Universidad Francisco Gavidia

Tecnología, Humanismo y Calidad

DIRECCION DE POSTGRADOS Y EDUCACION CONTINUA

Trabajo de graduación:

"IMPLEMENTACIÓN DE SERVICIO DE VOZ SOBRE IP PARA EL PERSONAL DE LA F.A. EN EL EXTRANJERO A TRAVES DE LA PLATAFORMA ASTERISK"

Presentan:

ANDRES ZAMORA GONZALEZ.
LUIS ENRIQUE FUENTES SANCHEZ.

Para optar al título de:

MAESTRO EN INFORMÁTICA APLICADA EN REDES

San Salvador, 20 de Enero de 2009

UNIVERSIDAD FRANCISO GAVIDIA

Dirección de Postgrados y Educación Continua.

AUTORIDADES UNIVERSITARIAS

RECTOR:

ING. MARIO ANTONIO RUIZ RAMIREZ

VICE RECTORA:

DRA. LETICIA ANDINO DE RIVERA

SECRETARIA GENERAL:

LIC. TERESA DE JESUS GONZALEZ DE MENDOZA

DIRECTOR DE POSTGRADOS Y EDUCACION CONTINUA:

LIC. ADALBERTO ELIAS CAMPOS BATRES

No. 05836

Universidad Francisco Gavidia

ACTA DE LA DEFENSA DE TRABAJO DE GRADUACION DE POSTGRADO

Acta No. 02/2009

En la Sala de Conferencias del quinto nivel del Edificio EBLE, de la Universidad Francisco Gavidia, a las dieciocho horas y cero minutos del trece de marzo de dos mil nueve; siendo estos el día y la hora señalada para el análisis y la defensa del trabajo de graduación:" IMPLEMENTACIÓN DEL SERVICIO DE VOZ IP PARA EL PERSONAL DE LA FUERZA ARMADA EN EL EXTRANJERO A TRAVÉS DE LA PLATAFORMA ASTERISK", presentado por los egresados: Andrés Zamora González y Luis Fuentes Sánchez de la carrera de MAESTRÍA EN INFORMATICA APLICADA EN REDES.

Y estando presentes los interesados y el Jurado, se procedió a dar cumplimiento a lo estipulado, habiendo llegado el Jurado, después del interrogatorio y las deliberaciones correspondientes, a pronunciarse por este fallo:

Andrés Zamora González — *Fallo:* Aprobado
Nombre — *(Aprobado ó Reprobado)*

Luis Enrique Fuentes Sánchez — *Fallo:* Aprobado
Nombre — *(Aprobado ó Reprobado)*

Y no habiendo más que hacer constar, se da por terminada la presente.

Presidente
Ing. Julio Adalberto Rivera Pineda

Vocal
Lic. Mauricio Orlando Guzmán Hernández

Vocal
Ing. Jonathan Rodríguez Seoane

Lic. Mario Antonio Ruiz Aguilar
Representante de Dirección de Postgrados y Educación Continua

AGRADECIMIENTOS

A DIOS: Que se lo debo todo, por haber sembrado en mi alma el deseo de aprender más y el de superación, acompañándome siempre en los buenos y malos momentos, ofreciéndome la mejor alternativa en las diferentes etapas de mi vida.

A MIS PADRES: A mi madre Carmen Edelmira que aunque ya no esta con nosotros siempre fue la fuente de inspiración para alcanzar esta meta; a mi padre Luis por su total apoyo a lo largo del camino y esa palmada en el hombre justo en el momento que se necesitaba.

A MIS HERMANOS: Oscar que por circunstancias de la vida no le permitieron alcanzar esta meta, a Mario por su apoyo de ayer, hoy y siempre.

Luis Enrique Fuentes.

A DIOS: Todo poderoso por haberme iluminado con su luz de sabiduría y entendimiento, gracias a ti mi dios que me acompañaste y me protegiste para no caer en malos pasos… Gracias a ti Jesús por brindarme salud y amor para mis hermanos.

Gracias Dios mió, por haberme permitido alcanzar la meta deseada, por que este logro en mi vida a sido gracias a tu voluntad y humildad.

A MI ESPOSA: Por haberme brindado su apoyo y comprensión al tener que cederme su tiempo, que de una u otra manera lo utilizaba para fortalecer mis conocimientos.

Gracias por tomar mi lugar en las responsabilidades del hogar, cuando me encontraba ausente. por tener paciencia y alentarme a seguir adelante, por tener fe en mi y brindarme su atención cuando le comentaba mis problemas, ya fueran de estudios, de trabajo o familiares. gracias por tu cariño y comprensión …. que Dios te bendiga.

A MI HIJA: Gracias mi hijita por darme tu amor y alegría, hoy en esta vez es la segunda oportunidad en que elevo mis agradecimientos por tenerte a mi lado, han pasado 15 años desde que naciste y para mi ha sido una gran bendición y siempre le estaré eternamente agradecido a Dios por bendecirme con amor.

A MIS PADRES: Deseo dar las gracias a mi papa y mama por estar siempre conmigo y brindarme su apoyo, por aconsejarme y guiarme en el camino correcto de la vida, por que gracias a ustedes he podido llegar hasta donde estoy.

Gracias a dios por permitir que estén conmigo y yo con ustedes. que Dios los bendiga queridos papa y mama.

A MIS HERMANOS: José Adán, Paquita, Adela, Salvador, Jesús, Gertrudis, Pablo, Jesús, Salvador y Sandra que han estado cerca de mi y que de una u otra forma me motivaron a seguir adelante, gracias por su cariño y su tiempo.

Que Dios los cuide a todos ustedes por ser excelentes hermanos.

A MI COMPAÑERO DE TESIS : Gracias Luís por ser un buen compañero de trabajo en los estudios que cursamos, fueron dos años de estudio continuo, pero gracias a Dios salimos adelante, te deseo lo mejor y que todo lo aprendido te sea de mucho beneficio en tu vida.

Andrés Zamora González.

TABLA DE CONTENIDO

IV METODOLOGIA DE DESARROLLO.

V RESULTADOS ALCANZADOS.

RESUMEN

El objetivo del presente trabajo profesional consiste en la implementación del servicio de voz sobre IP, como una alternativa de comunicación para el personal de la Fuerza Armada de El Salvador, que se encuentra cumpliendo misiones en el Extranjero, sean estas a través de contingentes, observadores militares, Agregadurías de Defensa o en estudios académicos.

Dicha solución se propone debido a los altos costos que tiene que cancelar el Ministerio de la Defensa Nacional, en concepto de llamadas telefónicas Internacionales o en su defecto las erogaciones que tienen que realizar el personal de la Institución, que en un momento determinado desean mantener algún tipo de comunicación con personal de la misma y/o familiares.

La metodología empleada para lograr la implementación del servicio VoIP, ha sido a través de la configuración, estabilización y aseguramiento de la PBX por software denominada Trixbox, la cual esta basada en Asterisk sobre una distribución libre del sistema operativo Centos, así como también el empleo de software para corta fuego IpCop y Zerina para habilitar un canal seguro en las llamadas provenientes de la red publica de Internet.

Para lograr la comunicación entre los usuarios en el extranjero y personal de la Fuerza Armada en El Salvador, se configuró los servicios de extensiones telefónicas, que pueden funcionar en un computador a través de software libre para telefonía o por medio de teléfonos IP, los cuales utilizan el protocolo SIP y CODEC para codificación de voz, como son G711 y G729. De igual forma se habilitaron los servicios de salas de conferencia, correo de voz y contestadora digital. Todos estos servicios son resueltos a través de un servidor operando con Trixbox, el cual enrrutará las llamadas provenientes de Internet hacia la red telefónica (abonados), privada de la Fuerza Armada.

Con la anterior solución se concluye que la utilización de software de código abierto para la implementación de servicios de voz sobre IP, constituye una alternativa viable, económica, fácil de administrar y con niveles de seguridad que brindan protección a la comunicación entre los diferentes usuarios (abonados), garantizando la confiabilidad, integridad y autenticidad de la misma.

INTRODUCCION

En la actualidad la tecnología Informática, ha alcanzado increíbles avances, permitiéndonos desde almacenar una pequeña carta en un dispositivo de almacenamiento hasta envío de datos, voz y video a través de medios alambricos, inalámbricos y que por que no decirlo comunicaciones satelitales, que permiten comunicar a individuos y/o instituciones ubicadas en cualquier parte del planeta y fuera de éste (interespacial).

Es así como hoy en día, algunos servicios como la telefonía convencional (por conmutación de circuitos), han pasado a otro entorno, nos referimos a la telefonía IP (por conmutación de paquetes), que aprovechando la Tecnología sobre IP, implementa la comunicación de Voz sobre el Protocolo de Internet (VoIP). Gracias a esta novedosa tecnología, se pueden brindar servicios de comunicaciones de voz entre redes de datos (LAN, WAN, Internet), que se encuentren en lugares geográficamente distantes. Así como también implementarlo en telefonía fija en hogares y empresas.

La tecnología de voz sobre protocolo de Internet VoIP, junto con nuevas aplicaciones Web, son para muchos la tecnología del futuro en las comunicaciones.

De igual forma y en paralelo a estos avances, se han desarrollado herramientas de software, que permiten implementar servicios de telefonía a través de una PBX virtual basada en IP, mediante el empleo de protocolos como H.323, SIP, IAX, entre otros. Es así como hoy en día encontramos software como: Asterisk, Elastix, Trixbox, 3CXPHONE (versión Windows pagada), con soporte para VoIP.

