
IMPLEMENTACIÓN DE UNA CENTRAL PBX CON SOPORTE DE H.323 Y SIP, UTILIZANDO ASTERISK Y GNU GATEKEEPER.



Resumen : El objetivo de este documento es presentar el desarrollo paso a paso el proyecto citado, de modo de hacer repetible la experiencia práctica y sirva como instrucción a quienes recién comienzan a introducirse en el mundo de la telefonía IP.

Autor : Aldo Rubio Adasme

1.- Índice

1.- Índice	2
2.- Introducción	3
3.- H.323	4
3.1.- Arquitectura	4
3.2.- Protocolos.	5
3.3.- Modelos de control de llamada.	6
4.- SIP (Session Initiation Protocol)	7
4.1.- Arquitectura	7
5.- Implementación de servicios VoIP.	9
5.1.- Un ejemplo básico con H.323	10
5.1.1.- Instalación de un servidor con GNU Gatekeeper (Ubuntu).	10
5.1.2.- Configuración y ejecución de GNU Gatekeeper.	10
5.1.3.- Instalación y configuración de PC-TONE Softphone.	11
5.1.4.- Registrar PC-TONE Softphone con el gatekeeper	12
5.1.5.- Una llamada entre dos clientes H.323 pasando por el gatekeeper.	13
5.2.- Un ejemplo práctico con Asterisk y SIP.	13
5.2.1.- Instalación de la central PBX.	13
5.2.2.- Configurar terminales SIP (extensiones).	17
5.2.3.- Configurar softphones.	20
5.2.4.- Una llamada SIP a través de Asterisk.	21
5.3.- Integrando Asterisk a la Zona H.323.	21
5.3.1.- Agregando el canal OOH323 a Asterisk.	21
5.3.2.- Configurando el canal OOH323.	22
5.3.3.- Configurando GNU Gatekeeper.	24
5.3.4.- Configurando las extensiones H.323.	25
5.3.5.- Comunicación entre terminales SIP y H.323.	26
6.- Conclusiones.	27
7.- Anexos.	28
7.1.- Configuración avanzada de GNU Gatekeeper.	28
7.1.1.- Parámetros.	28
7.1.2.- Archivo de Configuración.	29
7.1.3.- La herramienta "addpasswd".	32
7.2.- Creación de una cuenta de usuario en Elastix.	32
7.3.- Algunos enlaces de interés.	33
7.3.1.- Configurar Chan Mobile en Elastix	33
7.3.2.- EcuLUG.org. Ecuador Linux User Group.	33
7.3.3.- Trixbox.	34
7.3.4.- Comunidad de usuarios de GNU Gatekeeper.	34
7.3.5.- AsteriskClub.org	34
8.- Referencias.	35

2.- Introducción

En los años 80, cuando la red de telefonía pública estaba ya consolidada como el canal de comunicación más importante y mayoritariamente usado el mundo, internet era algo relativamente nuevo, una red destinada a la comunicación de datos que operaba sobre la arquitectura de la red de telefonía conmutada. Ya desde ese entonces se tenía como desafío la transmisión de información en tiempo real, esencialmente para la transmisión de contenido multimedia (audio/video). Comenzando así a surgir un sinnúmero de protocolos, normas y estándares para este tipo de comunicación.

A mediados de los años 90 las tecnologías estaban lo suficientemente maduras para salir a luz y ser utilizadas en forma masiva, sin embargo, la gran cantidad de protocolos existentes en ese momento, hacen necesaria la creación de una norma que estandarice las videoconferencias. Así, en Junio de 1996 la **ITU-T (International Telecommunication Union, Telecommunication Standardization Sector)** crea la recomendación **H.323** como un estándar para la videoconferencia en redes con calidad de servicio no garantizada.

Con la interoperabilidad con red telefónica conmutada, el uso de la telefonía IP aumentó, principalmente con la finalidad de abaratar costos en empresas.

A fines de los 90 el interés se centró en un protocolo más nuevo que **H.323**, **SIP**, que con su facilidad de implementación y su rápida adaptación de los cambios se ha convertido rápidamente en el protocolo de videoconferencia y telefonía IP más usado en la actualidad.

En este documento se desarrolla una experiencia práctica en la cual se utilizan ambos protocolos. La primera parte está dedicada a **H.323**, en una implementación básica de este utilizando **GNU Gatekeeper**. En la segunda parte se hará algo similar para **SIP**, esta vez usando **Asterisk**. Por último para terminar se integrarán ambas experiencias de modo de comunicar **H.323** y **SIP** dentro de una misma red.

3.- H.323

El estándar **H.323**, presentado por **ITU-T** en 1996, es un conjunto de recomendaciones, las cuales, proporcionan la base para la transmisión de voz, datos y vídeo sobre redes no orientadas a conexión y que no ofrecen un grado de calidad del servicio, como son las basadas en IP, de manera tal que las aplicaciones y productos puedan ínter operar, permitiendo la comunicación entre los usuarios sin que éstos se preocupen por la compatibilidad de sus sistemas.

El estándar contempla el control de la llamada, gestión de la información y ancho de banda para una comunicación punto a punto y multipunto, dentro de la LAN, así como define interfaces entre la LAN y otras redes externas, como puede ser la RDSI. Es una parte de una serie de especificaciones para videoconferencia sobre distintos tipos de redes, que incluyen desde la H.320 a la H.324, estas dos válidas para RTB (Red Telefónica Básica) y RTC (Red Telefónica Conmutada), respectivamente.

Cuando se origina una llamada telefónica sobre Internet, los dos terminales deben negociar cual de los dos ejerce el control, de manera tal que sólo uno de ellos origine los mensajes especiales de control (relación **maestro-esclavo**). Una cuestión importante es que se deben determinar las capacidades de los sistemas, de forma que no se permita la transmisión de datos si no pueden ser gestionados por el receptor.

La principal ventaja de **H.323** es que se trata de un estándar grande, complejo y rígido, que especifica toda la pila de protocolos en cada capa lo que facilita la tarea de interoperabilidad. Fue creado para ser compatible con la red telefónica pública conmutada (**PSTN**) y lo demuestra. Su principal desventaja es que es difícil de adaptar a aplicaciones futuras, es difícilmente escalable y solo funciona con configuraciones de IP fija. A pesar de esto, se niega a desaparecer, ahora en noviembre de 2009 fue aprobada la versión 7 de este protocolo.

3.1.-Arquitectura

Los componentes principales de la arquitectura **H.323** son los siguientes:

Terminal Endpoint (EP):

Son puntos de la red que proveen comunicación en tiempo real bidireccional usando los protocolos definidos por la recomendación **H.323**. Es decir, un terminal puede ser un teléfono IP que usa la tecnología H.323 o un software que emula un teléfono IP con H.323 (softphone).

Gateway (GW):

Es un tipo especial de terminal, que se encarga de comunicar la red **H.323** con otras redes, que pueden ser: **PSTN** (red telefónica pública conmutada), **ISDN** (red digital de servicios integrados), otros protocolos de conferencia (**SIP**, por ejemplo), entre otros. Por lo tanto se trata de una máquina o computadora que posee el hardware y las interfaces necesarias para interconectar las tecnologías que debe interconectar.

Gatekeeper (GK):

Son un elemento opcional en la comunicación entre terminales **H.323**. No obstante, son el elemento más importante de una red **H.323**. Actúan como punto central de todas las llamadas dentro de una zona y proporcionan servicios a los terminales registrados y control de las llamadas. De alguna forma, el gatekeeper **H.323** actúa

como un conmutador virtual. A la colección de todos los Terminales, Gateways y MCU's gestionados por un gatekeeper se la conoce como **Zona H.323**.

Unidad de Control Multipunto (MCU):

Es una máquina dentro de la red que provee la capacidad para que tres o más terminales y gateways puedan participar en una conferencia multipunto.

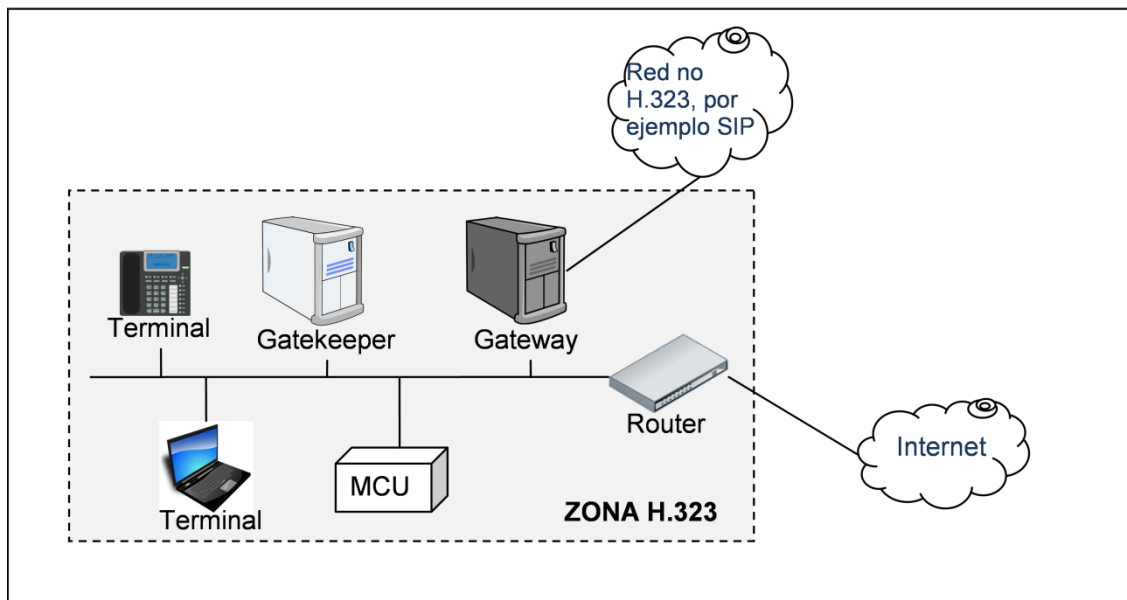


Figura 1. Arquitectura H.323.

