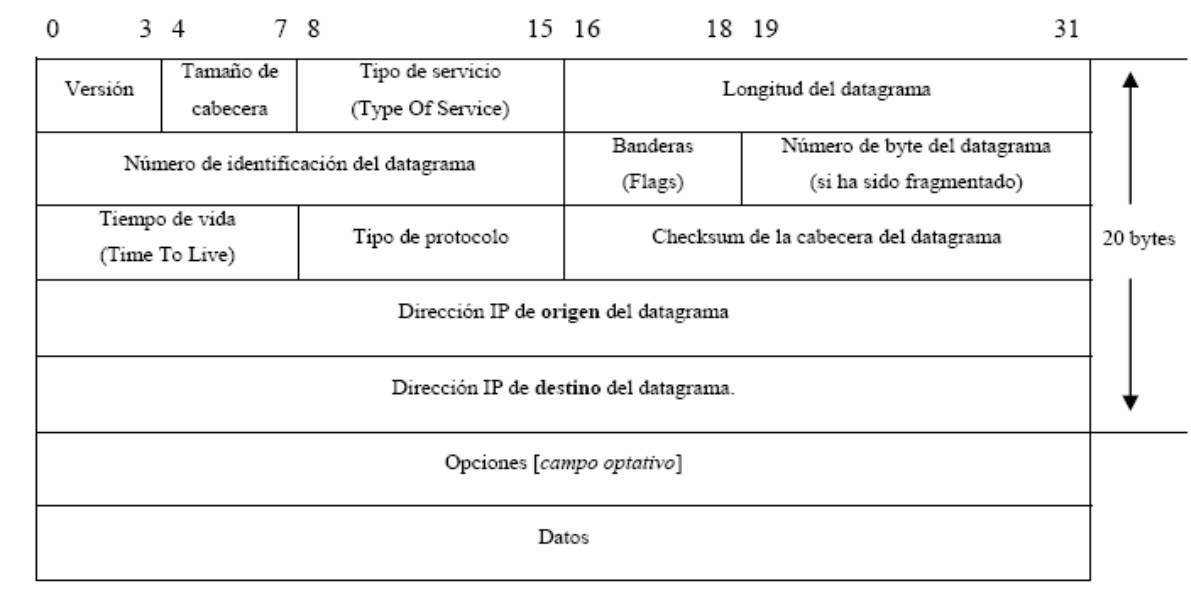


Figura. 2.3.- Estructura de un datagrama IPv4

Los datos del encabezado son importantes ya que son la manera de dar a conocer al ruteador o al otro host lo que se está enviando.

Para tener más claros los campos se detalla su contenido a continuación.

2.9.1.1 Versión.-

Especifica que formato de versión es el datagrama, ésta información solamente lo utilizan los ruteadores y la capa IPv4 de la conexión, permite que coexistan varias versiones de IPv4 en las diferentes redes conectadas al Internet sin que el usuario sepa de su existencia.

2.9.1.2 Tamaño del Encabezado.-

Indica el número de palabras de 32 bits que ocupa el encabezado, estos 4 bits limitan el tamaño de la encabezado a 60 bytes, sin embargo por lo regular se ocupan 20 bytes.

2.9.1.3 Tipo de Servicio.-

Son 8 bits, los primeros 3 no se usan, los siguientes 4 definen el tipo de servicio, el cual se detalla en la tabla 2.1 y el último bit no se utiliza pero debe de tener valor de 0 siempre, en los bits de tipo de servicio, solamente uno puede estar activo a la vez.

El tipo de servicio se tiene para darle a entender al ruteador la política de servicio que se debe de tener con el datagrama, minimizar el retrazo, maximizar el rendimiento, maximizar la

fiabilidad del transporte y minimizar el costo económico del transporte.

Tipo de aplicación	Minimizar retraso	Maximizar rendimiento	Maximizar fiabilidad	Minimizar costo	Valor en hexadecimal
TELNET	1	0	0	0	0x10
FTP	0	1	0	0	0x08
SMTP	0	1	0	0	0x08
DNS (UDP)	1	0	0	0	0x10
DNS (TCP)	0	0	0	0	0x00
ICMP	0	0	0	0	0x00
BOOTP	0	0	0	0	0x00

Tabla 2.1.- Valores típicos del tipo de servicio según la aplicación.

2.9.1.4 Longitud del Datagrama.-

Mide 16 bits y dice cuanto espacio se debe guardar en la memoria para la recepción de cada datagrama, también dice cuantos bytes se deben leer por datagrama, con esto se puede tener un control muy sencillo de si los datagramas llegan completos o no, también limita el tamaño máximo de los datagramas a 65515 bytes, el Maximum Tranfer Unit (MTU) es 216 bytes 65525 – 20 bytes de encabezado.

En dado caso que un paquete que se quiera enviar por la red excede el máximo disponible para dicha red, se divide en varios pedazos.

2.9.1.5 Número de Identificación.-

Del datagrama indica el número de paquete que se esta recibiendo o enviando cuando se tiene que dividir en pedazos un paquete, así cuando se recibe el paquete se puede ordenar adecuadamente, mide 16 bits, por lo que un datagrama se puede dividir hasta en 65535 fragmentos.

2.9.1.6 Banderas.-

Mide 3 bits y especifica diferentes actividades según el bit que esté encendido, si el primero está encendido quiere decir que el datagrama es parte de un datagrama mayor, si el segundo está encendido quiere decir que el datagrama no debe de ser fragmentado y el tercero no se utiliza, teniendo siempre el valor 0.

2.9.1.7 Número de byte en el Datagrama.-

Indica cual es la posición en bytes que ocupan los datos en el datagrama original, obviamente solo se ocupa si el fragmento es parte de un paquete mayor, mide 13 bits y sirve para reconstruir el paquete original.

2.9.1.8 Tiempo de Vida.-

Mide 8 bits y es el que indica cuanto tiempo vivirá el datagrama en transición, es decir, cuanto tiempo tiene el datagrama para llegar a su destino para que los datagramas no circulen para siempre por la red, éste campo tiene un valor máximo de 255 y cada vez que pasa por un ruteador su valor

se decrementa en uno, si el valor llega a cero, el ruteador que le toca proporcionar ese valor, envía un ICMP al origen para que el datagrama sea retransmitido.

2.9.1.9 Tipo de Protocolo.-

Indica el protocolo superior que se esta utilizando, ya sea TCP, UDP, ICMP, etc. El campo se ocupa ya que todos los protocolos de Internet utilizan IP como medio de transporte y al llegar al destino hay que entregarlo en los medios adecuados.

2.9.1.10 Suma de Comprobación ("checksum") del Encabezado del Datagrama.-

Se utiliza solo para verificar el encabezado, ya que tanto UTP, TCP y demás protocolos tienen su propio "checksum" y verificarán sus datos de manera autónoma, sirve para verificar que el encabezado llegue completo y no se descarte el datagrama por pérdida de información en el camino.

2.9.2 Direccionamiento IPv4

La dirección IP origen y la dirección IP destino son dos números de 32 bits, cada una. Cada equipo tiene un número específico, dentro del protocolo IPv4 se denominan 4 octetos de 8 bits separados por

un punto para especificar cada equipo en la red. Existen varios tipos de redes las cuales se describen en la tabla 2.2:

CLASE	DESDE	HASTA
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Tabla 2.2.- Clases de direcciones IPv4 en Internet

Las clases de redes sirven para definir el tamaño de las redes, como se vio en la figura anterior existen 5 clases de redes, en la tabla 2.3 se puede ver la cantidad de equipos que se pueden conectar a cada red:

Clase A	0	Identificador de red (7 bits)						Número de equipo (24 bits)
Clase B	1	0	Identificador de red (14 bits)					Número de equipo (16 bits)
Clase C	1	1	0	Identificador de red (21 bits)				Número de equipo (8 bits)
Clase D	1	1	1	0	Identificador de red (28 bits)			
Clase E	1	1	1	1	0	Reservado para uso futuro (27 bits)		

Tabla 2.3.- Subdivisión de los 32 bits para las clases A, B, C, D Y E

Cabe mencionar que el número máximo en cada octeto es 255 ya que al ser de 8 bits (28=256) el rango es entre 0 y 255 para cada octeto.

Se definieron los diferentes tipos de redes para hacer más fácil la ubicación de redes chicas, medianas y grandes, es decir:

- La red clase A es para redes grandes, se pueden tener 128 (2^7) redes de 16,777,216

  (2^{24}) equipos conectados en cada una.

- La red clase B es para redes medianas, se pueden tener 16,348 (214) redes de 65,535

  (2^{16}) equipos conectados cada una.

- La red clase C es para redes chicas, se pueden tener 2,097,154 (221) redes de 256

  (2^8) equipos conectados.

- Las redes clase D y E son de multicast y reservada respectivamente, también para futuros usos.

La numeración de las direcciones puede variar desde 0.0.0.0 hasta 255.255.255.255, entonces el aprenderse cada una de las direcciones para acceder a ellas sería muy difícil, pera ayudarnos a recordar las direcciones más fácilmente, existen los DNS (Domain Name Server), ellos hacen la traducción de la dirección en números a una dirección que se pueda recordar más fácilmente, por ejemplo una dirección 164.149.10.1 sería más fácil recordarla como www.nombre.com.ec.

La estructura también tiene una especificación definida, la última parte define por lo regular donde se encuentra la página, ".ec" es Ecuador, ".mx" es México, ".uk" es Inglaterra, ".es" es España, etc. El único país que no tiene definida una abreviación es Estados Unidos,

ya que ellos generaron la terminología, para éste caso la última parte y en los demás en la penúltima parte, se define el tipo de red, ".gov" para empresas de gobierno, ".net" para empresas de telecomunicaciones, ".com" para empresas del ámbito general, ".mil" para militares y ".edu" para universidades o empresas educativas, se han agregado algunas como ".tv" para la televisión pero no están bien especificadas.

La segunda parte define el nombre de la empresa o la página a donde se quiere acceder, la primera parte en cambio define el acceso a una página de Internet (www), recientemente se ha desechado ésta parte ya que siempre es lo mismo y algunas empresas mejor la ocupan para diferenciar servidores.

2.10 Protocolo de Internet Versión 6 (IPv6)

La versión 6 del protocolo para Internet, denominada (IPV6), fue adoptada a finales del año 1994 por la Internet Engineering Task Force (IEFT), luego de que las pruebas iniciales de la versión 5 no pasaran las pruebas de fase experimental, este nuevo protocolo de Internet también llamado IP Next Generation" o (IPng), cuenta con un pequeño porcentaje de las direcciones públicas de Internet dominadas y utilizadas aún por el protocolo de Internet versión 4 (IPV4).

Las modificaciones que se introducen en esta nueva versión han sido diseñadas para dar solución a todos los problemas estructurales que surgieron para la versión 4, y también para soportar nuevas redes de comunicación de alto rendimiento como; ATM, Gigabit Ethernet, etc.

Es necesario destacar, que debido al impulso actual que se está dando a nivel mundial con el paulatino número de aplicaciones que necesitan direcciones IP públicas globales y válidas para conexiones extremo a extremo "enrutables", unido al crecimiento de la nueva generación de telefonía móvil (UMTS) que funcionará sobre IP, hace que la transición del IPv4 a IPv6 sea impostergable.

También se incluyen mejoras con respecto a la implementación nativa de seguridad de datos (Ipsec), calidad de servicios (Qos), autoconfiguración de nodos (Neighbour Discovery), movilidad e innovaciones en dispositivos de red mejorando la calidad y velocidad de los datos, ya que las expectativas actuales hablan de un agotamiento de espacios de direcciones bajo la tecnología de Internet IPV4, para los años 2007 y 2008. Tomando como claro ejemplo las diversas iniciativas de redes experimentales en Ipv6, en Europa y especialmente en Asia, donde el espacio disponible de direcciones para IPv4 ya ha sido agotado; lo cual ha provocado que muchos proveedores de Internet asiáticos hayan comenzado a trabajar con Ipv6 de manera comercial.

Una de las características mas destacadas en este protocolo es el nuevo sistema de direcciones que maneja, el mismo que pasa de 32 bits en la versión 4 a los 128 bits definidas para la versión 6, según lo descrito en el RFC 2460, esto corresponde a 32 dígitos hexadecimales ($2^{128} \approx 3.4 \times 10^{38}$) determinadas en dos partes lógicas: el **prefijo** de 64 bits y la parte **complementaria** de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección. Además cuenta con varias características principales que describen el nivel de servicio; siendo:

- Nuevo formato de encabezado.
- Gran espacio de direcciones.
- Direccionamiento jerárquico e infraestructura de enrutamiento eficientes.
- Configuración de direcciones sin estado y con estado.
- Seguridad integrada.
- Mayor compatibilidad con QoS.
- Nuevo protocolo para la interacción de nodos vecinos.

2.10.1 Nuevo Formato de Encabezado de IPv6

IPv6 presenta un nuevo formato diseñado para que la carga de trabajo del encabezado sea mínima, para lo cual algunos campos de la cabecera de la versión 4 han sido eliminados o han pasado a ser

opcionales, tanto para reducir el coste de procesamiento como el tamaño de la cabecera. Además provee un procesamiento más eficiente en los enrutadores intermedios.

Para que los encabezados de IPv4 puedan funcionar, deben utilizar una implementación de IPv4 e IPv6 para reconocer y procesar ambos formatos de encabezado.

2.10.2 Gran Espacio de Direcciones en IPv6

La versión 6 del protocolo para Internet, maneja un total de 128 bits (16 bytes) por espacio de direcciones, el cual ha sido diseñado para establecer varios niveles de subredes y asignaciones de redes de la red troncal de Internet

Con esto se deja aún lado las técnicas de conservación de direcciones, como la distribución de ***NAT***, para IPV4. Es necesario destacar que para la nueva versión del protocolo de Internet IPv6 no existen las direcciones de difusión (broadcast), para simular esto se lo hace a través del uso de la dirección multicast FF01::1 para todos los nodos

2.10.3 Direccionamiento Jerárquico e Infraestructura de Enrutamiento Eficientes en IPv6

El direccionamiento de IPv6 está diseñado para crear una infraestructura de enrutamiento jerárquica eficiente mostrando

múltiples niveles de proveedores de servicios Internet. Para lo cual fue necesario ampliar el tamaño de las direcciones de 32 bits (IPv4) a 128 bits, con el fin de soportar más niveles en la jerarquía de direccionamiento, un número mayor de nodos direccionables, y un sistema de auto configuración de direcciones.

Se incluye además un nuevo tipo de dirección, llamada anycast, la cual permite identificar múltiples interfaces y enviar un paquete a cualquier nodo o un grupo de nodos sin la perdida de paquetes, creando ámbitos de redundancia. En términos de "routing" se determina que, para que los paquetes se entreguen a la dirección más cercana, el direccionamiento de la red debe conocer qué interfaz anycast tiene más cercana y cual es su respectiva distancia.

IPV6 permite 3 tipos de direcciones:

2.10.3.1 Unicast - "Unidistribución".-

Tipo de dirección de *identificador* para una interfaz individual. Es utilizada cuando un paquete enviado a una dirección de este tipo se entrega a la interfaz identificada por esa dirección.

2.10.3.2 Anycast – "Monodistribución".-

Tipo de dirección de *identificador* para un conjunto de interfaces, pertenecientes a diferentes nodos. Es utilizada cuando un paquete enviado a una dirección monodistribución se entrega a una de las direcciones más cercanas de las

interfaces identificadas por esa dirección, de acuerdo a la distancia establecida por el protocolo de encaminamiento.

2.10.3.3 Multicast – "Multidistribución".-

Tipo de dirección de *identificador* para un conjunto de interfaces, pertenecientes a diferentes nodos. Es utilizada cuando un paquete enviado a una dirección multidistribución se entrega a todas las interfaces identificadas por esa dirección.

2.10.4 Configuración de Direcciones sin estado y con estado en IPv6

Esta versión de protocolo para Internet permite obtener la configuración de direcciones con estado (stateful), a través de un servidor DHCP de forma manual, o de forma automática sin estado (stateless). Este tipo de auto configuración está diseñada específicamente para el uso de host o estaciones, y mas no para "routers" o encaminadotes de ruta. El mecanismo de autoconfiguración " stateless " se utiliza cuando no importa la dirección exacta que se asigna a un host, sino tan sólo para determinar que es única y correctamente enrutable. Por otro lado el mecanismo de autoconfiguración "stateful", asegura que cada host tiene una determinada dirección, asignada manualmente.

"El mecanismo de auto configuración de las interfaces de IPV6 permite determinar que la versión 6 del protocolo para Internet es "Plug & Play"".[1]

2.10.5 Seguridad Integrada en IPv6

IPV6 utiliza IPSec, un estándar que proporciona servicios de seguridad al protocolo de Internet y a todos los protocolos superiores basados en IP como TCP, UDP, entre otros, el mismo proporciona una solución basada en estándares en respuesta a las necesidades de seguridad de red, permitiendo la interoperabilidad entre distintas aplicaciones de IPv6.

IPSec se aplica tanto para la versión 4 del protocolo para Internet, así como para la versión 6 del mismo, y ha sido diseñado mediante un conjunto de tecnologías (RSA) y algoritmos (DES, IDEA, Blowfish), para proporcionar confidencialidad, integridad y autenticación de datagramas IP. Así también se encuentra compuesto por dos protocolos principales dos protocolos de seguridad:

[1] Tomado de la fuente de información: http://www.6sos.org

2.10.5.1 Autenticación de Cabecera IP (AH).-

Que cumple la función de proporcionar un medio al receptor de los paquetes IP para autenticar el origen de los datos y verifica que dichos datos no hayan sido alterados en tránsito. También se encuentra,

2.10.5.2 Seguridad y Encapsulamiento IP de Carga Util (ESP).-

Proporciona confidencialidad, especificando el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en un datagrama IP.

Estos protocolos, proporcionan mecanismos de seguridad para proteger el tráfico generado por el protocolo de Internet (IP). Además de estos componentes, cuenta con un protocolo de gestión de claves Internet Key Exchange (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

2.10.6 Mayor Compatibilidad con Calidad de Servicio (QoS) en IPv6

La QoS (Quality of Service) permite y asegura una mayor calidad de servicios en un tiempo dado durante la transmisión de datos. Para el caso de la versión 6 del protocolo de Internet, la calidad de servicios se incorpora en la cabecera, la que se divide en dos campos específicamente (ver tabla 2.4), por cuanto permiten definir cómo se identifica y se controla el tráfico. Permitiendo a los enrutadores

identificar y proporcionar un tratamiento especial a los paquetes que pertenecen a un flujo.

Clase de Tráfico (6 bits)	Identificador de Flujo (20 bits)

Tabla 2.4.- Estructura de QoS en la cabecera de IPV6

2.10.6.1 Clase de Tráfico.-

Se basa en la división de diferentes clases de tráfico y en la asignación de prioridades para el transporte de datos por la red, reduciendo la carga en dispositivos de la red a través de un mapeo entre flujos de tráfico y niveles de servicio

2.10.6.2 Identificador de Flujo.-

Permite identificar flujos de datagramas desde un origen a un destino (unicast o multicast) para los que se solicita una determinada QoS.

2.10.7 Nuevo Protocolo para la Interacción de Nodos en IPv6

Este protocolo implementado a través de la función (Neighbor Discovery) para IPV6, permite administrar la interacción de nodos del mismo vínculo mediante un conjunto de mensajes de control de protocolo para Internet (ICMPv6) “Internet Control Message Protocol for IPv6”. Este protocolo permite reemplazar al Protocolo de resolución de direcciones ARP (Address Resolution Protocol)

utilizado en IPv4, el mismo que se basa en mensajes de multidifusión.

2.10.8 Sintaxis para los Tipos de Direcciones

Los tipos de direcciones del protocolo de Internet IPv6 pueden identificarse tomando en cuenta los primeros bits de cada dirección.

- **"::/128"** – la dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.

- **"::1/128" –** la dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (correspondiente con la dirección 127.0.0.1 de IPv4). La cual no puede asignarse a ninguna interfaz física.

- **"::/96"** – La dirección IPv4 se usa como un mecanismo de transición en las redes duales para las versiones de IPv4 e IPv6.

- **"::ffff:0:0/96"** – La dirección IPv4 mapeada es usada como un mecanismo de transición en terminales duales.

- **"fe80::/10"** – Prefijo de enlace local (link local) específica que la dirección sólo es válida en el enlace físico local.

- **“fec0::/10**” – Prefijo de emplazamiento local (site-local) específica que la dirección sólo es válida dentro de una organización local. LA RFC 3879 lo declaró obsoleto, estableciendo que los sistemas futuros no deben implementar ningún soporte para este tipo de dirección especial.

- **“ff00::/8”** – Prefijo de multicast es usado para las direcciones multicast

2.10.9 Direcciones Reservadas para IPV6.

Dirección IPv6	Longitud del Prefijo (Bits)	Descripción	Notas
::	128 bits	sin especificar	como 0.0.0.0 en IPv4
::1	128 bits	dirección de bucle local (loopback)	como las 127.0.0.1 en IPv4
::00:xx:xx:xx:xx	96 bits	direcciones IPv6 compatibles con IPv4	Los 32 bits más bajos contienen una dirección IPv4. También se denominan direcciones “empotradas.”
::ff:xx:xx:xx:xx	96 bits	direcciones IPv6 mapeadas a IPv4	Los 32 bits más bajos contienen una dirección IPv4. Se usan para representar direcciones IPv4 mediante direcciones IPv6.

Dirección IPv6	Longitud del Prefijo (Bits)	Descripción	Notas
fe80:: - feb::	10 bits	direcciones link-local	equivalentes a la dirección de loopback de IPv4 – 127.0.0.1
fec0:: - fef::	10 bits	direcciones site-local	Equivalentes al direccionamiento privado de IPv4
ff::	8 bits	Multicast	
001 (base 2)	3 bits	direcciones unicast globales	Todas las direcciones IPv6 globales se asignan a partir de este espacio. Los primeros tres bits siempre son “001”.

Tabla 2.5.- Esquema de direcciones reservadas para IPV6

La Tabla 2.5 muestra el esquema del direccionamiento bajo el protocolo de Internet IPV6.

Las direcciones ipv6 se representan por 16 octetos, en grupos de 2 separados por dos puntos, con relación a las direcciones ipv4 que se representan por 4 octetos en forma decimal y separados por puntos.

Ejemplo:

Dirección ipv4 = 200.123.125.59

Dirección ipv6 = 2000:BA98:A654:4567:FEDC:BA89:7654:3210

Ejemplo de una dirección ipv6 igual que una ipv4:

0:0:0:0:0:0:10:10:10:120 ≈ 10.10.10.120

Las direcciones ipv6 se representan con nombres a través del servidor Domain Name Server 6 (DNS6).

2.10.10 Estructura de IPV6.

La estructura en la que se basa la versión 6 del protocolo para Internet, está diseñada para crecer de un modo secuencial según las necesidades o aplicaciones que lo vayan requiriendo de forma paulatina, permitiendo así el uso de un formato extendible en la cabecera del mismo.

El formato de cabecera de IPV6 cuenta con 40 bytes, el mismo que ha excluido campos redundantes utilizados por IPV4, cuya longitud es de 20 bytes. Se determina además que gracias a la propiedad del formato de cabecera **fija** esta versión permite una mayor facilidad de procesamiento de paquetes de datos en los encaminadotes y conmutadores, implicando mayor prestación de servicios.

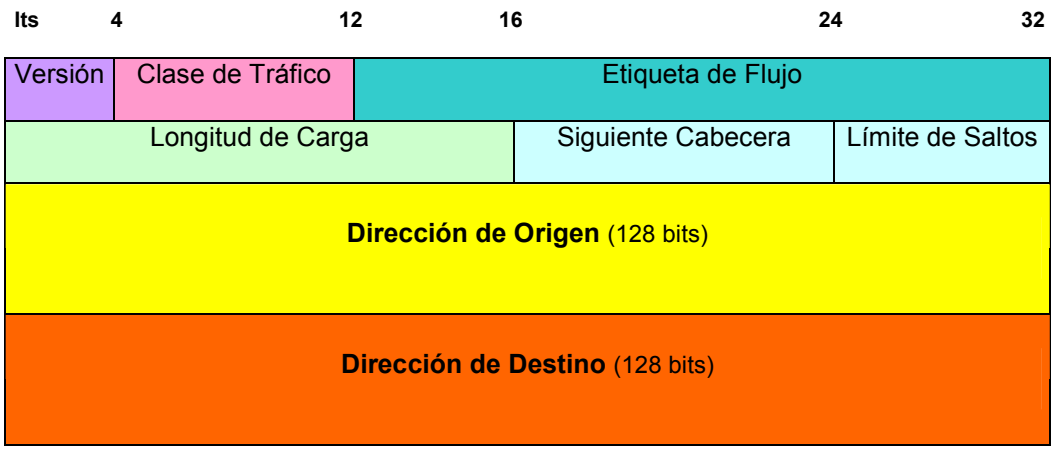


Figura 2.4.- Esquema de Cabecera de IPv6

El formato de cabecera de IPv6 está compuesto de los siguientes campos (figura 2.4).

2.10.10.1 Versión.-

Identifica la versión de protocolo, en este caso es la versión 6, el mismo es solo para identificación del formato de cabecera.

2.10.10.2 Clase de Tráfico – Prioridad.-

Indica la prioridad del paquete asociada a los aplicativos o servicios, entre los diferentes encaminadotes y nodos de la red de datos. Los valores de prioridad se dividen en los siguientes rangos:

- De **0 a 7**: Para paquetes en los cuales el remitente espera una respuesta en caso de congestión.
- De **8 a 15**: Para paquetes que no deben ser respondidos en caso de congestión.
- El **valor 8**: Es usado para cuando el remitente está dispuesto a que sus paquetes sean descartados en caso de congestión. (Ejemplo. *Video en alta calidad*)
- El **valor 15**: usado para cuando el remitente está muy poco dispuesto a que algún paquete sea descartado. (Ejemplo: *Audio de baja calidad*).

2.10.10.3 Etiqueta de Flujo.-

Valor aleatorio que se tiene para toda la comunicación del mensaje, el mismo es usado por el remitente para indicar que

sus paquetes sean tratados de forma especial por los routers, como en servicios de alta calidad o en tiempo real.

Es necesario tener en cuenta que todos los paquetes del mismo flujo, deben tener valores similares en los campos de; dirección de origen, dirección de destino, prioridad, y etiqueta de flujo.

2.10.10.4 Longitud de Carga.-

Mediante este campo se establece la longitud del paquete que sigue a la cabecera.

2.10.10.5 Siguiente Cabecera.-

Indica la cabecera del protocolo próximo de comunicación, este campo se presenta en todas las cabeceras, en el caso de que esta cabecera muestre el valor = 59 indicaría que nada hay a partir de esa cabecera. En el caso de que se presente octetos más allá del final de una cabecera deberán ser descartarse.

2.10.10.6 Límite de Saltos.-

Indica el número de saltos o tiempo de vida del paquete, por cada salto disminuye el valor en uno del tiempo de vida “TTL” del paquete hasta llegar a cero y ser eliminado. Este campo sustituye al campo “TTL” o tiempo de vida del paquete, de IPv4.

2.10.10.7 Dirección de Origen.-

Dirección del origen de la transferencia de paquetes.

2.10.10.8 Dirección de Destino.-

Dirección de destino de la transferencia de paquetes.

La estructura de IPV6 soporta, además de la cabecera principal, cabeceras opcionales de extensión, las mismas que prestan varios servicios adicionales, evitan que los fragmentos de paquetes compartan campos que no utilizan. Tanto la cabecera principal como las cabeceras de extensión, utilizan obligatoriamente el campo de siguiente cabecera, para poder identificar el protocolo de nivel superior subsiguiente.

IPV6, maneja diferentes tipos de cabeceras de extensión, como las siguientes:

2.10.10.9 Cabecera de Opciones Salto a Salto "Hop by Hop".-

Contiene la información especial para los routers en cada salto.

2.10.10.10 Cabecera de Encaminamiento "Routing".-

Permite determinar la ruta a seguir, ya sea de manera parcial o total, indicando todos los nodos intermedios entre el origen y el destino del paquete.

2.10.10.11 Cabecera de fragmentación "Fragment".-

Permite establecer la información de fragmentación y reensamblaje de los paquetes transmitidos por la red, es usado para que el emisor pueda transmitir un paquete de mayor tamaño al que cabría en la ruta del MTU “Maximum Transfer Unit”.

2.10.10.12 Cabecera de Autenticación “AH”.-

Verifica la autenticidad del equipo emisor del mensaje, aportando servicios de integridad de datos, a través de la autenticación del origen de los datos, esta cabecera proporciona una propiedad bastante alta en seguridad para IPV6.

2.10.10.13 Cabecera de Encapsulado de Seguridad de Longitud de Carga “ESP”.-

Mediante esta cabecera, se puede identificar la información de los mecanismos de seguridad, integridad y autenticación del origen de los datos empleados para garantizar los servicios de integridad del contenido de los paquetes IP.

2.10.10.14 Cabecera de Opciones para el Destino.-

Permite manejar la información que debe ser procesada por la dirección de destino final del datagrama.

Para la transmisión de datos a través de varias cabeceras de extensión en un mismo paquete, se establece su uso en el siguiente orden:

1. Cabecera IPv6.
2. Cabecera de opción “Hop-by-Hop”.
3. Cabecera de Opción “Destination”.
4. Cabecera “Routing”.
5. Cabecera “Fragment”.
6. Cabecera “Authentication”.
7. Cabecera “Encapsulating Security Payload”.
8. Cabecera de opción “Destination
9. Cabecera de la capa superior.

2.11 Diferencias entre IPv4 e IPv6

A continuación se detallan varias características generales que diferencian a los protocolos tanto de Internet versión 4 como versión 6.

2.11.1 Expansión de las Capacidades de Direccionamiento.

IPv6 incrementa el tamaño de las direcciones de 32 bits (IPv4) a 128 bits, para soportar más niveles en la jerarquía de direccionamiento, un número mayor de nodos direccionables, y un sistema de autoconfiguración de direcciones. IPV6 añade un nuevo tipo de dirección “anycast”, de forma que es posible enviar un paquete a cualquier nodo entre un grupo de ellos.

2.11.2 Simplificación de la Cabecera.

Algunos campos de la cabecera del IPv4 son eliminados o pasan a ser opcionales, con el objetivo, tanto para reducir el coste de procesamiento así como el tamaño de la cabecera.

2.11.3 Mayor Flexibilidad para Extensiones y Nuevas Opciones.

La gestión de opciones en IPV6 se realiza por un campo “siguiente cabecera” (next header), eliminando así las limitaciones de tamaño en la cabecera, permitiendo introducir una gran flexibilidad en el desarrollo de nuevas opciones.

2.11.4 Capacidades de Control de Flujo.

Se añaden capacidades que permiten marcar los paquetes que pertenezcan a un determinado tipo de tráfico, para el cual el remitente demanda una calidad mayor a la especificada por defecto o servicios en tiempo real.

2.11.5 Capacidades de Autenticación y Privacidad de Datos.

IPv6 provee extensiones para soportar autenticación, integridad y confidencialidad de datos.