El presente trabajo de graduación, se ha enfocado a solventar una problemática, mejorar la comunicación entre el Ministerio de la Defensa y el personal de la F.A. que se encuentra en misiones oficiales en el extranjero, ofreciéndoles como una alternativa la transmisión de la voz sobre protocolo de Internet VoIP.

Para esto se implementará un servicio de voz sobre IP VoIP sobre la

plataforma de código abierto Asterisk.

Esto se logrará utilizando solamente herramientas con licenciamiento GPL de software libre, donde el sistema operativo será una versión de Linux llamada CentOS, sobre el cual se montará una IP PBX basada en el software Asterisk, llamada TrixBox, que es una PBX con soporte para VoIP, que trae pre configurado Asterisk y se administra vía Web.

La seguridad es un factor crítico en todo servicio vía Internet, por lo cual se configura un cortafuego con IPCop y su Addons ZERINA, el cual es un software que nos ayuda configurar OpenVPN sobre IPCop, con lo cual se conseguirá una red con autenticación y un túnel encriptado para el establecimiento de una comunicación VoIP.

Los usuarios de esta red se podrán comunicar entre ellos utilizando una variedad de dispositivos, como lo son una computadora con teléfono por software (softphone), teléfonos VoIP con puerto USB, teléfonos IP y teléfonos analógicos con gateways FXS.

CAPITULO I
MARCO TEORICO CONCEPTUAL.

1.- Antecedentes Históricos de Telefonía IP.

La tecnología de transmisión de voz sobre el protocolo IP nace en los años 70 para la ARPANET (el antecesor de Internet), en aquel momento fue un desarrollo experimental para obtener comunicación por voces entre los integrantes de la entonces pequeña red de redes, comunicación de PC a PC.

Con el crecimiento y uso extendido de las redes IP, el fenómeno de Internet, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP (**QoS**), se creo un entorno donde ya es posible transmitir la voz sobre IP.

La voz sobre redes IP **VoIP** (*Voice over IP*) inicialmente se implementó para reducir el ancho de banda mediante compresión vocal, aprovechando los procesos de compresión diseñados para sistemas celulares en la década de los años 80. En consecuencia, se logró reducir los costos en el transporte internacional. Luego tuvo aplicaciones en la red de servicios integrados sobre la LAN e Internet. Con posterioridad se migró de la LAN (aplicaciones privadas) a la WAN (aplicaciones públicas) con la denominación **IP-Telephony**.

La transmisión de voz sobre el protocolo de IP ó **VoIP** (Voice Over Internet Protocol), es una tecnología que permite la transmisión de voz a través de las redes IP (Internet, red IP pública, Intranet), y nace en el año 1995 como resultado del trabajo de un grupo de estudiantes en Israel. Ese mismo año Vocaltec anuncia el lanzamiento del primer Softphone que llamaron “Internet Phone Software”. El software funcionaba comprimiendo la señal de voz, convirtiéndola en paquetes de voz que eran enviados por Internet, la comunicación es de PC a PC.

En marzo de 1997 la compañía MCI de Estados Unidos lanza su proyecto llamado VAULT, esta nueva arquitectura de red permite interconectar y combinar las redes tradicionales de telefonía con redes de datos. El sistema "empaqueta" las conversaciones (es decir, las transforma en bloques de información manejables por una red de datos) y las envía vía Internet.

A finales del año 1997 el VoIP forum del IMTC (International Multimedia Telecommunications Consortium) llega a un acuerdo que permite la interoperabilidad de los distintos elementos que pueden integrarse en una red VoIP. Debido a la ya existencia del estándar H.323 del ITU-T (International Telecommunication Union), que cubría la mayor parte de las necesidades para la integración de la voz, se decidió que el H.323 fuera la base del VoIP. De este modo, el VoIP debe considerarse como una clarificación del H.323, de tal forma que en caso de conflicto, y a fin de evitar divergencias entre los estándares, se decidió que H.323 tendría prioridad sobre el VoIP. El VoIP tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, y estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF).

En el año 1998 se comenzaron a fabricar los primeros **ATA/Gateways** para permitir las primeras comunicaciones PC a teléfono convencional y finalmente las primeras comunicaciones teléfono convencional a teléfono convencional (con ATAs en cada extremo). También se comenzó a fabricar Switches de Layer 3 con QoS.

En el año 1999 Cisco vende sus primeras plataformas corporativas para VoIP. Se utilizaba principalmente el protocolo H.323 de señalización. El marco de voz con el software integrador Cisco IOS ofrece la integración completa y sin fisura de voz, video y datos. Permite a los clientes corporativos y a los proveedores de servicio manejar grandes redes y servicios basados en VoIP. En enero de 1999, 3Com lanzó con éxito las capacidades de VoIP, construido en parte sobre la base del servidor de Microsoft Windows NT y en la plataforma Total Control multi-servicio, un sistema avanzado basado en DSP (Digital Signal Processor).

En el año 2000 VoIP representaba más del 3% del tráfico de voz. Ese mismo año Mark Spencer un estudiante de la Universidad de Auburn crea **Asterisk**, la primer central telefónica/conmutador basada en Linux con una PC hogareña con un código fuente abierto. Asterisk hoy ofrece una solución freeware para hogares/pequeñas empresas y soluciones IP-PBX corporativas. **Ver figura No. 1.**

Figura No. 1

En el año 2002 el protocolo SIP (Session Initiation Protocol) que es un protocolo de señalización desarrollado por la IETF (Internet Engineering Task Force), empieza a desplazar al protocolo H.323.

En el año 2003 dos jóvenes universitarios - Jan Friis y Niklas Zenntrom - crean un softphone gratuito fácilmente instalable en cualquier PC que puede atravesar todos los firewalls y routers inclusive los corporativos. Ese producto es Skype, que se propaga con una velocidad increíble.

En el año 2007 Linksys, una división de Cisco, lanzó un teléfono móvil IP llamado iPhone que cuenta con clientes Skype y Yahoo! Messenger para realizar llamadas y mantener presencia en línea.

2.- Conceptos sobre VoIP.

La Voz sobre Protocolo de Internet, también llamada Voz sobre IP, VoIP, Telefonía IP, Telefonía por Internet, Telefonía *Broadband* y Voz sobre *Broadband,* consiste en el uso de redes de dados que utilizan un conjunto de protocolos de redes IP (TCP/UDP/IP), para la transmisión de señales de Voz en tiempo real en forma de paquetes de dados.

Los Protocolos que son usados para llevar las señales de voz sobre la red IP son comúnmente llamados como protocolos de Voz sobre IP o protocolos IP. Ellos pueden ser vistos como implementaciones comerciales de la Red experimental de Protocolo de Voz (1973) inventado por ARPANET. El tráfico de Voz sobre IP puede ser llevado por cualquier red IP, incluyendo aquéllas conectadas a la red de Internet, como por ejemplo, en una red de área local (LAN).

Ventajas.

- En general, el servicio de telefonía vía VoIP cuesta menos que el servicio equivalente tradicional y similar a la alternativa que los proveedores del servicio de la Red Pública Telefónica Conmutada (PSTN) ofrecen.
- Algunos ahorros en el costo son debido a la utilización de una misma red para llevar voz y datos, especialmente cuando los usuarios tienen sin utilizar una parte importante de la capacidad de una red ya existente, la cual pueden usar para VoIP sin un costo adicional.
- Las llamadas de VoIP a VoIP entre cualquier proveedor son generalmente gratuitas, en contraste con las llamadas de VoIP a PSTN que generalmente tiene un costo para el usuario de VoIP.

Funcionalidad.

VoIP puede facilitar tareas que serían más difíciles de realizar usando las redes telefónicas tradicionales:

- Las llamadas telefónicas locales pueden ser automáticamente enrutadas a un teléfono VoIP, sin importar dónde se este conectado a la red.
- Números telefónicos gratuitos para usar con VoIP están disponibles en Estados Unidos de América, Reino Unido y otros países, de organizaciones como “Usuario VoIP”.
- Los agentes de *Call Center* usando teléfonos VoIP pueden trabajar en cualquier lugar, con una conexión a Internet lo suficientemente rápida.
- Algunos paquetes de VoIP incluyen los servicios extra por los que PSTN (Red Telefónica Conmutada) normalmente cobra un cargo adicional, o que no se encuentran disponibles en algunos países, como son las llamadas de conferencia, retorno de llamada, remarcado automático o identificación de llamadas.

Movilidad.

Los usuarios de VoIP pueden viajar a cualquier lugar en el mundo y seguir haciendo y recibiendo llamadas de la siguiente forma:

- Los subscriptores de los servicios de las líneas telefónicas pueden hacer y recibir llamadas locales fuera de su localidad. Por ejemplo, si un usuario tiene un número telefónico en la ciudad de San Salvador, pero está viajando por Europa y alguien llama a su número telefónico, esta llamada se recibirá en Europa. Además, si una llamada es hecha de Europa a San Salvador, ésta será cobrada como una llamada local, por supuesto, debe de haber una conexión a Internet disponible para hacer esto posible.
- Los usuarios de Mensajería Instantánea basada en servicios de VoIP pueden también viajar a cualquier lugar del mundo y hacer y recibir llamadas telefónicas.

- Los teléfonos VoIP pueden integrarse con otros servicios disponibles en Internet, incluyendo vídeo-llamadas, intercambio de datos y mensajes con otros servicios en paralelo con la conversación, audio conferencias, administración de libros de direcciones e intercambio de información con otros (amigos, compañeros, etc.).