3.2.-Protocolos.

Normalmente se suele identificar a **H.323** como un protocolo más de videoconferencia. Sin embargo, en realidad **H.323** es una recomendación que involucra un conjunto de protocolos, arquitecturas y estándares. Esencialmente son 4 los protocolos principales que participan en una llamada **H.323**, los cuales se describen a continuación:

RAS (Registration Admission and Status):

Se utiliza para llevar el registro, admisión, cambios de ancho de banda y mensajes de estado entre los equipos terminales (EP's y GW's) y el gatekeeper.

Q.931:

Protocolo de señalización para configuración de llamada y desmontaje. Es una variación del protocolo **Q.931** definido para **PSTN**.

H.245 (MeGaCo, Media Gateway Control):

Se utiliza para el control de la conexión, permitiendo que dos terminales puedan negociar las capacidades de procesamiento de medios, tales como los codecs de audio/video a usar en cada uno de los canales.

RTP (Real-Time Transmission Protocol):

Protocolo para el transporte de paquetes en tiempo real. Es el encargado de hacer llegar la voz desde un punto hasta otro.

3.3.-Modelos de control de llamada.

Dependiendo de la cantidad de elementos en la red, y de la existencia de gatekeepers, existen dos modelos soportados por el protocolo **H.323**, el de llamada directa (**direct call**) y el de llamada enrutada por gatekeeper (**GK-routed call**).

Modelo de llamada directa (direct call model):

Consiste en que los terminales involucrados en la llamada se comunican directamente utilizando para ello los protocolos **Q.931**, **H.245** y **RTP**. El gatekeeper es opcional, solo es necesario cuando los terminales desconocen sus direcciones. En este caso el gatekeeper hará de mediador antes que los terminales se comuniquen. La comunicación entre los terminales y el gatekeeper se efectúa mediante el protocolo **RAS**.

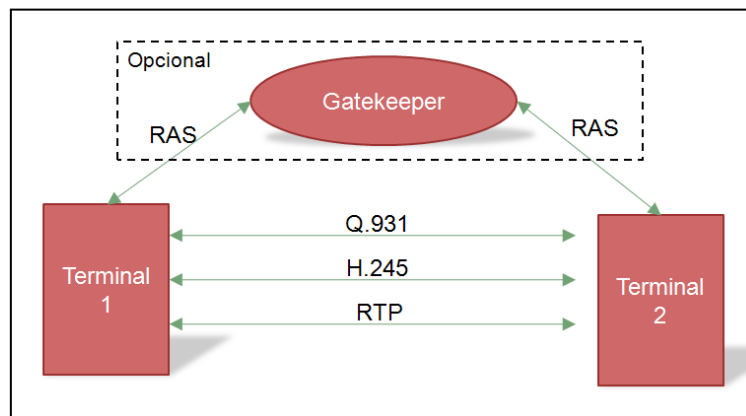


Figura 2. Modelo de llamada directa.

Modelo de llamada enrutada por gatekeeper (GK-routed call model):

En este modelo, todo el proceso de señalización se realiza a través del gatekeeper, es decir, la comunicación en los protocolos **RAS**, **Q.931** y **H.245** se realiza usando el gatekeeper como intermediario. El único momento en el cual los terminales están comunicados directamente es durante la llamada, en el momento que los terminales están hablando usando **RTP**.

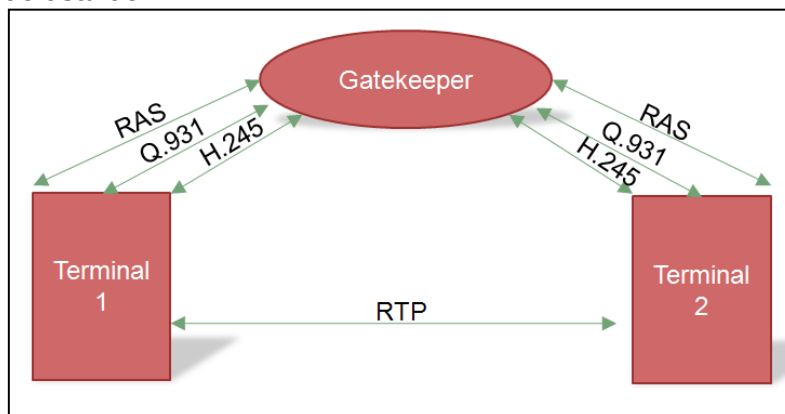


Figura 3. Modelo de llamada enrutada por gatekeeper.

4.- SIP (Session Initiation Protocol)

SIP es un protocolo de señalización simple utilizado para telefonía y videoconferencia por Internet. Basado en el Protocolo de Transporte de correo simple (**SMTP**) y en el Protocolo de Transferencia Hipertexto (**HTTP**), fue desarrollado dentro del grupo de trabajo de **Control de Sesión Multimedia Multipartidaria (MMUSIC)**. **SIP** especifica procedimientos para Telefonía, Videoconferencia y otras conexiones multimedia sobre Internet. **SIP** es un protocolo de la capa de aplicación independiente de los protocolos de paquetes subyacentes (TCP, UDP, ATM, X.25). **SIP** está basado en una arquitectura cliente servidor en la cual los clientes inician las llamadas y los servidores responden las llamadas. Es un protocolo abierto basado en estándares, **SIP** es ampliamente soportado y no es dependiente de un solo fabricante de equipos.

SIP es un protocolo más nuevo que **H.323** y no tiene madurez y soporte industrial al mismo tiempo. Sin embargo, por su simplicidad, escalabilidad, modularidad y comodidad con la cual integra con otras aplicaciones, este protocolo es atractivo para uso en arquitecturas de voz packetizada. **SIP** puede establecer sesiones de dos partes (llamadas ordinarias), de múltiples partes (en donde todos pueden oír y hablar) y de multidifusión (un emisor, muchos receptores). Las sesiones pueden contener audio, video o datos. **SIP** solo maneja establecimiento, manejo y terminación de sesiones. Para el transporte de datos, se utilizan otros protocolos, como **RTP/RTCP**. **SIP** es un protocolo de capa de aplicación y puede ejecutarse sobre UDP o TCP.

Su principal ventaja es su escalabilidad, modularidad y compatibilidad con otros protocolos de videoconferencia. Su principal desventaja es que goza de una madurez frente a **H.323**, es menos robusto y no proporciona un control de “piso” dentro de una sesión.

4.1.-Arquitectura

Para implementar los servicios proporcionados por **SIP**, se requieren una serie de componentes, los cuales se clasifican principalmente en agentes del usuario (**UA**) y **servidores**.

User Agent (UA):

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

Los servidores SIP:

Pueden ser de tres tipos:

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

varias (forking), con la finalidad de la localización en paralelo de la llamada y obtener la mejor respuesta para enviarla al usuario que realizó la llamada.

- **Stateless Proxy:** no mantienen el estado de las transacciones durante el procesamiento de las peticiones, únicamente reenvían mensajes.
- **Registrar Server:** es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla.
- **Redirect Server:** es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor.

La división de estos servidores es conceptual, cualquiera de ellos puede estar físicamente una única máquina, la división de éstos puede ser por motivos de escalabilidad y rendimiento.

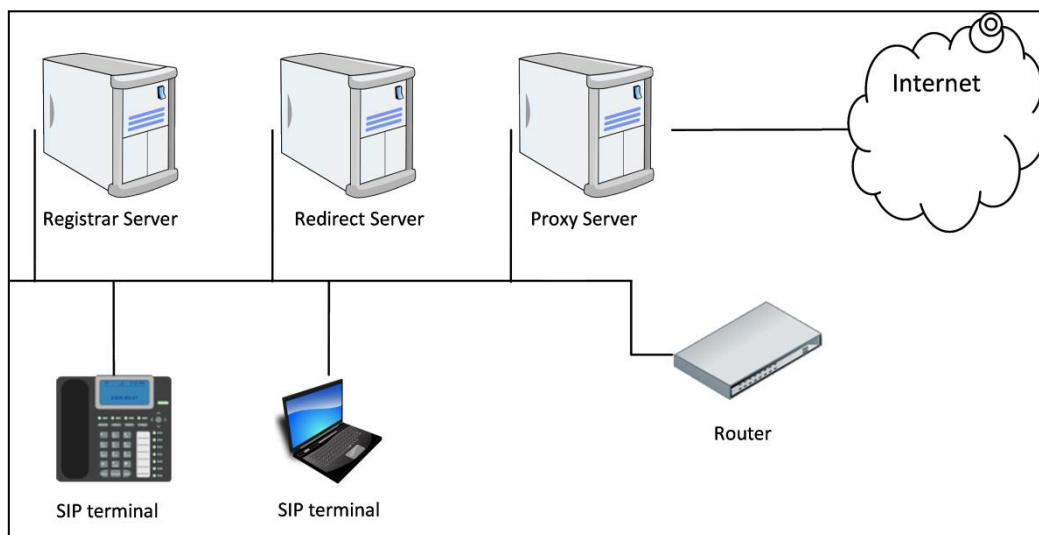


Figura 4. Arquitectura SIP.