2.11.6 Seguridad.

IPv6 incluye seguridad en sus especificaciones como es la encriptación de la información y la autentificación del remitente de dicha información.

2.11.7 Aplicaciones en Tiempo Real.

IPv6 incluye etiquetado de flujos en sus especificaciones. Con este mecanismo los encaminadores o routers pueden reconocer a qué flujo extremo a extremo pertenecen los paquetes que se transmiten.

2.11.8 Plug and Play.

IPv6 incluye en su estándar el mecanismo "plug and play", lo cual facilita a los usuarios la conexión de sus equipos a la red. La configuración se realiza automáticamente.

2.11.9 Movilidad.

IPv6 incluye mecanismos de movilidad más eficientes y robustos.

2.11.10 Especificaciones más Claras y Optimizadas

IPv6 seguirá las buenas prácticas de IPv4 y elimina las características no utilizadas u obsoletas de IPv4, con lo que se consigue una optimización del protocolo de Internet.

CAPITULO III

DISEÑO, ESTRUCTURA E IMPLEMENTACIÓN DE RED PARA LOS SISTEMAS DE VIDEOCONFERENCIA

El presente capítulo muestra a detalle el diseño, estructura, configuración e implementación de los sistemas de Videoconferencia bajo los protocolos de red: IPV4 e IPV6. Así mismo se detallan los pasos necesarios para el correcto funcionamiento de las dos infraestructuras de red, con el fin de realizar una evaluación de desempeño y funcionalidad en tiempo real de una Videoconferencia.

3.1 Prototipo de Diseño y Estructura de red para Implementación del Sistema de Videoconferencia.

H.323 fue diseñado para establecer una videoconferencia sobre redes basadas en arquitecturas como Ethernet, Token Ring, FDDI, etc., utilizando los protocolos TCP/IP.

Tomando en cuenta el punto anterior se requiere diseñar una estructura de red, la cual tenga la capacidad de soportar la transmisión de audio, voz y datos en línea para poder establecer un sistema de videoconferencia.

La figura 3.1 muestra el diseño de un prototipo de red que consta de diferentes equipos como son: un router, dos equipos servidores, dos switch,

dos estaciones de trabajo (clientes), la cual nos servirá como base para el diseño e implementación final del sistema de videoconferencia.

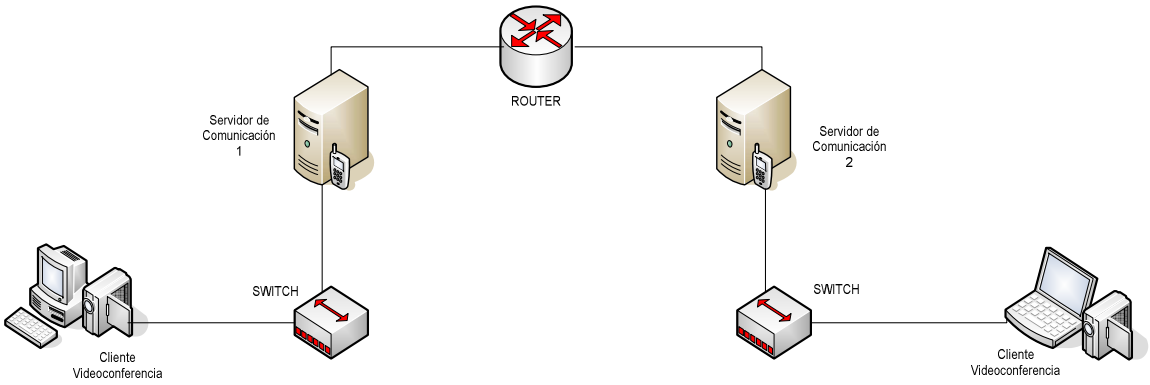


Figura 3.1.- Prototipo de estructura de red para un sistema de videoconferencia

3.2 Diseño, Estructura e Implementación de Red sobre IPV4

La Figura 3.2 muestra la infraestructura de red implementada bajo el protocolo de red IPV4.

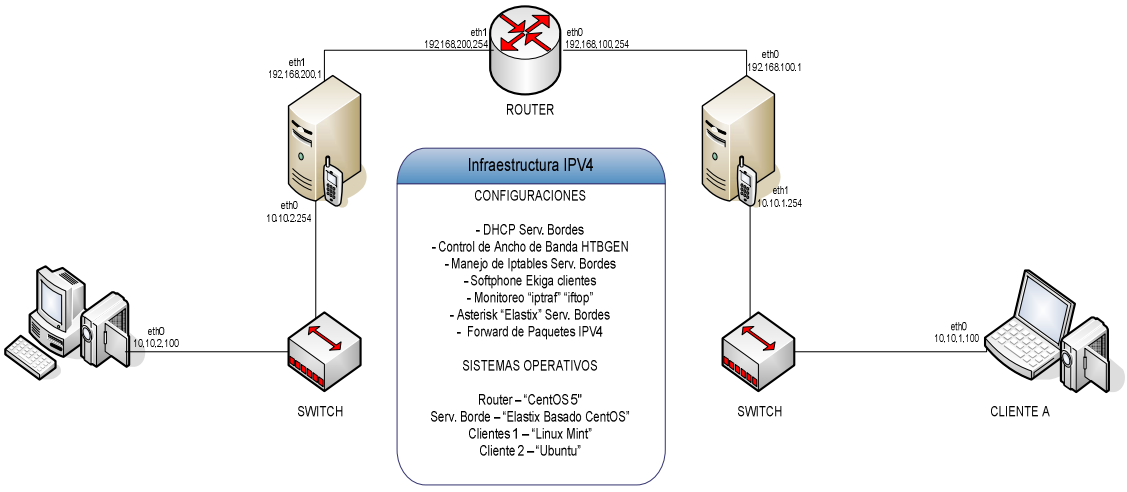


Figura 3.2.- Estructura de red bajo el protocolo de red IPV4

A continuación se detallan los componentes de la infraestructura de red determinada, sus características técnicas y su respectivo funcionamiento.

3.2.1 Equipo Ruteador de Paquetes (ROUTER)

Este equipo permite el encaminamiento de paquetes entre toda la infraestructura de red IPV4 para unir redes diferentes, el objetivo principal de este equipo es redireccionar el tráfico de forma correcta a los servidores de comunicación, a continuación se detallan las características del mismo:

Características	Descripción
Computador	Portátil
Procesador	Pentium IV - 2,2 GHz
Memoria	1 GB RAM
Disco Duro	30 GB
Interfaz de red	2 tarjetas 10/100 Mbps
Velocidad Dispositivo USB	1.0 Mbps
Sistema Operativo Instalado	Centos 5.0

Tabla 3.1.- Características técnicas Equipo Ruteador

3.2.2 Equipos para Servidores de Comunicación (Servidores de Borde).

Estos equipos permiten el enlace y comunicación entre las dos redes LAN a través del ruteador. Estos equipos actúan como servidores para la comunicación de los clientes de Videoconferencia a través de la implementación de la herramienta que permitirá ejecutar la funcionalidad del sistema de Videoconferencia (ELASTIX),

conjuntamente están configurados para establecer el control de ancho de banda y asignación dinámica de direcciones IP a sus respectivos clientes; a continuación se detallan las características de los mismos:

Características	Descripción
Computador	Portátil
Procesador	Pentium IV - 2,2 GHz
Memoria	512 MB RAM
Disco Duro	40 GB
Interfaz de red	2 tarjetas 10/100 Mbps
Velocidad Dispositivo USB	1.0 Mbps
Sistema Operativo Instalado	Elastix – Centos 5.0

Tabla 3.2.- Características técnicas Equipo Servidor de Borde No. 1 (Srv1)

Características	Descripción
Computador	Desktop
Procesador	Pentium III - 750 MHz
Memoria	256 MB RAM
Disco Duro	40 GB
Interfaz de red	2 tarjetas 10/100 Mbps
Velocidad Dispositivo USB	1.0 Mbps
Sistema Operativo Instalado	Elastix – Centos 5.0

Tabla 3.3.- Características técnicas Equipo Servidor de Borde No. 2 (Srv2)

3.2.3 Equipos Clientes para Videoconferencia.

Estos equipos cumplen la función de emisión y recepción de los paquetes de voz, video y datos para el funcionamiento de la Videoconferencia sobre la infraestructura de red IPV4, a continuación se detallan las características de los mismos:

Cliente A para Videoconferencia IPV4

Características	Descripción
Computador	Portátil
Procesador	Pentium IV - 2,0 GHz
Memoria	512 MB RAM
Disco Duro	40 GB
Interfaz de red	1 tarjeta 10/100 Mbps
Velocidad Dispositivo USB	2.0 Mbps
Sistema Operativo	Ubuntu 7.0

Tabla 3.4.- Características técnicas Equipo Cliente A

Cliente B para Videoconferencia IPV4

Características	Descripción
Computador	Desktop
Procesador	Pentium IV – 3,0 GHz
Memoria	2 GB RAM
Disco Duro	160 GB
Interfaz de red	1 tarjeta 10/100 Mbps
Velocidad Dispositivo USB	2.0 Mbps
Sistema Operativo	Linux Mint

Tabla 3.5.- Características técnicas Equipo Cliente B

3.2.4 Dispositivos de Comunicación en Red (SWITCH).

Estos dispositivos de comunicación permiten la interconexión entre las dos redes LAN y la red WAN; a continuación se detallan las características físicas de los mismos:

Equipo de Comunicación "SWITCH"

Características	Descripción
Modelo	DES-1008D
Tipo de Dispositivo	Switch
Número de puertos	8
Velocidad de transmisión	10/100 Mbps autonegociables
Tipo de conector	RJ45

Tabla 3.6.- Características técnicas Equipos de comunicación para red de datos

3.2.5 Cables Conectores para Interfaces de Red.

Permite la interconexión física entre los diferentes dispositivos que conforman la infraestructura de red tanto equipos servidores como estaciones clientes; a continuación se detallan las características físicas de los mismos:

Cables Patch Cord

Características	Descripción
Categoría	5E
Cables cruzados	2
Cables punto a punto	4

Tabla 3.7.- Descripción de cables UTP

3.3 Diseño, Estructura e Implementación de Red sobre IPV6

Tomando como referencia, la estructura de red base, que se muestra en la Figura 3.1, se ha implementado un diseño para que soporte la transmisión de voz, video y datos a través del protocolo IPV6.

La Figura 3.3 muestra la infraestructura de red implementada bajo el protocolo de red IPV6, manteniendo en toda su estructura y diseño la transmisión de paquetes bajo el protocolo de red IPV6, Para la implementación de la infraestructura de red se determina el uso de los siguientes equipos.

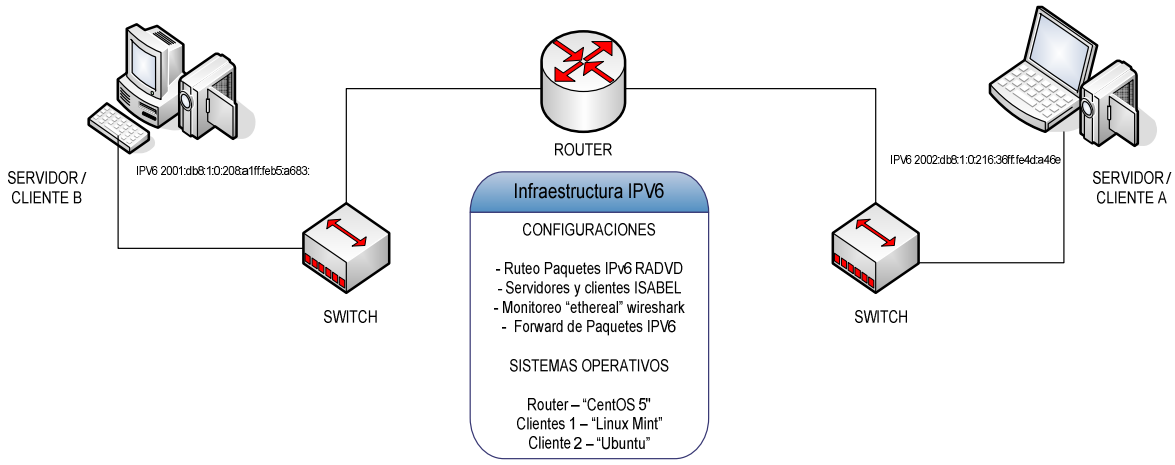


Figura 3.3.- Estructura de red bajo el protocolo de red IPV6

3.3.1 Equipo Ruteador de Paquetes (ROUTER)

Este equipo permite el encaminamiento de paquetes entre toda la infraestructura de red IPV6, el objetivo principal de este equipo es redireccionar el tráfico de paquetes de forma correcta a los equipos emisores-receptores del sistema de Videoconferencia, además de asignar dinámicamente las direcciones de red IPV6 para los equipos que efectúan la Videoconferencia mediante el servicio RADVD, las características técnicas del equipo se detallan en la tabla 3.1

3.3.2 Equipos Servidores / Clientes para Videoconferencia.

Estos equipos cumplen la función tanto como servidores así como clientes para establecer el sistema de Videoconferencia, permitiendo según su configuración tanto la emisión como recepción de los paquetes de voz, video y datos para el funcionamiento de la Videoconferencia sobre la infraestructura de red IPV6, la aplicación de Videoconferencia se realiza a través de la aplicación ISABEL; las características técnicas de los equipo se detallan en las tablas 3.4 y 3.5 respectivamente.

3.3.3 Dispositivos de Comunicación en Red (SWITCH).

Estos dispositivos de comunicación permiten la interconexión entre las dos redes WAN, estos equipos son utilizados para la transmisión de paquetes tanto bajo el protocolo IPV4 e IPV6, las características de los dispositivos se detallan en la tabla 3.6

3.3.4 Cables Conectores para Interfaces de Red.

Permite la interconexión física entre los diferentes dispositivos que conforman la infraestructura de red. Es importante recalcar que no se requieren de cables o conectores especiales para la transmisión de paquetes bajo el protocolo de red IPV6. En la tabla 3.7 se detallan las características de los mismos.

3.4 Configuración de la Estructura para Videoconferencia en IPV4

A continuación se detallan los procedimientos necesarios para determinar la configuración e implementación de las diferentes aplicaciones que son necesarias para establecer el sistema de Videoconferencia bajo el protocolo de red IPV4.

3.4.1 Configuración del Equipo Ruteador "Direccionamiento IP – forward de paquetes"

Para cumplir las funciones de un equipo ruteador se ha realizado la instalación del sistema operativo de uso libre LINUX, con su distribución CENTOS 5.0 cuyo detalle de instalación se encuentra en el **ANEXO 5.1**.

Para que este equipo funcione como ruteador de paquetes debe cumplir los siguientes parámetros de configuración:

3.4.1.1 Configuración de las Interfaces de Red como Redes Independientes

Para realizar la configuración de las interfaces de red, es necesario editar los archivos **/etc/sysconfig/network-scripts/ifcfg-eth0 y /etc/sysconfig/network-scripts/ifcfg-eth1,** mediante el comando **vim** de la siguiente forma:

 # vim /etc/sysconfig/network-scripts/ifcfg-eth0 y

 # vim /etc/sysconfig/network-scripts/ifcfg-eth1

Las figuras 3.4 y 3.5, muestran la configuración realizada en las interfases de red eth0 y eth1, en ellas se puede observar que cada una tiene asignada diferente dirección estática tipo "C" para la simulación de una red WAN.

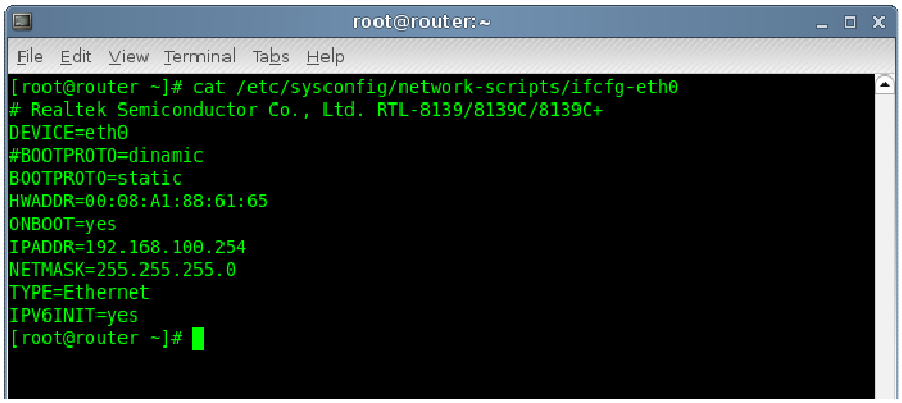


Figura 3.4.- Configuración interfase de red eth0

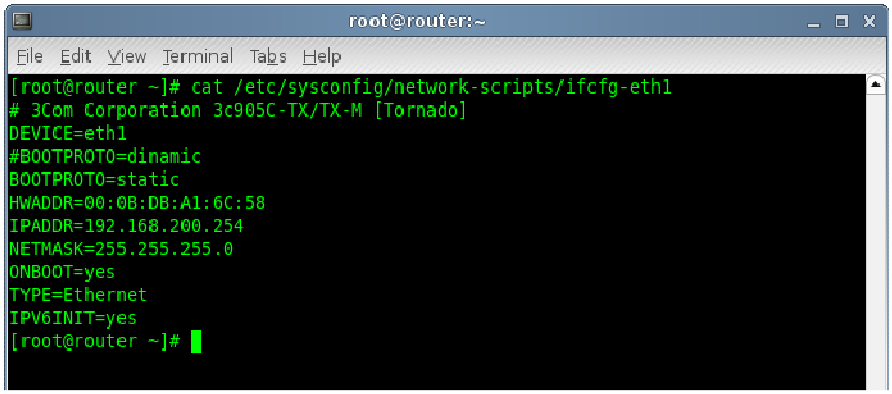


Figura 3.5.- Configuración interfase de red eth1

3.4.1.2 Activación del servicio enrutador de Paquetes "ip_forward".

Para realizar la configuración de ruteo de paquetes, es necesario editar el archivo **/proc/sys/net/ipv4/ip_forward,**

mediante el comando **vim.** El cual debe estar configurado en estado igual a “1” (ver figura 3.6), para configurar el estado del **ip_forward** se debe digitar el siguiente comando:

 # vim /proc/sys/net/ipv4/ip_forward

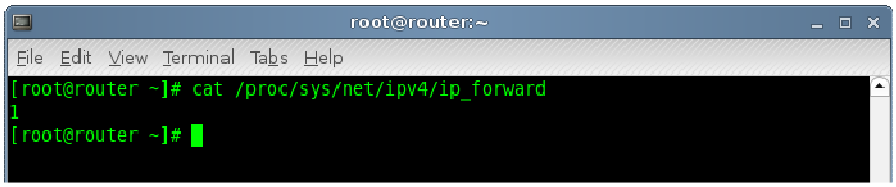


Figura 3.6.- Configuración ip_forward

3.4.1.3 Información de Configuración de DNS

Es necesario revisar la configuración del archivo “**/etc/resolv.conf”,** a través del comando **cat** (ver figura 3.7), en este archivo se registran las configuraciones de “DNS” del equipo, el mismo no debe contener dato alguno, ya que podría causar un conflicto de direccionamiento de paquetes entre los servidores de comunicación del sistema de Videoconferencia. Se debe digitar el siguiente comando para revisar el contenido del archivo resolv.conf.

 # cat /etc/resolv.conf

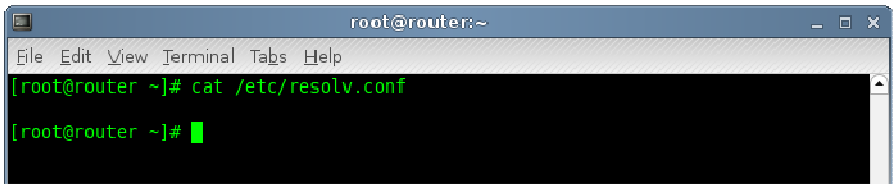


Figura 3.7.- Configuración interfase de red eth1

En caso de que el archivo contenga algún tipo de información será necesario borrar su contenido mediante el comando **vim** de la siguiente manera:

 # vim /etc/resolv.conf

3.4.2 Configuración Equipos Servidores de Borde

Para cumplir las funciones de comunicación en los equipos servidores de borde, se realiza la instalación de la aplicación ELASTIX, la cual se ejecuta en base al sistema operativo de uso libre LINUX, con su distribución CENTOS 5.0. El detalle de esta instalación se encuentra en el **ANEXO 5.2**.

Para que estos servidores de comunicación puedan desempeñar un funcionamiento óptimo, se deben ejecutar los respectivos parámetros de configuración tanto en el Sistema Operativo, como en las aplicaciones ELASTIX, HTBGEN (herramienta para el control del ancho de banda de cada red LAN) y el servicio DHCP, como serán descritas más adelante.

3.4.2.1 Configuración Interfaces de Red

Para realizar la configuración de las interfaces de red, es necesario editar los archivos **/etc/sysconfig/network-scripts/ifcfg-eth0 y /etc/sysconfig/network-scripts/ifcfg-eth1,** en cada uno de los equipos servidores de comunicación, mediante el comando **vim** de la siguiente forma:

 # vim /etc/sysconfig/network-scripts/ifcfg-eth0 y

 # vim /etc/sysconfig/network-scripts/ifcfg-eth1

Cada configuración tiene un sufijo de red diferente, para el caso de las interfaces con sufijo: 192.168.X.X (red tipo C), simulan la recepción de una dirección IP para la conexión con una red WAN, y para el caso de las interfaces con el sufijo: 10.10.X.X (red tipo A), la conexión con una red LAN, como se muestran en las siguientes figuras:

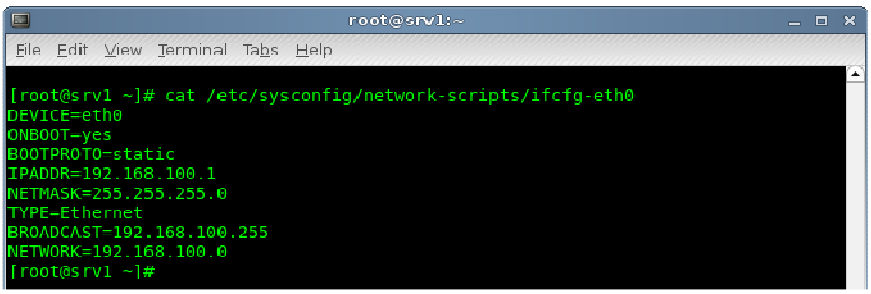


Figura 3.8.- Configuración interfase de red “eth0” SRV1

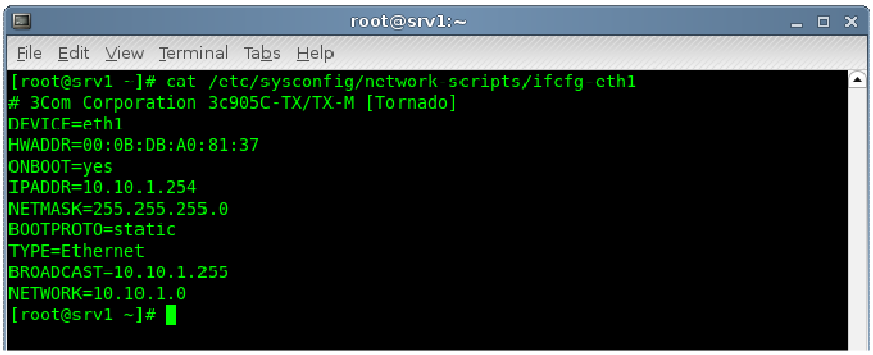


Figura 3.9.- Configuración Interfase de red “eth1” SRV1

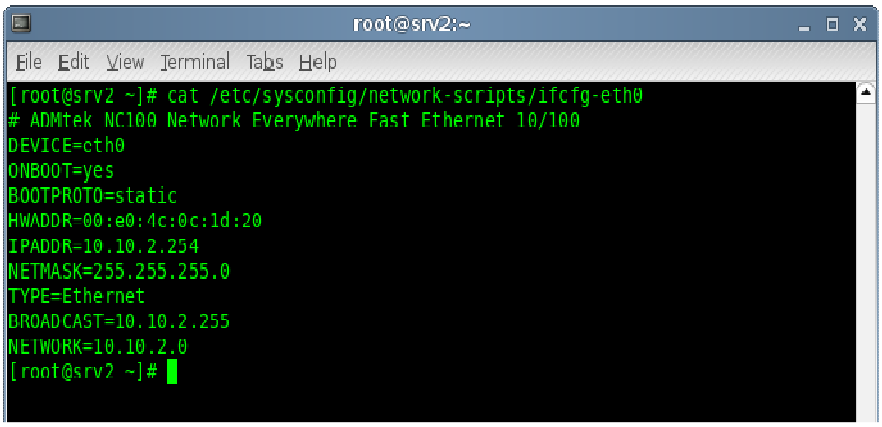


Figura 3.10.- Configuración Interfase de red “eth0” SRV2

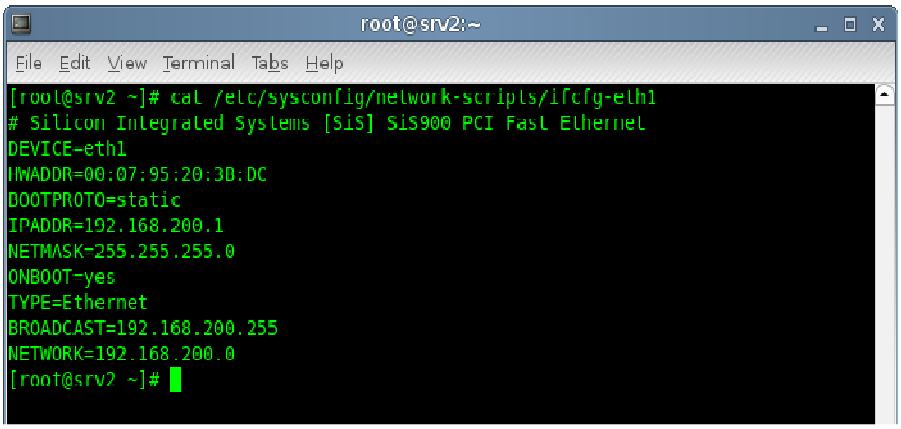


Figura 3.11.- Configuración Interfase de red “eth1” SRV2

3.4.2.2 Configuración del Servicio DHCP

Es necesario activar en cada uno de los servidores de comunicación, el servicio de asignación dinámica de direcciones de red (DHCP) para los clientes de cada estructura de red LAN, con la finalidad de que estos servidores asignen direcciones IP a cada uno de los clientes que necesiten solicitar los servicios de conexión para realizar una Videoconferencia sobre el protocolo de red IPV4:

Para realizar la configuración del servicio DHCP, es necesario editar el archivo **/etc/sysconfig/dhcpd.conf,** en cada uno de los equipos servidores de comunicación **SRV1 y SRV2** (ver figuras 3.12 y 3.13), mediante el comando **vim** de la siguiente forma:

 # vim /etc/sysconfig/dhcpd.conf

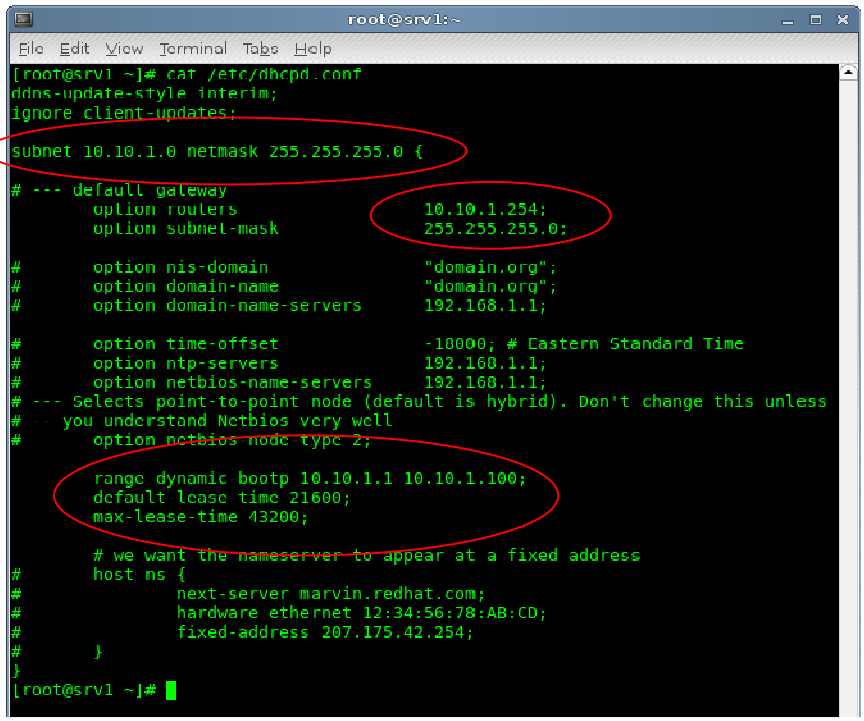


Figura 3.12.- Configuración servicio DHCP Servidor 1 -SRV1-

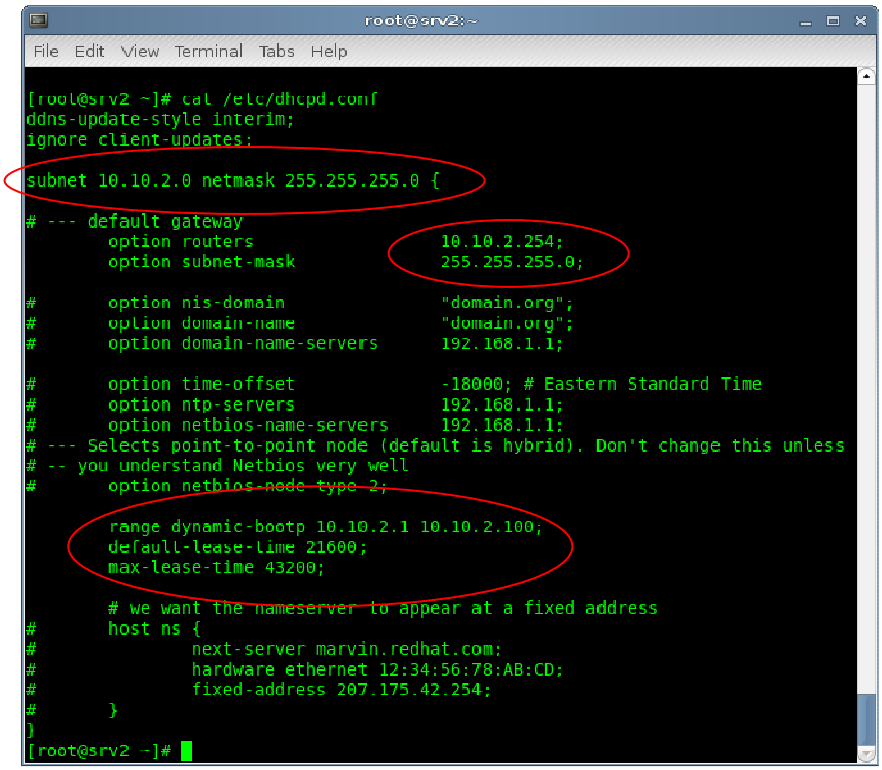


Figura 3.13.- Configuración servicio DHCP Servidor 2 –SRV2-

3.4.2.3 Activación del enrutador de Paquetes “ip_forward”

Para realizar la configuración de ruteo de paquetes, es necesario editar el archivo **/proc/sys/net/ipv4/ip_forward,** en cada uno de los equipos servidores de comunicación **SRV1 y SRV2** (ver figuras 3.14 y 3.15) mediante el comando **vim,** El cual debe estar configurado en estado igual a “1”

 # vim /proc/sys/net/ipv4/ip_forward

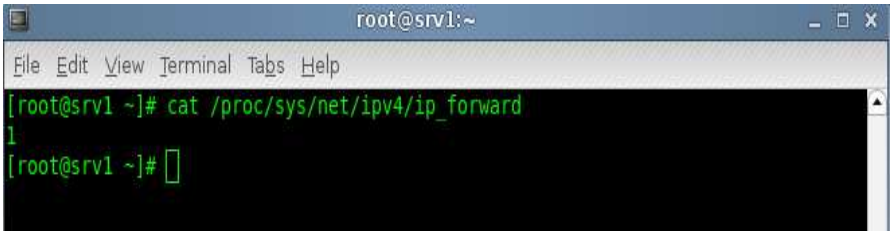


Figura 3.14.- Configuración ip_forward Servidor 1 –SRV1-

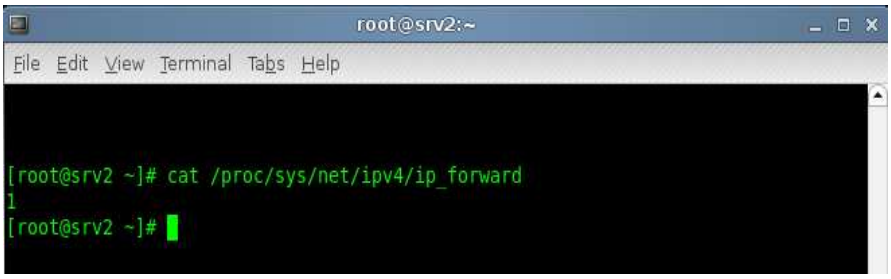


Figura 3.15.- Configuración ip_forward Servidor 2 –SRV2-

3.4.2.4 Configuración de la Tabla de Ruteo de Paquetes “IPTABLES”.

Esta configuración permite enmascarar las direcciones IP de los clientes de cada una de las redes locales LAN

conformadas para la Videoconferencia, permitiendo la independencia y seguridad en las mismas, a fin de que no puedan ser accedidas por equipos externos.