Arquitectura de red.

El propio estándar define tres elementos fundamentales en su estructura:

- *Terminales:* Son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en *software* como en *hardware*.
- *Gatekeepers GK*: Son el centro de toda la organización VoIP y serían el sustituto para las actuales centrales. Normalmente implementados en *software* y, en caso de existir, todas las comunicaciones pasarían por éstos, realizando tareas de autenticación de usuarios, control de admisión, control de ancho de banda, encaminamiento, servicios de facturación y temporización, etc.
- *Gateways GW*: Se encargan del enlace de las redes VoIP con la red telefónica tradicional, actuando de forma transparente para el usuario.

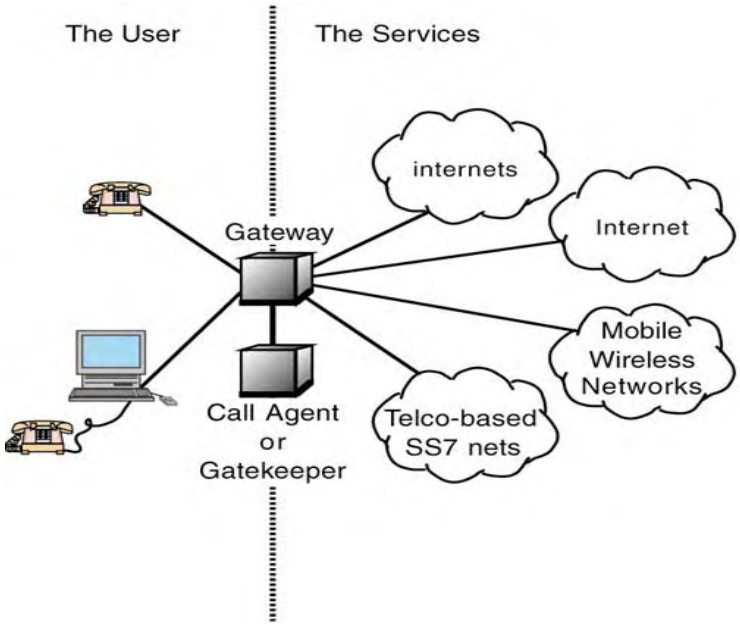


Figura No. 2 -Componentes de una red VoIP.

Con estos tres elementos, la estructura de la red VoIP podría ser la conexión de dos oficinas de una misma empresa. La ventaja es inmediata: todas las comunicaciones entre las oficinas son completamente gratuitas. Este mismo esquema se podría aplicar para proveedores, con el consiguiente ahorro que esto conlleva. Un ejemplo de conexión entre dos (2) empresas, se muestra en la figura siguiente:

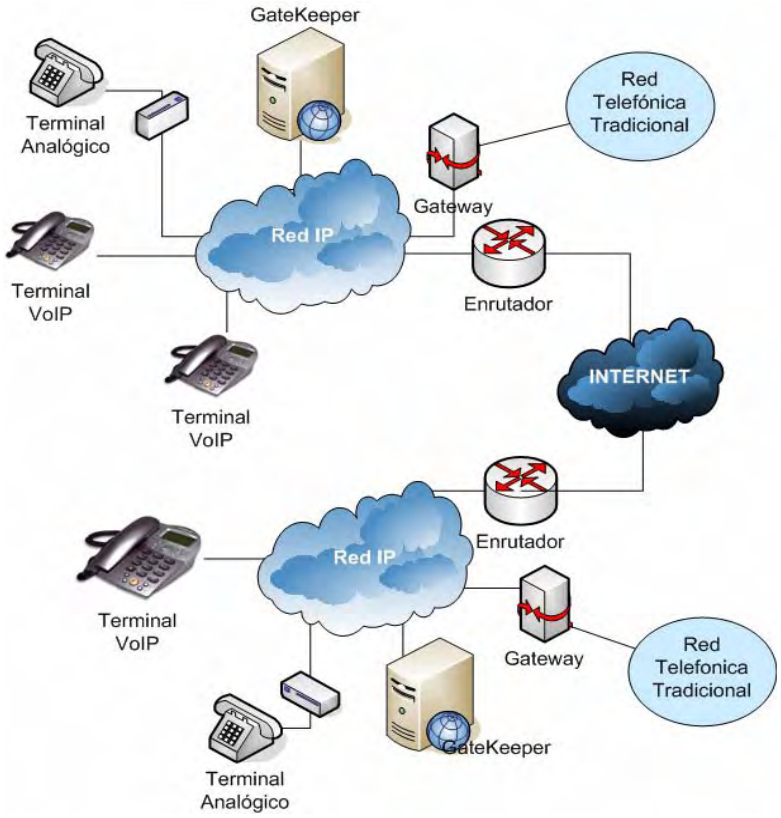


Figura No. 3 -Red básica de dos oficinas conectadas a través de Internet.

Factores a considerar en la VoIP.

El principal problema que presenta hoy en día la penetración tanto de VoIP como de todas las aplicaciones de IP, es el de "**garantizar la calidad de servicio sobre una red IP**", ya que con la existencia de retardos y limitaciones de ancho de banda, actualmente es muy difícil tener una buena calidad del servicio, encontrándonos con los siguientes problemas:

- *La Codificación de la Voz*: La voz ha de codificarse para poder ser transmitida por la red IP. Para ello se hace uso de ***Codecs*** que garanticen la codificación y compresión del audio o del vídeo, para su posterior decodificación y descompresión, antes de poder generar un sonido o imagen utilizable. Según el *Codec* utilizado en la transmisión, se utilizará más o menos ancho de banda. La cantidad de ancho de banda suele ser directamente proporcional a la calidad de los datos transmitidos. Entre los *codecs* utilizados en VoIP encontramos los G.711, G723.1 y el G.729.
- Retardo o latencia: Una vez establecidos los retardos de procesado y retardos de tránsito, la conversación se considera aceptable por debajo de 150ms.
- Calidad del servicio: La calidad de servicio se está logrando basándose en los siguientes criterios:

  - La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda al transmitir menos información.
  - Compresión de cabeceras aplicando los estándares RTP/RTCP.
  - Priorización de los paquetes que requieran menor latencia. Las tendencias actuales son:
    - CQ (*Custom Queuing*): Asigna un porcentaje del ancho de banda disponible.
    - PQ (*Priority Queuing*): Establece prioridad en las colas.
    - WFQ (*Weight Fair Queuing*): Se asigna la prioridad al tráfico de menos carga.
    - DiffServ: Evita tablas de encaminados intermedios y establece decisiones de ruta por paquete.

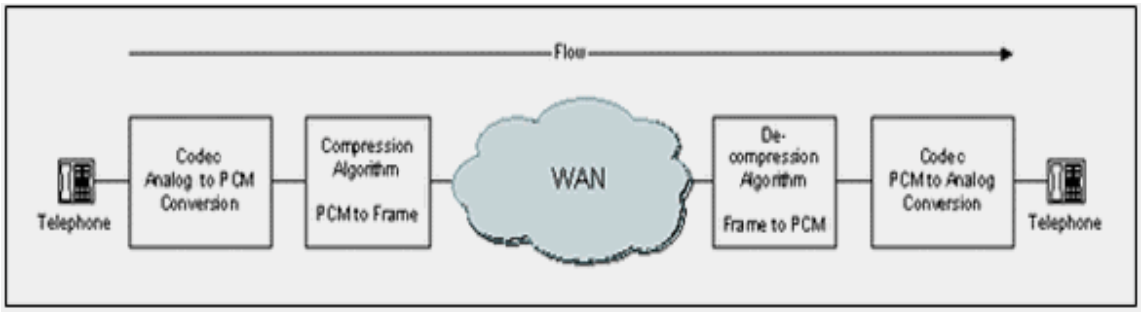


Figura No.4 -Flujo de un circuito de voz comprimido.

3.- Servicio PBX para Comunicación Analógica.

Un PBX o PABX (Private Branch Exchange o Private Automatic Branch Exchange), es la red telefónica privada utilizada dentro de una empresa, y puede ser cualquier central telefónica conectada directamente a la RTPC (Red Telefónica Pública Conmutada o PSTN, Public Switched Telephone Network) por medio de líneas troncales para gestionar, además de las llamadas internas, las entrantes y/o salientes con autonomía sobre cualquier otra central telefónica. Este dispositivo generalmente pertenece a la empresa que lo tiene instalado y no a la compañía telefónica.

La RTPC es una red de conmutación de circuitos, sobre la cual se transmiten múltiples llamadas a través de un mismo medio de transmisión. Una red de conmutación de circuitos es una red en la que existe una conexión dedicada. Una conexión dedicada es un circuito o un canal establecido entre dos nodos para que estos se puedan comunicar. Cuando se establece una llamada entre dos nodos, esa conexión sólo la pueden usar estos dos nodos. Cuando uno de los dos nodos termina la llamada, la conexión se cancela, liberando el circuito para que pueda utilizarse en otra conexión.