5.- Implementación de servicios VoIP.

En esta sección se realiza la implementación de la parte práctica la cual consiste en crear una red de máquinas y terminales usando ambas tecnologías, **H.323** y **SIP**, logrando la comunicación entre estos. La primera parte consta de una implementación básica de una **Zona H.323** que constará de un gatekeeper y varios terminales. Posteriormente, en la segunda parte, se implementará un central telefónica **Asterisk** en la misma red en donde está implementada la **Zona H.323**, aunque en forma totalmente independiente, con la finalidad de entablar comunicación entre distintos terminales **SIP**. Finalmente, con pocos cambios, el trabajo realizado en ambas partes será integrado mediante la configuración de **Asterisk** para que se conecte como gateway con el gatekeeper, permitiendo que terminales **H.323** y **SIP** hablen entre sí.

Para llevar a cabo esta parte son necesarios algunos componentes de software y hardware que se detallan a continuación.

Para la **Zona H.323** se requiere:

Hardware:

- Una máquina real o virtual con sistema operativo 8.04 o superior, para hacer de gatekeeper usando el software **GNU Gatekeeper**.
- A lo menos, dos máquinas reales que harán de clientes o endpoints. Por limitaciones del softphone estas máquinas deben usar el sistema operativo Microsoft Windows XP. Deben contar con una tarjeta de sonido full-duplex (que sea capaz de grabar y reproducir sonido simultáneamente), audífonos o parlantes y micrófono.
- Una red que interconecte los elementos mencionados, ya sea mediante un switch, un router o similar.

Software:

- **GNU Gatekeeper**, en su versión para Ubuntu Linux, instalable desde los repositorios preconfigurados en la distribución.
- Softphone compatible con **H.323**, estos son un tanto difíciles de encontrar, uno de los pocos que funciona correctamente es **PC-Tone**, para Windows XP, cuya versión de pruebas se puede encontrar en: http://www.pc-tone.com/en/support/support_demo.htm

Para la red **SIP** se requiere:

Hardware:

- Una máquina virtual, para hacer de central telefónica usando el software **Asterisk** en una distribución especialmente acondicionada para ello llamada **Elastix**. Esta máquina debe tener al menos 256 MB de RAM.
- A lo menos, dos máquinas reales que harán de clientes. Pueden usar cualquier sistema operativo compatible con el softphone (en el caso de **X-Lite**, hay versiones para Windows, Linux y MacOS). Dado que se trata de programas distintos, pueden coexistir en una misma máquina los softphone para **SIP** y para **H.323**. Deben contar con una tarjeta de sonido full-duplex (que sea capaz de grabar y reproducir sonido simultáneamente), audífonos o parlantes y micrófono.
- Una red, la misma en donde estará la **Zona H.323** para integrar ambas tecnologías en la última parte de esta experiencia.

Software:

- **Elastix**, una distribución de GNU/Linux basada en **Centos 5**, la cual trae, entre otras cosas, **Asterisk** y **FreePBX** (web GUI para **Asterisk**). Tiene la ventaja de estar bajo licencia GPL y contar con gran cantidad de documentación. Una imagen ISO puede ser descargada gratuitamente desde: <http://www.elastix.org/content/view/137/60/lang.es/>
- **X-Lite**, un softphone **SIP** gratuito, existen versiones para Windows, Linux y MacOS. Puede ser descargado desde: <http://www.counterpath.com/x-lite.html>

5.1.-Un ejemplo básico con H.323

A continuación se muestran los pasos necesarios para implementar **GNU Gatekeeper** que definirá una **Zona H.323** junto a los terminales o endpoints, de modo de lograr que estos se puedan comunicar entre ellos.

5.1.1.- Instalación de un servidor con GNU Gatekeeper (Ubuntu).

La instalación de **GNU Gatekeeper** en una distribución Ubuntu (o similar) es muy sencilla y carece de todos los inconvenientes presentes en la compilación de los paquetes para otras distribuciones.

Para efectuar la instalación, usando el gestor de paquetes Synaptic se debe buscar e instalar el paquete **gnugk**.

Como siempre existe la alternativa de instalarlo usando la consola, para ello basta ejecutar la siguiente línea:

```
$sudo apt-get install gnugk
```

Se debe tomar nota de la dirección IP de la máquina a usar como Gatekeeper, ya que se necesita para configurar los otros componentes.

5.1.2.- Configuración y ejecución de GNU Gatekeeper.

El comportamiento del gatekeeper está completamente determinado por los parámetros de la línea de comandos y del archivo de configuración. Algunas opciones de la línea de comandos pueden sustituir a opciones del archivo de configuración. Por ejemplo, la opción `-l` sustituye al atributo `TimeToLive` del archivo de configuración. Para más información sobre la configuración de **GNU Gatekeeper**, consultar el anexo, o dirigirse a la documentación en la página oficial. <http://www.gnugk.org/>.

En general para este ejemplo se usará la siguiente configuración, mediante parámetros:

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

```
$gnugk -tt
```

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

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

```
$gnugk -rr -tt
```

Usando `-rr`, se le dice al gatekeeper que debe enrutar los canales **Q.931** y **H.245**, lo cual corresponde al modo enrutado teórico. Es posible enrutar solamente el canal **Q.931** usando `-r` en lugar de `-rr`.

5.1.3.- Instalación y configuración de PC-TONE Softphone.

La instalación de este software en Windows es tan sencilla como cualquier software para este sistema operativo, tan solo basta ejecutar el archivo descargado, seguir los pasos y listo. Hay que tener cuidado, una librería de gran importancia para el programa puede ser reconocida falsamente como virus, por lo cual es recomendable añadir una excepción para evitar estropear este programa.

Una vez instalado y ejecutado, el aspecto del software es el siguiente:

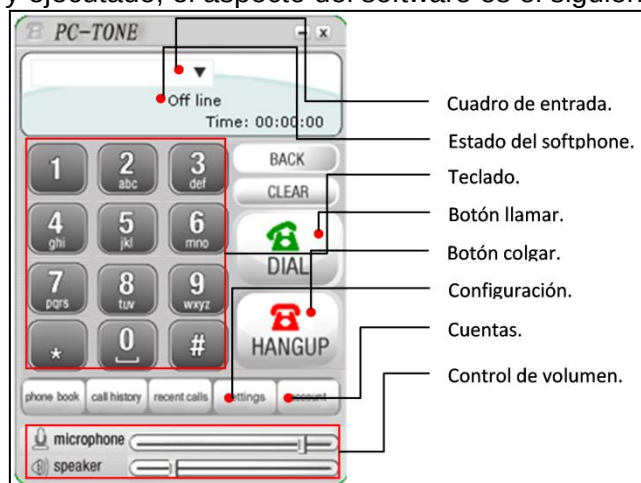


Figura 5. Elementos principales de PC-Tone Softphone.

- **Cuadro de entrada:** Permite ingresar los números cuando se realiza una llamada. Además de números se pueden usar alias.
- **Estado del softphone:** Indica si el software está conectado con el gatekeeper, si hay problemas de conexión, etc.
- **Teclado:** Permite introducir números, además emite tonos, por lo cual puede ser usado para servicios que responden a tonos.
- **Botón llamar:** Al presionarlo, el teléfono intenta llamar al número o alias ingresado en cuadro de entrada.
- **Botón colgar:** Permite rechazar una llamada o finalizarla.
- **Configuración:** Muestra la pantalla de configuración en donde se configuran los dispositivos de entrada/salida de sonido, el codec preferido, el tamaño del buffer de jitter, además de los puertos de red y los modos a usar.

- **Cuentas:** Permite configurar las cuentas **H.323**, es decir, permite especificar la dirección del gatekeeper, nombre (**H323ID**, o alias h.323), alias (E164), y contraseña de autenticación.
- **Control de volumen:** Permite ajustar el volumen del micrófono y de los parlantes.

Con la configuración por defecto, el teléfono debiera estar en condiciones de funcionar correctamente, y faltaría solamente configurar las cuentas, pero es recomendable asegurarse de que en el panel de configuración (Settings), no esté activado **H.245 tunneling** ya que esta opción se utiliza para una determinada configuración del gatekeeper que no será utilizada en ninguno de los ejemplos aquí descritos. También es importante chequear en esta pantalla que los dispositivos de audio (entrada y salida) estén correctamente configurados. No es necesario, especificar un codec ya que mediante el protocolo **H.245** los terminales negocian el codec, aunque si en la red hay presencia de un gateway que solo soporta un determinado codec, es importante especificarlo para evitar problemas.