Para realizar la configuración del servicio IPTABLES, es necesario editar en la categoría de **"ENMASCARAMIENTO"** del archivo **/etc/sysconfig/iptables,** en cada uno de los equipos servidores de comunicación (ver figuras 3.16 y 3.17), mediante el comando **vim,** el siguiente parámetro:

 # vim /etc/sysconfig/iptables,

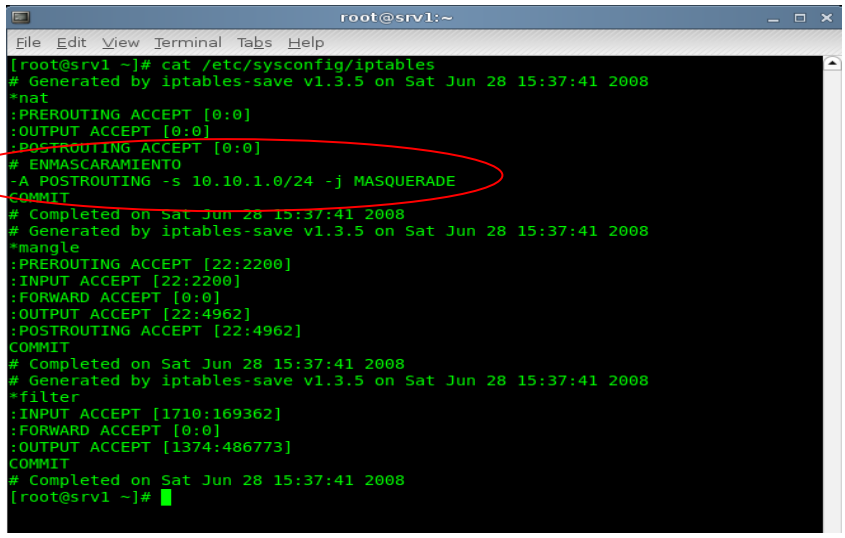


Figura 3.16.- Iptables Servidor de Comunicaciones 1 -SRV1-

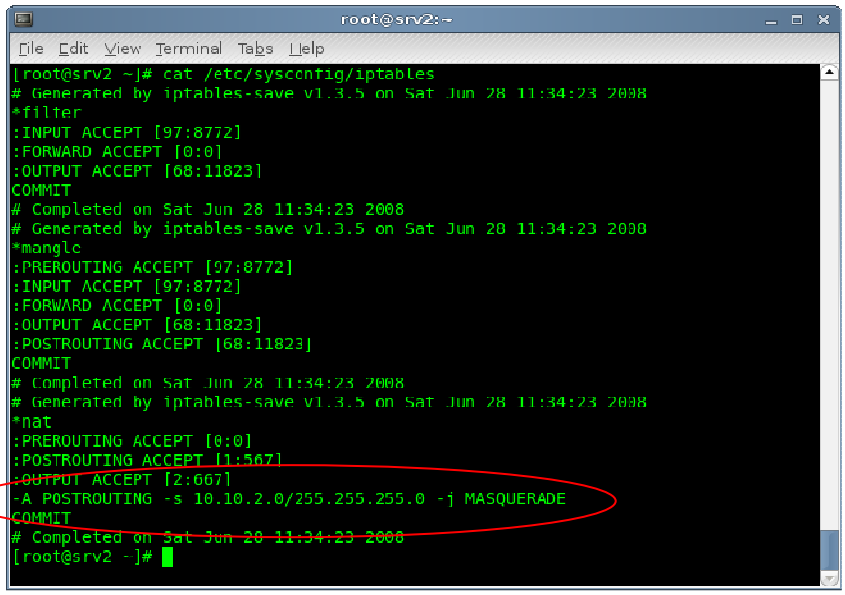


Figura 3.17.- Iptables Servidor de Comunicaciones 2 -SRV2-

3.4.2.5 Configuración del Servicio HTB-GEN para el Control de Ancho de Banda de la Red LAN

Esta configuración permite controlar el ancho de banda para cada una de las subredes LAN dentro de la infraestructura de red bajo el protocolo de IPV4, permitiendo controlar el rango de entrada o salida de paquetes que emiten o reciben cada uno de los equipos que ejecutan la Videoconferencia.

Para realizar la configuración del servicio HTB-GEN, es necesario editar los archivos **/etc/htb-gen/htb-gen.conf y /etc/htb-gen/htb-gen-rates.conf,** en cada uno de los equipos servidores de comunicación (ver figuras 3.18, 3.19, 3.20 y 3.21), mediante el comando **vim,** con los siguientes parámetros:

 # vim /etc/htb-gen/htb-gen.conf

 # vim /etc/htb-gen/htb-gen-rates.conf

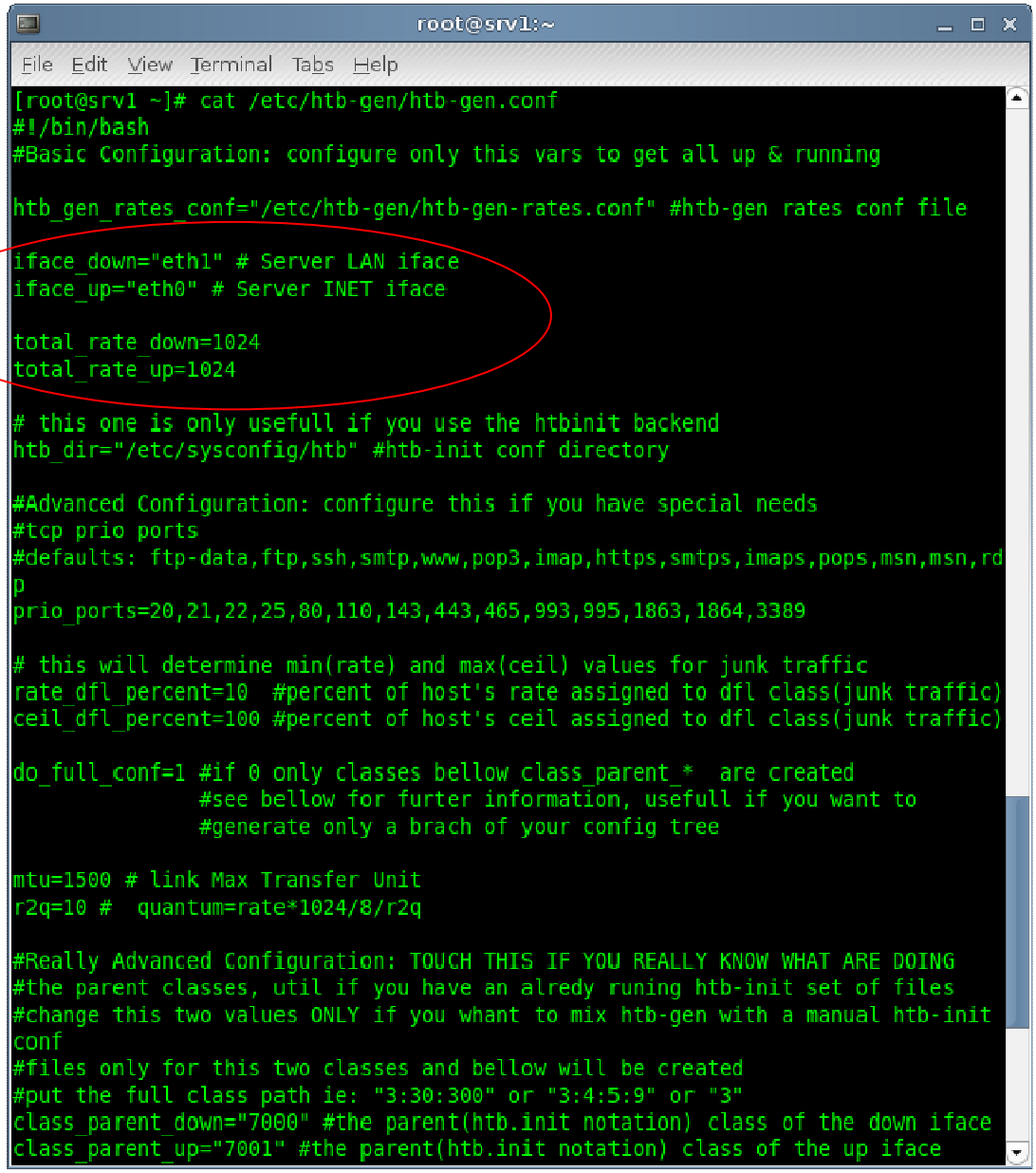


Figura 3.18.- Archivo de configuración “htb-gen.conf” SRV1

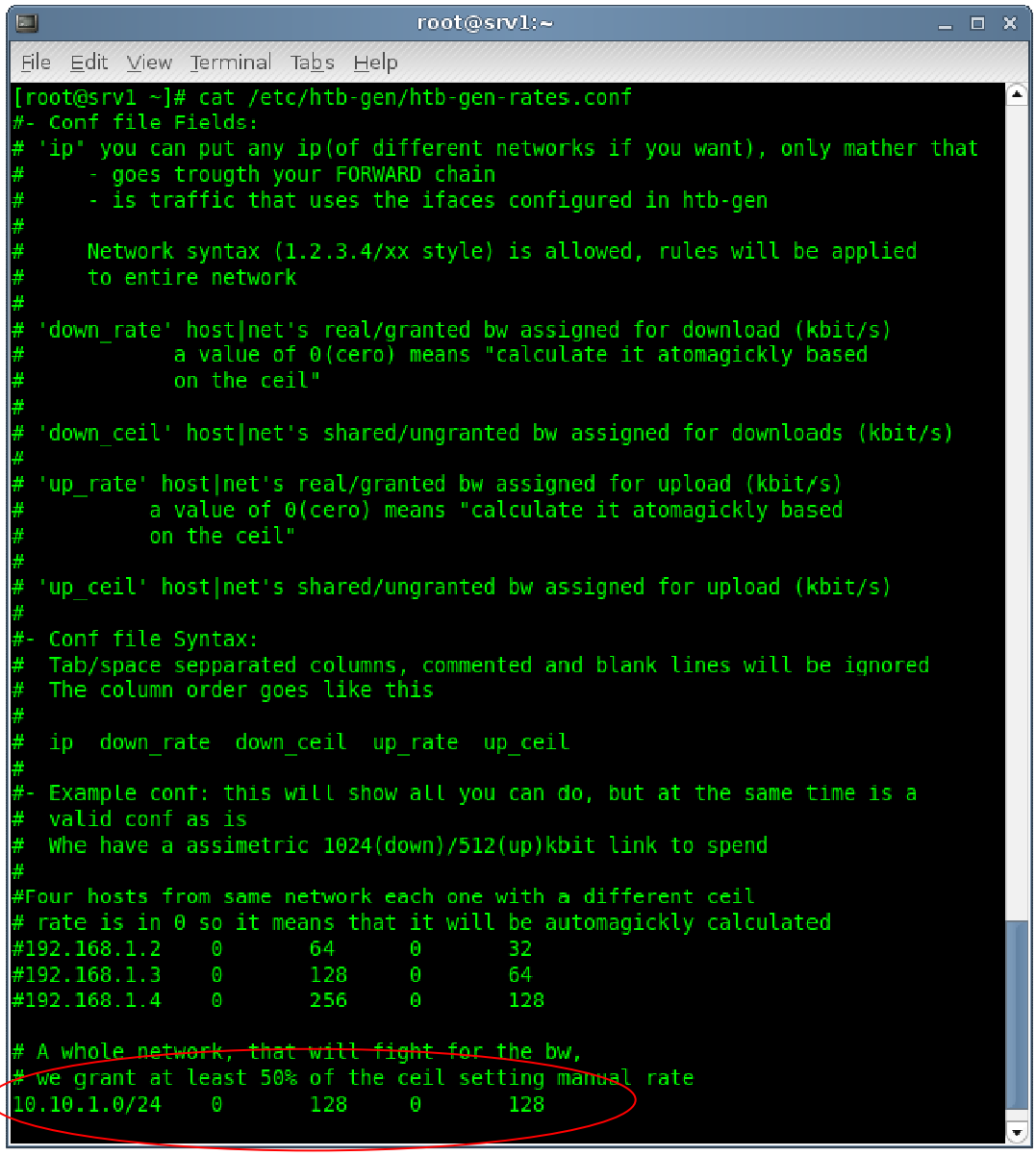


Figura 3.19.- Archivo de configuración “htb-gen-rates.conf” SRV1

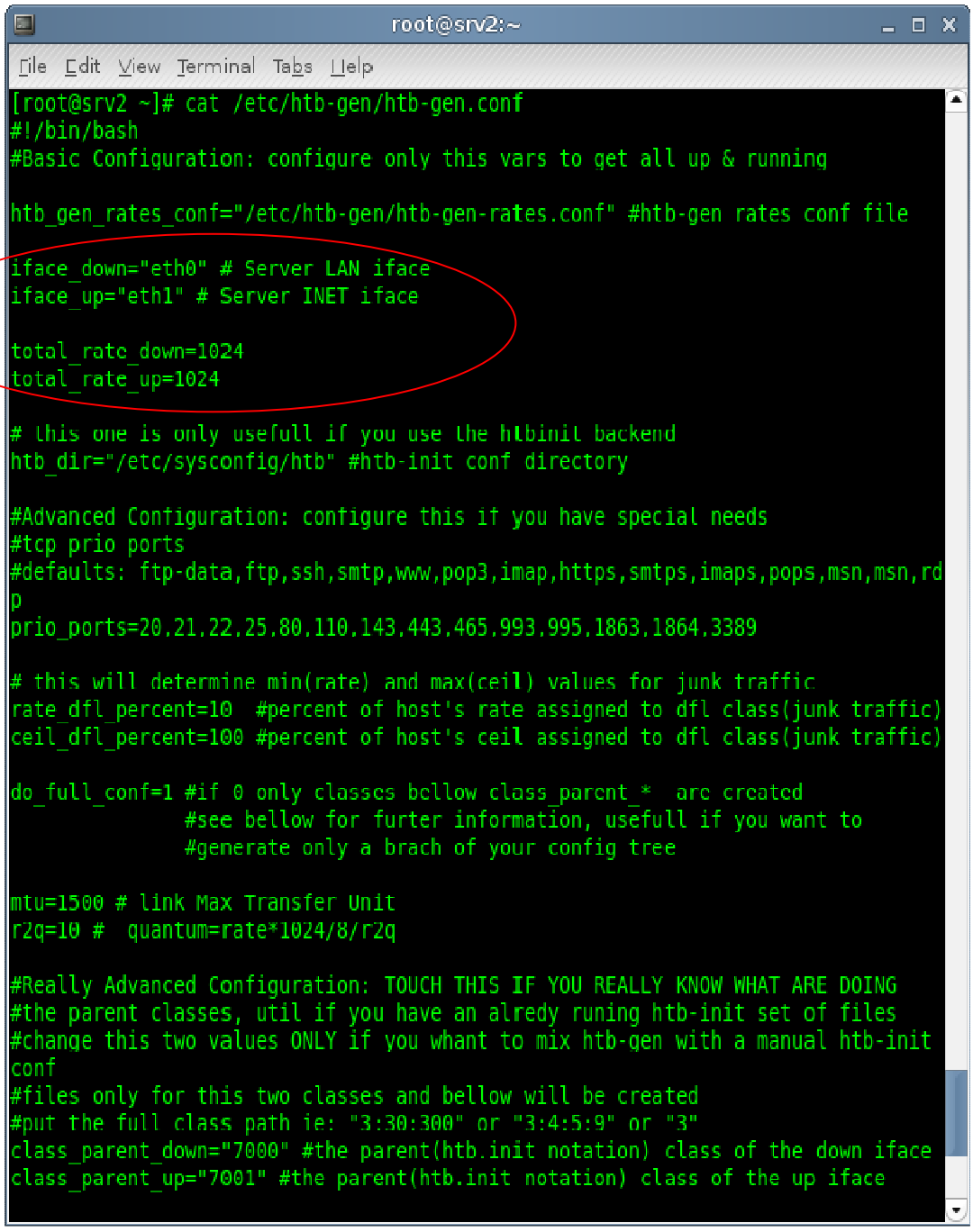


Figura 3.20.- Archivo de configuración “htb-gen.conf” SRV2

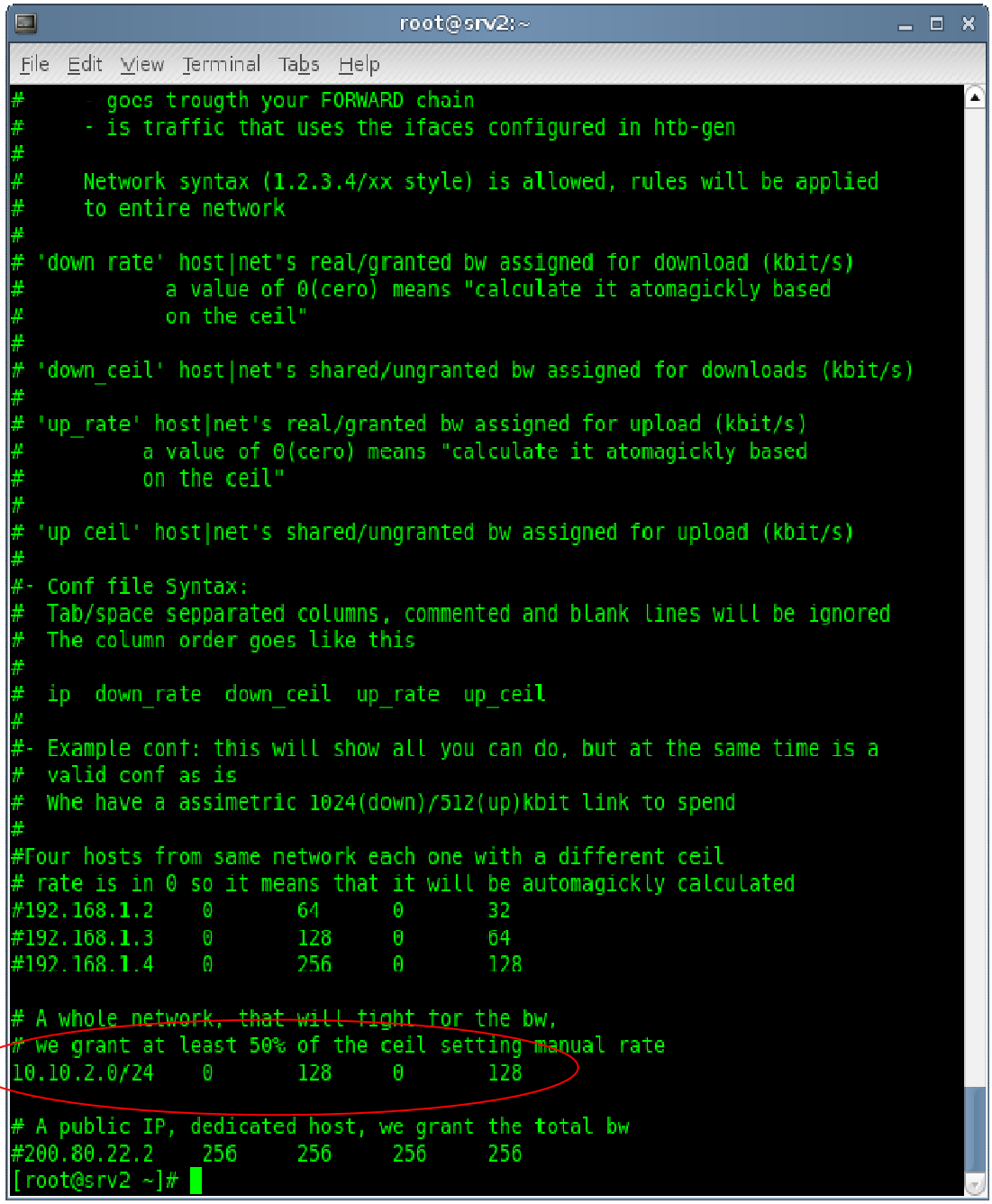


Figura 3.21.- Archivo de configuración "htb-gen-rates.conf" SRV2

3.4.2.6 Configuración de la Aplicación ELASTIX

ELASTIX es una aplicación para servidores de comunicaciones de uso libre GPL, que incorpora diferentes funciones como: PBX, Fax, mensajería instantánea, e Email. Para el desarrollo del presente proyecto de investigación, se utiliza esta aplicación para realizar el sistema de Videoconferencia sobre la infraestructura de red sobre el protocolo de red IPV4, la misma aplicación debe estar configurada únicamente para soporte de voz y video a través de su implementación de voz sobre IP.

Esta aplicación debe instalarse y ejecutarse en los equipos servidores de borde, la misma realiza la interconexión entre los clientes de la Videoconferencia a través de la red WAN. Para que esta aplicación funcione de manera adecuada debe contemplar los siguientes parámetros de configuración una vez instalada la aplicación:

- **Configuración para Soporte de Voz**

  Esta aplicación una vez instalada se configura automáticamente por defecto el soporte para Voz.

- **Configuración para Soporte de Video**

Para realizar la configuración del soporte de video, es necesario editar el archivo **/etc/asterisk/sip.conf,** en cada uno de los equipos servidores de comunicación (ver figura 3.22), mediante el comando **vim,** con el siguiente parámetro:

vim /etc/asterisk/sip.conf

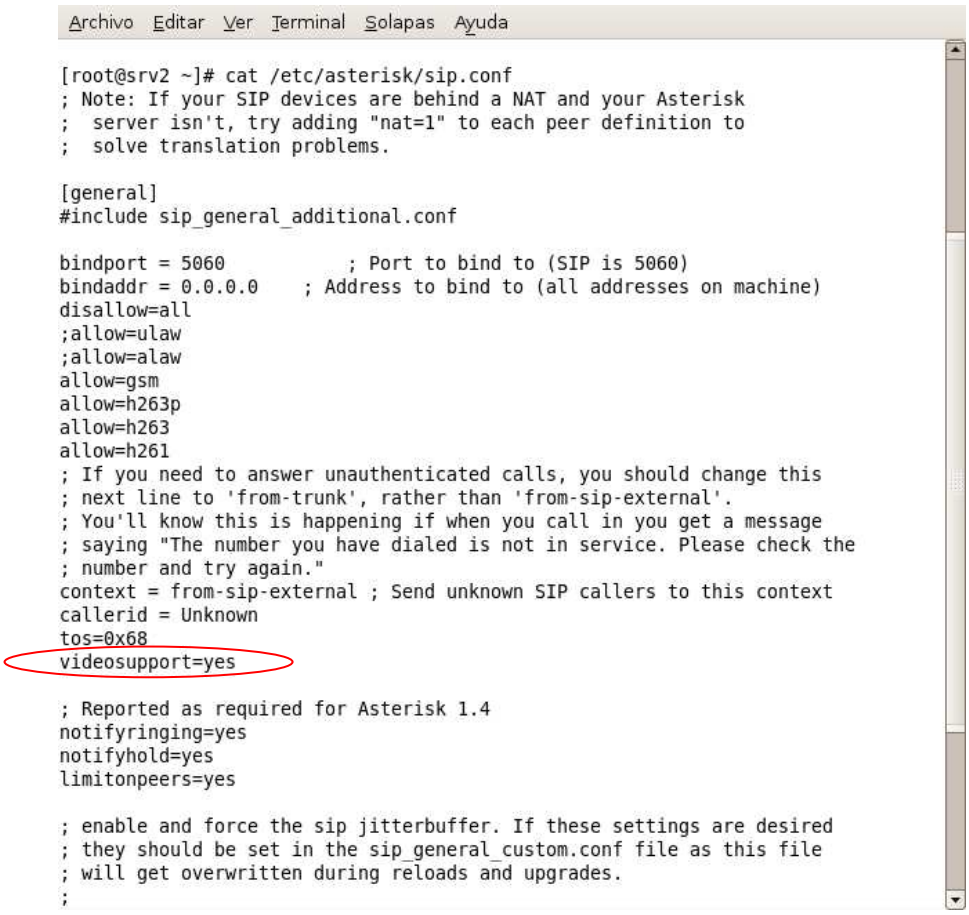


Figura 3.22.- Configuración para soporte de video SRV1 – SRV2

En la línea: **videosupport** debe estar el valor "**yes"**

- **Configuración de las Troncales para la Interconexión de los Servidores de Comunicación.**

Para realizar la configuración de las troncales de comunicación de los equipos servidores de borde, es necesario acceder a través de una interfaz WEB desde un equipo cliente de cada una de las redes LAN a la dirección IP que tenga su respectivo servidor, tal como se muestra en la Figura 3.23. Para el presente caso de estudio se determina el enlace de acceso a la Interfaz de configuración de Elastix de la siguiente manera:

- Servidor 1 -SRV1- http://10.10.1.254
- Servidor 1 -SRV1- http://10.10.2.254

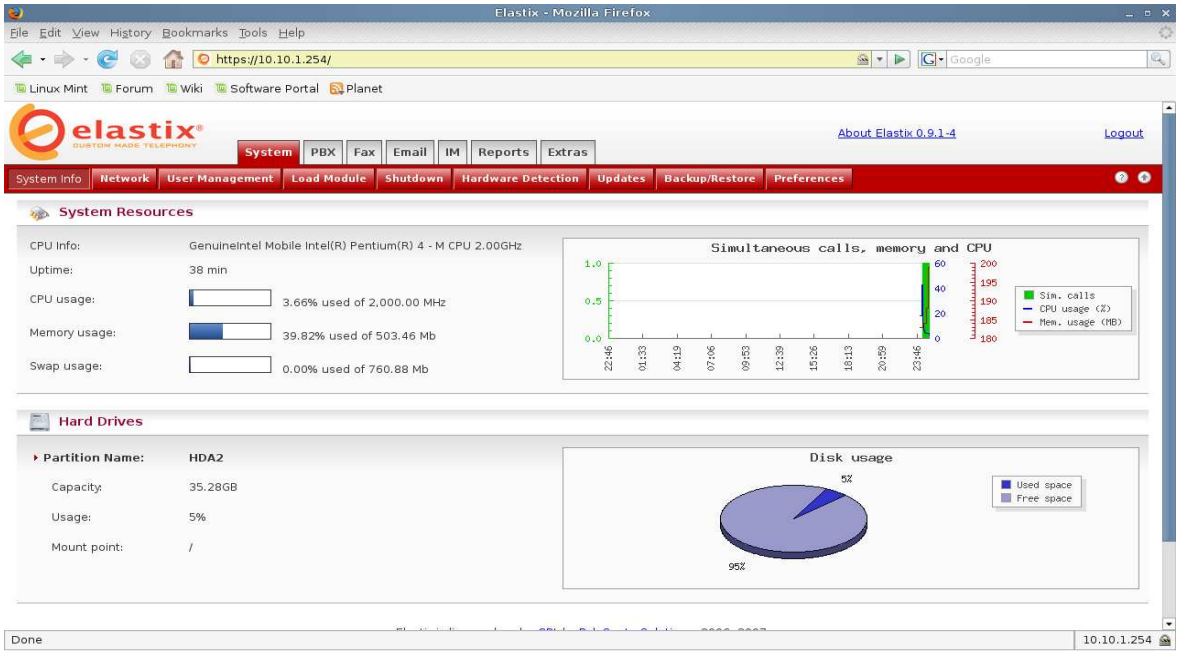


Figura 3.23.- Interfaz de configuración general de Elastix

Una vez que se accede al sistema de administración de la aplicación ELASTIX, se debe ubicar dentro de la pestaña **PBX** el acceso a la configuración de las troncales **"Trunks"** y elegir la opción "**Add SIP Trunk**", tal como se muestra en la Figura 3.24, ya que a través del protocolo SIP se realizará el sistema de Videoconferencia para la infraestructura de red sobre el protocolo IPV4.