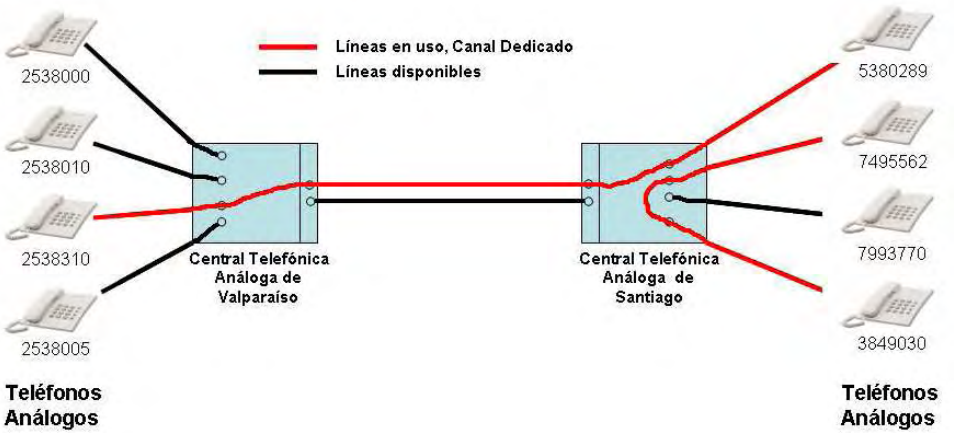


Figura No.5 - Esquema de telefonía tradicional, conmutación de circuitos.

Una PBX es un dispositivo que actúa como una ramificación de la RTPC, por lo que los usuarios no se comunican al exterior mediante líneas telefónicas convencionales, sino que al estar el PBX directamente conectado a la RTPC, será esta misma la que enrute la llamada hasta su destino final mediante enlaces unificados de transporte de voz llamados Enlaces PABX, también conocidos como líneas troncales.

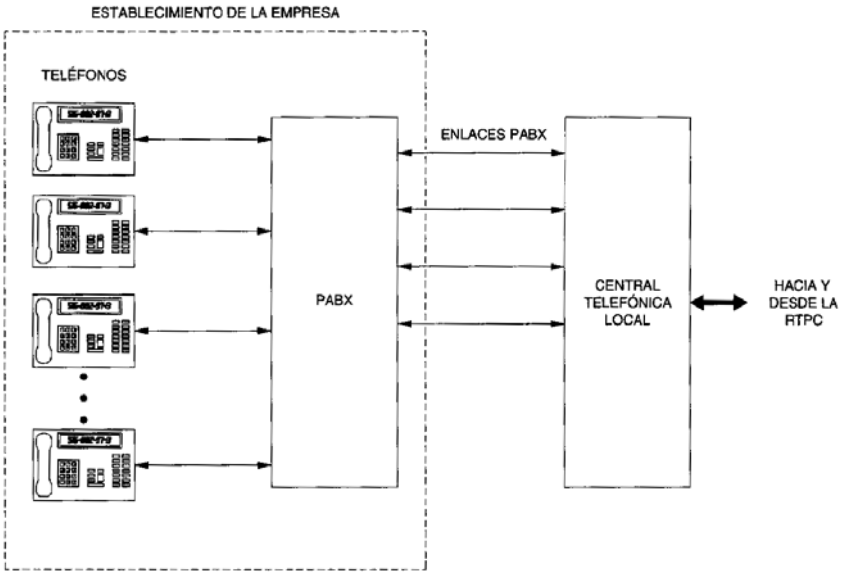


Figura No.6 - Conexión de teléfonos de una empresa a la RTPC por medio de una PABX.

Los enlaces pueden ser analógicos o digitales. En la actualidad, los enlaces digitales se utilizan para interconectar oficinas de conmutación de la RTPC (centrales telefónicas, centrales interurbanas), y los enlaces analógicos siguen siendo usados para conectar PABX con centrales telefónicas.

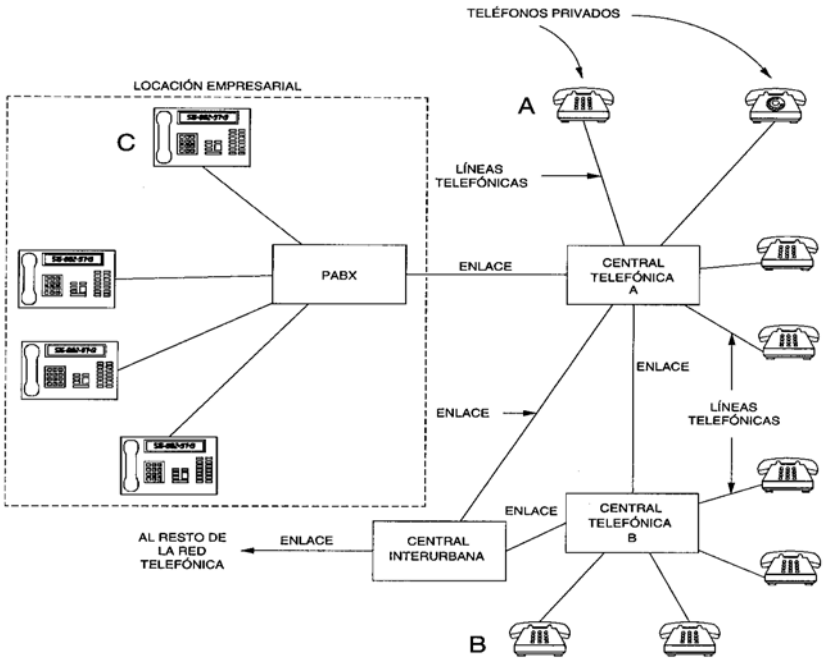


Figura No. 7 – Enlaces entre las oficinas de conmutación de la RTPC y las PABX.

Una PABX realiza tres funciones esenciales:

- Crear conexiones o circuitos entre los teléfonos de dos usuarios.(Llamadas internas o externas).
- Mantener la conexión el tiempo que los usuarios la necesiten.
- Proporcionar información para la contabilidad y/o facturación de llamadas.

Además existen los denominados Servicios Adicionales, entre los cuales podemos mencionar:

- Marcado automático.
- Contestador automático.

- Distribuidor automático de tráfico de llamadas.
- Desvió de llamadas.
- Transferencia de llamadas.
- Llamada en espera.
- Llamada en conferencia.
- Mensaje de bienvenida.
- Marcado interno directo (DID).
- No molestar (DND).
- Música en espera.
- Contestador automático de buzón de voz.

Las PABX pueden ser analógicas o digitales. Las PABX analógicas envían la voz y la información de señalización de llamada, como los tonos de teclado del número marcado, como sonido analógico. Por tanto, el sonido no se digitaliza nunca. Para dirigir correctamente la llamada, la PBX y la oficina central de la compañía telefónica tienen que escuchar la información de señalización.

Las PABX digitales codifican o digitalizan el sonido analógico en un formato digital. Normalmente, las PABX digitales codifican los sonidos de voz mediante un códec de audio estándar del sector como G.711 o G.729. Después de codificar la voz digitalizada, la envían por un canal mediante conmutación de circuitos.

En la actualidad las PABX analógicas se han quedado obsoletas, y son las PABX digitales las que dominan el mercado, siendo estas ultimas una computadora especializada, donde es el usuario el que puede configurar los parámetros de las llamadas entrantes y salientes. Generalmente el usuario conecta el PABX por un único enlace digital, como E1 ó T1, utilizando tan solo 2 pares de cables en lugar de *2n* hilos para las *n* líneas externas contratadas. Estos enlaces tienen capacidad de portar hasta 30 líneas sin llegar a comprimir la información de la voz lo suficiente

como para degradarla, mas 2 líneas que ocupan para la transmisión y recepción de información.

Se están desarrollando en el mundo del software libre, programas que realizan las funciones de una central PABX bajo Linux, tal es el caso del programa Asterisk. Con estos sistemas es posible integrar esta y más funciones en un solo computador que brinda comunicación telefónica, Internet y fax entre otros. Asterisk reemplaza completamente a una PABX, ya que realiza todas sus funciones y más, sin costos de licencia asociados.

Mientras la telefonía convencional ha levantado muros a la innovación, facilidad de uso (habitualmente se conocen un 20% de las funcionalidades de las PBX y se usan menos de un 10%) y reducción de costes, los servicios a través de Internet como el e-mail y las aplicaciones Web, han revolucionado el entorno empresarial debido en gran medida a la innovación constante en aplicaciones y servicios impulsada por los propios usuarios, basándose en estándares abiertos que han contribuido a su elevada difusión y a unos costos altamente competitivos, que han permitido su rápida implantación en empresas y organizaciones de todo tipo.

Hoy en día las aplicaciones en Internet manejan datos, multimedia, vídeo y música y la red se está convirtiendo en un componente esencial del negocio y de las soluciones IT de las empresas. Sólo en los últimos diez años, Internet y la Web han generado mas innovaciones que la telefonía convencional en toda su historia, por lo que no es descabellado apuntar que la siguiente etapa de innovación en las aplicaciones y servicios Web será en el ámbito de las comunicaciones telefónicas.

4.- Protocolos.

El protocolo para VoIP es el lenguaje que nos permite el transportar conversaciones telefónicas en tiempo real sobre redes basadas en IP, o dicho de otra manera, transportarlas en forma de paquetes IP.

En las comunicaciones VoIP, podemos diferenciar dos grupos importantes de protocolos, los cuales tienen bien definidas sus funciones:

- Los protocolos **de transporte y control**, que son los tradicionales de las redes IP como RTP/ RTCP/ TCP/ UDP/ IP.
- Los protocolos de **señalización**, que se han estado desarrollando a medida que los requerimientos de VoIP y sus servicios crecen. Estos protocolos los podemos dividir en:
  - Propietarios: como Skype y Cisco Skinny (SCCP).
  - De código abierto: como H.323, SIP, MGCP e IAX.

a.- Protocolos de Transporte y Control.