5.1.4.- Registrar PC-TONE Softphone con el gatekeeper

En esta parte se deben configurar al menos 2 clientes, o usuarios para que se conecten con el gatekeeper. Como el gatekeeper está configurado para aceptar cualquier usuario y no solicitar contraseña, entonces no es necesario configurar el gatekeeper para que reconosca a los usuarios, aunque se debe ser cuidadoso en no repetir los alias (**H323ID**) ya que el gatekeeper rechazará cualquier endpoint repetido.

Accediendo al menú Cuentas (Accounts) en **PC-Tone**, se debe ingresar los siguientes datos:

Registration Port: Puerto que usará para las comunicaciones. No es necesario cambiar el valor por defecto (1719), salvo que haya conflictos.

ServerIP: Dirección IP del gatekeeper.

H323ID (Name): Nombre único o alias **H.323** del terminal. Debe ser único en la **Zona H.323**. Por ejemplo: juan, diego, oficina, recepción, etc.

E164 (Alias): Dejar en blanco, no se usará en este ejemplo.

Password: Aunque el gatekeeper no lo tomará en cuenta con la configuración actual, no debe dejarse en blanco. Usar cualquier valor.

Para terminar, pulsar OK.

Ahora el teléfono se intentará conectar al gatekeeper, si es aceptado el estado del teléfono cambiará a "Logged in".

Cuando un usuario se intenta registrar con el gatekeeper, la salida de **gnugk** es similar a esta:

```
2009/11/08 14:00:25.991 2 RasSrv.cxx(191) RAS Read from 192.168.0.101:1071
2009/11/08 14:00:25.991 2 RasSrv.cxx(242) RAS Received GRQ
2009/11/08 14:00:25.991 1 RasSrv.cxx(370) RAS GRQ Received
2009/11/08 14:00:25.992 2 RasSrv.cxx(415) GCF|192.168.0.101|juan|terminal;
2009/11/08 14:00:25.992 2 RasSrv.cxx(254) RAS Send GCF to 192.168.0.101:1071
2009/11/08 14:00:25.997 2 RasSrv.cxx(191) RAS Read from 192.168.0.101:1071
2009/11/08 14:00:25.997 2 RasSrv.cxx(242) RAS Received RRQ
2009/11/08 14:00:25.998 1 RasSrv.cxx(370) RAS RRQ Received
2009/11/08 14:00:25.998 1 RasTbl.cxx(88) New EP|192.168.0.101:1732|juan:h323_ID|terminal|9272_endp
2009/11/08 14:00:25.999 2 RasSrv.cxx(415) RCF|192.168.0.101:1732|juan:h323_ID|terminal|9272_endp;
2009/11/08 14:00:25.999 2 RasSrv.cxx(254) RAS Send RCF to 192.168.0.2:1071
```

Aquí se observa que el gatekeeper recibe un mensaje **GRQ (Gatekeeper Request)** desde la dirección del cliente 192.168.0.101, tras lo cual el gatekeeper responde con un **GCF (Gatekeeper Confirm)**. Luego, el gatekeeper recibe desde la misma dirección un **RRQ (Registration Request)** a lo cual el gatekeeper accede registrándolo como un endpoint (**EP**) del tipo terminal, usando el **H323ID** proporcionado por este. Para finalizar el gatekeeper manda un **RCF (Registration Confirm)**. Todos estos mensajes se efectúan usando el protocolo **RAS**.

Se debe repetir este procedimiento para registrar al menos un segundo cliente, antes de seguir con el ejemplo.

5.1.5.- Una llamada entre dos clientes H.323 pasando por el gatekeeper.

Si todos los pasos anteriores fueron efectuados correctamente, los terminales deberían estar listos para llamarse entre sí y comenzar a hablar. Para llamar desde un terminal a otro, basta con escribir el **H323ID** del terminal al que se desea llamar (por ejemplo **diego**), en el cuadro de entrada de **PC-Tone** y pulsar el botón de llamada. Tras unos segundos, el teléfono destinatario (en este caso **diego**) comenzará a sonar, y tras aceptar la llamada será posible hablar.

5.2.-Un ejemplo práctico con Asterisk y SIP.

Asterisk es un software de código abierto **PBX** creado por la empresa **DIGIUM**. Proporciona los servicios, características y funcionalidad de una **PBX** (o central telefónica) tradicional. Implementa **VoIP** en varios protocolos y puede interoperar con equipos de telefonía **PSTN** utilizando hardware de fácil instalación y configuración.

Adicionalmente Asterisk proporciona servicios de voicemail (correo de voz) con directorios, conferencias, respuesta de voz interactiva, y llamadas en espera. Soporta varios protocolos, tales como: **SIP**, **ZAP**, **IAX** y **H.323**.

En este ejemplo se usará **Asterisk** para proporcionar los servicios necesarios para efectuar llamadas entre terminales **SIP**, en donde la máquina **Asterisk** hará las veces de servidor.

Sin embargo, **Asterisk** es un tanto difícil de instalar y configurar, razón por la cual se usará **Elastix**, una distribución de GNU/Linux pre-configurada para el uso de **Asterisk** y que además implementa **FreePBX**, software que proporciona una interfaz web para administrar y configurar **Asterisk**.

5.2.1.- Instalación de la central PBX.

En esta parte se detalla el proceso de instalación de **Elastix**, cuya instalación se asemeja a la instalación de Centos en modo texto, aunque de forma algo más simplificada ya que como no trae todos los paquetes de Centos, por lo cual, hay varios pasos de la instalación de Centos que no están presentes en la instalación de **Elastix**. Es necesario usar una máquina virtual donde montar la imagen ISO, ya que **Elastix** carece de una herramienta para el particionamiento del disco, y está preparada para borrar todo el contenido del disco duro durante su instalación ocupando todo el espacio disponible. Sin embargo existe además la herramienta **Centos2Elastix**, la cual se puede descargar desde la misma página, y permite instalar **Elastix** sobre

Centos, lo cual es la mejor alternativa si se desea instalar **Elastix** en una máquina real.

Tras montar la imagen en la unidad de la máquina virtual y arrancar el sistema desde el CD se mostrará una pantalla como la siguiente:



Figura 6. Pantalla de arranque del disco de Elastix.

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

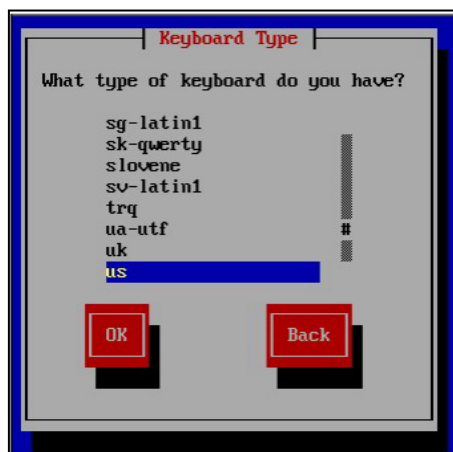


Figura 7. Configuración del tipo de teclado.

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

Del mismo modo se debe seleccionar la zona horaria:



Figura 8. Configuración de zona horaria.

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

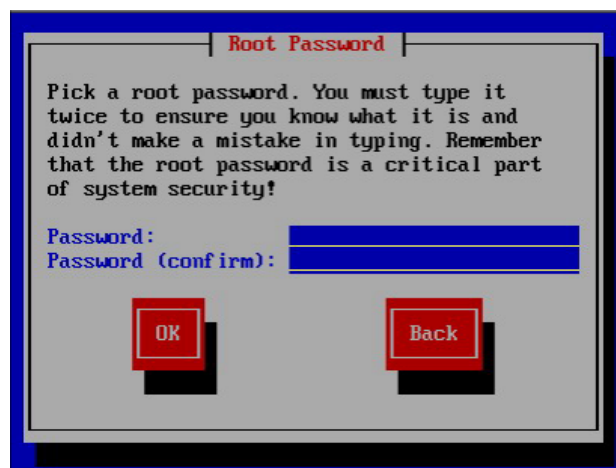


Figura 9. Configuración de contraseña del root.

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

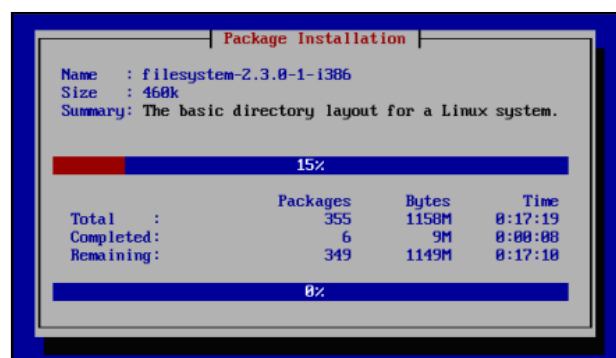


Figura 10. Instalación de paquetes.