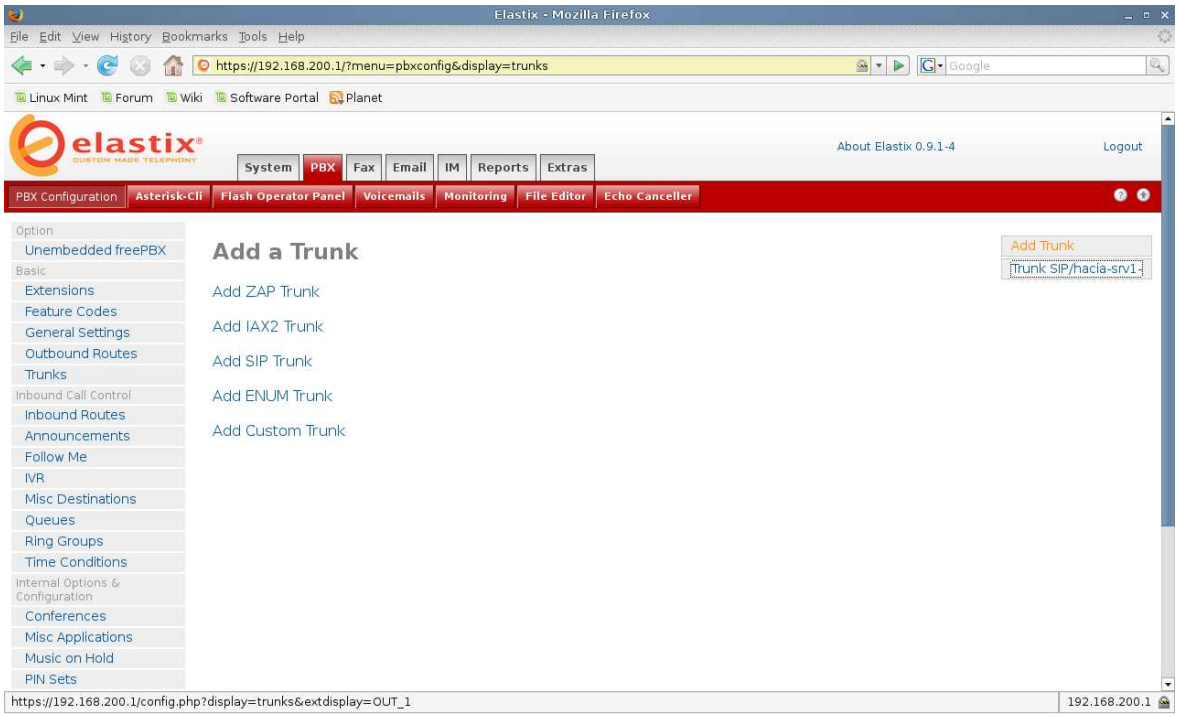


Figura 3.24.- Interfaz de configuración del Protocolo SIP para las troncales de comunicación de Voz sobre IP.

Seguidamente se procede a editar los parámetros de configuración en la troncal SIP, dentro de las opciones "Outgoing Settings", "Ingcoming Settings" y "Register

String", tal como se muestra en la Figura 3.24 para el servidor de comunicación 1 -SRV1- y la Figura 3.25 para el servidor de comunicación 2 -SRV2- :

- **Servidor de Comunicaciones 1 –SRV1-**

Figura 3.25.- Configuración de Troncal SIP SRV1

- **Servidor de Comunicaciones 2 –SRV2-**

Figura 3.26.- Configuración de Troncal SIP SRV2

- **Configuración de los Clientes PBX para la Aplicación de la Videoconferencia.**

Para realizar la configuración de las extensiones PBX para cada uno de los clientes que se establecen para determinar el funcionamiento del sistema de Videoconferencia en cada uno de los equipos servidores

de borde, es necesario acceder al sistema de administración de la aplicación ELASTIX tal como se menciono en la Figura 3.23, para lo cual se debe ubicar dentro de la pestaña **PBX** el acceso a la configuración de las extensiones **"Extensions"** y elegir la opción "**Add an Extension**", tal como se muestra en la Figura 3.27.

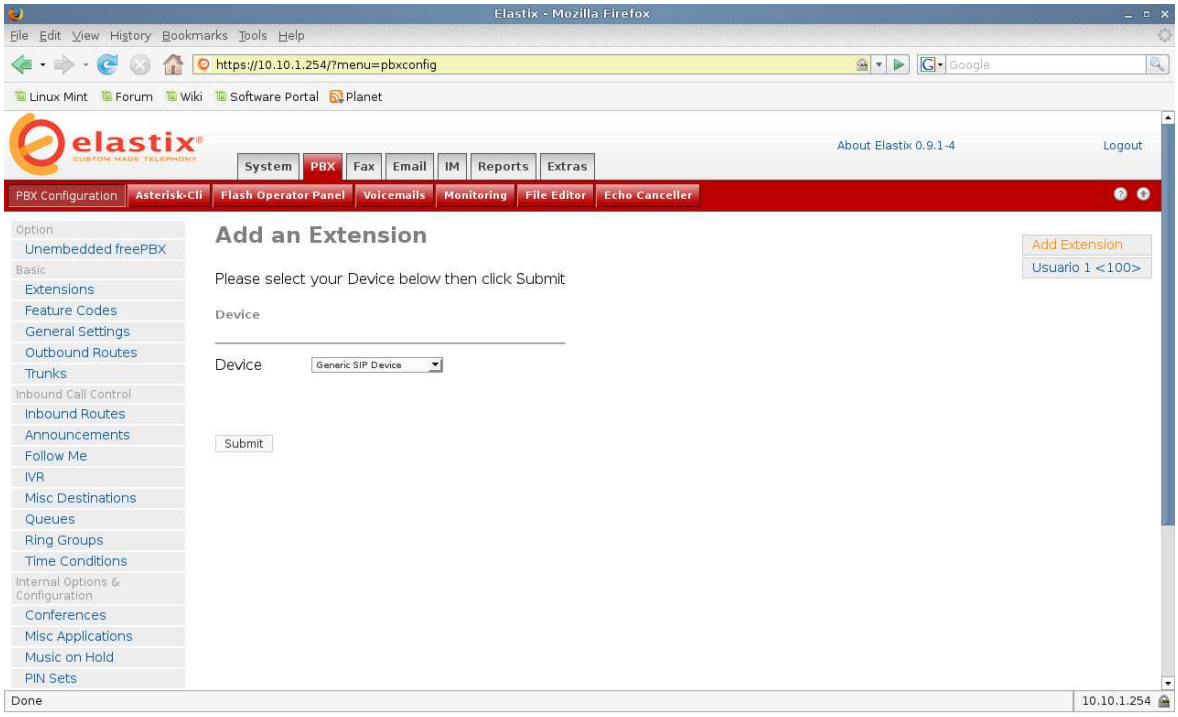


Figura 3.27.- Interfaz de creación de extensiones PBX para los clientes de la Videoconferencia sobre el protocolo de red IPV4

Seguidamente se procede a editar los parámetros de configuración en las extensiones, dentro de las opciones "Edit Extension", "Extensions Options", y "Device Options", tal como se muestra en la Figura 3.28 para el servidor de comunicación 1 -SRV1- y la Figura 3.29 para el servidor de comunicación 2 -SRV2- :

- **Servidor de Comunicaciones 1 –SRV1-**

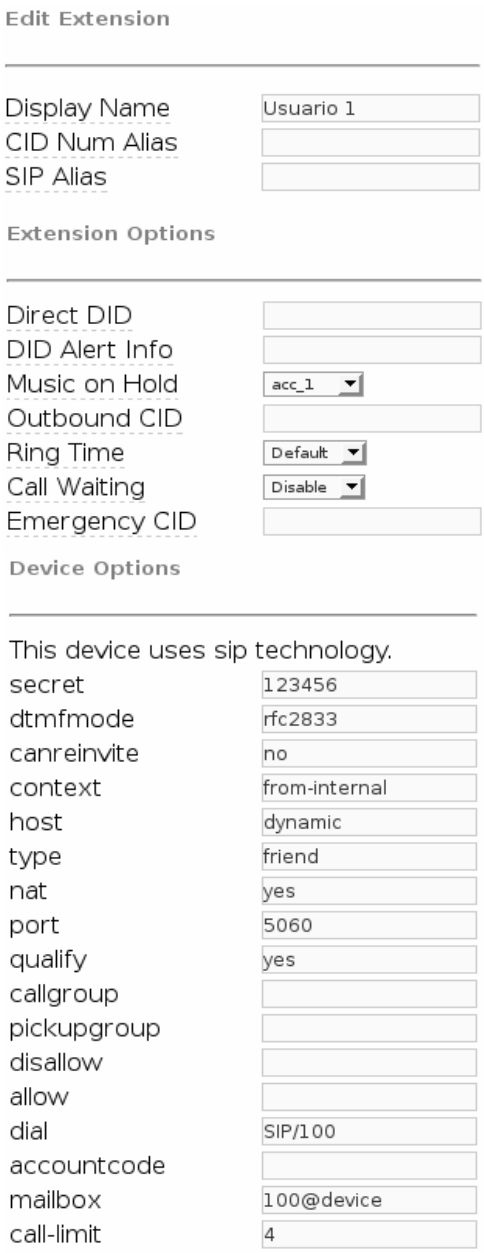


Figura 3.28.- Configuración de la extensión PBX SRV1

- **Servidor de Comunicaciones 2 –SRV2-**

Figura 3.29.- Configuración de la extensión PBX SRV2

3.4.3 Configuración Equipos Clientes

Para determinar el funcionamiento del sistema de Videoconferencia en la infraestructura de red implementada bajo el protocolo de red IPV4, es necesario establecer la instalación y configuración de los equipos clientes dentro de cada una de las redes LAN, tal como la estructura que se muestra en la Figura 3.2. Para lo cual se determina la instalación de los sistemas operativos de uso libre LINUX, tanto en su distribución MINT 4.0 para el equipo cliente A, así como la distribución UBUNTU 7.0 para el equipo cliente B, ambas instalaciones detalladas en el ANEXO 5.3

Para que los equipos clientes puedan desempeñar un funcionamiento óptimo en el sistema de Videoconferencia, se debe ejecutar los respectivos parámetros de configuración tanto en la configuración de red de cada Sistema Operativo, como en la aplicación EKIGA (Cliente Softphone para Videoconferencia).

3.4.3.1 Configuración Interfaces de Red

Para realizar la configuración de las interfaces de red en cada uno de los equipos clientes que efectuaran el sistema de Videoconferencia sobre la estructura de red de IPV4, es necesario acceder a las propiedades de red dentro del sistema operativo tanto del cliente Linux UBUNTU así como del cliente Linux MINT, y determinar la configuración de la

interfaz de red en modo automático (DHCP), tal como se muestra en la Figura 3.30

Figura 3.30.- Configuración dinámica de red equipos clientes de red

3.4.3.2 Configuración de la Aplicación Softphone -EKIGA- para Cliente de Videoconferencia

A través del uso de esta herramienta softphone, se determina la implementación del sistema de Videoconferencia entre los equipos clientes de la infraestructura de red bajo el protocolo IPV4. Para lo cual se establecen los parámetros de configuración dentro de las categorías General, Protocolos, Códecs y Dispositivos, tal como se muestra en la Figura 3.31

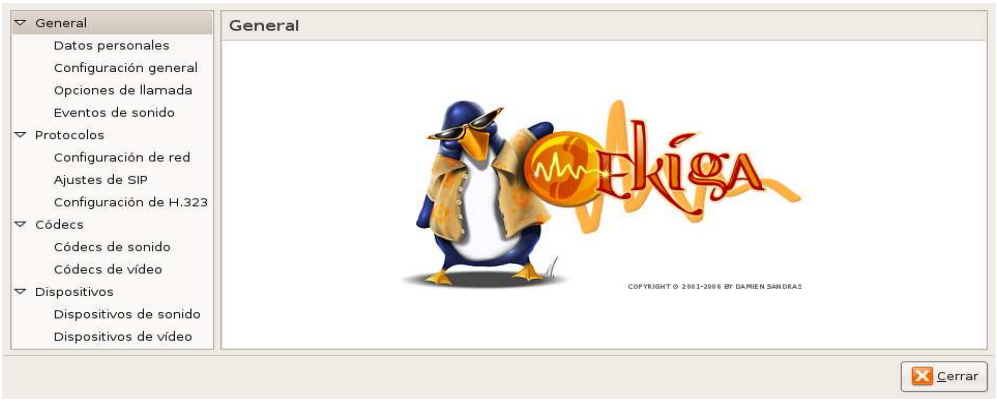


Figura 3.31.- Interfaz de configuración general aplicación EKIGA

- **Opciones de Configuración General**

  Dentro de la categoría de opciones generales es necesario determinar los parámetros de configuración únicamente en la sección de Datos personales, tal como se muestra en la Figura 3.32, el resto de secciones se determinan con las configuraciones predeterminadas que se instalan por defecto en la aplicación.

Figura 3.32.- Configuración de datos personales aplicación EKIGA

- **Opciones de Configuración de Protocolos**

  Dentro de la categoría de protocolos es necesario determinar los parámetros de configuración de red, con el objetivo de que la aplicación escuche a través de la interfaz de red correspondiente, tal como se muestra en la Figura 3.33. Para el presente análisis de investigación, se determina la interfaz eth0, el resto de ítems se determinan con las configuraciones predeterminadas que se instalan por defecto en la aplicación.

Figura 3.33.- Configuración de red aplicación EKIGA

Seguidamente, es necesario determinar los parámetros de Ajustes de SIP, con el fin de que la aplicación funcione a través del protocolo SIP, tal como se muestra en la Figura 3.34.

El resto de ítems se determinan con las configuraciones predeterminadas que se instalan por defecto en la aplicación.

Figura 3.34.- Configuración Ajustes de SIP aplicación EKIGA

A continuación se determina los parámetros de configuración de H.323, con el fin de que la aplicación funcione a través del protocolo H.323, tal como se muestra en la Figura 3.35, El resto de ítems se determinan con las configuraciones predeterminadas que se instalan por defecto en la aplicación

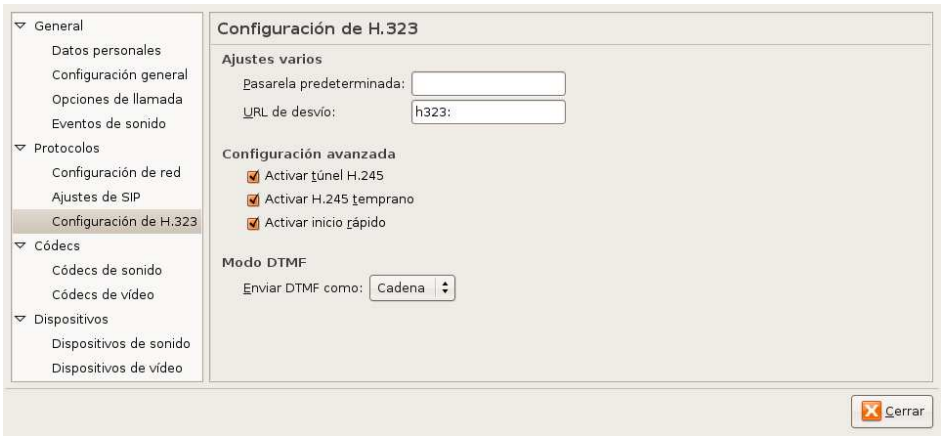


Figura 3.35.- Configuración de H.323 aplicación EKIGA

- **Opciones de Configuración de Códecs**

  Dentro de la categoría de códecs es necesario determinar los parámetros de configuración de sonido y video, con el objetivo de que la aplicación utilice los adecuados paquetes de codificación y decodificación para enviar y recibir tanto audio como video de un extremo al otro de la Videoconferencia. Para el caso de los códecs de sonido disponibles, el principal códec utilizado para la transmisión de audio es el SPEEXS 20,8 Kbps – 16 Khz, así también es necesario activar la opción "cancelación de eco" para que no exista eco en la comunicación, tal como se muestra en la Figura 3.36, el resto de ítems se determinan con las configuraciones predeterminadas que se instalan por defecto en la aplicación.

Figura 3.36.- Configuración de códecs de sonido aplicación EKIGA

Una vez configurado los códecs de audio, es necesario configurar los diferentes parámetros para los códecs de video a utilizar, en donde se pueden configurar tanto el soporte de video, el máximo de ancho de banda para el video y la tasa de fotogramas de video. Estos parámetros son variables y deben ser modificados según la necesidad de calidad y desempeño para el sistema de Videoconferencia. Sin embargo es necesario que la opción de Activar soporte de video se encuentre activa, tal como se muestra en la Figura 3.37

Figura 3.37.- Configuración de códecs de video aplicación EKIGA

- **Opciones de Configuración de Dispositivos**

  Dentro de la categoría de dispositivos es necesario determinar los parámetros de configuración de dispositivos tanto de sonido como de video, con el objetivo de que la aplicación utilice los medios de

hardware de audio y video que se encuentran configurados por defecto en el sistema, para el caso de los dispositivos de audio en cada uno de los equipos clientes son las tarjetas de sonido que automáticamente son detectadas por la aplicación EKIGA., tal como se muestra en la Figura 3.38.

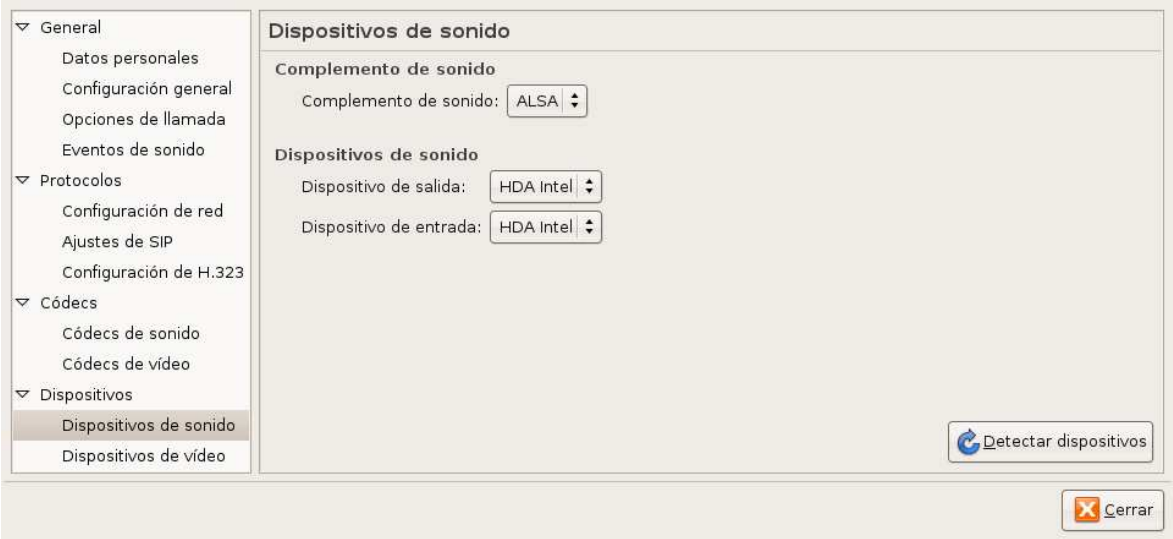


Figura 3.38.- Configuración de dispositivos de audio aplicación EKIGA

Una vez que se determina la configuración de los dispositivos de sonido, es necesario configurar los dispositivos de video, en donde se configura tanto los parámetros de ejecución de video; Formato, canal e imagen, así como el medio de entrada para video, en este caso la aplicación EKIGA detecta automáticamente la cámara conectada a cada uno de los equipos clientes, tal como se puede observar en la Figura 3.39.

Figura 3.39.- Configuración de dispositivos de video aplicación EKIGA

- **Configuración de Cuentas de Usuario para los Equipos Clientes del Sistema de Videoconferencia.**

  Para determinar el funcionamiento del sistema de Videoconferencia, es necesario establecer en cada uno de los equipos clientes, las configuraciones respectivas de las cuentas de usuario que serán validadas a través de los servidores de comunicación ELASTIX de cada red de datos LAN, para lo cual se de efectuar la creación de cuentas, a través de la opción "**Herramientas" – "cuentas",** añadiendo las características específicas para cada uno de los clientes, tal como se muestra en la Figura 3.40 y Figura 3.41.

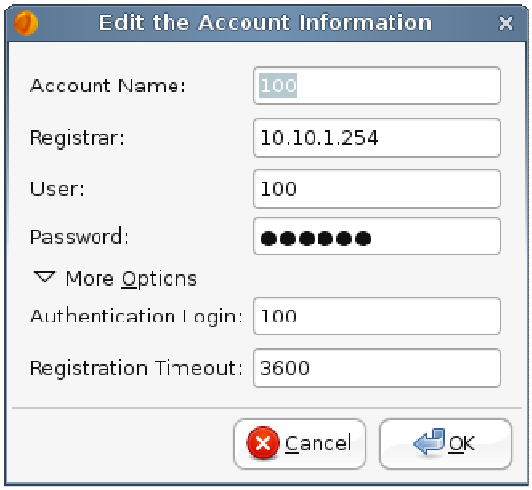


Figura 3.40.- Creación cuenta usuario 100 en EKIGA

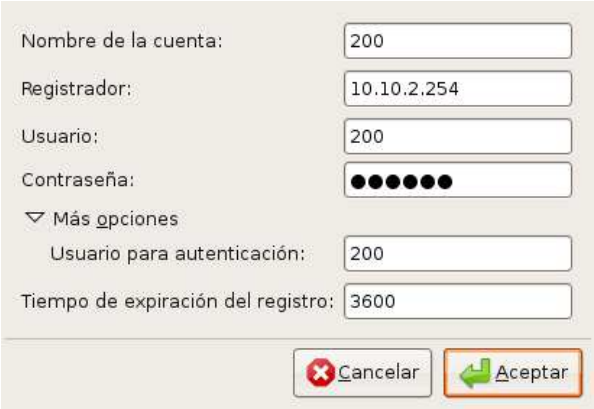


Figura 3.41.- Creación cuenta usuario 200 en EKIGA

Una vez creadas las cuentas para la conexión del sistema de Videoconferencia, es necesario activarlas **(A)** para que la aplicación EKIGA, funcione sin ningún inconveniente, tal como se muestra en el ejemplo de la Figura 3.42.

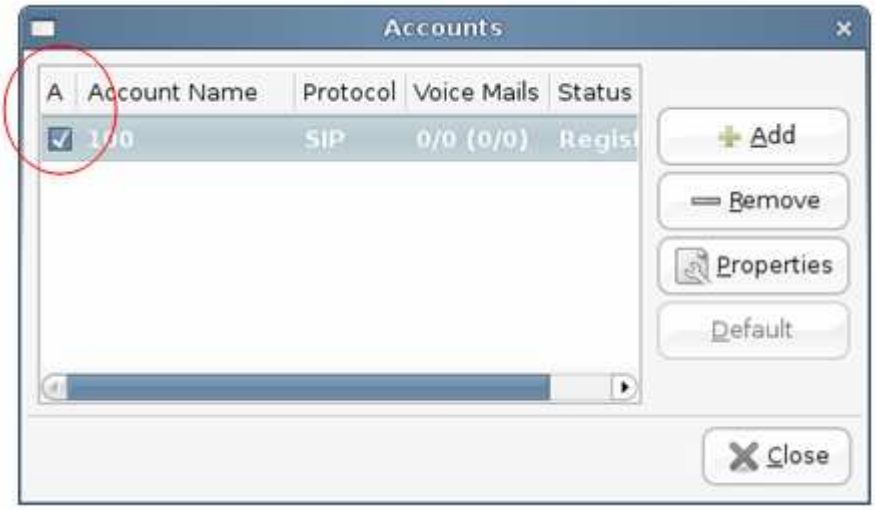


Figura 3.42.- Activación cuenta usuario aplicación EKIGA

3.5 Configuración de la Estructura para Videoconferencia en IPV6

Una vez que se realiza la configuración e implementación de la Videoconferencia bajo la estructura de red IPV4, se debe efectuar las configuraciones respectivas en cada uno de los equipos que integran el sistema de Videoconferencia para la infraestructura de red sobre el protocolo IPV6.

A continuación se detallan los procedimientos necesarios para determinar la configuración e implementación de las diferentes aplicaciones que son necesarias para establecer el sistema de Videoconferencia bajo el protocolo de red IPV6

3.5.1 Configuración del Equipo Ruteador "Direccionamiento IP – forward de paquetes"

Para cumplir las funciones de un equipo ruteador al igual que la estructura de red bajo el protocolo de red IPV4, se ha realizado la instalación del sistema operativo de uso libre LINUX, con su distribución CENTOS 5.0. En el equipo en mención se deben configurar los siguientes parámetros para que funcione ruteo de paquetes:

3.5.1.1 Configuración de las Interfaces de Red como Redes Independientes

Para realizar la configuración de las interfaces de red, es necesario editar los archivos **/etc/sysconfig/network-scripts/ifcfg-eth0 y /etc/sysconfig/network-scripts/ifcfg-eth1** (ver figuras 3.43 y 3.44)**,** mediante el comando **vim** de la siguiente forma:

 # vim /etc/sysconfig/network-scripts/ifcfg-eth0

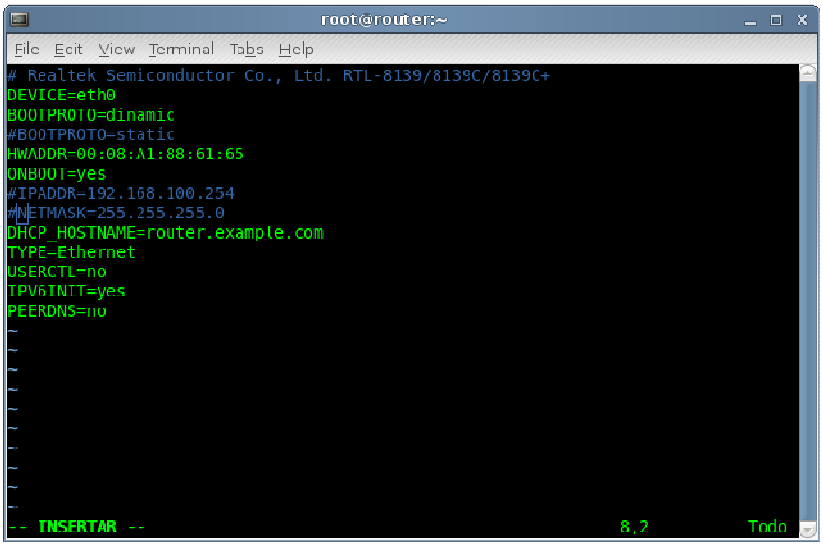


Figura 3.43.- Configuración Interfase de red "eth0" IPV6

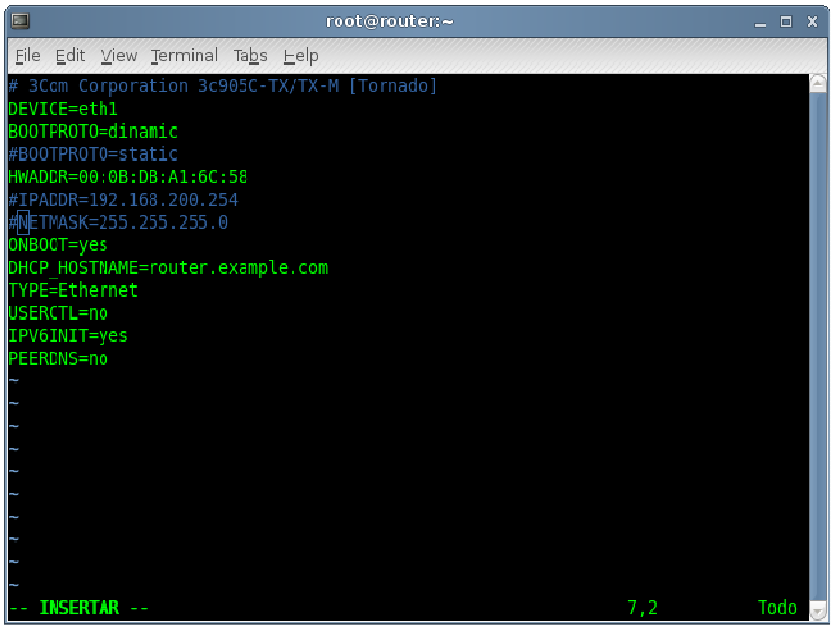


Figura 3.44.- Configuración Interfase de red “eth1” IPV6

3.5.1.2 Configuración de DNS

Es necesario revisar la configuración del archivo “**/etc/resolv.conf”,** a través del comando **cat**, en este archivo se registran las configuraciones de “DNS” del equipo. El mismo no debe contener dato alguno, ya que podría causar un conflicto de direccionamiento de paquetes entre los servidores de comunicación del sistema de Videoconferencia.

 # cat /etc/resolv.conf

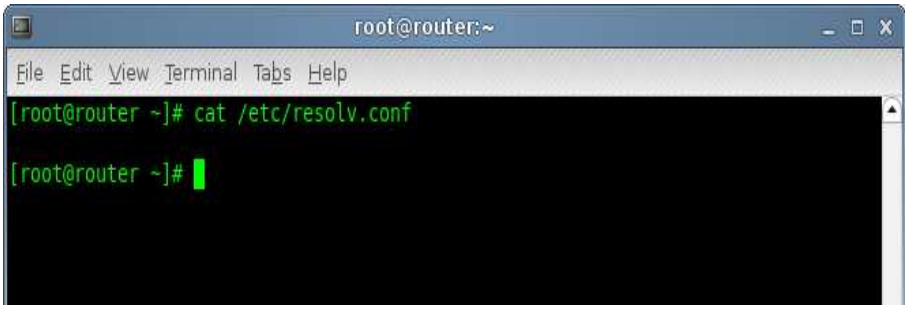


Figura 3.45.- Contenido archivo resolv.conf IPV6

En caso de que el archivo contenga algún tipo de información será necesario borrar su contenido mediante el comando **vim.**

 # vim /etc/resolv.conf

3.5.1.3 Activación del enrutador de Paquetes "ip_forward" para el Protocolo de Red IPV6

Para la activación del enrutamiento de paquetes para los clientes que efectúan el sistema de Videoconferencia bajo el protocolo de red IPV6, es necesario determinar varios parámetros de configuración dentro del sistema de configuración de red para el protocolo IPV6 del equipo configurado como ruteador de paquetes.

Para lo cual es necesario generar un script ejecutable, el cual permitirá activar el reenvío de los paquetes de un cliente a otro a través de la estructura de red de IPV6, en cada uno de

los archivos de configuración del sistema que se ubican dentro del directorio **"/proc/sys/net/ipv6/conf/all",** siendo:

- **autoconf**
- **accept_ra**
- **accept_redirects**
- **forwarding**
- **router_solicitations**

El script generado para el presente caso de investigación, se denomina **"flag_ipv6"** y puede ser ejecutado a través del comando **"sh",** desde una consola de terminal en el equipo que cumple la función de ruteo de paquetes.

 # sh flag_ipv6

El contenido de este script permite asignar valores de "0" y "1" a los archivos de configuración para el ruteo de paquetes del protocolo IPV6, como se muestra en la figura:

Figura 3.46.- Contenido archivo flag_ipv6 IPV6

3.5.1.4 Configuración del Servicio RADVD

La configuración y activación de este servicio permite asignar automáticamente direcciones IPV6 a través de un sufijo de red predeterminado y establecido en el archivo de configuración **"radvd.conf"**, para los equipos clientes del sistema de Videoconferencia, el servicio RADVD **"router advertisement daemon"** es una aplicación tipo DHCP, el cual asigna la ruta de paquetes para un sistema de red, determinando un mapa de circulación de paquetes para un óptimo desempeño del protocolo IPV6.