TCP, UDP, IP.

Estos protocolos son los más usados e importantes de la familia de protocolos de Internet. Fueron desarrollados por el departamento de defensa de los Estados Unidos en 1972, para la red ARPANET.

- IP (Internet Protocol). El Protocolo de Internet, es un protocolo no orientado a la conexión, usado tanto por el origen (host) como por el destino (host) para la comunicación de datos a través de una red de paquetes conmutados. Es un protocolo de capa 3 (Red o Internet), y los datos son enviados en bloques conocidos como paquetes o datagramas. Esta definido en la IETF (Internet Engineering Task Force – Grupo de Trabajo en Ingeniería de Internet) RFC 791 (Request For Comments – Petición de Comentarios) (IPv4) y en la IETF RFC 2460 (IPv6), implementando dos funciones básicas: Direccionamiento y Fragmentación.

- TCP (Transmission-Control-Protocol). El Protocolo de Control de Transmisión, es uno de los protocolos fundamentales de Internet. Es un protocolo de comunicación orientado a la conexión y fiable de capa 4 (Transporte), definido en la IETF RFC 793. TCP añade las funciones

necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe libre de errores, sin pérdidas y con seguridad, enviando todos los datos correctamente en la secuencia especificada. Esto puede convertirse en una desventaja en flujos en tiempo real, como lo es VoIP.

- UDP (User Datagram Protocol). Es un protocolo de capa 4 (Transporte), basado en el intercambio de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el datagrama incorpora suficiente información de direccionamiento en su cabecera. Esta definido en la IETF RFC 768. UDP al contrario de TCP, no tiene confirmación ni control de flujo, debido a esto es el protocolo usado en la transmisión de video y voz a través de una red, ya que no hay tiempo para enviar de nuevo paquetes perdidos cuando se esta escuchando a alguien o se esta viendo un video en tiempo real.

b.- Protocolos de Señalización de Código Abierto.

SUITE H.323.

El objetivo principal de este protocolo, cuando se diseño, era el de proveer a los usuarios con tele-conferencias que tuvieran capacidad de voz, video y datos sobre redes de conmutación de paquetes. En la actualidad es utilizado comúnmente para voz sobre IP (VoIP o telefonía IP) y para videoconferencia basada en IP.

H.323 es en realidad una recomendación paraguas que engloba un conjunto de protocolos, especifica los *codecs* que se deben emplear, tanto para manejar voz como vídeo, además de los protocolos necesarios para el transporte de la información (ya sea audio, vídeo o datos) o el intercambio de señalización de control entre los terminales y el elemento encargado del control de la red.

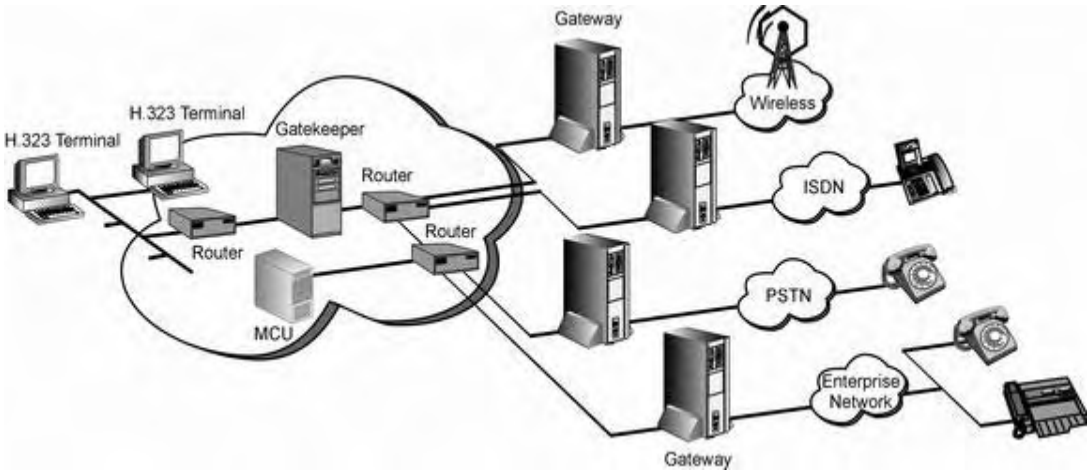


Figura No.8 –Típica Red H.323

Fuente: http://www.protocols.com/papers/voip2.htm

SIP.

El protocolo SIP nació en 1996 cuando Mark Handley y Eve Schooler presentaron el primer borrador ante la IETF (Internet Engineering Task Force -Grupo de Trabajo en Ingeniería de Internet), de lo que sería un protocolo de comunicaciones IP, que solucionaría gran parte de los inconvenientes de protocolos anteriores, como el H.323.

- SIP (Protocolo de Inicialización de Sesiones): Es un protocolo desarrollado por el grupo de trabajo IETF MMUSIC con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el vídeo, voz, mensajería instantánea, juegos en línea, aplicaciones CRM, realidad virtual y VoIP.
- SIP es un protocolo diseñado para ser utilizado en la Internet, con arquitectura cliente/servidor y mensajes tipo texto, similares a los mensajes HTTP.
- Los clientes SIP usan el puerto 5060 en TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*) para conectar con los servidores SIP. SIP permite iniciar y terminar llamadas de voz y vídeo, todas las comunicaciones de voz/vídeo van sobre RTP (*Real-time Transport Protocol*).

- SIP funciona en colaboración con otros muchos protocolos, pero sólo interviene en la parte de señalización, al establecer la sesión de comunicación. SIP actúa como envoltura al SDP (Protocolo de Descripción de Sesiones, publicado por la IETF en el RFC 2327), que describe el contenido multimedia de la sesión, por ejemplo, qué puerto IP y *codec* se usarán durante la comunicación. En un uso normal, las sesiones SIP son simplemente flujos de paquetes RTP (*Real-time Transport Protocol*). RTP es el verdadero portador para el contenido de voz, datos y vídeo.

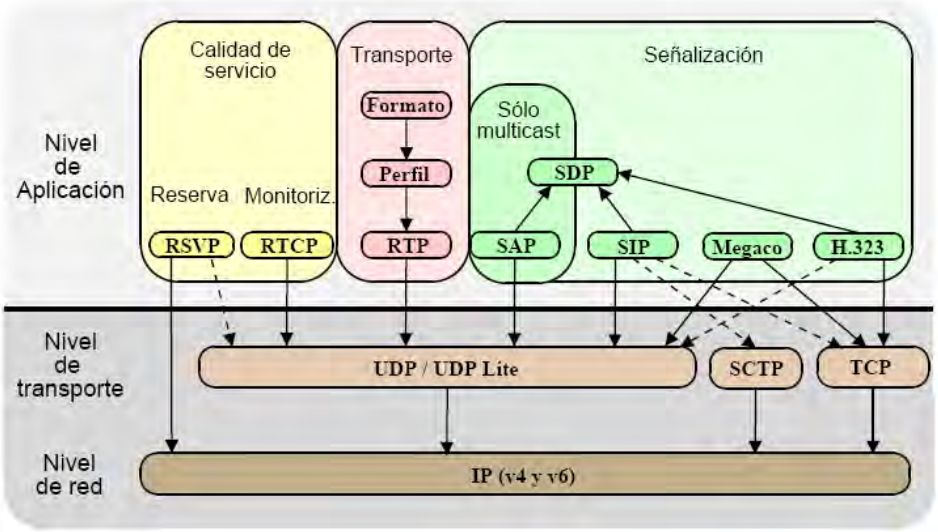


Figura No.9 – Protocolo SIP y su relación con otros protocolos.

SIP es similar a HTTP y comparte con él algunos de sus principios de diseño: es legible por humanos y sigue una estructura de petición-respuesta. Los promotores de SIP afirman que es más simple que H.323. Sin embargo, aunque originalmente SIP tenía como objetivo la simplicidad, en su estado actual se ha vuelto tan complejo como H.323. SIP comparte muchos códigos de estado de HTTP, como el familiar "404 no encontrado" (*404 not found*).

SIP y H.323 no se limitan a comunicaciones de voz y pueden mediar en cualquier tipo de sesión desde voz hasta vídeo y futuras aplicaciones todavía sin realizar.

MGCP.

MGCP (*Media Gateway Control Protocol*) define la comunicación entre los elementos de control de llamada denominados agentes de usuario o controladores de pasarela (MGC, *Media Gateway Controller*) y las pasarelas de voz sobre paquetes.

MGCP es un protocolo interno de VoIP, cuya arquitectura se diferencia del resto de protocolos VoIP por ser del tipo cliente-servidor. Este protocolo esta definido informalmente en la RFC 3435, y aunque no ostenta el rango de estándar, su sucesor, MEGACO o H.248 esta aceptado y definido como una recomendación en la RFC 3015. El Internet Engineering Task Force (IETF) creó MGCP para tratar algunos de los defectos percibidos de H.323.

El MGCP es un protocolo basado en texto y soporta un modelo de llamada centralizado. De hecho, este protocolo es una desviación del SGCP (Simple Gateway Control Protocol) y del IPDC (Internet Protocol Device Control).

MGCP simplifica las pasarelas al máximo, limitando sus funciones a la interconexión con redes de conmutación de circuitos, la notificación a los MGC de los eventos que ocurren en los terminales y la ejecución de comandos procedentes de los MGC. La inteligencia del control de llamadas se ubica en los MGC que envían comandos a las Pasarelas que están bajo su control.