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

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

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

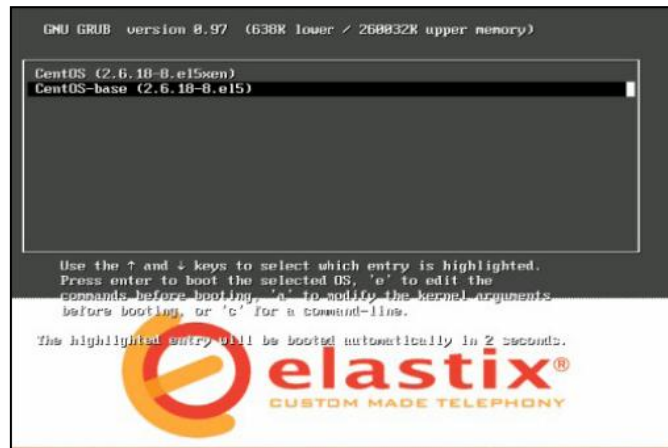


Figura 11. Pantalla de arranque de Elastix.

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



Figura 12. Consola de Elastix.

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

Para ello se debe usar el comando:

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

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

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

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

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

Y para instalar esta herramienta:

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

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

```
$service network restart
```

Por último, se debe chequear la configuración IP usando:

```
$ifconfig
```

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

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

5.2.2.- Configurar terminales SIP (extensiones).

Para configurar un nuevo terminal **SIP** se debe entrar a la interfaz web del sistema usando la dirección <http://<direccion-IP-de-Elastix>>, como se mencionó anteriormente. Se debe ingresar usando la cuenta de administrador, cuyo nombre de usuario es **admin** y la contraseña es **palosanto**. Esta y otras contraseñas se pueden encontrar y modificar en el archivo **/etc/ampportal.conf**.



Figura 13. Interfaz web de Elastix.

Una vez adentro, la primera pantalla en mostrarse es la pantalla de información del sistema, aunque en otras versiones puede mostrarse el dashboard. Independientemente de eso, se puede acceder a ambas pantallas usando el menú superior. Otra cosa que se puede hacer, opcionalmente, es dirigirse a **Preferences** y cambiar el idioma de la interfaz al español.

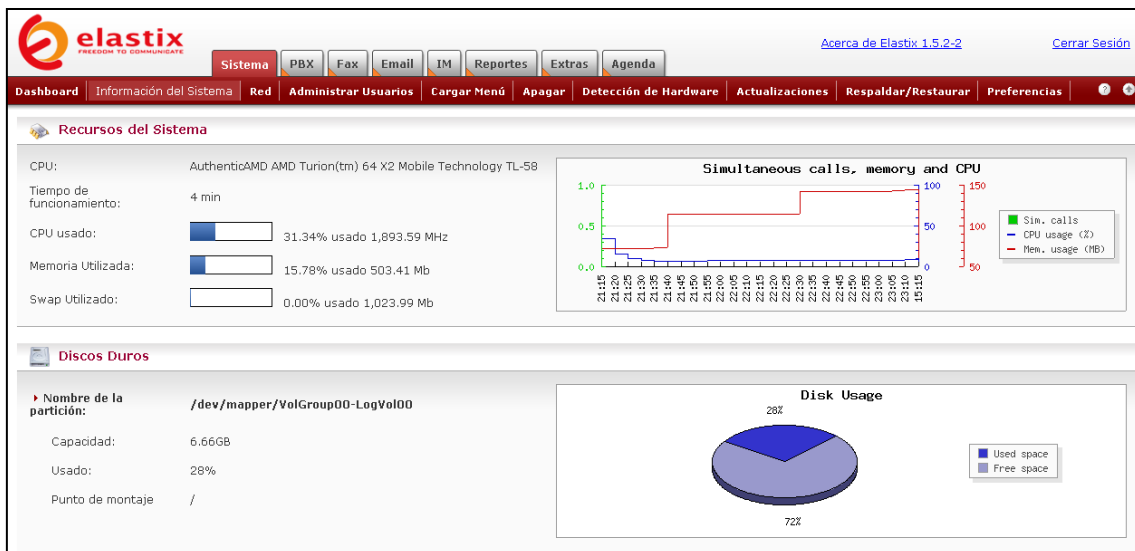


Figura 14. Pantalla de información del sistema.

Ahora llega el momento de agregar los terminales **SIP**. Para esto hay que ir, a través del menú superior a la sección **PBX**, y dentro de ésta a **Configuración PBX**. En menú vertical, a la izquierda de la pantalla se debe seleccionar **Extensiones**. También es posible, llegar hasta aquí usando el acceso directo situado a la derecha de la pantalla. Cualquiera sea el camino, la pantalla que se mostrará es la siguiente:

Figura 15. Menú para añadir una nueva extensión.

Aquí, se debe seleccionar el tipo de extensión (o terminal) que se desea configurar, los tipos disponibles son **SIP**, **IAX2** y **ZAP**. Además de **Custom** que permite configurar otro tipo de terminales que no están completamente soportados por esta versión, como lo es **H.323** entre otros protocolos.

En este caso, ya que se desea trabajar con **SIP**, se debe seleccionar **Generic SIP Device** y pulsar el botón **Submit** para avanzar a la siguiente pantalla. Se mostrará un formulario, algo extenso, donde se ingresan los datos de la extensión. No es necesario llenar por completo este formulario. A continuación, el significado de algunos de estos datos:

User Extension: (obligatorio). **Asterisk**, como una central telefónica, requiere que todos los terminales posean un número único (extensión), para poder identificar a cada terminal y permitir que todos los protocolos se logren comunicas usando como única

sintaxis el número de extensión. En otras palabras, este dato es el número de teléfono que tendrá el terminal dentro de la red de **Asterisk**.

Display Name: Nombre a mostrar en pantalla, para el terminal. Es útil para reconocer a quién pertenece cada número. Por ejemplo: recepción (lo cual hace referencia al terminal usado en la oficina de recepción), juan (el terminal de Juan), etc.

SIP Alias: Similar al anterior, con la particularidad de que este será reconocido por los dispositivos **SIP**.

Secret: Código secreto o contraseña para que el terminal se registre con **Asterisk**. La mayoría de los teléfonos IP viene con un secret de fábrica, por lo cual se debe considerar en el caso de que el terminal que se intenta configurar sea un teléfono IP. En el caso de los softphones, este número puede ser usado como una contraseña.

Language Code: Código de idioma, indica el idioma en el cual el sistema debe transmitir los mensajes hacia ese terminal (por ejemplo, el idioma en el cual hablará la contestadora). Si se deja en blanco, el sistema usará **en** (english), para dejarlo en español usar **es**.

Record Incoming: Indica si se permite grabar las llamadas entrantes. Y si esto se hace automáticamente y bajo demanda.

Record Outgoing: Igual que la opción anterior, esta vez para llamadas salientes.

Voicemail & Directory – Status: Permite activar correo de voz para la extensión señalada.

Voicemail password: Contraseña del correo de voz. Importante si se quiere resguardar la privacidad del usuario.

Para esta primera prueba, se usarán solo los siguientes datos:

- **User Extensión:** Usar un número de al menos tres dígitos, el primero de estos fijo de modo de usarlo de prefijo para toda la red y evitar confusiones. Por ejemplo, hacer que todas las extensiones comiencen sean números de 4 cifras que comienzan con un 5 (5520, 5504, etc).
- **Display Name:** Por ejemplo: luis, juan, gerente, etc.
- **SIP Alias:** Usar el mismo que Display Name.
- **Secret:** Alguna contraseña numérica.
- **Language Code:** es
- **Voicemail & Directory – Status:** Enabled

Tras ingresar, los datos se pulsa el botón **Submit**, con lo cual la extensión quedará registrada y al lado derecho de la pantalla aparecerá un acceso directo a modo de lista de extensiones, a través del cual se podrá ver la configuración de esa extensión, editarla o eliminarla.

Este procedimiento se debe repetir hasta ingresar todas las extensiones que se desee. Para este ejemplo, se requieren al menos dos extensiones.

Falta hacer una cosa, antes de que las extensiones creadas puedan iniciar sesión. Cuando se hacen cambios en la configuración, es necesario reiniciar **Asterisk** para que los cambios tengan efecto. Para esto, **Elastix** muestra un link que permite realizar esta tarea directamente. Dependiendo de la configuración, el reinicio se llevará a cabo

inmediatamente (cortando cualquier comunicación que haya en curso) o en el momento más propicio (evita en lo posible cortar la configuración).



Figura 16. La barra rosa muestra un link para aplicar los cambios realizados.

5.2.3.- Configurar softphones.

La instalación de **X-Lite** varía de acuerdo al sistema operativo a usar, pero en general no causa ningún problema y es un proceso fácil y rápido.

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



Figura 17. Interfaz de X-Lite Softphone.

Para configurarlo se debe acceder a la opción **SIP Account Settings...** en el **menú principal**. Aparecerá un listado de cuentas (en este momento vacío), al lado derecho se debe pulsar **Add...** y luego, en la primera pestaña, **Account**, se deben ingresar los datos: **Display Name**, **User Name** (corresponde a **User Extension**), **Password (secret)** y **Domain** (dominio o dirección IP de la máquina **Asterisk**). Todos los datos deben coincidir con los que se usaron al momento de crear la extensión. Posteriormente se debe pulsar **Accept**, y luego en el listado de cuentas marcar la casilla **Enabled** junto a la cuenta que se acaba de crear.