Para acceder a la configuración de este servicio es necesario editar el archivo "**/etc/radvd.conf",** mediante el comando **vim,** tomando en cuenta los siguientes parámetros:

- **Prefijo de red**
- **Tiempo de vida del prefijo**
- **La frecuencia de envío de anuncios**

 # vim /etc/radvd.conf

- **Configuración del Archivo "radvd.conf"**

Es necesario establecer los sufijos de red IPV6 para la asignación automática de los equipos clientes, con el objetivo de que puedan establecer un sistema de Videoconferencia puro bajo el protocolo de red IPV6, como se muestra en la figura 3.47.

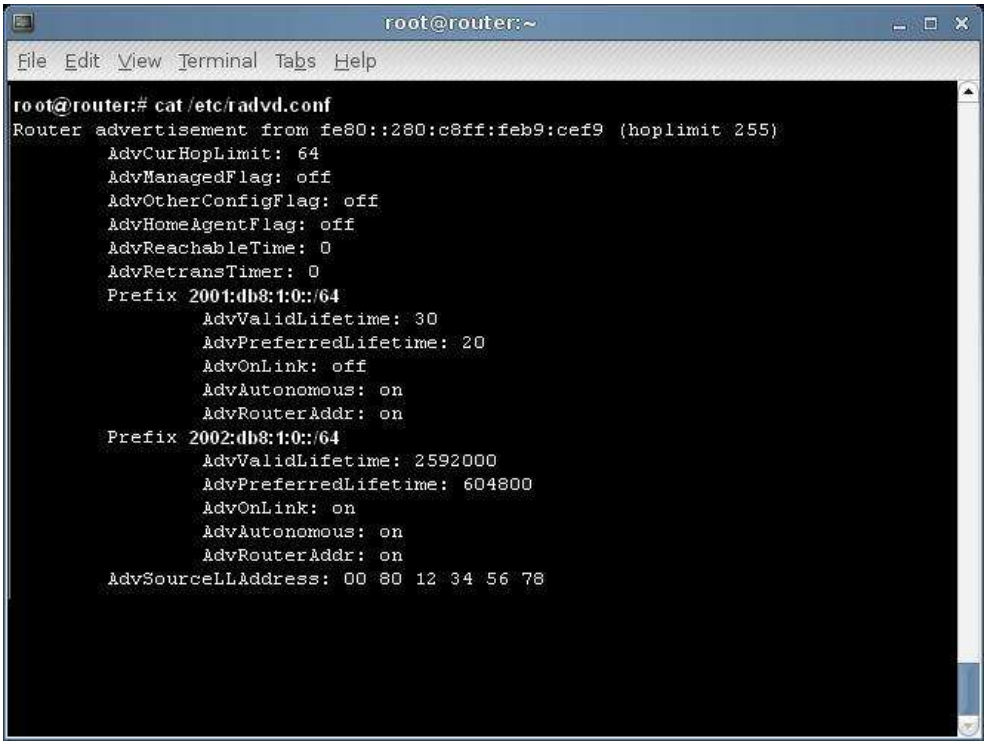


Figura 3.47.- Configuración archivo radvd.conf IPV6

Los sufijos de red IPV6; **2001:db8:1:0** y **2002:db8:1:0** son asignados a las interfaces de red de los equipos clientes B y A respectivamente para que puedan interactuar de manera adecuada y bajo una infraestructura transparente de IPV6 el sistema de Videoconferencia.

3.5.2 Configuración Equipos Clientes para el Sistema de Videoconferencia

3.5.2.1 Configuración Interfaces de red

Para realizar la configuración de las interfaces de red en cada uno de los equipos clientes que efectuaran el sistema de

Videoconferencia sobre la estructura de red de IPV6, es necesario acceder a las propiedades de red dentro del sistema operativo tanto del cliente Linux UBUNTU así como del cliente Linux MINT, y determinar la configuración de la interfaz de red en modo automático (DHCP), tal como se muestra en la Figura 3.48

Figura 3.48.- Configuración dinámica de red equipos clientes de red

3.5.2.2 Configuración de Nombres de Equipos "Hostname"

Es necesario determinar en la configuración del nombre "HOSTNAME" de cada uno de los equipos clientes para el sistema de Videoconferencia bajo la infraestructura de red IPV6, la dirección IP de cada uno de los equipos que integran el sistema de Videoconferencia sobre IPV6 con sus respectivos nombres, tal como se muestra en la configuración, con la finalidad de simplificar la notación de la dirección de la interfaz de red para el momento en que se requiera

determinar si los equipos se encuentran activos y asignados la IP correspondiente.

 # ping6 srv1

 # ping6 2001:db8:1:0:208:a1ff:feb5:a683

Para la configuración del archivo “HOSTNAME” de los dos equipos clientes del sistema de Videoconferencia IPV6 es necesario editar el archivo **“/etc/hosts”** (ver figura 3.49)**,** con los siguientes parámetros:

Figura 3.49.- Configuración /etc/hosts IPV6

3.5.2.3 Configuración de la Aplicación Softphone -ISABEL- para Cliente de Videoconferencia.

A través del uso de esta herramienta softphone, se determina la implementación del sistema de Videoconferencia entre los equipos clientes de la infraestructura de red bajo el protocolo IPV6. Para lo cual se establecen los parámetros de

configuración dentro de la categoría "**Edit Local Configuration**", tanto para la sesión de Servidor como la sesión cliente, se determinan los parámetros de: **Site ID, Role** y **Parameters**, tal como se muestran en los siguientes gráficos, el resto de opciones, se las debe dejar con la configuración que se establece por defecto al momento de la instalación de la aplicación.

- **Configuración de "SIte ID"**

  Como se muestra en la Figura 3.50, se configura el nombre del usuario y la locación tanto para el cliente como para el servidor del sistema de Videoconferencia.

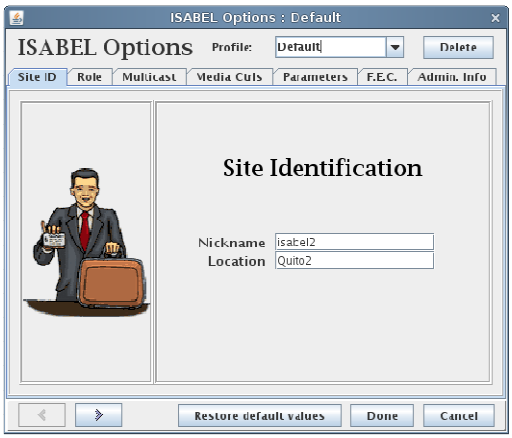


Figura 3.50.- Configuración dinámica usuario aplicación ISABEL

- Configuración de **"Role"**

  Como se muestra en la Figura 3.51, se configura el tipo de modo de la conexión tanto para el cliente como para el servidor del sistema de Videoconferencia, el modo

interactivo permite que ambos lados de la Videoconferencia interactúen con las diversas aplicaciones que se pueden ejecutar en la herramienta ISABEL.

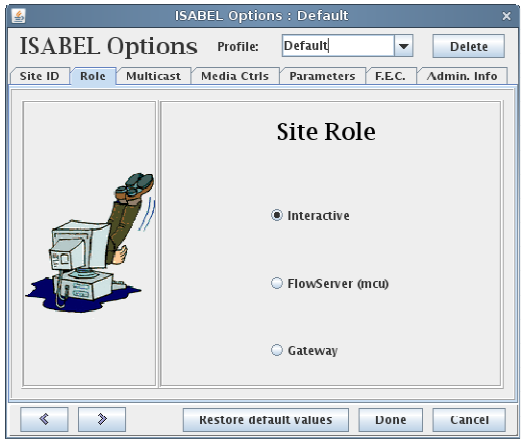


Figura 3.51.- Configuración modo de conexión aplicación ISABEL

- Configuración de **"Parameters"**

  Como se muestra en la Figura 3.52, se configura el tipo de parámetros utilizados para la conexión, tanto para el cliente como para el servidor del sistema de Videoconferencia, los mismos deben contemplar cada uno de los términos referidos como se muestran a continuación:

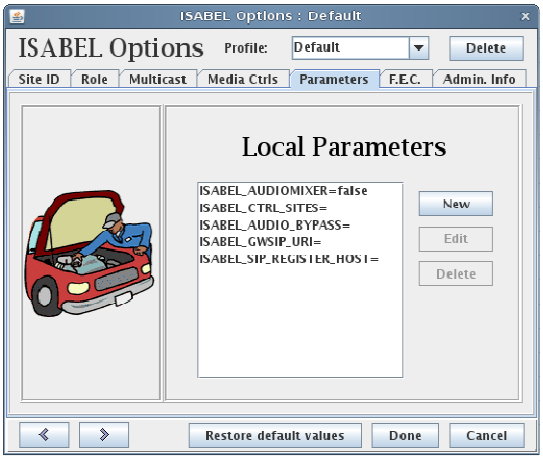


Figura 3.52.- Configuración de parámetros aplicación ISABEL

Una vez que se detalla los parámetros de configuración de las opciones generales de la aplicación ISABEL, es necesario determinar los parámetros de validación para establecer los equipos tanto para ejecutar la aplicación como servidor de Videoconferencia o a su vez como equipo cliente de la misma, para lo cual se estructuran los siguientes parámetros:

- **Configuración para Servidor de Videoconferencia.**

  Para el presente caso de estudio, se determina el equipo cliente A como Servidor de la Aplicación de Videoconferencia para la infraestructura de red sobre el protocolo de red IPV6, tal como se muestra en la Figura 3.53, en donde se configuran los siguientes parámetros.

  - **Nombre de la sesión para la conexión.**
  - **Tipo de Servicio: Tele-Meeting** (opción para interactuar entre los clientes de la conexión).
  - **Calidad de la conexión: 128 / 256 Kbps** (por defecto).
  - **Password:** (solo si se lo requiere para brindar seguridad a la conexión)

  Una vez que se determina estos parámetros, y se revisa la conexión de los dispositivos de audio y video, se puede ejecutar el inicio de la sesión servidor

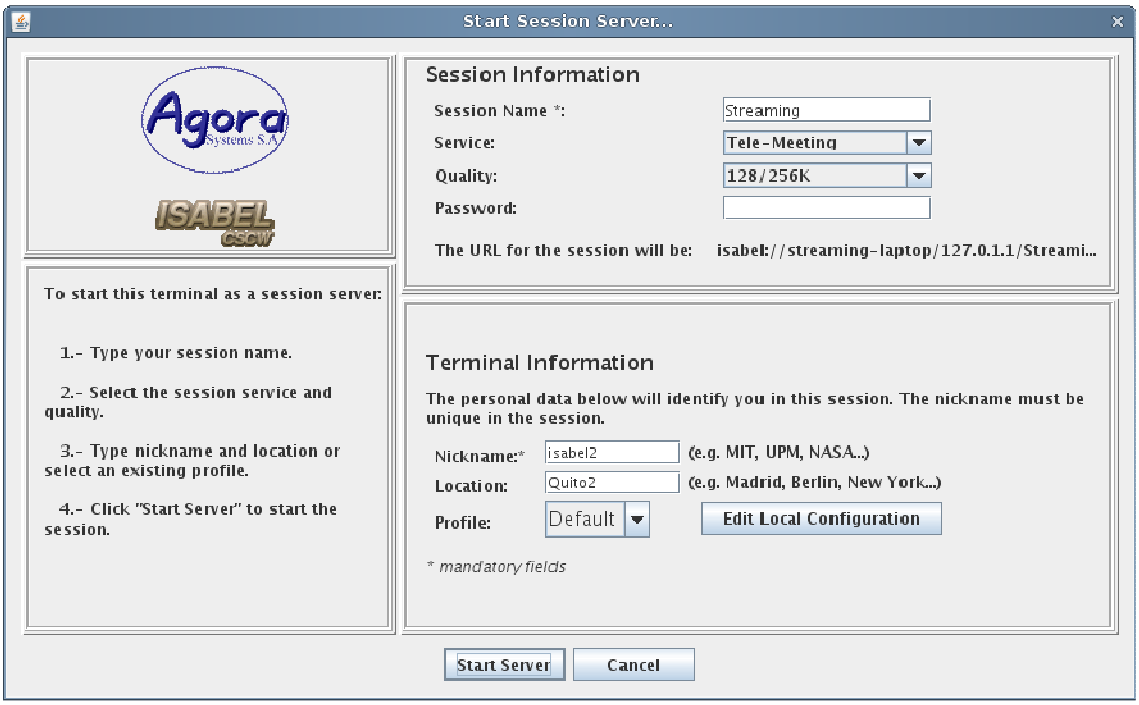


Figura 3.53.- Configuración parámetros para sesión servidor ISABEL

- **Configuración para Cliente de Videoconferencia.**

  Para el presente caso de estudio, se determina el equipo B como cliente de la Aplicación de Videoconferencia para la infraestructura de red sobre el protocolo de red IPV6, tal como se muestra en la Figura 3.54, en donde se configuran los siguientes parámetros.

  - **URL / IP:** (Dirección de red del servidor de Videoconferencia)
  - **Password:** (solo si la sesión Servidor lo ha declarado)

  Una vez que se determina estos parámetros, y se revisa la conexión de los dispositivos de audio y video, se puede ejecutar el inicio de la sesión cliente.

Figura 3.54.- Configuración parámetros para sesión cliente ISABEL

3.6 Funcionamiento de la Videoconferencia bajo la Estructura de Red sobre IPV4

Para poder establecer una Videoconferencia entre dos puntos o estaciones clientes bajo el protocolo de red IPV4, se toma como referencia la estructura de red que se muestra en la Figura 3.2.

Esta infraestructura se encuentra compuesta por un router, dos servidores de borde, dos switch y dos equipos clientes conectados entre sí, para la simulación de una red WAN (Internet) y dos redes LAN, las mismas que trabajan de forma independiente.

Es necesario revisar que todos los parámetros y servicios de comunicación que intervienen en está estructura de red, se encuentren levantados y establecidos de forma correcta, tal como se detalla en el ítem 3.3.

A continuación se procede a realizar la conexión de la Videoconferencia entre los dos equipos clientes, los que se denotan como CLIENTE A y CLIENTE B, como se muestra en la Figura 3.2.

En cada cliente se encuentra instalado el aplicativo EKIGA (ver ANEXO 5.4.2), con el cual estableceremos la Videoconferencia.

En cada uno de los clientes es necesario ejecutar el aplicativo EKIGA tal como muestra la Figura 3.55

Figura 3.55.- Inicio aplicativo EKIGA

Una vez abierto el aplicativo se carga la siguiente interfaz:

Figura 3.56.- Interfaz cliente B Ekiga

Como se muestra en la Figura 3.56, la interfaz de EKIGA se encuentra en estado de espera, la cual indica que el aplicativo está listo para la conexión de la Videoconferencia entre los clientes.

Luego se procede a marcar a la cuenta que está configurada en el otro cliente de la siguiente forma:

Figura 3.57.- Conexión hacia el cliente A Ekiga

Como se muestra en el gráfico 3.57 se debe colocar el número de la cuenta que está configurada en el cliente B y presionar el botón de conexión para que la Videoconferencia se establezca.

En el otro extremo, el cliente A debe aceptar la llamada para que la Videoconferencia quede establecida como se muestra en la siguiente Figura 3.58:

Figura 3.58.- Aceptación de conexión con el cliente B Ekiga

Una vez que se acepta la llamada tal como se muestra en la anterior Figura se levanta la Videoconferencia y se visualiza de la siguiente forma:

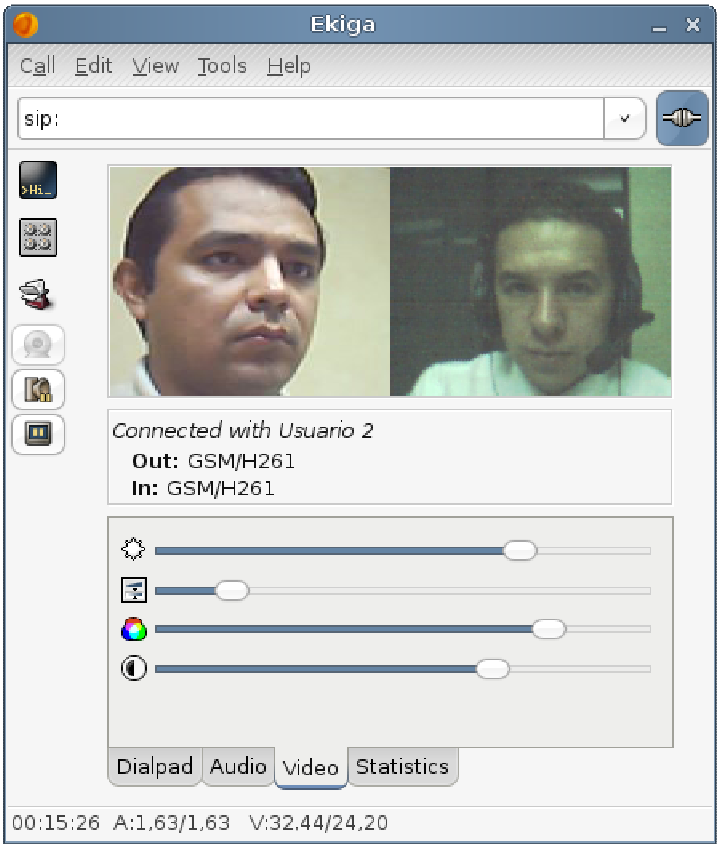


Figura 3.59.- Videoconferencia entre los clientes A y B Ekiga

Una vez establecida la conexión se pueden configurar los siguientes parámetros:

Figura 3.60.- Configuración parámetros de sonido Ekiga

La Figura 3.60 muestra los parámetros generales de configuración del sonido, aquí se establece el volumen del micrófono y auricular para poder hablar y escuchar de forma adecuada en la Videoconferencia.

Figura 3.61.- Configuración parámetros de video Ekiga

En la Figura 3.61 se muestra los parámetros generales de configuración del video, aquí se establece la nitidez con la que el video local se ve en la Videoconferencia.

Figura 3.62.- Estadísticas de transmisión de paquetes Ekiga

En la Figura 3.62 se muestra las estadísticas de los paquetes transmitidos a través de la Videoconferencia.

3.7 Funcionamiento de la Videoconferencia bajo la Estructura de Red sobre IPV6.

Para poder establecer una Videoconferencia entre dos puntos o estaciones clientes bajo el protocolo de red IPV6, se toma como referencia la estructura de red que se muestra en la Figura 3.3.

La misma está compuesta por un router, dos switch y dos equipos clientes conectados entre sí; cabe recalcar que toda la estructura de red trabaja sobre el protocolo de red IPV6, sin la necesidad de realizar un túnel, es decir la conversión del tráfico de paquetes de IPV6 a IPV4 y viceversa.

Es necesario revisar que todos los parámetros y servicios de comunicación que intervienen en está estructura de red, se encuentren levantados y establecidos de forma correcta, tal como se detalla en el ítem 3.4.

A continuación se procede a realizar la conexión de la Videoconferencia entre los dos equipos clientes, los que se denotan como CLIENTE A y CLIENTE B tal como se muestra en la Figura 3.3.

En cada cliente se encuentra instalado el aplicativo ISABEL en versión “DEMO” (ver ANEXO 5.4.3), con el cual se establece la Videoconferencia bajo el protocolo de red IPV6.

En cada uno de los clientes es necesario ejecutar el aplicativo ISABEL el mismo puede ser ejecutado como servidor o a su vez se lo puede conectar como cliente tal como muestra la Figura 3.63.

Figura 3.63.- Ingreso aplicativo ISABEL

La Figura 3.64, muestra al CLIENTE A ejecutándose como servidor para establecer la Videoconferencia entre los dos extremos.

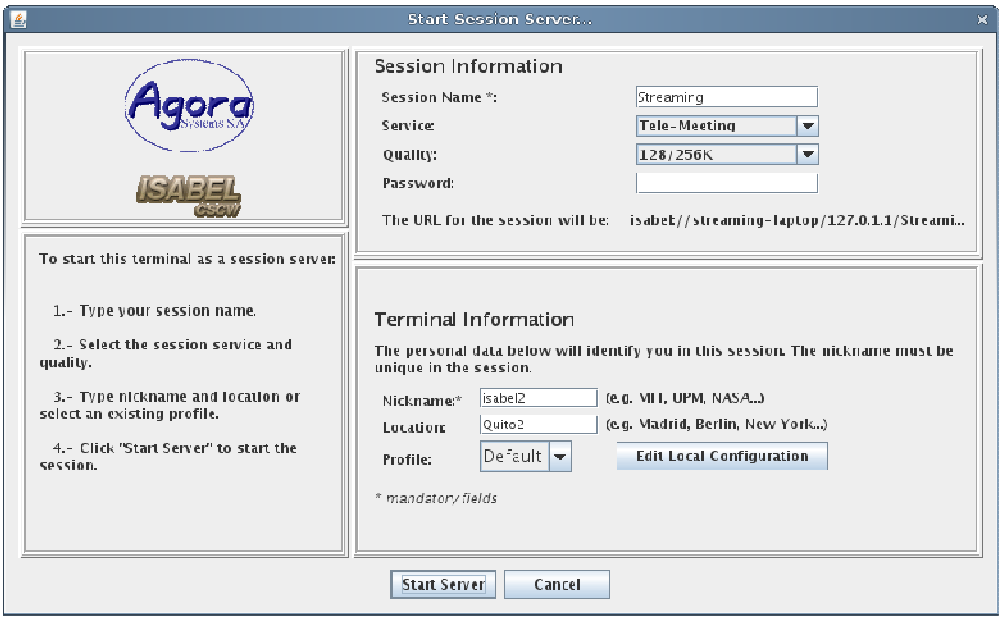


Figura 3.64.- Inicio de servidor ISABEL

Aquí se muestra la información de la sesión a ser levantada como servidor, luego se debe presionar el botón “Start Server” para iniciar el servicio.

Una vez que se ha levantado el servicio, la sesión se verá como muestra la Figura 3.65

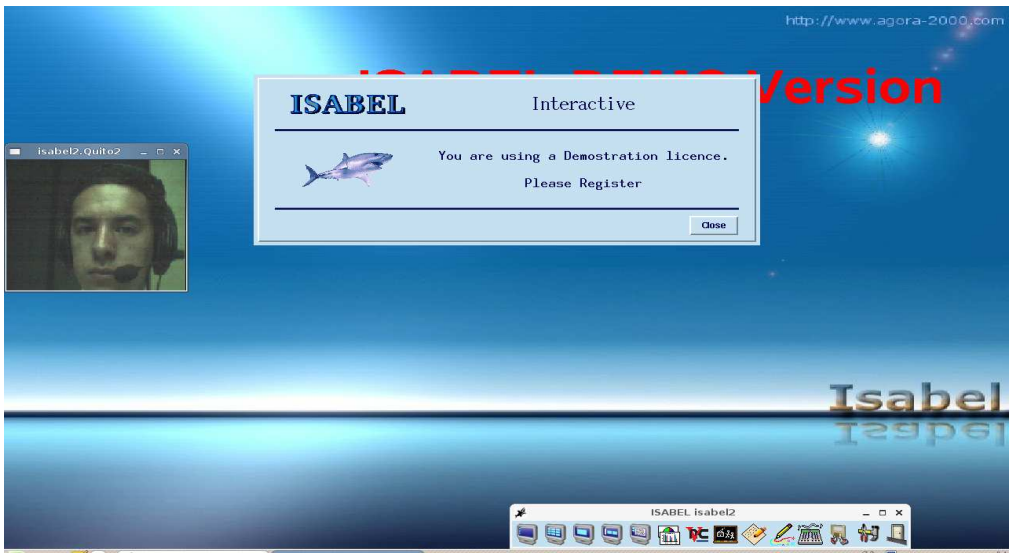


Figura 3.65.- Sesión de servidor ISABEL iniciada

Como es una versión demo, siempre aparecerán pantallas de advertencia, en las cuales se recuerda la adquisición de licencias para este aplicativo.

Ahora el CLIENTE B debe conectarse hacia el CLIENTE A, en el cual se ha levantó el servicio de servidor de sesión para la Videoconferencia, donde aparecerá la siguiente pantalla, tal como se muestra en la Figura 3.66.

Figura 3.66.- Conexión de cliente B hacia servidor ISABEL

Luego se debe presionar el botón “Connect”, donde aparecerá la Figura 3.67, la cual indica el estado de la conexión hacia el servidor ISABEL

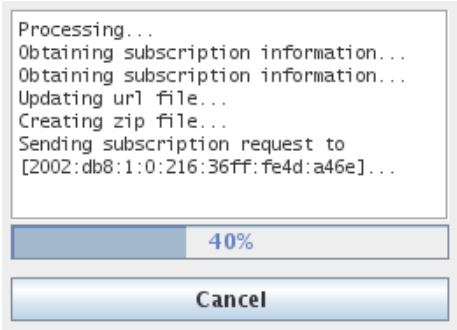


Figura 3.67.- Estado de conexión hacia el servidor ISABEL

Una vez establecida la conexión de forma correcta aparecerán las siguientes pantallas:

Figura 3.68.- Videoconferencia sesión cliente ISABEL

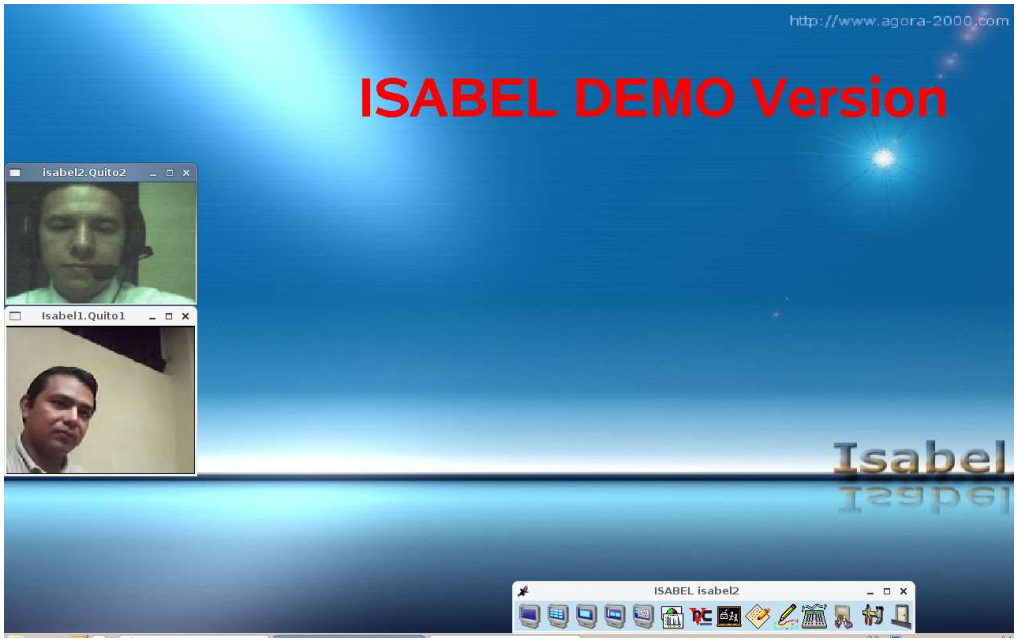


Figura 3.69.- Videoconferencia sesión servidor ISABEL

3.8 Análisis de Desempeño y Funcionalidad

Para determinar el análisis de las diferencias que se establecen entre ambos sistemas de videoconferencia se estructura la tabulación de resultados de desempeño, tanto para el tiempo de retardo en la transmisión de paquetes, como para la variación de los pulsos de las transmisiones digitales a través del “jitter”.

Para realizar la captura de datos, se establecen los siguientes métodos:

3.8.1 Cálculo del Retardo de Transmisión:

Se lo realiza a través de la medición cronometrada de tiempo entre la emisión de la señal de audio hasta el momento que es receptada por el otro extremo de la Videoconferencia.

3.8.2 Cálculo de la Variación de Pulsos:

Esta medición se realiza a través de las estadísticas del tiempo de “buffer de jitter” generado por las aplicaciones clientes de los sistemas de videoconferencia tanto “Ekiga” para IPV4, como “Isabel” para IPV6.

De la tabulación de datos efectuados para los dos ítems de medición, se determina la aplicación de la Media Aritmética con la finalidad de obtener

un valor promedio para realizar el análisis de desempeño entre los dos sistemas de red.

Para determinar el tiempo de retardo en la transmisión de paquetes y la variación de pulsos se efectúa la captura de 100 datos al azar durante el transcurso de una hora tanto en el uso de la aplicación “Ekiga” para el sistema de red IPV4, como en el uso de la aplicación “Isabel” para el sistema de red IPV6, proceso del cual se establece los siguientes resultados:

	IPV4	**IPV6**
Retardo (ms)	42	36
Jitter (ms)	305	108

Tabla 3.8.- Resultados de la medición del retardo en la transmisión de paquetes y la variación de pulsos entre IPV4 e IPV6

De los datos obtenidos se determina el siguiente análisis:

- El retardo en IPV6 es 14.28 % menor al de IPv4.
- La fluctuación para IPV6 es 64.59 % menor al de IPV4

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- A través del presente proyecto se ha logrado diseñar e implementar una estructura de red tipo dual, la misma que ha permitido implementar un sistema de Videoconferencia bajo los protocolos de red IPV4 e IPV6 de manera independiente.

- Mediante el análisis de los datos estadísticos de transmisión de paquetes obtenidos en cada uno de los clientes de las aplicaciones de Videoconferencia se ha determinado el tiempo de retardo y la fluctuación de pulsos que existen entre las dos estructuras de red IPV4 e IPV6.

- La estructura de red de IPV6 permite reducir en un 14.28 % la variación del retardo de paquetes y en un 64.59 % la fluctuación de pulsos en un sistema de videoconferencia, según el análisis de desempeño realizado en tiempo real.

- La diferencia que existe entre la fluctuación y el retardo para cada protocolo, se debe básicamente a la realización de procesos que sufren los paquetes desde su origen hasta el destino en cada estructura de red.

- El control de ancho de banda únicamente se determina para la implementación de la estructura de red IPV4, ya que no existe al momento un tipo de servicio o aplicación que permita controlar el tráfico de paquetes para la estructura de red IPV6.

- El uso de las herramientas de captura de paquetes sniffers, permiten determinar que tanto la estructura de red IPV4 e IPV6 utilizan protocolos de comunicación similares, como: UDP, ICMP, IGMP, BGP, con sus respectivas modificaciones en su estructura para el tratamiento de paquetes de IPV6 como UDPV6, ICMPV6, IGMPV6, BGPV6.

- La implementación del control de ancho de banda para la estructura de red IPV4, permite evaluar únicamente el desempeño de la calidad del video ya que al aplicar este tipo de control se deteriora de manera notoria.

- La diferencia que existe entre la fluctuación y el retardo para cada protocolo, se debe básicamente a la realización de procesos que sufren los paquetes desde su origen hasta el destino en cada estructura de red.

- Para la implementación de los sistemas de videoconferencia en las dos estructuras de red IPV4 e IPV6, se realizaron pruebas de funcionamiento con varios tipos de aplicaciones tanto para los equipos servidores como las estaciones clientes, de donde se obtuvieron los siguientes resultados:

    - Centos 5: Plataforma Linux de Sistema Operativo para los servidores de ruteo y comunicación, funcionamiento: estable y operativo.