El MGCP utiliza el protocolo SDP (Session Description Protocol) para describir la sesión, lo que quiere decir: el nombre y el propósito de la sesión, tiempo en que la sesión está activa y requerimientos de ancho de banda entre otros.

MGCP se transporta sobre UDP, conformándose la pila MGCP/UDP/IP de tal forma que los mensajes MGCP constituyen el cuerpo de datos de los datagramas UDP.

La comunicación entre los MGC y las MG se basa en el intercambio de comandos y la recepción de señales que indican el resultado de la ejecución de dichos comandos

en la MG. Debido a la simplicidad del protocolo, el número de comandos y señales definidos en MGCP es muy reducido.

MGCP facilita a un usuario de la red pública localizar el dispositivo de destino y establecer una sesión. Proporciona el interfaz gateway-to-gateway para SIP. MGCP simplifica los estándares de la tecnología VoIP eliminando complejidad, eliminando la necesidad de dispositivos IP que requieran muchas tareas de procesamiento y simplificando y reduciendo los costes de los terminales.

MGCP y MEGACO, Son protocolos utilizados principalmente por los proveedores de servicios de telefonía ya que permiten controlar de manera eficiente una gran cantidad de Gateways que a su vez poseen una gran cantidad de abonados POTS. De manera similar que entre H.323 y SIP, MGCP se utiliza mucho aunque poco a poco MEGACO le ha ido quitando terreno en soluciones con troncales o grandes cantidades de abonados POTS. Le especificación de MGCP no se desarrolla más y toda modificación sobre este tipo de arquitectura se realiza sobre la especificación de MEGACO/H.248.

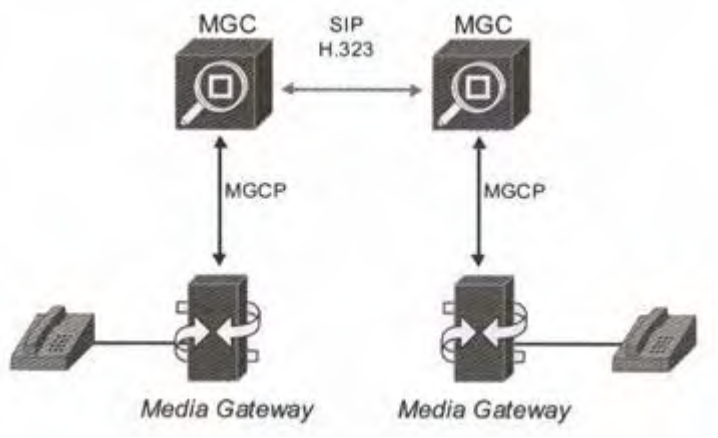


Figura No.10 – Arquitectura básica del Protocolo MGCP.

IAX.

IAX (*Inter-Asterisk eXchange protocol)* y su nueva versión IAX2, fueron creados por Mark Spencer (también creador de AsterisK) para subsanar una serie de

problemas o inconvenientes que se encontró al utilizar SIP en VoIP y que pensó que debían de ser mejorados.

IAX2 es robusto, lleno de novedades y muy simple en comparación con otros protocolos. Permite manejar una gran cantidad de *códecs* y un gran número de *streams*, lo que significa 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. El tráfico de voz es transmitido *in-band*, lo que hace a IAX2 un protocolo casi transparente a los cortafuegos y realmente eficaz para trabajar dentro de redes internas. En esto se diferencia de SIP, que utiliza una cadena RTP *out-of-band* para entregar la información.

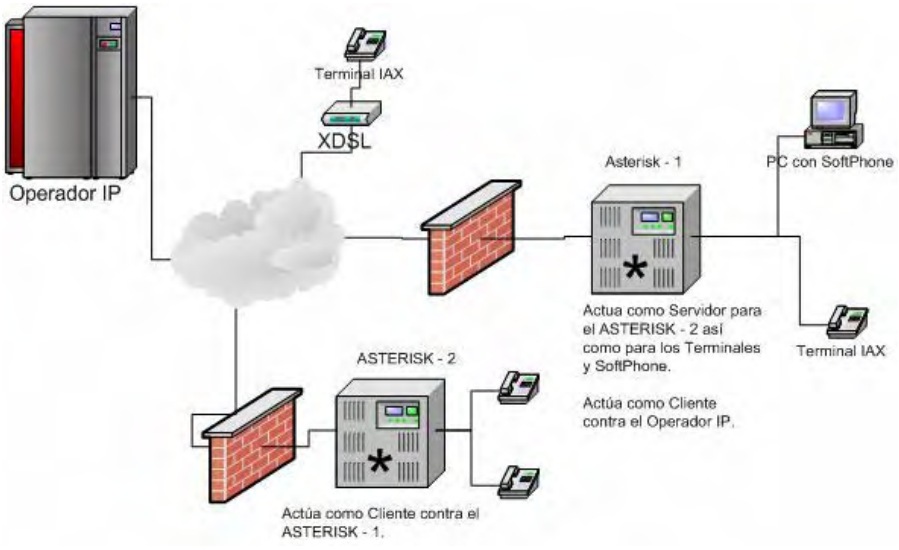


Figura No. 11 – Protocolo IAX con Asterisk como servidor y como cliente.

Las principales diferencias ente IAX y SIP son las siguientes:

- Ancho de banda.

IAX utiliza un menor ancho de banda que SIP ya que los mensajes son codificados de forma binaria mientras que en SIP son mensajes de texto. Asimismo, IAX intenta reducir al máximo la información de las cabeceras de los mensajes reduciendo también el ancho de banda.

- NAT.

En IAX la señalización y los datos viajan conjuntamente con lo cual se evitan los problemas de NAT que frecuentemente aparecen en SIP. En SIP la señalización y los datos viajan de manera separada y por eso aparecen problemas de NAT en el flujo de audio cuando este flujo debe superar los routers y firewalls. SIP suele necesitar un servidor STUN para estos problemas.

- Estandarización y uso.

SIP es un protocolo estandarizado por la IETF hace bastante tiempo y que es ampliamente implementado por todos los fabricantes de equipos y software. IAX está aun siendo estandarizado y es por ello que no se encuentra en muchos dispositivos existentes en el mercado.

- Utilización de puertos.

IAX utiliza un solo puerto (4569) para mandar la información de señalización y los datos de todas sus llamadas. Para ello utiliza un mecanismo de multiplexión o “trunking”. SIP, sin embargo utiliza un puerto (5060) para señalización y 2 puertos RTP por cada conexión de audio (como mínimo 3 puertos). Por ejemplo para 100 llamadas simultáneas con SIP se usarían 200 puertos (RTP) más el puerto 5060 de señalización. IAX utilizaría sólo un puerto para todo (4569).

- Flujo de audio al utilizar un servidor.

En SIP si utilizamos un servidor la señalización de control pasa siempre por el servidor pero la información de audio (flujo RTP) puede viajar extremo a extremo sin tener que pasar necesariamente por el servidor SIP. En IAX al viajar la señalización y los datos de forma conjunta todo el tráfico de audio debe pasar obligatoriamente por el servidor IAX. Esto produce un aumento en el uso del ancho de banda que deben soportar los servidores IAX sobretodo cuando hay muchas llamadas simultáneas.

- Otras funcionalidades.

IAX es un protocolo pensado para VoIP y transmisión de video y presenta funcionalidades interesantes como la posibilidad de enviar o recibir planes de marcado (dialplans) que resultan muy interesante al usarlo conjuntamente con servidores Asterisk. SIP es un protocolo de propósito general y podría transmitir sin dificultad cualquier información y no sólo audio o video.

Figura No. 12 – Troncal IAX entre dos servidores Asterisk.

5.- Codec de Voz.

La comunicación por voz es una señal analógica, y la transmisión de información por una red de datos es una señal digital. El proceso de convertir señales analógicas a señales digitales se hace con un COdificador-DECodificador

(CODEC), cuya finalidad es digitalizar la voz humana para ser enviada por las redes de datos.

Los CODECs son algoritmos utilizados para traducir una señal analógica (voz y video), en un fichero digital lo más compacto posible, y posteriormente reproducir la forma original de la onda con la mayor fidelidad posible.

La compresión de la forma de onda representada puede permitir el ahorro del ancho de banda. Esto es especialmente interesante en los enlaces de poca capacidad y permite tener un mayor número de conexiones de VoIP simultáneamente. Otra manera de ahorrar ancho de banda es el uso de la supresión del silencio, que es el proceso de no enviar los paquetes de la voz entre silencios en conversaciones humanas.

En el proceso de conversión análogo-digital, la mayoría de CODECs utilizan PCM (Pulse Code Modulation), que se realiza en tres pasos:

1) Muestreo (sampling). Consiste en tomar valores instantáneos (muestras) de una señal analógica, a intervalos de tiempo iguales.

2) Cuantificación (quantization). Es el proceso mediante el cual se asignan valores discretos, a las amplitudes de las muestras obtenidas en el proceso de muestreo.

3) Codificación (codification). Es el proceso mediante el cual se representa una muestra cuantificada, mediante una sucesión de “1”s y “0”s, es decir, mediante un número binario.

Para elegirlos se debe tener en cuenta:

– Calidad de sonido.
– Ancho de banda requerido.
– Requisitos de computación.