Después de unos segundos, y si todo se ha hecho correctamente, el estado del teléfono cambiará a conectado.

Además mediante la interfaz web de **Elastix** se podrá apreciar qué teléfonos están conectados, además de mostrar su actividad en el **Flash Operator Panel (FOP)** al cual se accede recorriendo los menús **PBX -> Flash Operator Panel**, la contraseña por defecto se encuentra en el archivo **/etc/ampportal.conf** y por defecto es **'eLaStlx.2007'**.



Figura 18. El Flash Operator Panel.

Otra prueba que se puede realizar para comprobar que el terminar se comunica correctamente con **Asterisk** es llamar al correo de voz (*97 por defecto), donde una grabación proveniente de **Asterisk** contestará.

5.2.4.- Una llamada SIP a través de Asterisk.

Para llamar a otro terminal **SIP** solo basta discar su número de extensión y pulsar llamar, el otro teléfono comenzará a sonar y si contesta se podrá comenzar a hablar. Si transcurridos unos segundos el otro teléfono no contesta, una grabación atenderá, permitiendo dejar un mensaje en el voicemail.

5.3.-Integrando Asterisk a la Zona H.323.

En esta parte, se configurará **Asterisk** y **GNU Gatekeeper**, de modo que **Asterisk** se registre como gateway con el gatekeeper y permita la comunicación desde terminales **H.323** hacia terminales **SIP** y viceversa.

Los cambios en la configuración no afectarán a los softphones. Aunque se debe tener en cuenta que se debe suspender temporalmente las comunicaciones dada la magnitud de los cambios.

5.3.1.- Agregando el canal OOH323 a Asterisk.

Para esta tarea es necesario recurrir a la consola de **Asterisk** e instalar los complementos de **Asterisk** de la siguiente manera:

```
$yum install asterisk-addons
```

Tras la instalación es necesario reiniciar **Asterisk** con el comando:

```
$amportal restart
```

Para comprobar que el canal **OOH323** está presente, es necesario entrar a la consola de **Asterisk**, usando:

```
$asterisk -r
```

Ya dentro de la consola de **Asterisk** se debe ingresar:

```
core show channeltypes
```

Ahora aparece un listado de los canales de **Asterisk**, entre los cuales deberá aparecer el canal **OOH323**.

Type	Description	Devicestate	Indications	T
transfer	-----	-----	-----	-
Phone	Standard Linux Telephony API Driver	no	yes	n
o				
SIP	Session Initiation Protocol (SIP)	yes	yes	y
es				
Local	Local Proxy Channel Driver	yes	yes	n
o				
MGCP	Media Gateway Control Protocol (MGCP)	yes	yes	n
o				
Agent	Call Agent Proxy Channel	yes	yes	n
o				
IAX2	Inter Asterisk eXchange Driver (Ver 2)	yes	yes	y
es				
DAHDI	DAHDI Telephony Driver w/PRI w/OPENR2	no	yes	n
o				
OOH323	Objective Systems H323 Channel Driver	no	yes	n
o				
-----I>				
8 channel drivers registered.				
-- Remote UNIX connection				
-- Remote UNIX connection disconnected				

Figura 19. El canal OOH323 ya instalado.

Para salir de la consola, basta ingresar:

```
Quit
```

Ahora será necesario configurar este canal, el cual no está soportado por **FreePBX** por lo cual se debe hacer de la manera tradicional en **Asterisk**, editando los archivos de configuración.

5.3.2.- Configurando el canal OOH323.

Para realizar esta tarea, es necesario editar el archivo **ooh323.conf** localizando en **/etc/asterisk/**, para ello se puede usar el editor GNU nano:

```
$nano /etc/asterisk/ooh323.conf
```

Las instrucciones para configurar este archivo se encuentran en el mismo archivo, pero, dado que es un poco complejo, se recomienda usar como guía el siguiente ejemplo:

Archivo ooh323.conf

```
;Sección general, usada para configurar parámetros globales
[general]

;Puerto que asterisk debe escuchar para llamadas H323 entrantes
port=1720

;Dirección IP que asterisk debe escuchar para llamadas H323 entrantes
;0.0.0.0 intenta encontrar la dirección por si solo
bindaddr=0.0.0.0

;H.323ID para el servidor (gateway) asterisk
h323id=ELA323

;ID para llamadas generadas por asterisk
callerid=asterisk

;Este parámetro indica si asterisk se debe registrar con el gatekeeper como
;gateway (yes) o como endpoint (no)
gateway=yes

;Dirección del gatekeeper (GNU Gatekeeper)
gatekeeper = 169.254.83.205

;Admitir el modo ruteado por gatekeeper
AllowGKRouted = yes

;Usar protocolo H.245 en la configuración de llamadas
h245inSetup=yes

;Ubicación del archivo de registro (log)
logfile=/var/log/asterisk/h323_log

;Contexto en el cual serán ubicados por defecto los terminales
context=default

;Alias para el cual se aplican las opciones siguientes
alias=asterisk

;Prefijo del gateway, con ésta configuración Asterisk se hará cargo siempre
;que el número marcado comience con 5 o 0
gwprefix=5
gwprefix=0

;Timeout del protocolo de transporte (RTP) para todos los clientes
;Con esta configuración la llamada se abortará si no hay actividad
;en el protocolo de transporte durante 60 segundos
rtptimeout=60

;Codecs utilizados. Los únicos codecs soportados son GSM, G.711 ulaw
;y G.711 alaw, por lo cual se debe inicializar esta parte deshabilitando
;todos los codecs, y luego activando solo los que serán usados
disallow=all
allow=gsm
allow=ulaw
allow=alaw
```

Archivo ooh323.conf (continuación)

```
;Modo DTMF que será usado por defecto por los clientes.
;El modo más usado (y por lo tanto más compatible) es el rfc 2833
dtmfmode=rfc2833

;Terminales H.323, cada terminal debe ser configurado usando su
;H.323ID, en una sección encabezada por [H.323ID del terminal]
[juan]

;El tipo de terminal será, user si puede enviar y recibir llamadas
type=user

;Dirección IP del terminal H.323, puede omitirse, pero cuando se especifica
;la configuración es más estable
ip=169.254.83.200

;Puerto que usa el terminal para comunicarse
port=1719

;Se debe repetir esta configuración por cada terminal H.323 existente
```

Una vez efectuados los cambios en el archivo de configuración, es necesario reiniciar **Asterisk**. Sin embargo, mientras vuelve a iniciar es probable que el gatekeeper rechace su conexión, además es necesario establecer las reglas con la cuales **GNU Gatekeeper** se comunicará con **Asterisk**.

5.3.3.- Configurando GNU Gatekeeper.

Ahora es necesario configurar efectivamente **GNU Gatekeeper**, ya que la configuración usada anteriormente es muy básica y no permitirá cumplir el objetivo. Es necesario crear un archivo de configuración gatekeeper.ini como el siguiente:

Archivo gatekeeper.ini

```
;Sección principal del archivo
[Gatekeeper::Main]

;Parámetro obligatorio para encabezar esta sección. Se usa para pruebas
Fortytwo=42

;Nombre del gatekeeper. De gran importancia, sobre todo cuando hay
;más de un gatekeeper
Name=GatekeeperH323

;Configuración del modo enrutado por gatekeeper
[RoutedMode]

;Se habilita en el enrutado del canal Q.931
GKRouted=1

;Se habilita el enrutado del canal H.245
H245Routed=1
```

Archivo gatekeeper.ini (continuación)

```
;Al igual que con la configuración inicial, el gatekeeper aceptará
;llamadas no registradas
AcceptUnregisteredCalls=1

;Sección de autenticación del gatekeeper
[GkStatus::Auth]

;Con este regla se permitirá cualquier conexión no autenticada
rule=allow

;Ahora se configura el endpoint cuyo H.323ID es ELA323 (Asterisk)
;es decir aquí se configura al gateway Asterisk
[EP::ELA323]

;Prioridad del gateway, como solo hay un gateway, se le asignará
;prioridad máxima (1)
GatewayPriority=1

;Prefijos del gateway
;Cualquier llamada a un número que comience con 5 o 0 será
;automáticamente transmitida hacia Asterisk
GatewayPrefixes=5, 0
```

Ahora, es necesario cerrar toda instancia de **gnugk**, y luego volver a iniciarlo usando:

```
$gnugk -c <ruta completa del archivo de configuración>
```

Una vez iniciado el gatekeeper, llega el turno de reiniciar **Asterisk** para que esta vez se registre como gateway con el gatekeeper. Para reiniciar **Asterisk** usar:

```
$amportal restart
```

En el gatekeeper se podrá ver un registro similar al que aparece cuando se registra un terminal, con la única diferencia de que **Asterisk** será registrado como gateway y no como terminal.

Hasta este momento aún no es posible efectuar llamadas desde un terminal **H.323** hacia un terminal **SIP** ni tampoco al revés. Es necesario asignar un número de extensión a cada uno de los terminales **H.323**.

5.3.4.- Configurando las extensiones H.323.

Ahora es necesario añadir cada terminal **H.323** como una extensión en **Asterisk**. Para ello se debe recurrir nuevamente a la interfaz web de **Elastix** tal y como se hizo al agregar las extensiones **SIP**, solo que esta vez se debe seleccionar como tipo de dispositivo **Other (Custom) Device**.