    - Elastix: Servidor de aplicación GPL para la provisión del servicio de videoconferencia y telefonía IP en la estructura IPV4, funcionamiento: estable y operativo.

    - Flumotion: Servidor de aplicación GPL para la provisión del servicio de videoconferencia en la estructura IPV6, funcionamiento: inestable y no operativo.

- Red5: Servidor de aplicación Demo para la provisión del servicio de videoconferencia en la estructura IPV6, funcionamiento: inestable y no operativo.

- Elastix v6: Servidor de aplicación Demo para la provisión del servicio de videoconferencia en la estructura IPV6, funcionamiento: inestable pero operativo.

- Microsoft Windows Vista: Sistema Operativo propietario para cliente de Videoconferencia en las estructuras IPV4 e IPV6, funcionamiento: inestable pero operativo.

- Linux Ubuntu: Sistema Operativo GPL para cliente de Videoconferencia en las estructuras IPV4 y IPV6, funcionamiento: estable y operativo.

- Linux Mint: Sistema Operativo GPL para cliente de Videoconferencia en las estructuras IPV4 y IPV6, funcionamiento: estable y operativo.

- Los navegadores Web sobre la plataforma Windows no soportan el uso de direcciones IPv6 en su formato hexadecimal, por lo cual es necesario registrar dichas direcciones en un servidor DNS y acceder a estas direcciones mediante su nombre.

- La principal contribución de este proyecto de investigación, fue determinar el desarrollo de un benchmark para medir el desempeño de un Sistema de Videoconferencia, tomando como métricas la variación del retardo de paquetes y la fluctuación de pulsos al utilizar protocolos de comunicación IPV4 e IPV6.

- Las herramientas y aplicaciones de software libre para servidores y clientes de videoconferencia para IPV4 e IPV6, presentan mayor estabilidad en su desempeño y funcionamiento que las herramientas de software propietario.

- Existe una amplia información de soporte técnico para las herramientas y aplicaciones de software libre, la misma que ha servido de gran apoyo para el desarrollo de este proyecto de investigación.

- Existe complicación al momento de realizar implementaciones prácticas bajo el protocolo de IPV6 ya que la misma no tiene aún el soporte técnico de aplicaciones estables ni documentos técnicos de referencia.

- No se pueden determinar pruebas de funcionamiento para la estructura de red IPV6 tal como se determina en el diseño e implementación de la estructura de red para IPV4, ya que el costo por licencia de servidor de ISABEL cuesta alrededor de 1600 €.

4.2 Recomendaciones

- Para la implementación de aplicaciones de sistemas de Videoconferencia se recomienda el uso de sistemas operativos y aplicaciones de Software Libre, ya que se cuenta con gran cantidad de información y soporte técnico disponible en el Internet.

- Se debe considerar a futuro un estudio profundo de las diversas aplicaciones que se pueden determinar con el uso de la tecnología de red IPV6, especialmente el uso de esta tecnología para el uso de la telefonía móvil.

- Es necesario que los candidatos a desarrollar proyectos de este tipo, se encuentren actualizados tanto en el uso y aplicación de este tipo de herramientas de comunicación para Videoconferencia, así como también en el uso de diferentes metodologías de investigación para un óptimo y eficaz desarrollo del proyecto a ejecutar.

- Para el desarrollo de este tipo de proyectos sobre aplicaciones de software libre, se recomienda que los estudiantes refuercen sus

conocimientos en plataformas LINUX. Ya que se requiere de un nivel de comprensión básico e intermedio sobre el tema para el desarrollo de cualquier tipo de proyecto.

- Es recomendable para este tipo de estudios de investigación, que se determine como factor principal el diseño y estructuración de sistemas de redes independientes, con la finalidad de establecer de manera adecuada una evaluación técnica de desempeño y funcionalidad de los protocolos de red IPV4 e IPV6.

- Se recomienda al departamento de Ciencias de la Computación, Carrera de Ingeniería de Sistemas e Informática que refuerce en su malla curricular materias que contengan el uso y aplicación de herramientas GPL, LINUX para el desarrollo a futuro de este tipo de proyectos de investigación.

ANEXOS

INSTALACIÓN DE SISTEMAS OPERATIVOS Y PAQUETES PARA LA INFRAESTRUCTURA DE VIDEOCONFERENCIA SOBRE IPV4 E IPV6

5.1. Instalación de Sistema Operativo Centos. 5.0 para Equipo ruteador

La primera pantalla que se mostrará será la del inicio del sistema **Isolinux,** donde se puede observar una serie de instrucciones, las cuales ayudarán en el proceso de instalación del sistema.

En esta pantalla se puede observar una línea de comandos (boot:), en la misma se pueden ingresar diferentes opciones para el inicio del proceso de instalación.

Para iniciar el modo gráfico, en español, se debe invocar el instalador Anaconda con los siguientes parámetros:

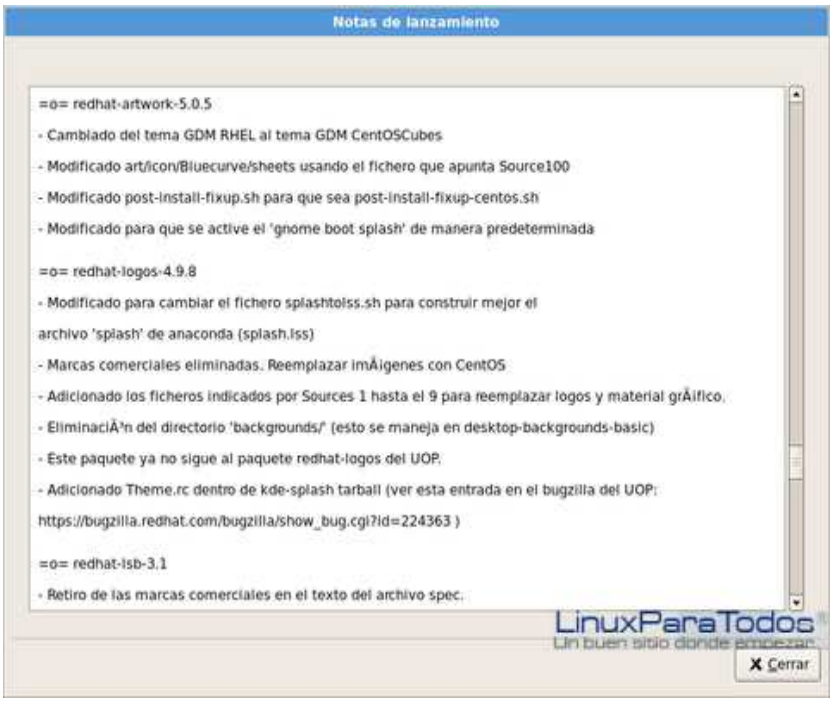
boot: linux lang=es

Si no se desea introducir ningún parámetro, y se quiere iniciar el proceso de instalación en modo gráfico, solamente se presiona en «Intro» o «Enter».

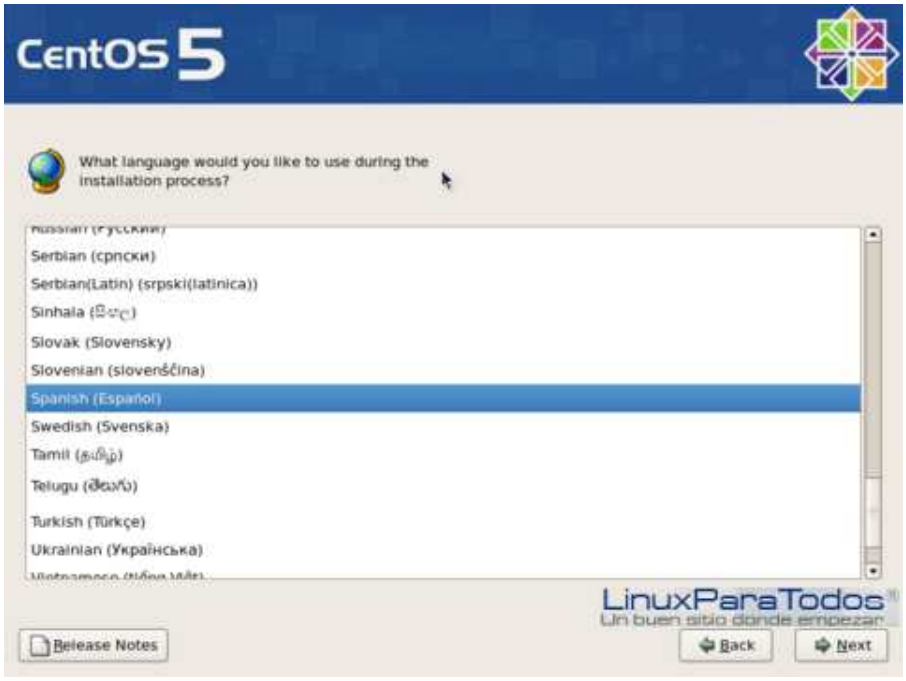
La siguiente pantalla indica si se desea verificar la integridad de los datos que se encuentran en el disco. Es recomendable realizar este procedimiento por lo menos la primera ocasión que se utiliza el disco de instalación, con la finalidad de comprobar que la información que se encuentra en el disco sea la correcta.

Una vez finalizado este paso, el sistema de instalación de Red Hat, Anaconda, efectuará un análisis de hardware para determinar la información del sistema necesaria para continuar con el proceso de instalación. Seguidamente, aparece la siguiente pantalla de bienvenida de Anaconda a CentOS 5

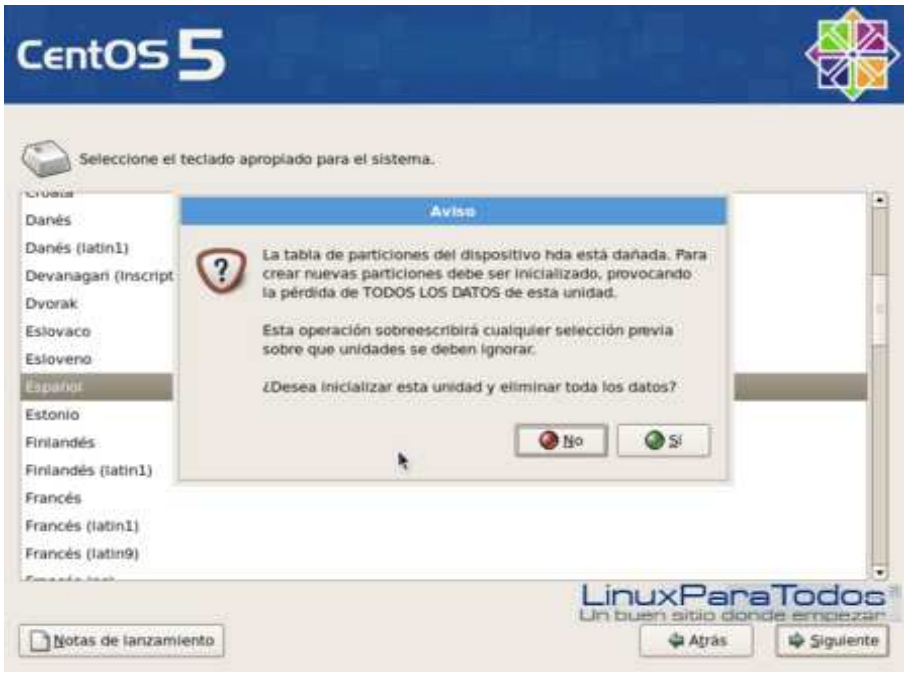
Al seleccionar la opción de “Notas de lanzamiento” se indicará la información sobre el sistema que se está instalando, así como algunas notas legales, descripción de cambios y cambios entre versiones.



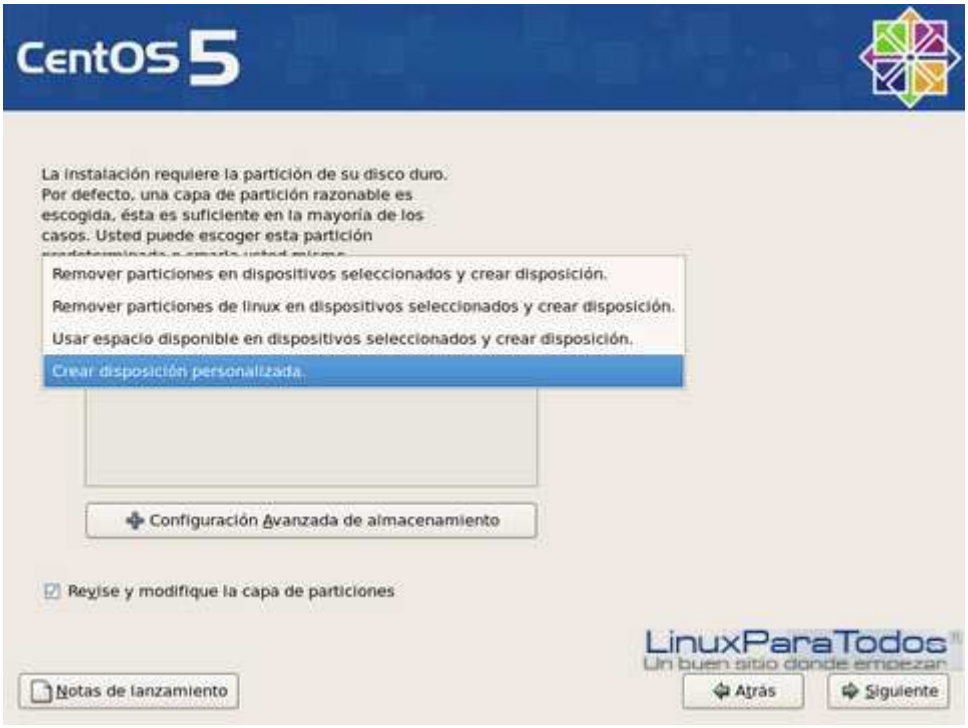
Seguidamente aparecerá la pantalla de selección del idioma predeterminado de instalación del sistema. Seleccionamos «Spanish (Español)», o el de preferencia del usuario.



Esta pantalla permite seleccionar la distribución del teclado que se encuentra físicamente instalado en el PC.



Después de seleccionar la distribución del teclado el sistema verificará e iniciará los procesos de administración de los discos duros. Si el sistema detecta que el disco duro es nuevo y no ha sido inicializado, indicará una notificación. Se escogerá «Si» para poder inicializar el dispositivo de almacenamiento.



Se debe tener mucho cuidado al momento de elegir la forma de manipulación del disco duro, a continuación se detalla cual es la función de cada una de las opciones:

5.1.1. Remover Particiones en Dispositivos Seleccionados y crear Disposición:

Esta opción eliminará cualquier partición encontrada en los discos seleccionados, y creará automáticamente una disposición de particiones por defecto.

5.1.2. Remover Particiones de Linux en Dispositivos Seleccionados y crear Disposición:

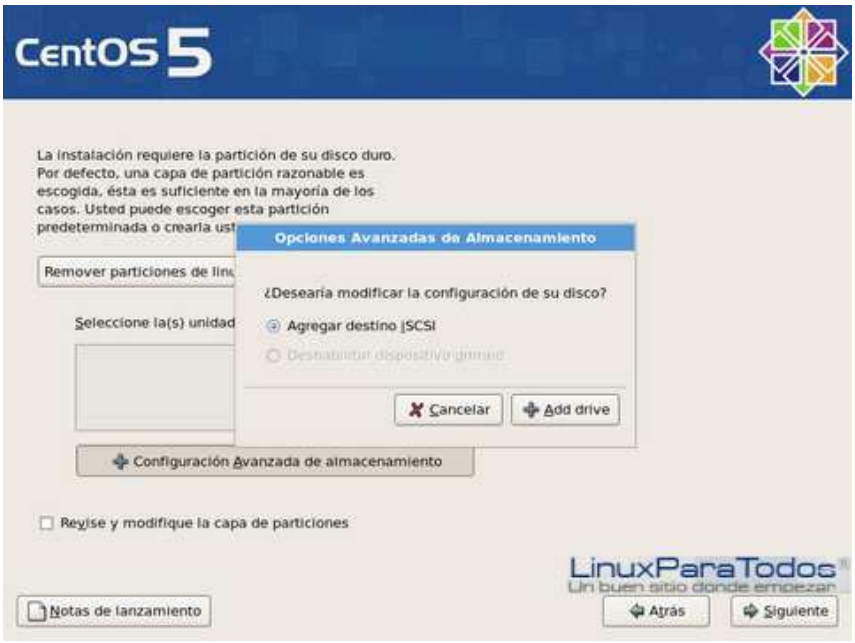
Esta opción solamente eliminará las particiones linux que se encuentren en dicho dispositivo. De igual forma creará automáticamente una disposición de particiones por defecto.

5.1.3. Usar Espacio Disponible en Dispositivos Seleccionados y crear Disposición:

Si el disco dispone de espacio libre NO PARTICIONADO, y con capacidad de particionar, el sistema tomará este espacio y creará en él una disposición de particiones por defecto.

5.1.4. Crear Disposición Personalizada:

Esta opción es para usuarios con un poco más de experiencia en el manejo de sistemas.



Una vez seleccionado el método de particionamiento, se podrá revisar y modificar la tabla de particiones del sistema. A continuación se muestra el procedimiento a efectuar con una disposición personalizada:

Para crear una nueva partición, se debe pulsar el botón «Nuevo», que desplegará la siguiente pantalla:

A continuación se detalla los parámetros que pueden ser modificados en la partición seleccionada:

5.1.5. Punto de Montaje:

El punto de montaje es la ruta en la cual se “montará” la partición.

5.1.6. Tipo de Sistema de Archivos:

Se escoge el tipo de sistema gestor de ficheros que utilizará el sistema (regularmente ext3: el sistema por defecto para Linux). Si se elige «swap», entonces no se requiere especificar un punto de montaje

5.1.7. Unidades Admisibles:

Si el equipo cuenta con más de un disco duro, o diversas unidades remotas para almacenamiento, se deberá especificar en cuales de ellas se reservará el espacio para la partición.

5.1.8. Opciones de Tamaño Adicionales:

Hay 3 opciones para asignar el espacio en disco:

- **Tamaño fijo:** Solamente tomará lo especificado en la casilla “Tamaño (MB)”, medida en megabytes y es la mejor aproximación a la geometría del disco duro, procurando ocupar sectores completos

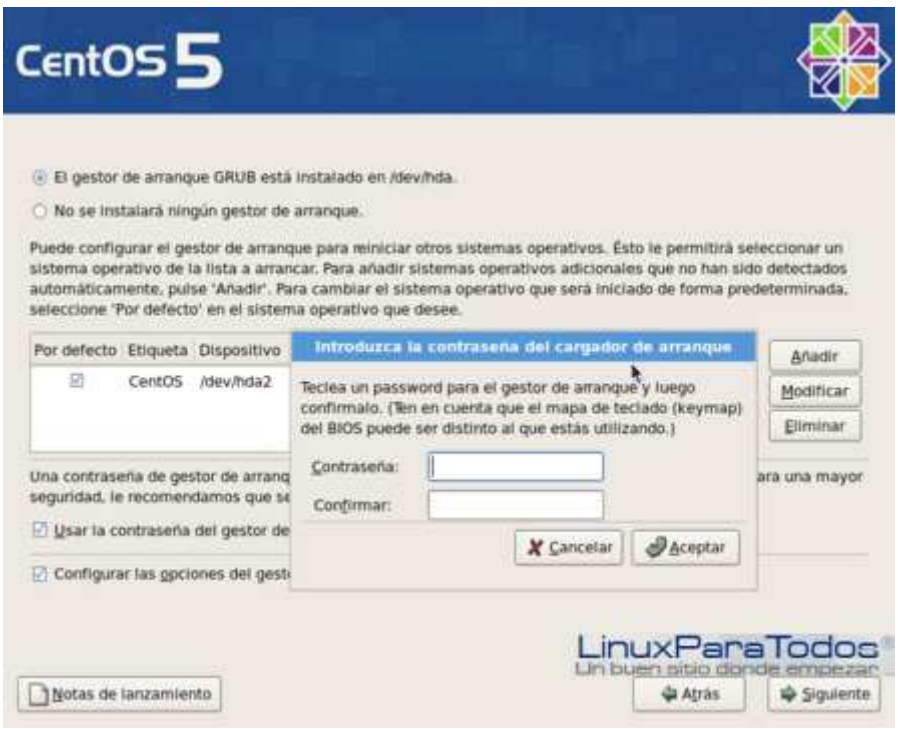
- **Completar todo el espacio hasta**: Lo mismo que la opción anterior, pero asignando la totalidad del espacio, aún cuando no queda en un sector completo del disco

- **Completar hasta el tamaño máximo permitido:** Ocupa todo el espacio disponible en el disco para crear la nueva partición.

5.1.9. Forzar a ser Partición Primaria:

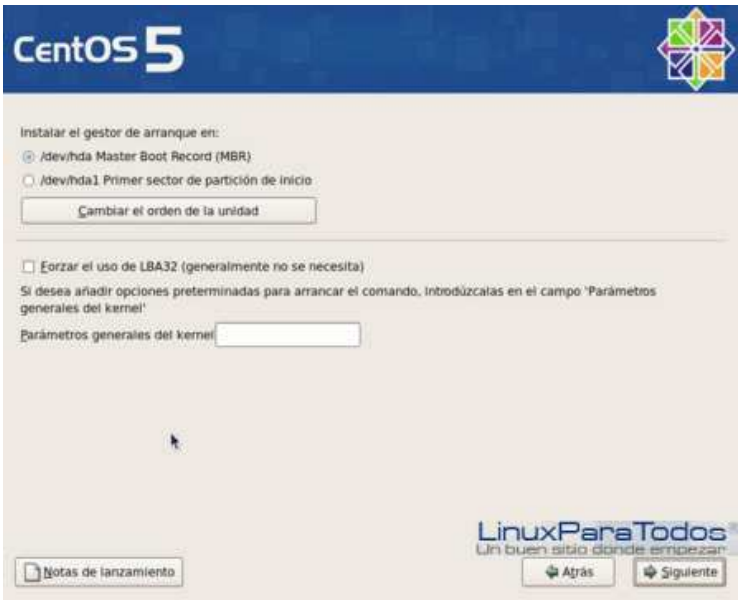
Cuando se requiere que la partición quede dentro de las definiciones de la partición primaria

Seguidamente se debe configurar el gestor de arranque GRUB, sistema que permite administrar y seleccionar el sistema operativo con el que iniciará el equipo (cuando se cuenta con múltiples sistemas instalados).



Para incrementar un poco más la seguridad del sistema, se puede implementar una contraseña para GRUB, la cual será necesaria si se desean modificar parámetros al inicio del sistema.

A continuación se debe indicar en que parte del disco instalar a GRUB. Por defecto se elige instalarlo directamente en el sector maestro de inicio (MBR):



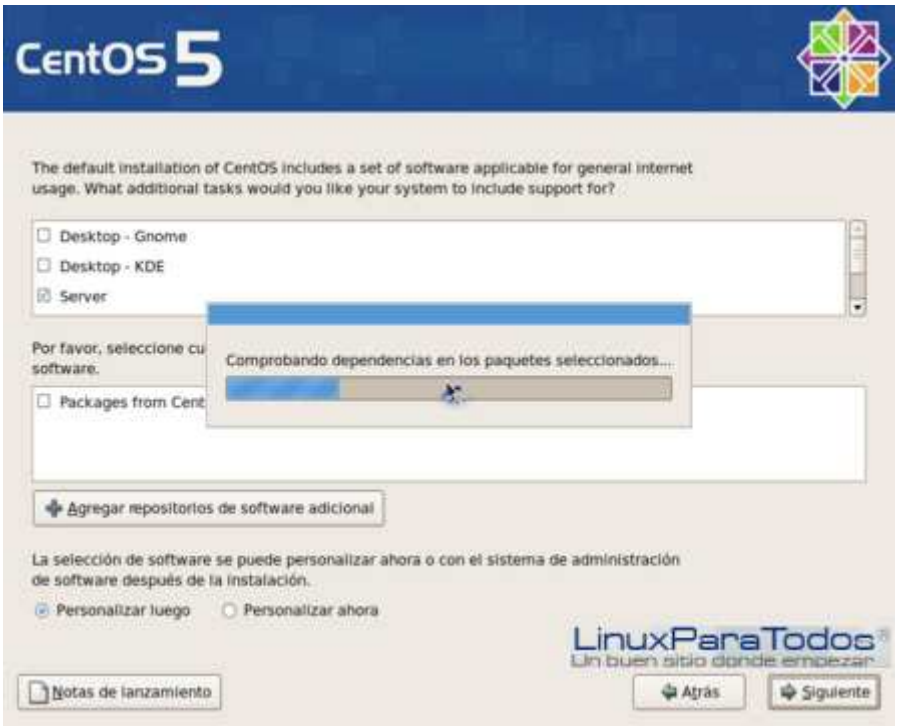
Si el sistema cuenta con alguna interfaz de red, y esta es compatible con el sistema operativo, se nos presentará la sección para la configuración de nuestra red:

Seguidamente continuamos con la configuración sobre la ubicación geográfica del equipo. Es conveniente tener ajustado el huso horario (o zona horaria) correctamente, para tener un mejor control sobre las bitácoras y mensajes generados por el sistema.

A continuación se debe ingresar la contraseña de superusuario root. Es importante recordar esta contraseña, ya que será con la que se ingresará al sistema para realizar las tareas administrativas.

Una vez ingresada y verificada la contraseña en ambos casilleros, el sistema de instalación analizará el equipo en búsqueda de instalaciones previas de algún sistema Red Hat compatible. Si este existe, solicitará elegir entre la actualización del sistema instalado, o el realizar una instalación completamente nueva.

A continuación se deben seleccionar los grupos de paquetes que vayan a ser instalados



Se llevará a cabo el cálculo de dependencias. En los paquetes seleccionados se analizarán cuales son los requerimientos propios de cada paquete.

La pantalla siguiente indica el punto de no regreso. Hasta estas instancias el equipo permanece sin modificaciones.

Una vez que se pulsa el botón «Siguiente», comenzará el formateo de las particiones:

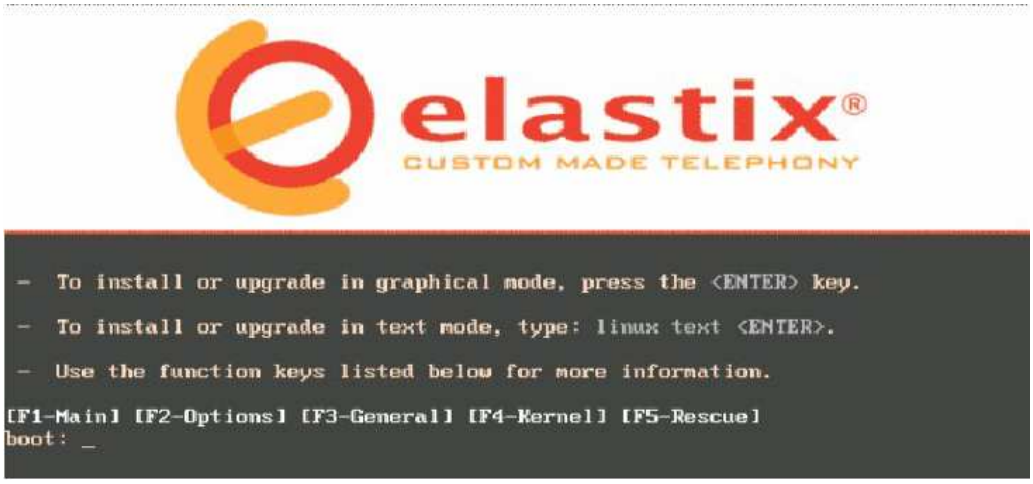
Así como la instalación de los paquetes seleccionados (y sus dependencias):

Si no existió ningún inconveniente en el proceso de instalación y dependiendo de la velocidad del equipo y de la cantidad de paquetes seleccionados para la instalación, se mostrará la pantalla que indica que el proceso de instalación ha culminado.

Con esto concluye todo el proceso de instalación de la distribución CentOS 5.

5.2. Instalación de sistema Operativo de Elastix para servidores de borde

Se debe insertar el CD de instalación de Elastix al momento de encender el PC. Una vez hecho esto aparecerá una pantalla como la siguiente:

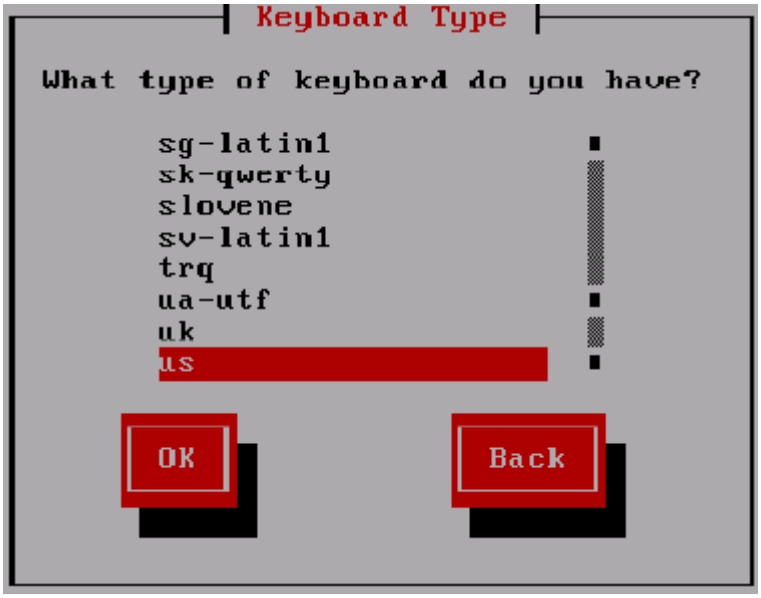


Si el usuario es experto puede comenzar la instalación en modo avanzado digitando el siguiente comando:

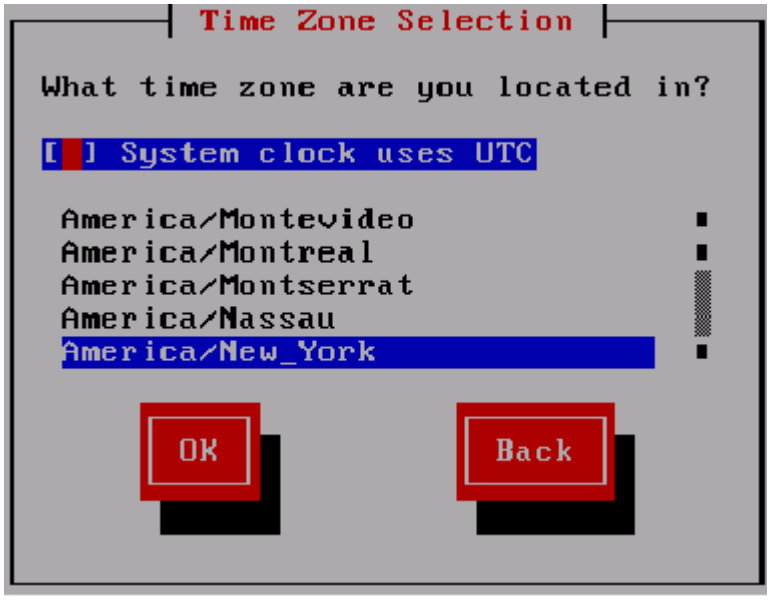
advanced

Caso contrario se debe presionar **enter** para comenzar la instalación automática desde el CD.