La ITU-T (Unión Internacional de Telecomunicaciones), define una serie de CODECs como una recomendación, de la siguiente manera:

- Recomendaciones G: La serie de recomendaciones G trata sobre los sistemas de transmisión y multimedia, sistemas digitales y redes; los más importantes utilizados en la actualidad son:

G.711: Estas recomendaciones definen los codificadores y decodificadores de voz que permiten una calidad de voz de 64 *Kilobits* por segundo (Kbps) mediante la utilización del método de modulación por codificación de pulsos (PCM). El G.711 utiliza *A-law* o *μ-law* para una compresión simple de amplitud y es el requisito básico de la mayoría de los estándares de comunicación multimedia de la ITU.

G.723.1: Estas recomendaciones definen el *ratio* dual de voz para el codificador, en comunicaciones multimedia que transmiten a 5.3Kbps y 6.3Kbps. Este codificador es ampliamente utilizado en aplicaciones para redes de voz sobre IP (VoIP) y para la codificación de la voz en aplicaciones de videoconferencias. En cualquier lugar que el protocolo G.723.1 es utilizado a una velocidad de 6.3Kbps, es comúnmente conocido como *MultiPulse-Maximum Likelihood Quantization* (MP-MLQ). Cuando G723.1 está funcionando a una velocidad de 5.3Kbps, es conocido como *Algebraic Code Excited Linear Prediction* (ACELP).

G.726: También llamadas *Adaptive Diferencial Pulse Code Modulation* (ADPCM) y es designada para comprimir la voz a 32Kbps por defecto. Este protocolo es recomendado para convertir canales PCM tipo *A-law* o *μ-law* de 8,000 muestras por segundo y 64Kbps hacia canales de 40Kbps, 32Kbps, 24Kbps o 16Kbps y viceversa.

G.728: Esta recomendación define un estándar de codificación de voz con bajo retardo, que permite compresiones de alta calidad para 8,000 muestras por segundo. La codificación funciona a un ratio de 16,000 bits por segundo (16 Kbps) y

es ampliamente utilizada para aplicaciones que requieren bajos algoritmos de retardo. G.728 es llamado a menudo *Low Density Code Excited Linear Prediction* (LD-CELP).

G.729: Establece la codificación de la voz a 8Kbps, utilizando el método llamado *Conjugate Structure Algebraic Code Excited Linear Prediction* (CSACELP). Estas recomendaciones codifican señales de audio cerca de la calidad tarificada con un ancho de banda de 3.4Khz para su transmisión a una velocidad de 8Kbps. G.729A requiere una potencia de ordenador más baja que G.729 y G.723.1. Tanto G.729 como G.729A tienen una latencia (el tiempo que necesita para convertir de analógico a digital) más baja que G.723.1. Se espera que G.729A tenga un impacto mayor en la compresión de voz para su transmisión sobre redes inalámbricas.

El codificador procesa tramas de muestreo de habla de 10ms a una velocidad de 8 Khz mínimo, que junto a una anticipación de 5ms se traduce en un retraso algorítmico total de 15ms. Para cada trama de 80 muestras de datos PCM lineales de 16 bits, el codificador obtiene cinco palabras de 16 bits. Las aplicaciones que utilizan el *vocoder* G.729 incluyen telefonía digital, comunicaciones vía satélite e inalámbricas y Voz sobre *Frame Relay* (VoFR).

Comparación de CODECs utilizados para VoIP.

- ✓ GIPS- 13.3 Kbps y mayores (la que usa Skype).
- ✓ GSM- 13 Kbps (full rate), frecuencias de 20ms, alta calidad (estándar en red celular GSM).
- ✓ iLBC- 15 Kbps, con frecuencia 20ms; 13.3 Kbps, con frecuencia 30ms. Alta calidad, alto uso de cpu.
- ✓ ITU G.711- 64 Kbps (conocido como aLaw/ uLaw PCM), calidad estándar TECO.
- ✓ ITU G.722- 48/56/64/ Kbps, alta calidad, casi igual que G.711.
- ✓ ITU G.723.1- 5.3/6.3 Kbps, frecuencia 30ms. Calidad baja, útil para módems.

- ✓ ITU G.726- 16/24/32/40 Kbps, alta calidad.
- ✓ ITU G.728- 16 Kbps, media calidad, alto uso de cpu.
- ✓ ITU G.729- 8 Kbps, frecuencia 10ms. Media calidad, muy usado.
- ✓ Speex- 2.15 a 44.2 Kbps, calidad variable, usa mucha cpu.
- ✓ LPC10- 2.5 Kbps, baja calidad, poco uso.
- ✓ DoD CELP- 4.8 Kbps, idem LPC10.

6.- Hardware Disponible para VoIP.

Con el estado de madurez que ha alcanzado la tecnología VoIP, hoy en día a la hora de seleccionar hardware, nos encontramos con que hay una gran variedad de fabricantes y modelos de equipos de donde seleccionar. Cada uno con sus ventajas y desventajas, a la hora de configurar y obtener soporte técnico.

En los inicios de la VoIP, para un usuario utilizar una aplicación de voz sobre el protocolo de Internet VoIP, significa conectar un micrófono y unos auriculares a la computadora. En la actualidad, gracias a diversos dispositivos y adaptadores para teléfonos, es posible utilizar los servicios VoIP sin depender de la computadora y mediante un teléfono normal.

Debido al gran número de hardware para VoIP que existe, se han dividido en tres grupos principales:

- Adaptadores telefónicos. Módulos externos como las pasarelas (Gateway), que sirven de puente entre las señales analógicas y las señales digitales.
- Teléfonos IP. Conectados a una computadora o conectados directamente a la red VoIP.
- Hardware interno para computadora. Diferentes tipos de tarjetas para la conexión de equipos analógicos y/o digitales, en una computadora.

El hardware que se necesite, dependerá de la aplicación y de la complejidad de la red VoIP, como se describe a continuación detallando todos los equipos que se utilizan:

1) **Pasarela FXO.** Se utiliza cuando necesitamos conectar líneas telefónicas analógicas con una central telefónica VoIP (IP PBX).

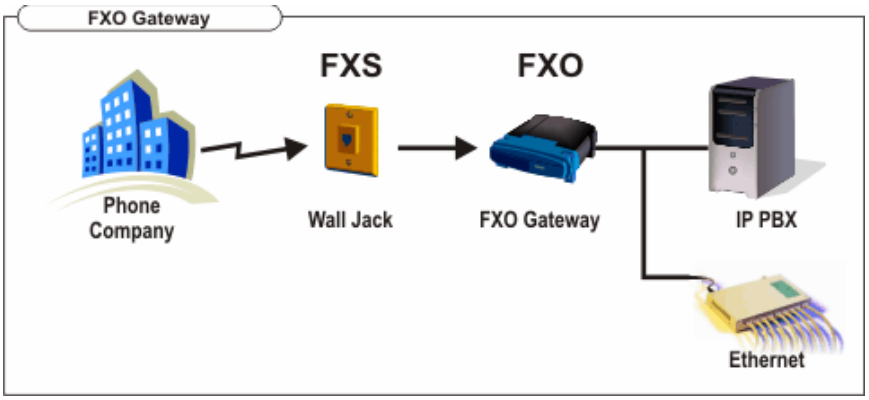


Figura No. 13 – Pasarela FXO con interfaces FXO.

Interfaz FXS. La interfaz de abonado externo, es el puerto que envía la línea analógica hacia el abonado.

Tarjeta FXS. Tarjeta con interfaz FXS para conectar teléfonos analógicos, hacia una red VoIP.

Figura No. 14 – Tarjeta con interfaces 1 FXS y 2 FXO.

Interfaz FXO. La interfaz de central externa, es el puerto que recibe la línea analógica.

Tarjeta FXO. Tarjeta con interfaz FXO para conectar líneas analógicas, hacia una red VoIP.

Figura No. 15– Pasarela FXO (FXO Gateway) con 6 interfaces (lines) FXO.

IP PBX. Son equipos con funciones de PBX, especialmente diseñados para aplicaciones de Voz sobre IP (VoIP), con conmutación local.

Figura No. 16– IP PBX con un puerto FXS (Fax/Phone) y un puerto FXO (Line).

2) **Pasarela FXS**. Se usan para conectar una o más líneas telefónicas analógicas de una PBX tradicional, con una IP PBX o con Internet.

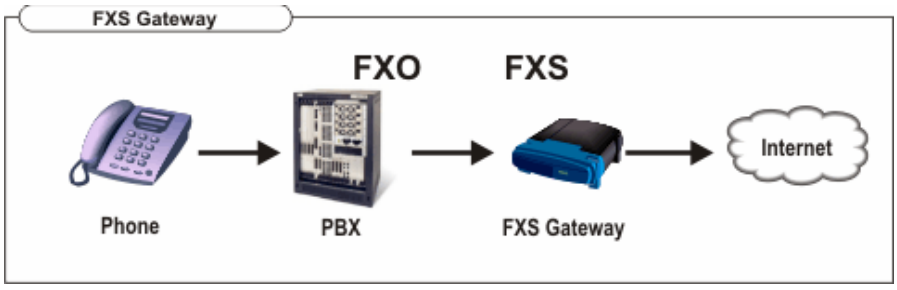


Figura No. 17 – Pasarela FXS con interfaces FXS.

Pasarela FXS con dos interfaces FXS, para conectar líneas analógicas de un sistema PBX tradicional, hacia una red VoIP o hacia Internet.

Figura No. 18 – Pasarela FXS (FXS Gateway) con 2 interfaces FXS.

3) Una variación de la pasarela FXS, es el **Adaptador FXS**, también denominado **Adaptador ATA**. Que se usa para conectar directamente teléfonos analógicos o aparatos de fax, con un sistema telefónico VoIP o Internet.