El formulario a llenar se asemeja bastante al de **SIP**, aunque tiene algunos campos adicionales que son de gran importancia, razón por la cual, se explica a continuación la configuración básica:

User Extension: Número de la extensión, vale recordar que en este punto todas las extensiones (tanto **SIP** como **H.323**) deben comenzar con los números configurados como prefijos del gateway **Asterisk**.

DisplayName: Lo recomendable es que coincida con el **H.323ID** del terminal.

SIP Alias: Alias con el cual los dispositivos **SIP** reconocerán a este terminal. Se recomienda usar también el mismo **H.323ID**.

Dial (This device uses custom technology): Este parámetro es muy importante, su valor debe ser **OOH323/<H323.ID del terminal>**. Debe coincidir por lo tanto con el **H323.ID** usado por el softphone para conectarse al gatekeeper, y debe coincidir con una de las entradas configuradas en el archivo **ooh323.conf**.

Voicemail & Directory – Status: Usar **Enabled**, para dejar activo el correo de voz, aunque desafortunadamente no se podrá consultar usando el ***97**. Pero existe otra forma, la cual se verá más adelante.

Una vez registradas todas las extensiones **H.323** se debe aplicar los cambios a **Elastix**. La configuración de los softphones se mantiene a como se dejó en un principio.

5.3.5.- Comunicación entre terminales SIP y H.323.

Hasta este punto ya es posible realizar llamadas desde terminales **H.323** hacia terminales **SIP** marcando el número de su extensión en el softphone, y del mismo modo desde un **SIP** se puede llamar hacia un terminal **H.323**. También es posible llamar desde un terminal **H.323** hacia otro terminal **H.323** pasando por **Asterisk** usando para ello el número de extensión en lugar del **H.323ID**. Los voicemail de todas las extensiones funcionan, pero no es posible consultar el voicemail desde un terminal **H.323**, a pesar de estar habilitado el servicio. Una alternativa es que el usuario consulte su correo de voz usando la interfaz web de **Elastix**, lo cual no solo permite consultar los mensajes, sino también ver su registro de llamadas y acceder a otros servicios proporcionados por **Elastix**. Las instrucciones para crear cuentas a los usuarios de **Elastix** se encuentran en el anexo.

6.- Conclusiones.

En este proyecto se han aprendidos los fundamentos principales de dos de los más importantes protocolos usados para la telefonía IP. **H.323** una recomendación antigua, madura, robusta y compleja, el primer estándar para la telefonía IP, y el más usado antes del auge de **SIP**, un protocolo un poco más simple, escalable, de fácil adopción y muy compatible con otros protocolos.

En el presente ya son pocos los usuarios de **H.323**, **SIP** le ha arrebatado dignamente una gran parte del mercado y se convertido rápidamente en el protocolo más usado a nivel mundial. Sin embargo, **H.323** sigue siendo usado por grandes empresas, que siendo fieles a su inversión en equipos compatibles con **H.323**, continúan usándolo a pesar de la tendencia a migrar a **SIP**.

En este proyecto se realizó una tarea de gran importancia, que consistió en comunicar ambos protocolos, lo cual puede permitir a una empresa que desea migrar a **SIP**, hacerlo de forma paulatina y sin dejar de lado sus equipos **H.323**.

Sin embargo, faltaron dos partes importantes. La primera, lograr salir hacia la red telefónica (**ISDN** y **PSTN**) para efectuar y recibir llamadas desde teléfonos corrientes. La segunda parte que estuvo ausente en esta experiencia es la salida hacia internet de las llamadas **VoIP**, de modo de comunicar puntos alejados usando la telefonía IP o mezclando redes IP con redes **PSTN**. Quedan por lo tanto como desafíos integrar a este proyecto estas funcionalidades de modo de convertirlo en una experiencia útil y lo suficiente rentable como para ser implementada para fines no académicos.

A modo complementario, es posible utilizar un teléfono celular conectado mediante bluetooth con la máquina **Asterisk** de modo de proveer a través de éste la salida hacia la red de telefonía celular para todos los extensiones. Esto debe efectuarse en una instalación de **Elastix** (o similar) en una máquina real ya que la interfaz bluetooth no funciona correctamente desde una máquina virtual. Un ejemplo práctico de esta configuración se puede encontrar en uno de los enlaces en el anexo de este documento.

La información incluida en este documento es fruto del aprendizaje logrado por el autor en desarrollar este proyecto, además de la recopilación de información de numerosas fuentes, algunas, no del todo confiables, pero siempre con la finalidad de compartir conocimientos y permitir que otros aprendan de sus experiencias.

7.- Anexos.

7.1.-Configuración avanzada de GNU Gatekeeper.

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

7.1.1.- Parámetros.

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

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

7.1.2.- Archivo de Configuración.

En general, el archivo de configuración permite establecer una mayor cantidad de opciones en la configuración del gatekeeper. A continuación solo se detallarán las opciones básicas.

El archivo de configuración es un archivo estándar de texto. El formato básico es el siguiente:

[Nombre de la sección]

Nombre de la clave = Valor de la clave

Los comentarios están marcados con un signo numeral (#) o un punto y coma (;) al inicio de cada línea.

Existen muchas secciones que se pueden añadir al archivo de configuración, pero en la mayoría de los casos no tiene sentido utilizar todas las secciones al mismo tiempo.

Sección [Gatekeeper::Main]

Fortytwo=42

Default: N/A

Esta opción permite probar la existencia del archivo de configuración (gatekeeper.ini o cualquiera que sea su nombre) con el que va a trabajar el gatekeeper. Un mensaje de advertencia se mostrará en caso de que no existiera dicho archivo.

Name=OpenH323GK

Default: OpenH323GK

Identificador del gatekeeper. El gatekeeper responderá solamente a los mensajes GRQs con este ID y utilizará éste en los mensajes enviados a sus endpoints.

Home=192.168.1.1

Default: 0.0.0.0

El gatekeeper escuchará por peticiones desde esta dirección IP. Por defecto, el gatekeeper escucha desde todas las interfaces del equipo. Se puede omitir esta opción, a menos que se desee que el gatekeeper se enlace solamente hacia una dirección IP específica. Pueden agregarse varias direcciones IP en este campo separadas por un punto y coma (;) o una coma (,).

NetworkInterfaces=192.168.1.1/24,10.0.0.1/0

Default: N/A

Aquí se deben especificar las interfaces de red del gatekeeper. Por defecto el gatekeeper detectará las interfaces automáticamente.

RedirectGK=Endpoints > 100 || Calls > 50

Default: N/A

Esta opción le permite redireccionar endpoints hacia gatekeeper alternos cuando el gatekeeper se sobrecarga. Por ejemplo, en la configuración anterior, el gatekeeper rechazará un RRQ si los endpoints registrados sobrepasan los 100 o rechazará un ARQ si las llamadas actuales sobrepasan las 50.

Sección [GkStatus::Auth]

En esta sección se definen un número de reglas para determinar quienes están permitidos de conectarse al gatekeeper vía puerto de estado (vía telnet). Quien quiera que tenga acceso al puerto de estado tiene un control completo sobre el gatekeeper. Asegúrese de que ésta sección esté configurada correctamente.

rule=allow

Default: forbid

Posibles valores son:

forbid - Niega cualquier conexión.

allow - Permite cualquier conexión.

explicit - Lee el parámetro ip=value donde ip es la dirección IP del cliente.

regex - La IP del cliente se hace corresponder con la expresión regular dada.

password - El usuario tiene un username y password apropiado para conectarse

(login). El formato de username/password es el mismo que el de la sección [SimplePasswordAuth].

Por otra parte, estas reglas puede ser combinadas por "|" o "&".

default=allow

Default: forbid

Esta opción es utilizada solamente cuando rule=explicit.

StatusPort=7000

Default: 7000

Este es el puerto de estado para monitorear el gatekeeper.

EncryptAllPasswords=1

Default: 0

Habilita la encriptación de todas las contraseñas en la configuración (SQL passwords, RADIUS passwords, [Password] passwords, [GkStatus::Auth] passwords). Si se habilita esta opción, todas las contraseñas deben estar encriptados utilizando la utilidad addpasswd. De otra manera sólo las contraseñas de [Password] y [GkStatus::Auth] son encriptadas (antiguo comportamiento).

Sección [RoutedMode]

En esta sección se configura el modo enrutado por gatekeeper, en sus distintas variantes.

*** GK Routed=1**

Default: 0

Si se habilita o no el ruteo de la señalización en modo gatekeeper (gatekeeper routed signaling mode). Lo cual enrutará la señalización (Q.931). Será el gatekeeper quien decida si enruta o no el canal H.245 y los canales lógicos, aunque lo más probable es que en este modo no lo haga.

*** H245 Routed=1**

Default: 0

Si se enruta también el Canal de Control H.245 a través del gatekeeper. Solamente tendrá efecto si el parámetro GK Routed=1 y el tunneling H.245 está deshabilitado para una llamada.