Seguidamente se procede a escoger el tipo de teclado de acuerdo a la distribución de idioma que tenga el mismo:



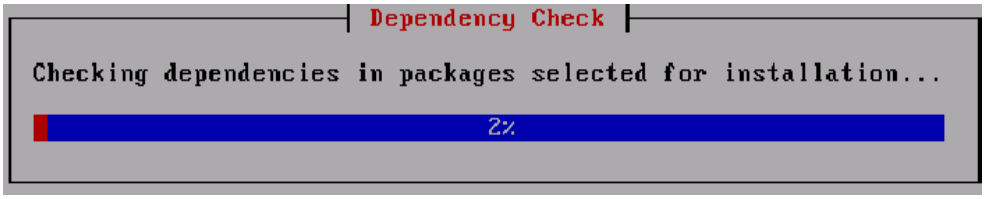
Luego se debe seleccionar el tiempo de la zona horaria de la región:



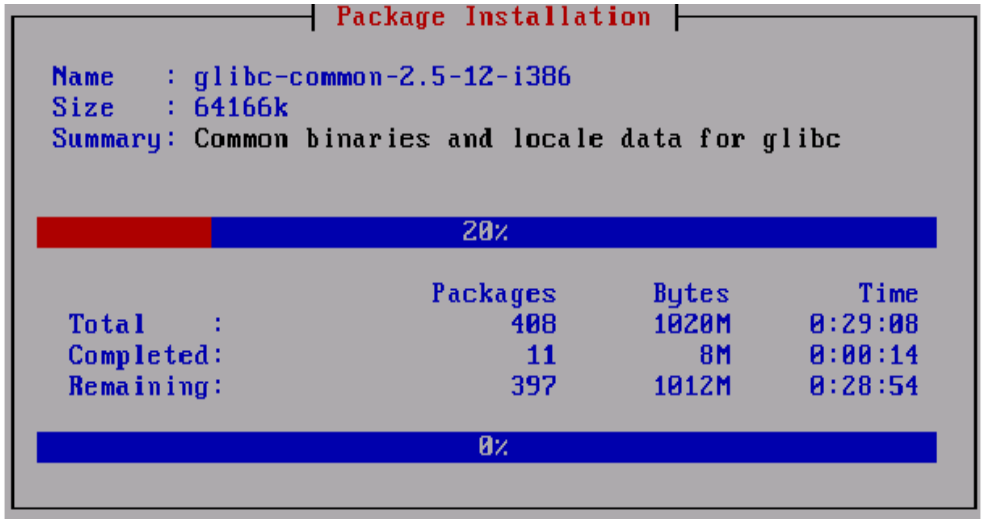
Seguidamente se debe digitar la contraseña que será usada por el administrador de Elastix. Se debe recordar que esta es una parte crítica para la seguridad del sistema.

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

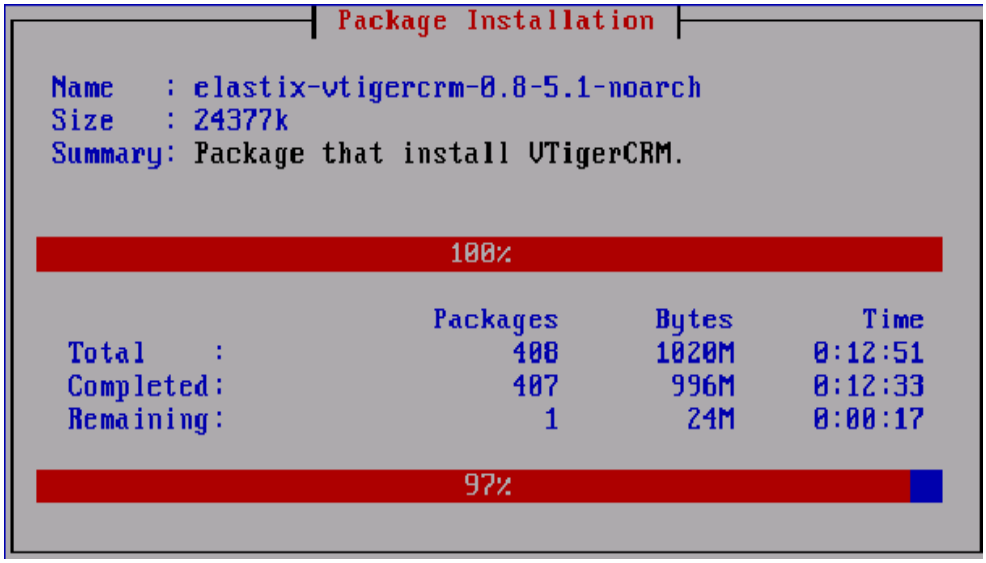
Primero buscará las dependencias necesarias para la instalación:



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

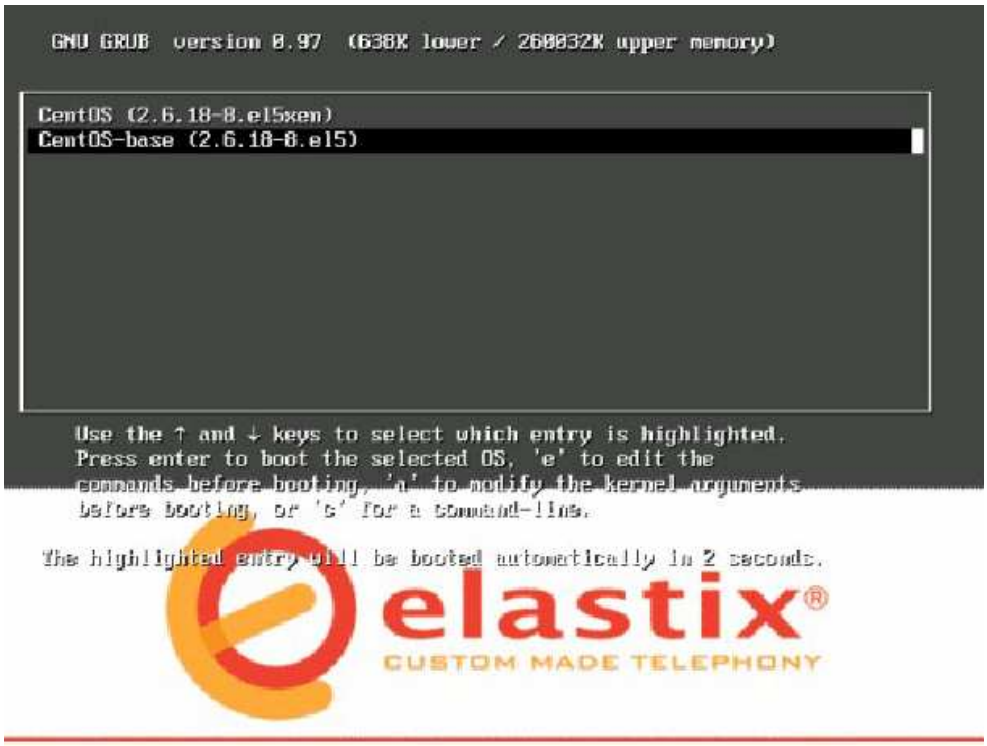


La siguiente imagen muestra que la instalación de los paquetes está por culminar:

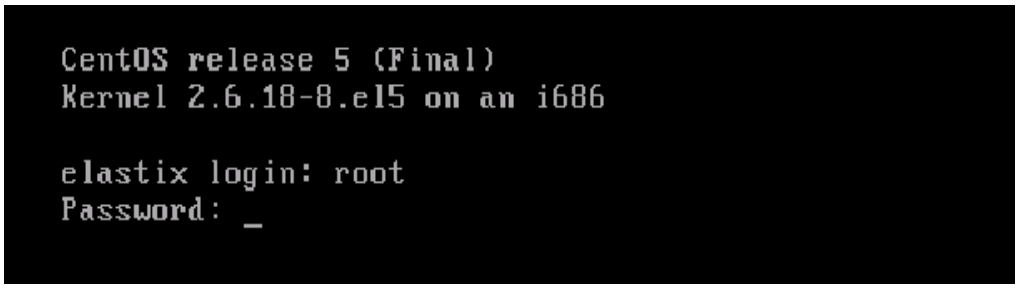


Una vez terminado el proceso de instalación, se debe reiniciar el sistema.

Luego de reiniciar el sistema aparecerá la siguiente pantalla, en la que se muestra a inicialización de **Elastix**, ya que su proceso de instalación concluyó con éxito.



Se debe ingresar como usuario **root** y la contraseña que fué digitada al momento de la instalación.

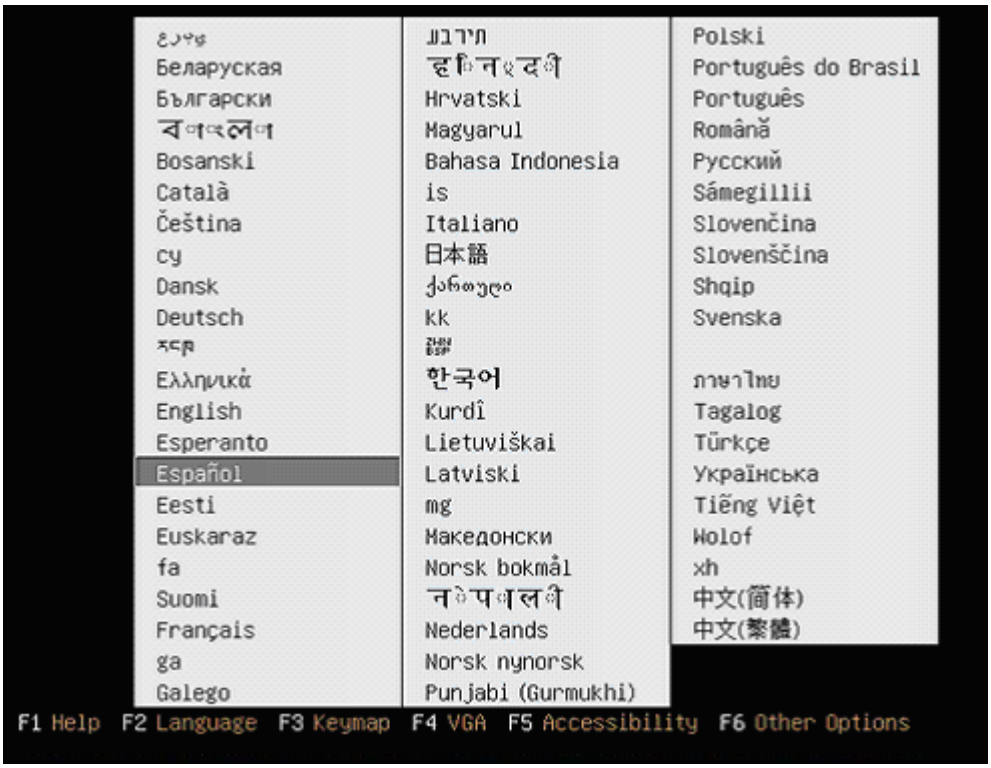


5.3. Instalación de sistema operativo para clientes IPV4 e IPV6

5.3.1. Instalación de sistema Operativo UBUNTU

Iniciar el equipo con el CD que tiene cargado el sistema operativo UBUNTU, luego aparecerá la siguiente pantalla de bienvenida (en inglés).

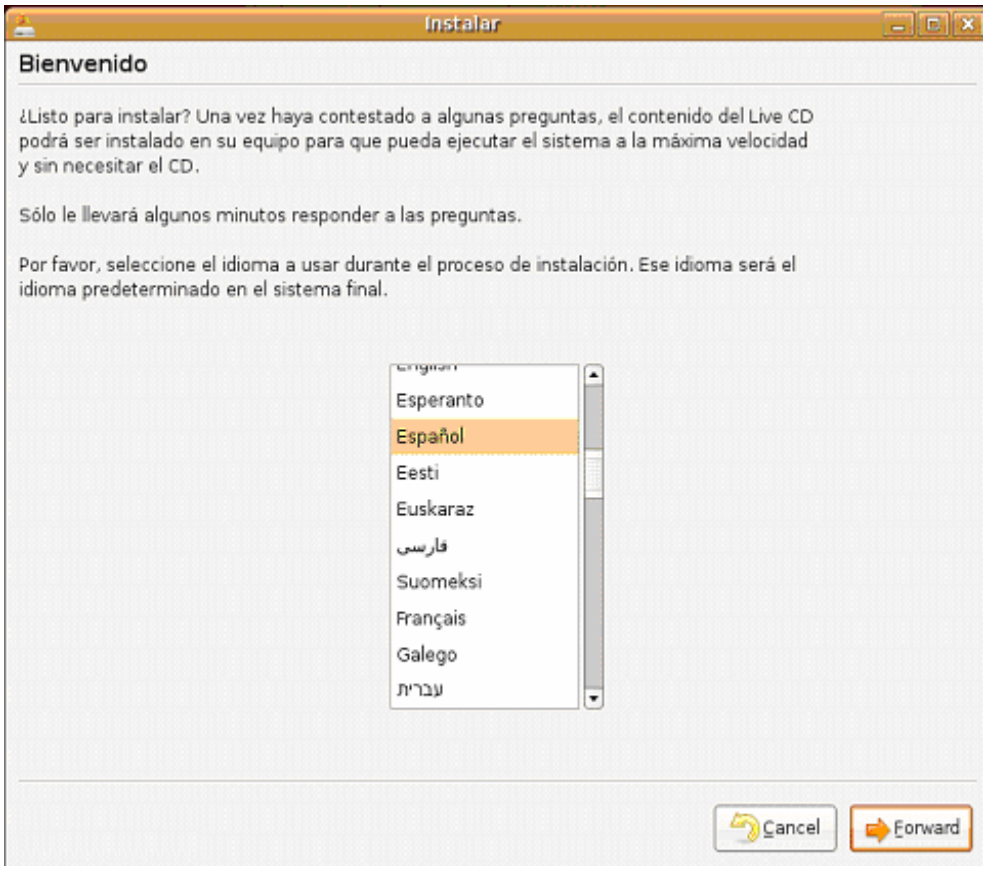
Para elegir el idioma español, solo hay que pulsar F2 y seleccionarlo de la lista.



Luego de unos instantes aparecerá el escritorio de Ubuntu, en el cual se encuentra un icono como el siguiente:

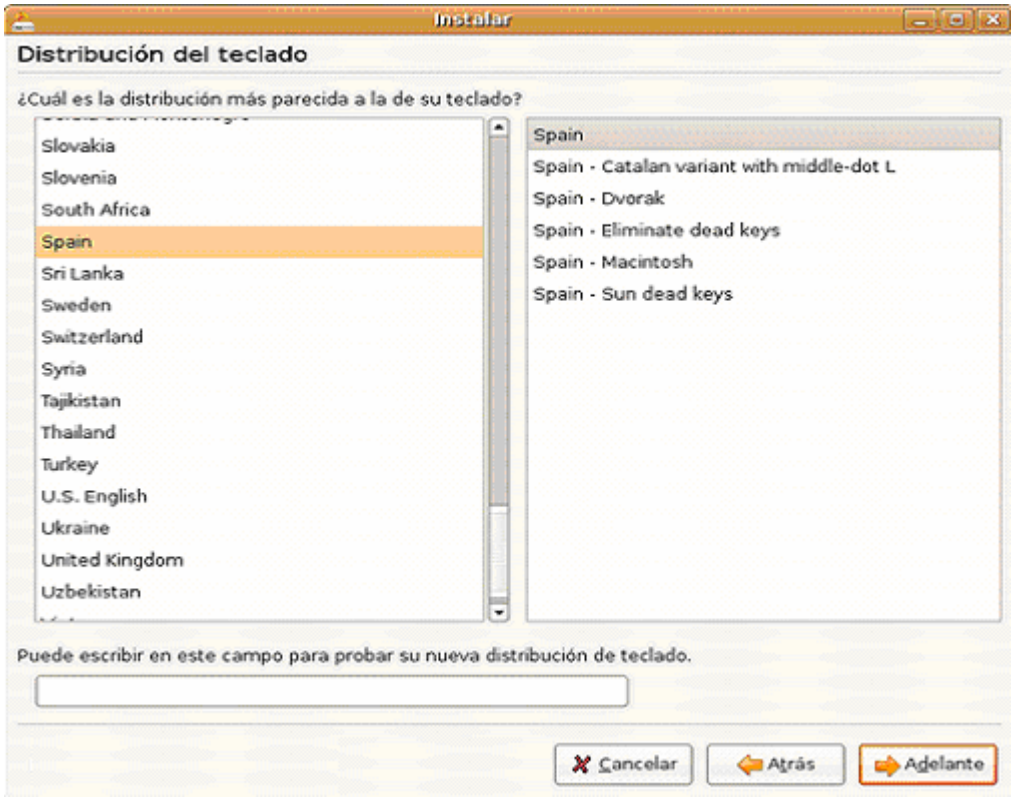
Haciendo doble clic, comenzará el proceso de instalación.

Escogemos el idioma con el cual se procederá a realizar la instalación:



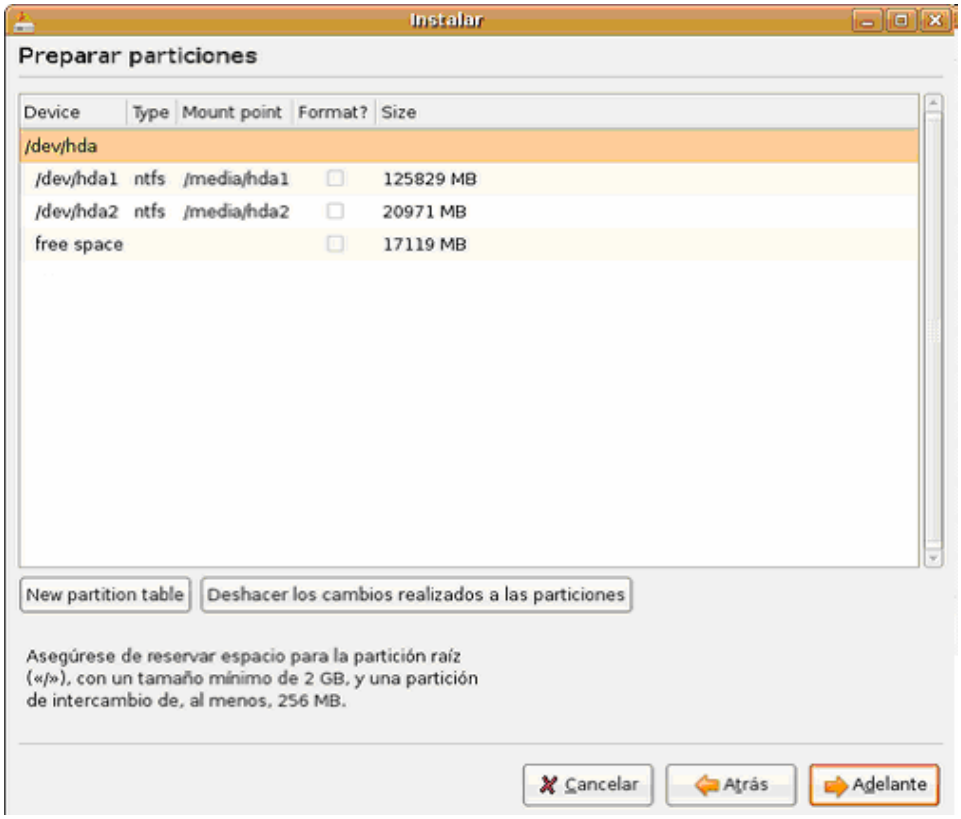
Seguidamente se debe escoger la zona horaria:

Luego debemos elegir la distribución correcta del teclado:



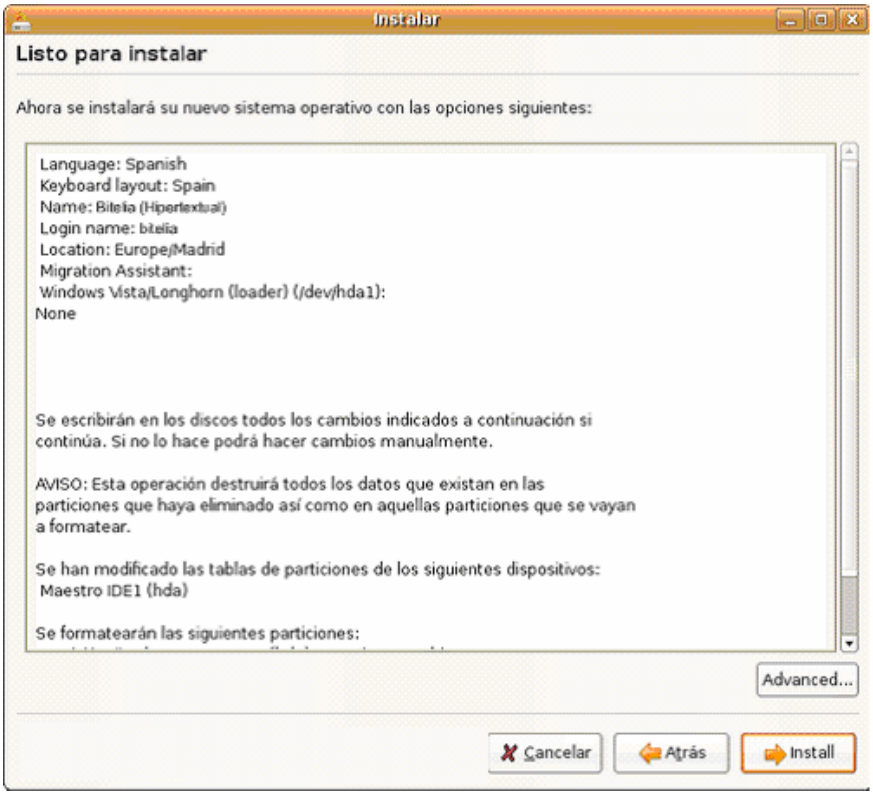
Seguidamente aparecerá la siguiente pantalla, en la cual se indica la forma en que se desea preparar el disco

Una vez preparado el disco procedemos a escoger la partición en donde el sistema operativo será instalado.

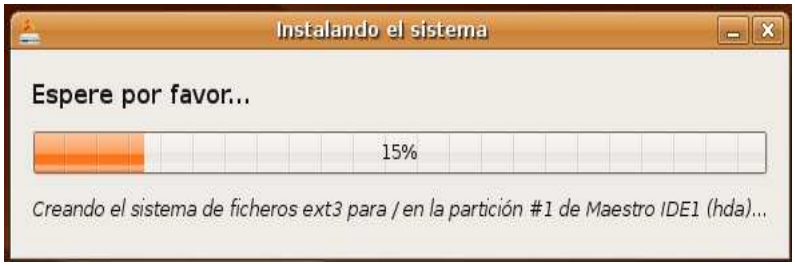


Una vez terminado este proceso se requiere introducir toda la información que el sistema por defecto solicita al momento de su instalación como se muestra en la siguiente pantalla:

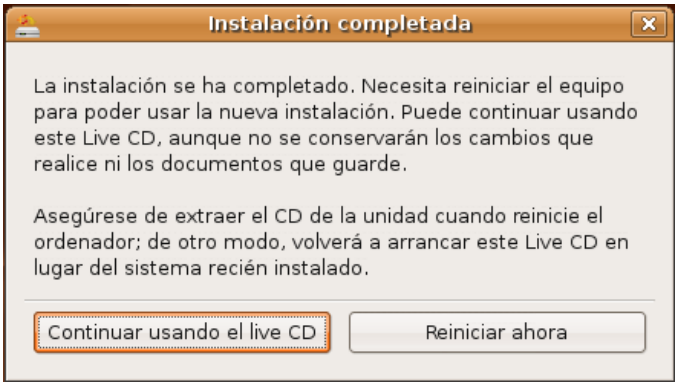
Una vez introducido los datos necesarios, el sistema nos indicará en resumen las características de los parámetros personalizados para la instalación del sistema operativo



AL momento de presionar el botón de **install** comenzará el proceso de instalación y aparecerá la siguiente pantalla:



Si no existió ningún inconveniente en el proceso de instalación y dependiendo de la velocidad, se mostrará la pantalla que indica que el proceso de instalación ha culminado.



5.3.2. Instalación de Sistema Operativo LINUX MINT

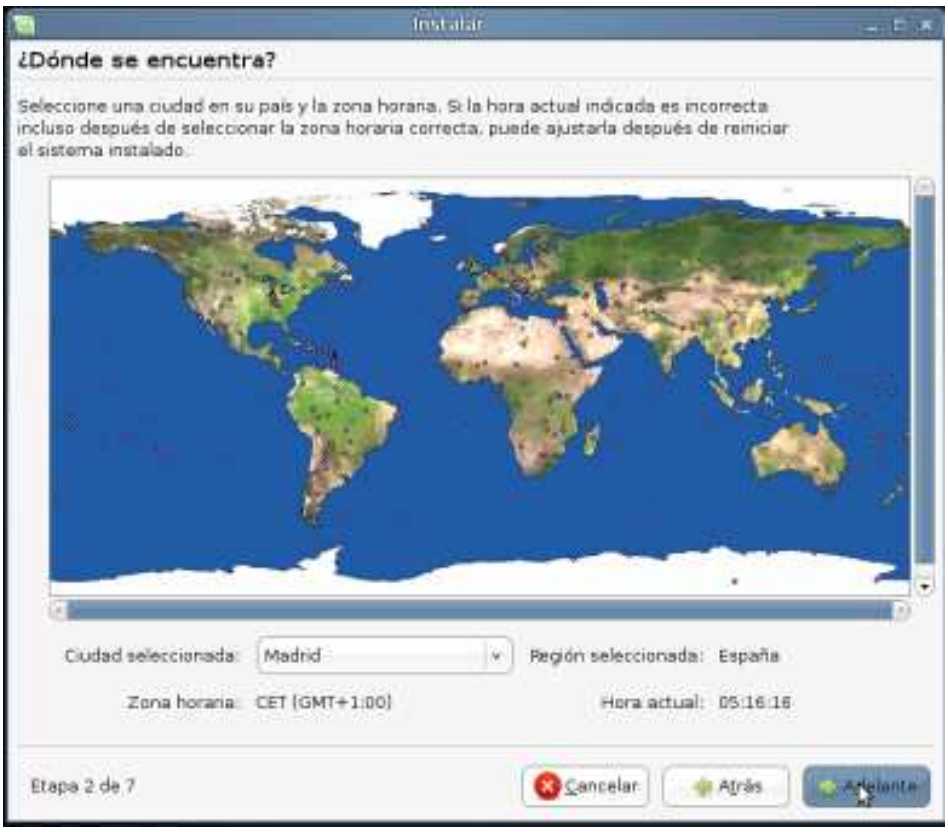
Iniciar el equipo con el CD que tiene cargado el sistema operativo LINUX MINT, luego aparecerá la siguiente pantalla de bienvenida.

Luego de unos instantes aparecerá el escritorio de LINUX MINT, en el cual se encuentra un icono como el siguiente:

Haciendo doble clic, comenzará el proceso de instalación.

Escogemos el idioma con el cual se procederá a realizar la instalación:

Seguidamente se debe escoger la zona horaria:

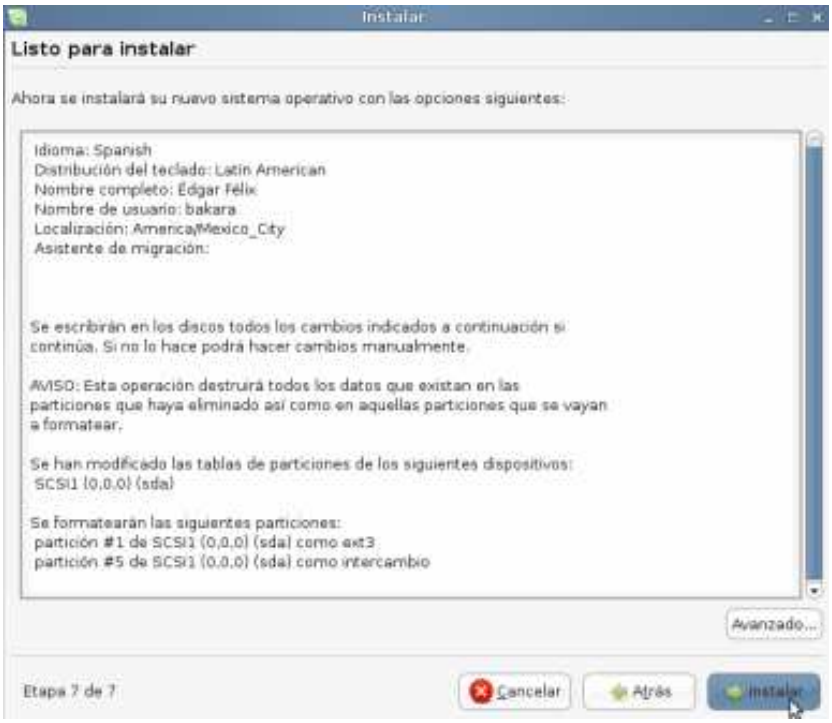


Luego debemos elegir la distribución correcta del teclado:

Seguidamente aparecerá la siguiente pantalla, en la cual se indica la forma en que se desea preparar el disco

Una vez terminado este proceso se requiere introducir toda la información que el sistema por defecto solicita al momento de su instalación, como se muestra en la siguiente pantalla:

Una vez introducido los datos necesarios, el sistema nos indicará en resumen las características de los parámetros personalizados para la instalación del sistema operativo



AL momento de presionar el botón **instalar** comenzará el proceso de instalación y aparecerá la siguiente pantalla:

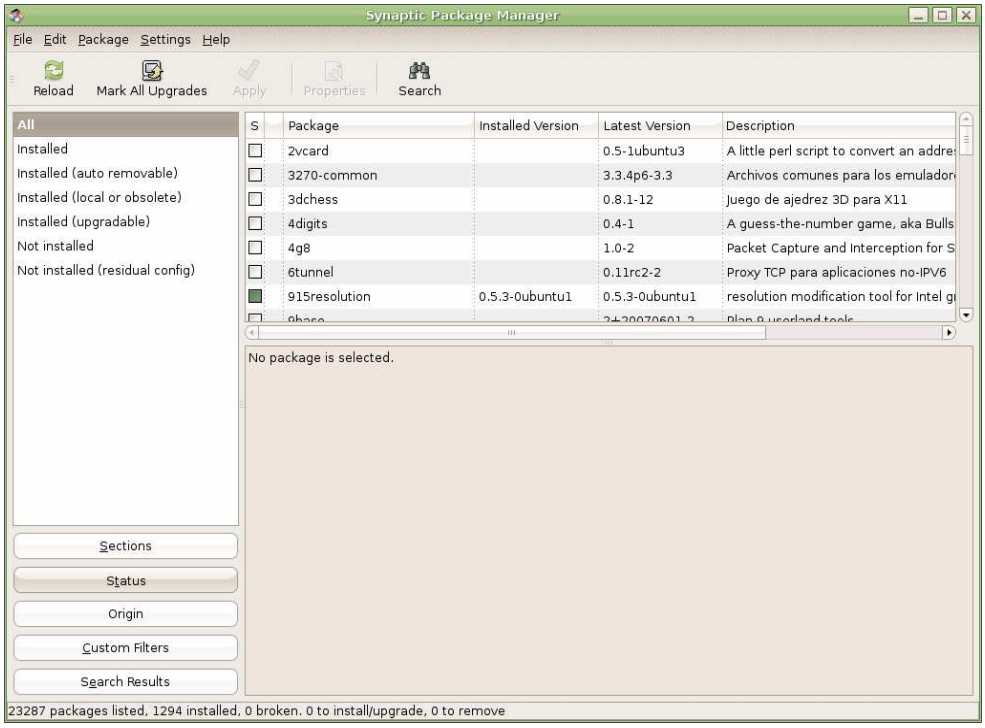
Si no existió ningún inconveniente en el proceso de instalación, al momento de reiniciar el equipo se mostrará la siguiente pantalla, la cual indica que tola la instalación concluyó con éxito y el sistema operativo se iniciará sin ningún inconveniente.

5.4. Instalación de Paquetes para el Sistema de Videoconferencia IPV4 e IPV6

5.4.1. Instalación EKIGA (IPV4)

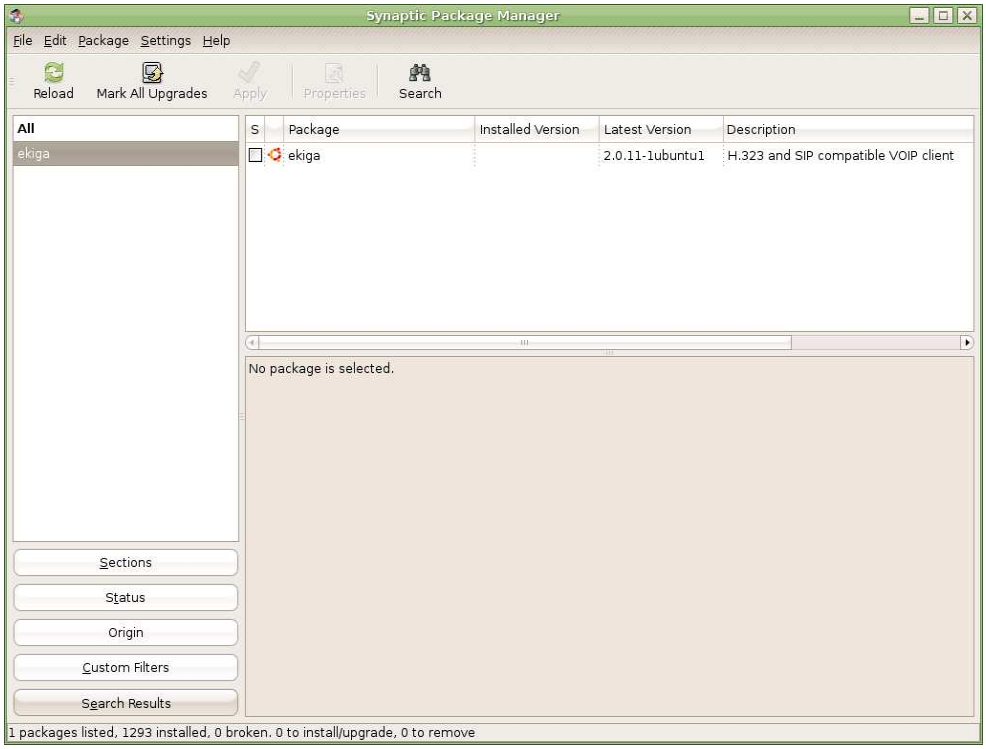
El primer paso para la instalación del aplicativo EKIGA es ubicarnos en el repositorio de paquetes (Synaptic), que viene por defecto en los sistemas operativos utilizados en los equipos clientes del presente proyecto.

La siguiente pantalla muestra la ventana del repositorio de paquetes, la misma sirve para agregar o quitar aplicativos dentro del sistema operativo.

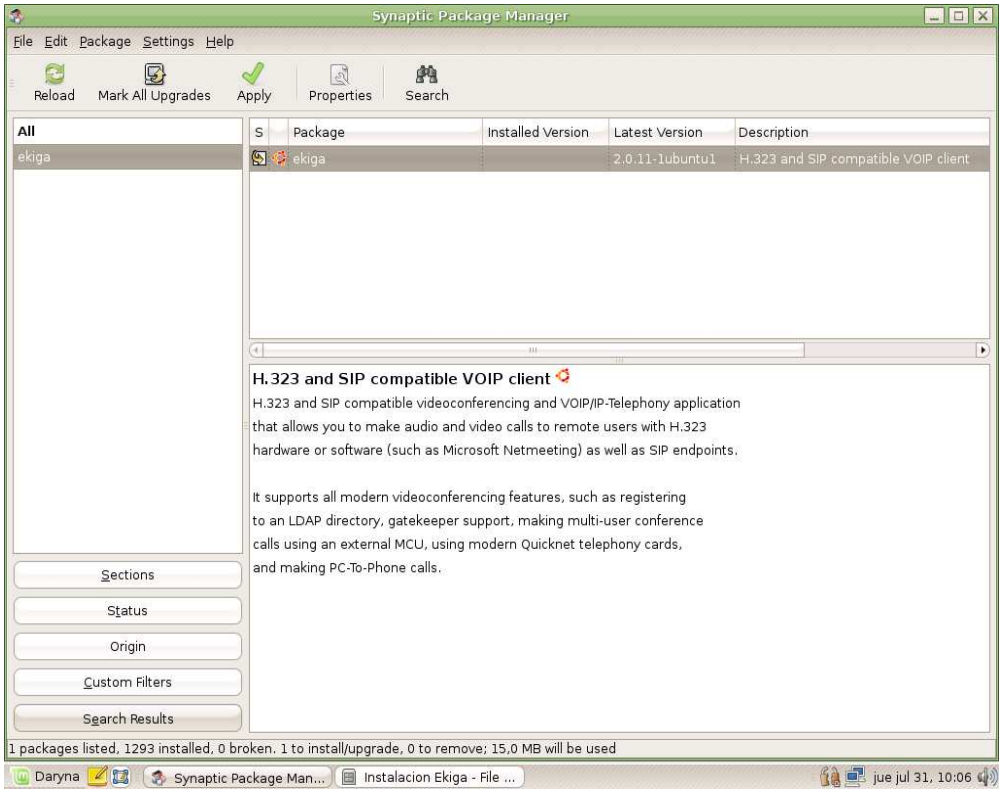


Seguidamente se debe presionar el botón “search”, el cual nos ayudará a encontrar el aplicativo a ser instalado como se muestra en la siguiente figura:

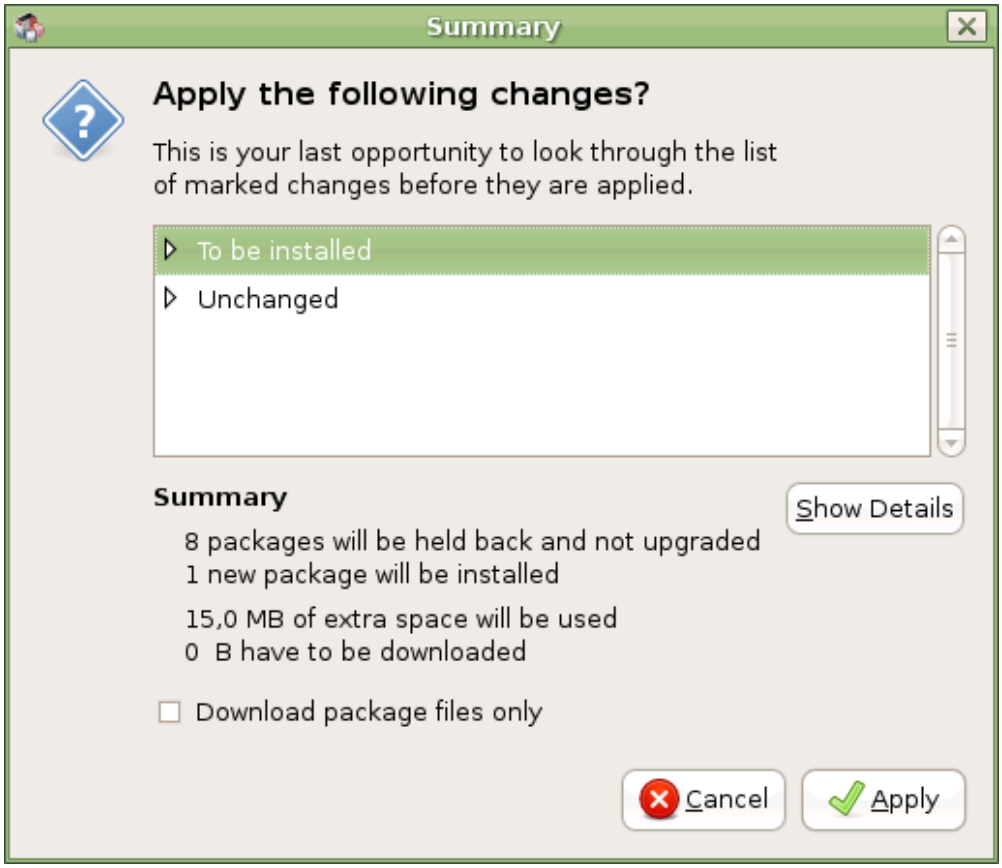
Una vez localizado el paquete a ser instalado, aparecerá lo siguiente:



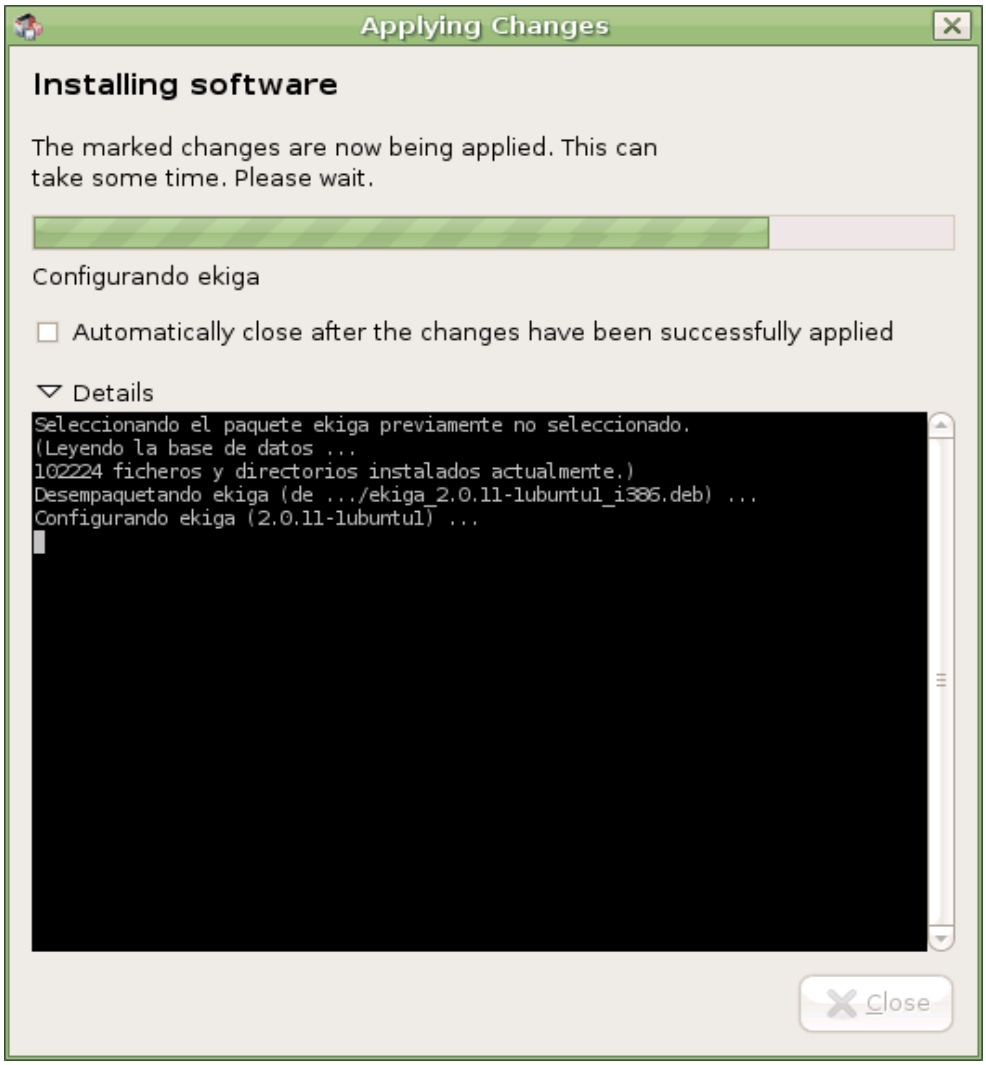
En esta parte se debe marcar el casillero para indicar que el paquete que requiere ser instalado. Una vez ya marcado el casillero aparecerá la siguiente pantalla:



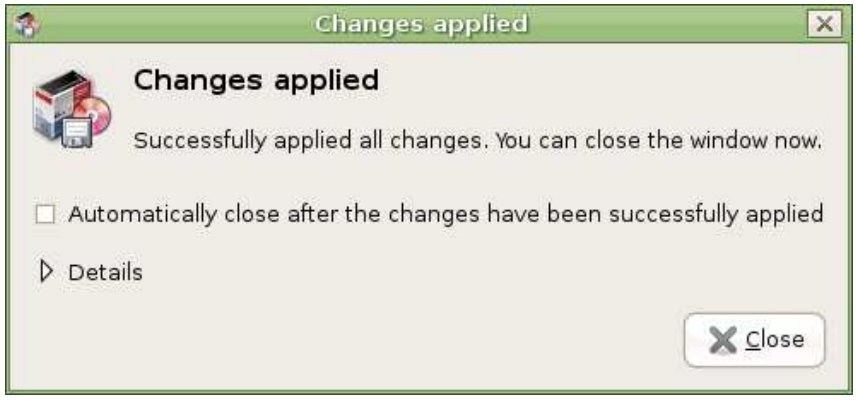
Se debe aplicar los cambios y aparecerá la siguiente pantalla, en la que se indica un resumen de los paquetes y dependencias a ser instalados.



Presionando el botón "**Apply**" comenzará el proceso de instalación como se muestra en la siguiente figura:



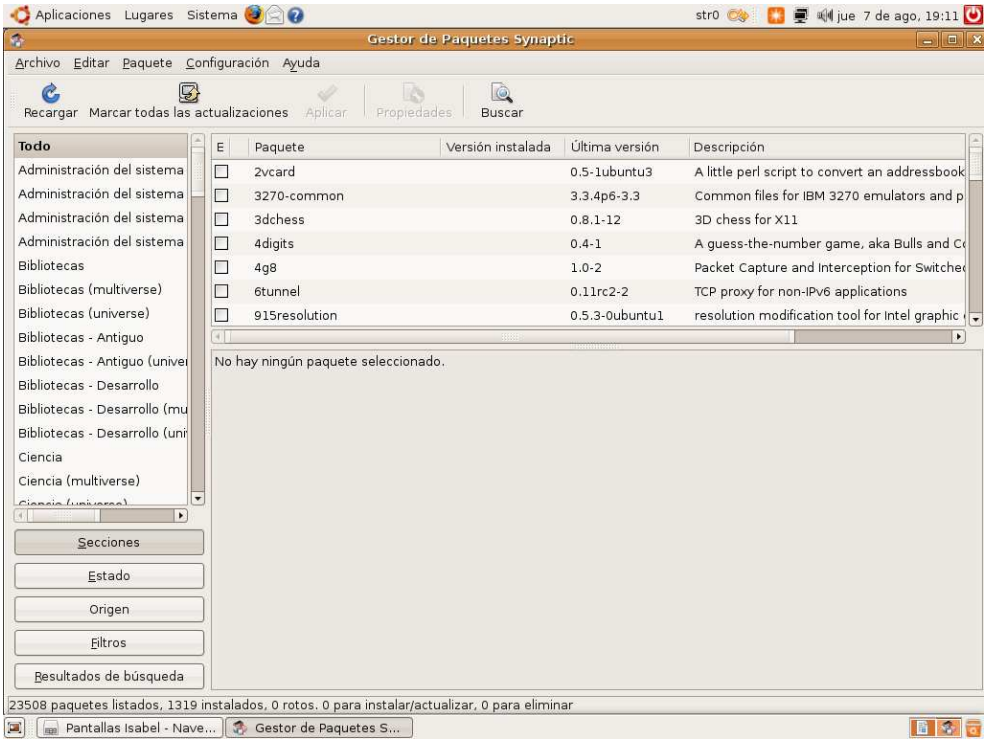
Si el proceso no tiene ningún inconveniente nos aparecerá la siguiente pantalla, la cual nos indica que el proceso de instalación a finalizado con éxito.



5.4.2. Instalación ISABEL (IPV6)

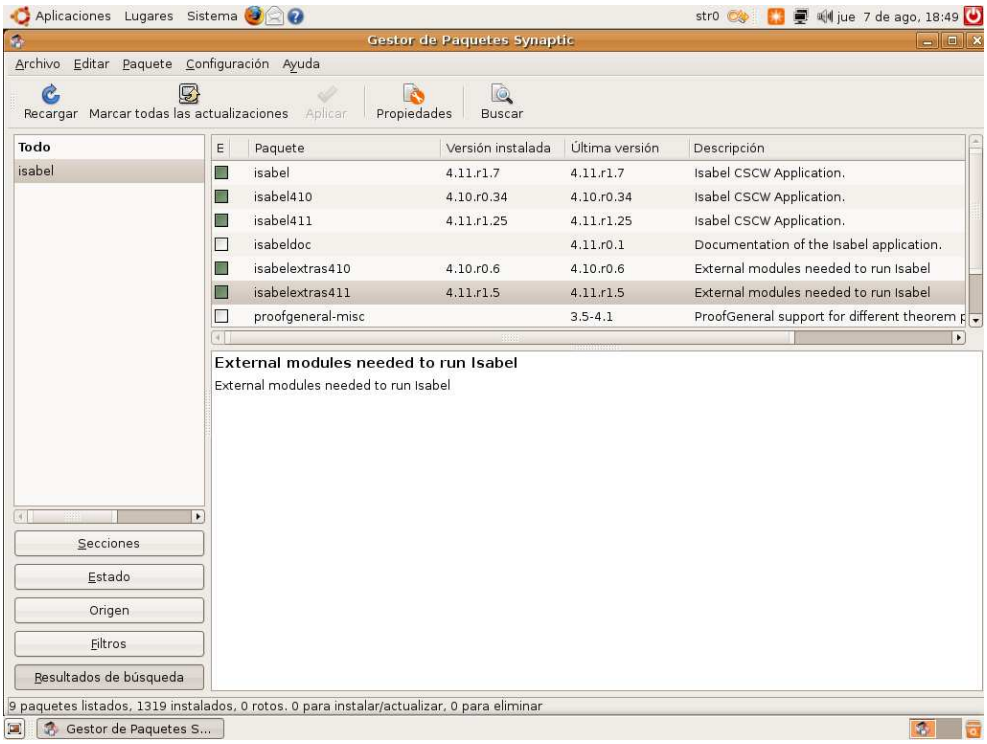
El primer paso para la instalación del aplicativo ISABEL en su versión DEMO es ubicarnos en el repositorio de paquetes (Synaptic), que viene por defecto en los sistemas operativos utilizados en los equipos clientes del presente proyecto.

La siguiente pantalla muestra la ventana del repositorio de paquetes, la misma sirve para agregar o quitar aplicativos dentro del sistema operativo.



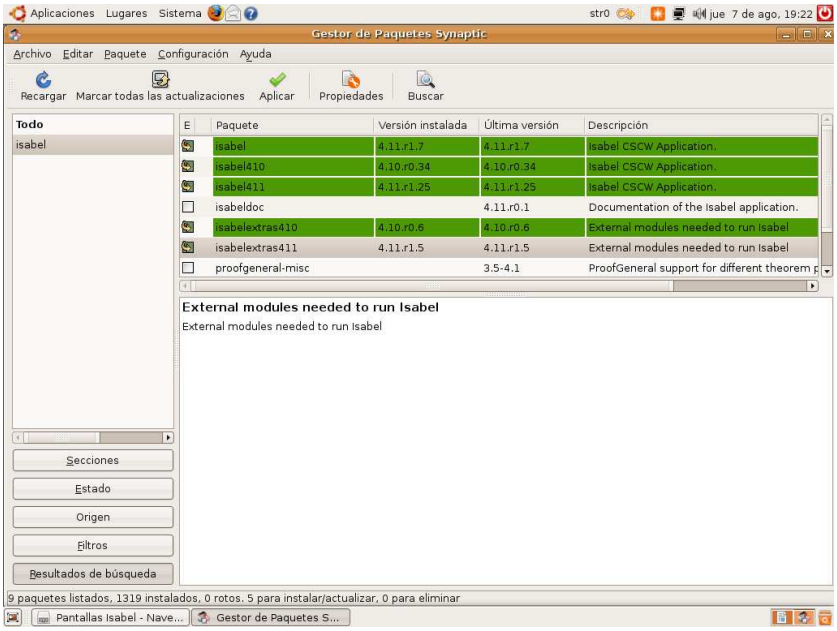
Seguidamente, debemos presentar el botón **Buscar** como se muestra en el siguiente gráfico:

Una vez que concluida la búsqueda dentro del repositorio de paquetes nos aparecerá la siguiente pantalla:

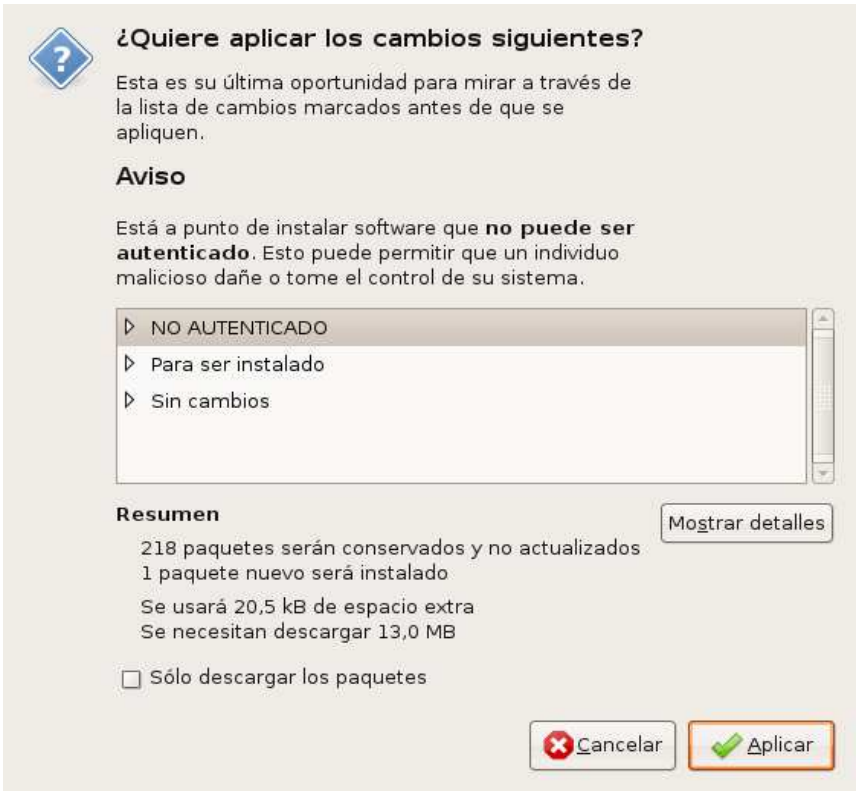


La anterior pantalla nos indica todos los componentes y dependencias que requieren ser instalados para que el aplicativo ISABEL funcione de forma correcta.

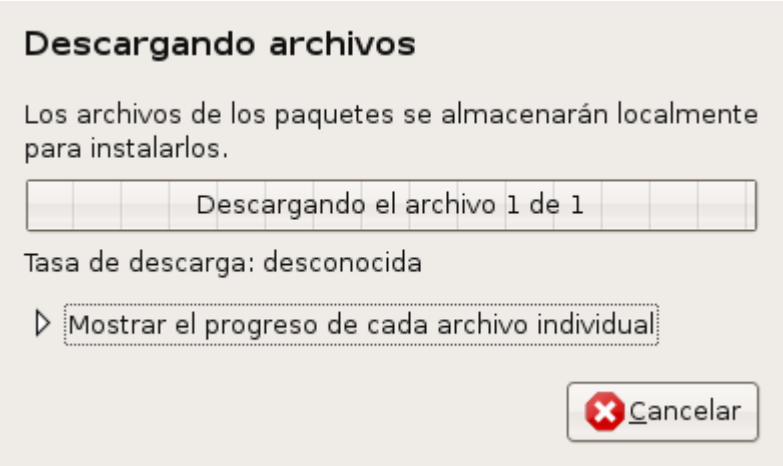
Marcamos los componentes necesarios a ser instalados y nos aparecerá la siguiente pantalla:



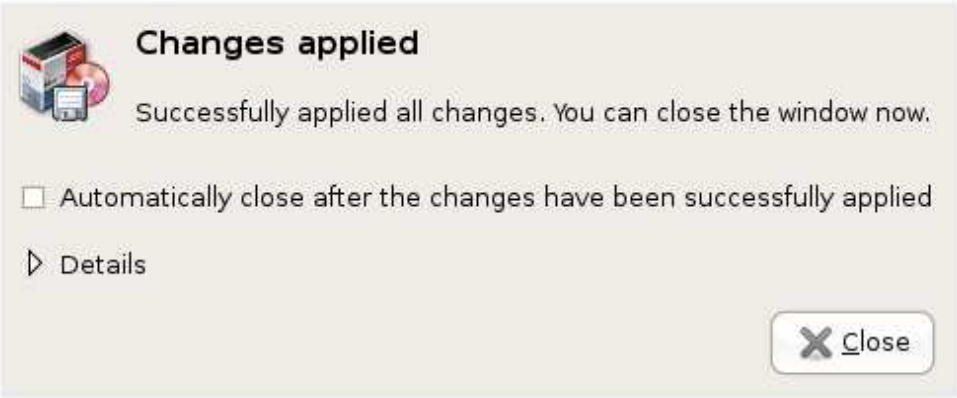
Seguidamente presionamos el botón aplicar cambios, y se desplegará la información de los componentes a ser instalados de la siguiente forma:



Una vez que presionamos el botón **Aplicar** comenzará la instalación del aplicativo.



Si el proceso no tiene ningún inconveniente nos aparecerá la siguiente pantalla, la cual nos indica que el proceso de instalación a finalizado con éxito.



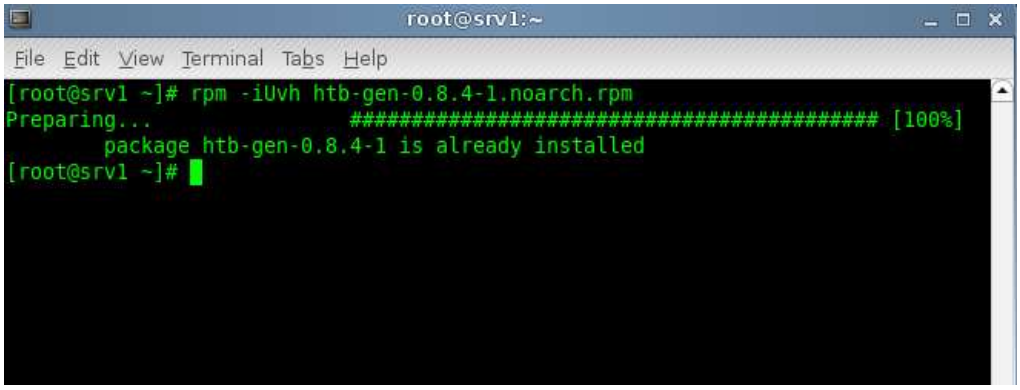
5.5. Instalación de paquete para el control de ancho de banda sobre el protocolo de red IPV4 “HTB-GEN”

A continuación se detallará la instalación del aplicativo HTB-GEN versión 0.8.4, el cual sirve para el control de ancho de banda sobre el protocolo de red IPV4.

Como primer paso se debe descargar el aplicativo **htb-gen** de la página oficial **http://www.praga.org.ar/wacko/DevPraga/htbgen/,** aquí se debe escoger el paquete más apropiado, y se debe digitar el siguiente comando en consola:

 # rpm –iUvh htb-gen-0.8.4-1.noarch.rpm

Con esto comenzará la instalación del paquete como muestra la siguiente pantalla:



Una vez instalado el paquete se procede a realizar la configuración de los archivos **htb-gen.conf** y **htb-gen-rates.conf,** necesarios para el control del ancho de banda.

REFERENCIAS BIBLIOGRÁFICAS

- Ettikan Kandasamy, "IPv6 Dual Stack Transition Technique Performance Analysis: KAME on FreeBSD as the Case", Proceedings MMU International Symposium on Information and Communication Technologies, Malaysia, 5th - 6th Oct., 2000. **http://www.my.apan.net/ipv6/Papers/M2USIC_Perf.PDF**

- "Global IPv6 allocations made by the Regional Internet Registries", **http://www.ripe.net/cgi-bin/ipv6allocs**

- S.Bradner, A.Mankin, "IP: Next Generation (IPng) White Paper Solicitation", RFC 1550, diciembre 1993, **http://www.ietf.org/rfc/rfc1550.txt?number=1550**

- C. Partridge, F. Kastenholz, "Technical Criteria for Choosing IP The Next Generation (IPng)", RFC 1726, diciembre 1994, **http://www.ietf.org/rfc/rfc1726.txt?number=1726**

- S. Bradner, A. Mankin, "The Recommendation for the IP Next Generation Protocol", RFC 1752, enero 1995, **http://www.ietf.org/rfc/rfc1752.txt**

- Hinden, R. and S. Deering, "IP Versión 6 Addressing Architecture", RFC 1884, diciembre 1995, **http://www.ietf.org/rfc/rfc1884.txt**

- Rekhter, Y., and T. Li. "An Architecture for IPv6 Unicast Address Allocation", RFC 1887, diciembre 1995, **http://www.ietf.org/rfc/rfc1887.txt**

- A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (Ipv6) Specification", RFC 2463, diciembre 1998, **http://www.ietf.org/rfc/rfc2463.txt**

- Software de Videoconferencia, Agora System S.A. Universidad Politécnica de Madrid, **http://www.agora-2000.com**

- Portal de consulta y aplicaciones de software libre para Ecuador, ECUALUG, **www.ecualug.org**

- Portal para configuración específica de red para el protocolo IPV6, **http://www.litech.org/radvd/**

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADO POR:

Valenzuela Garzón Gabriel Santiago	Mejía Campoverde Marcos David

COORDINADOR DE LA CARRERA:

Ing. Ramiro Delgado

Sangolquí, 30 de septiembre de 2008