*** CallSignalPort=0**

Default: 1721

El puerto por donde el gatekeeper realizará la señalización de llamada. El puerto por defecto es 1721. No se utiliza el puerto 1720 para que se tenga la posibilidad de ejecutar un endpoint H.323 en la misma máquina del gatekeeper. Se puede establecer este parámetro en 0 para permitirle al gatekeeper seleccionar un puerto arbitrario.

*** CallSignalHandlerNumber=2**

Default: 1

El numero de hilos dedicados al manejo de los canales de señalización/H.245. Es posible puede incrementar este número en un gatekeeper fuertemente cargado. Cada hilo puede procesar un mensaje de señalización a la vez, de esta manera incrementar este número incrementará el rendimiento de la llamada. Bajo Windows, existe un límite por defecto de 64 sockets utilizados por un simple hilo de señalización, así cada hilo de señalización está en condiciones de manejar al menos 32 llamadas (con el tunneling H.245 habilitado).

*** AcceptUnregisteredCalls=1**

Default: 0

Con esta característica habilitada, el gatekeeper aceptará llamadas desde cualquier endpoint no registrado. Sin embargo, esto permite riesgos en la seguridad.

Sección [EP::ALIAS]

Donde ALIAS es reemplazado con un alias actual para el endpoint al cual se va a aplicar la configuración. Donde un endpoint puede ser un terminal o un gateway. Actualmente, están reconocidas las siguientes opciones:

*** Capacity=10**

Default: -1

Capacidad de llamadas para un endpoint. En caso de puertas de enlace (gateways), si más de un gateway se corresponde con un número marcado, la llamada será enviada al primer gateway disponible (que tenga suficiente capacidad).

*** GatewayPriority=1**

Default: 1

Aplicado solo para gateways. Permite la prioridad basada en casos de encaminado, cuando más de un gateway se corresponde con un número marcado. El valor más pequeño es la prioridad más alta asignada a un gateway. Una llamada es encaminada hacia el primer gateway disponible (que tenga capacidad disponible) con la prioridad más alta (los valores más bajos en GatewayPriority).

*** GatewayPrefixes=0048, 0049, 0044**

Default: N/A

Prefijos adicionales para este gateway. Aplicado solo a gateways. Los caracteres especiales "." y "!" pueden ser usados aquí respectivamente para la correspondencia con cualquier dígito y desactivar el prefijo.

Sección [Password]

Al usar esta sección se habilita la autenticación de endpoints. Normalmente las entradas de esta sección se añaden usando la herramienta addpasswd. Las entradas corresponden a un listado de los endpoints (por ALIAS) seguido de la contraseña encriptada.

Para usar autenticación de endpoints se debe incluir esta sección en blanco, para luego ingresar las contraseñas de cada endpoint usando la herramienta addpasswd.

7.1.3.- La herramienta “addpasswd”.

Esta herramienta permite añadir contraseñas encriptadas en el archivo de configuración. En general se puede añadir contraseñas en cualquier sección del archivo, aunque solo en aquellas secciones que soportan en uso de contraseñas serán reconocidas correctamente.

Las secciones que más aprovechan el uso de esta herramienta son las secciones [GkStatus::Auth] y [Password].

El uso de la herramienta es como se sigue:

```
$addpasswd <ruta del archivo de configuración> <sección del archivo> <nombre de la clave> <contraseña>
```

Por ejemplo, para añadir la contraseña ‘1130aa’ al usuario ‘juan’, en la sección [Password] en el archivo ‘gatekeeper.ini’ ubicado en ‘/root/gnugk/’, la forma de hacerlo es la siguiente:

```
$addpasswd /root/gnugk/gatekeeper.ini Password juan secret
```

Si ahora, se abre el archivo de configuración se podrá ver en la sección [Password] una entrada que dice `juan = xxxxx` donde xxxxx es una serie de caracteres que representan la contraseña ‘secret’ encriptada.

7.2.- Creación de una cuenta de usuario en Elastix.

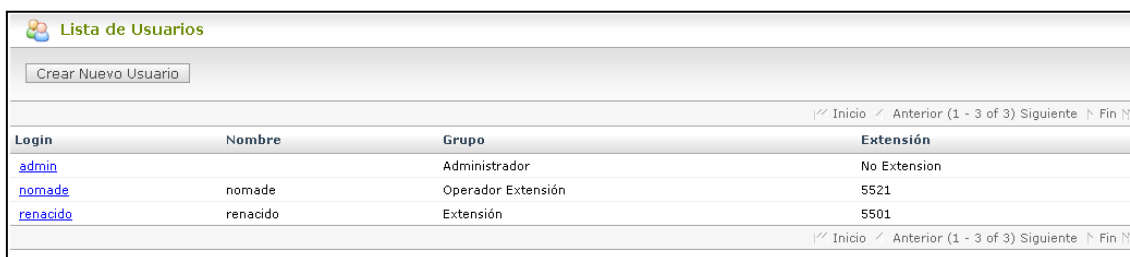
Para crear una cuenta de usuario en **Elastix**, de modo que el usuario pueda acceder mediante la interfaz web para ver y oír sus mensajes de voz y ver su registro de llamadas, entre otras cosas, es necesario ingresar a la interfaz web de **Elastix** usando la cuenta de administrador (por defecto, nombre de usuario **admin**, y password **palosanto**).

Una vez dentro se debe ingresar al menú **Sistema → Administrar Usuarios**:



Figura 20. El menú Sistema → Administrar Usuarios

Ahora en el menú del lado izquierdo de debe seleccionar **Usuarios**, lo cual lleva a la siguiente pantalla:



Login	Nombre	Grupo	Extensión
admin		Administrador	No Extension
nomade	nomade	Operador Extensión	5521
renacido	renacido	Extensión	5501

Figura 21. Lista de Usuarios

Aquí, se debe pulsar **Crear Nuevo Usuario**, y de deben llenar los siguientes datos:

Login: Nombre corto con el cual iniciar sesión.

Nombre: Nombre completo del usuario.

Contraseña: Contraseña que el usuario utilizará al iniciar sesión.

Grupo: Grupo al cual el usuario pertenece, puede ser **Administrador** (todos los permisos), **Operador** (permisos intermedios) o **Extensión** (permisos a nivel de la extensión del usuario).

Extensión: Extensión asociada al usuario.

En la parte inferior es posible además configurar el acceso a un **Webmail**, especificando el dominio, nombre de usuario y contraseña.

Una vez terminado, se debe pulsar el botón **Guardar**, para aceptar los cambios. Ahora el usuario puede iniciar sesión usando la interfaz Web de **Elastix**.

7.3.-Algunos enlaces de interés.

7.3.1.- Configurar Chan Mobile en Elastix

En el siguiente link se muestra como instalar el canal mobile en Elastix de modo conectar un teléfono móvil con tecnología bluetooth con la central Asterisk y proveer servicios adicionales por medio de este.

http://docs.google.com/View?id=dc6z76m4_73dmczs9gr

7.3.2.- EcuLUG.org. Ecuador Linux User Group.

Comunidad en la cual mediante foros y listas de correo se comparte información sobre Linux y sus aplicaciones. Existe abundantes temas en los cuales se comparte información sobre la configuración de Asterisk. Algunos problemas presentados en el desarrollo de este proyecto no hubiesen tenido solución de no ser por la valiosa información que puede ser encontrada aquí.

<http://www.ecualug.org>

7.3.3.- Trixbox.

Trixbox es una alternativa a Elastix en cuanto a soluciones Linux + Asterisk + FreePBX, en su página existe abundante información, la cual también es aplicable a Elastix.

<http://www.trixbox.org/>

7.3.4.- Comunidad de usuarios de GNU Gatekeeper.

En esta página es posible examinar las listas de correos de la comunidad usuarios de GNU Gatekeeper, en donde se puede encontrar información para resolver problemas de configuración de GNU Gatekeeper.

<http://www.mail-archive.com/openh323gk-users@lists.sourceforge.net/info.html>

7.3.5.- AsteriskClub.org

Noticias, manuales, foros y comentarios sobre Telefonía IP, Asterisk, Elastix, Trixbox, FreePBX, entre otros.

<http://www.asteriskclub.org/>

8.- Referencias.

- Implementación de una solución de voz sobre IP en Linux. Romain Barrallon. Universidad Técnica Federico Santa María, Valparaíso.
- TrixBox al descubierto. Alfredo Certain Yance. GECKO EU, GECKO NETWORKS, www.gecko.com.co
- VoIP: A comprehensive survey on a promising technology. Stylianos Karapantazis , Fotini-Niovi Pavlidou. Computer Networks 53 (2009).
- Diseño e Implementación de una Plataforma de Telefonía IP en HyC (Memoria). René Fuentes Riquelme. Universidad Técnica Federico Santa María, Valparaíso.
- Voice over IP Signaling: H.323 and Beyond. Hong Liu and Petros Mouchtaris, Telcordia Technologies. IEEE Communications Magazine, October 2000.
- Asterisk Desconsolado versión 2.0. Eduardo Viegas y Facundo Correa. Asterio, IT Efficiency.
- Manual oficial de GNU Gatekeeper. Version 2.3.1, Junio 2009. <http://www.gnuqk.org/h323download.html>
- Elastix without tears. Ben Sharif, Palosanto Solutions, 2008. <http://www.elastix.org>