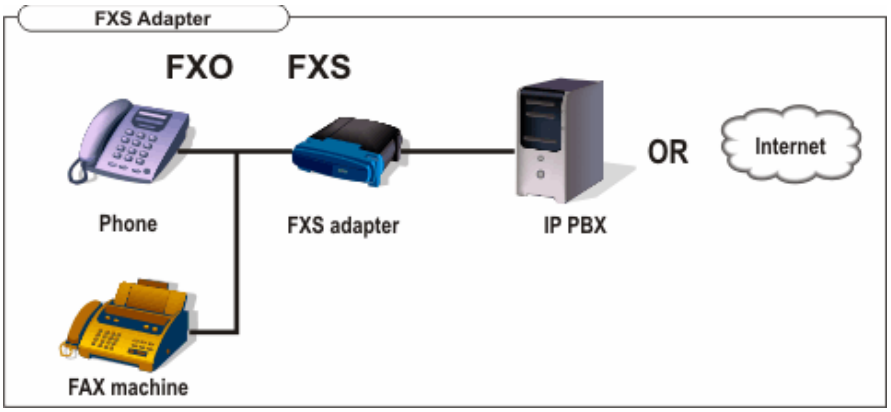


Figura No. 19 – Adaptador FXS (FXS adapter) con interfaces FXS.

Un adaptador ATA es un dispositivo que permite utilizar un teléfono convencional en servicios de VoIP. De esta manera, no es necesario adquirir un nuevo equipo para su uso en una red VoIP, facilitando la integración de la telefonía tradicional con la voz sobre IP.

Figura No. 19 – Adaptador ATA para VoIP.

También se cuenta con hardware que no necesita de otro equipo para conectarse a una red VoIP, entre los cuales tenemos:

Teléfonos VoIP mediante conexión USB.

Estos dispositivos se conectan al puerto USB de la computadora y hacen las veces de micrófono y auricular. Dependiendo del modelo, pueden estar preconfigurados para ser utilizados con los proveedores de VoIP más populares, así como ser compatibles con los sistemas de VoIP de Skype, Yahoo! Messenger, MSN Messenger, etc. Disponen de un teclado para poder realizar llamadas.

Teléfonos VoIP independientes.

Estos dispositivos están basados en hardware y no necesitan estar conectados a una computadora para funcionar. Externamente son similares a los teléfonos convencionales y disponen de varios puertos para su conexión de forma directa al router del usuario. Entre los modelos que se pueden encontrar en el mercado, destacan aquellos compatibles con servicios de VoIP y videoconferencias.

Dentro de esta misma categoría, existen dispositivos compatibles con Skype.
En cuanto a conectividad, puede enlazar con Internet mediante un cable Ethernet o bien por wifi.

Tarjetas telefónicas digitales.

Tarjetas que manejan varios puertos de entrada, que soportan cientos de llamadas de voz simultáneamente, sobre líneas T1, E1 o J1, a 32.8 Mbps en full dúplex.

PBXs Standalone, basadas en asterisk, para pequeños, medianos y grandes negocios. Una IP PBX completa que pueden manejar cientos de usuarios.

Figura No. 20 PBX Standalone Asterisk.

Enrutador Ethernet con puerto para teléfono VoIP. El puerto telefónico le permite usar una línea de teléfono estándar para hacer llamadas telefónicas convencionales o llamadas de voz sobre IP.

Figura No. 21 Errutador Ethernet.

7.- Distribuciones Libres para VoIP.

El software libre nos abre las puertas a un mundo de innovaciones y desarrollo tecnológico gracias a la disponibilidad del código fuente, lo cual nos permite entender mejor el funcionamiento de la misma y poder adaptar las aplicaciones a nuestras necesidades y/o mejorarlas, algo que normalmente no se puede con el software propietario o no libre.

La voz sobre IP (VoIP) tiene sus bases en el mundo del software libre, ya que la mayor parte de los protocolos de Internet fueron diseñados para trabajar originalmente sobre sistemas Unix, del cual se origina GNU/Linux.

Una aplicación de software libre que ha popularizado grandemente a la VoIP, es **Asterisk**, un software que proporciona funcionalidades de una central telefónica PBX, y que originalmente fue desarrollada para funcionar con el sistema operativo GNU/Linux, soportando muchos protocolos VoIP como lo son SIP, H.323, IAX y MGCP.

Actualmente existe una multitud de empresas relacionadas con Asterisk. La mayor parte de ellas siguiendo uno de los modelos de negocio más habituales del software libre, como es el de aportar valor añadido al software, en este caso mediante el diseño, instalación, formación y mantenimiento de centralitas telefónicas basadas en Asterisk.

La empresa Digium, fundada por Mark Spencer, administra y mantiene el código fuente de Asterisk, y vende hardware de calidad creado especialmente para Asterisk.

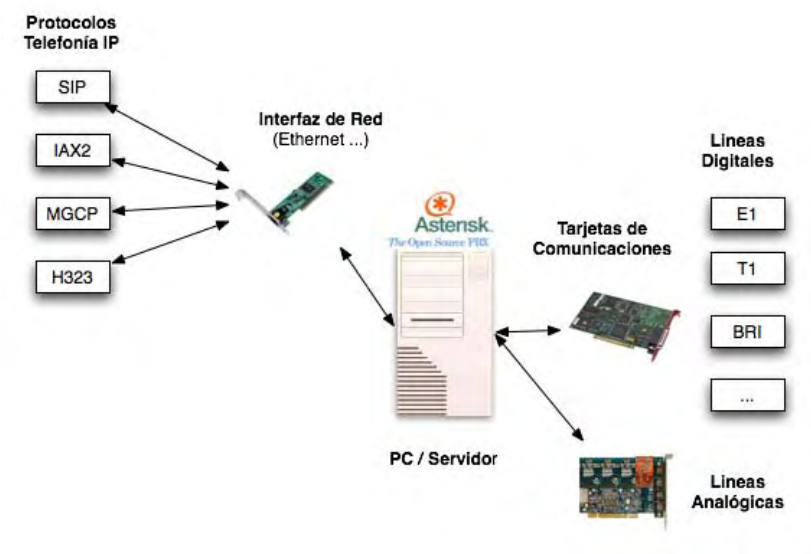


Figura No. 22 – Esquema conceptual.

La instalación y configuración de Asterisk puede llegar a ser larga y complicada, ya que se deben descargar varios paquetes, como Zaptel y Libpri, y ser instalados en un orden especifico, para evitar inconvenientes en su operación.

Para facilitarnos la instalación y posterior mente la administración de Asterisk, tenemos una serie de distribuciones libres con Asterisk preconfigurado e interfaz administrativa web, entre las que podemos mencionar:

- AsteriskNOW : Basada en rPath Linux, incluye Asterisk-GUI. Es una distribución ligera que incluye el mínimo de software, imprescindible para montar un servidor Asterisk dedicado.

- trixbox The Open Platform for Business Telephony : Basado en CentOS Linux, incluye FreePBX entorno grafico. Es una PBX con servicio para VoIP, diseñado para empresas de 2 a 500 empleados. Posee dos tipos de versiones:
  I. TrixBox CE (Community Edition). Se caracteriza por su flexibilidad y es utilizada por empresas de todo el mundo.
  II. TrixBox Pro (comercial de paga). Con tres versiones SE, EE y CCE. Es una versión empresarial que se ejecuta sobre tecnología PBXtra.
- elastix CUSTOM MADE TELEPHONY : Basado en CentOS Linux, incluye FreePBX. Distribución libre de Servidor de Comunicaciones Unificadas que incluye VoIP PBX, fax, mensajería instantánea, Email y colaboración.
- thirdlane technologies : Basado en Linux y FreeBSD, es fácil de instalar, adaptar al cliente y gestionar. Usa Webmin como plataforma para la administración. Es una distribución comercial de pago.
- asterisk : Es una distribución embebida basada en Linux e incluye herramientas como OpenSer, ocupando apenas 40Mb por lo que se puede hacer funcionar en una compact flash o llave USB.

8.- TrixBox sobre Plataforma Linux.

Trixbox es una distribución del sistema operativo GNU/Linux, basado en Centos que tiene la particularidad de ser una central telefónica (PBX) por software basada en la PBX de código abierto Asterisk. Como cualquier central PBX, permite interconectar teléfonos internos de una compañía y conectarlos la red telefónica convencional (RTB - Red telefónica básica).

El paquete **trixbox** incluye muchas características que antes sólo estaban disponibles en caros sistemas propietarios como creación de extensiones, envío de

mensajes de voz a e-mail, llamadas en conferencia, menús de voz interactivos y distribución automática de llamadas.

Trixbox, al ser un software de código abierto, posee varios beneficios, como es la creación de nuevas funcionalidades. Algo muy importante es que no sólo soporta conexión a la telefonía tradicional, sino que también ofrece servicios VoIP -voz sobre IP-, permitiendo así ahorros muy significativos en el costo de las llamadas internacionales, dado que éstas no son realizadas por la línea telefónica tradicional, sino que utilizan Internet. Los protocolos con los cuales trabaja pueden ser SIP, H.323, IAX, IAX2 y MGCP

Trixbox se ejecuta sobre el sistema operativo Centos y está diseñado para empresas de 2 a 500 empleados.

Componentes principales.

Los componentes principales de **TrixBox** son:

- **Linux Centos.**

  Es la distribución Linux que sirve como sistema operativo base, que a su vez está basada en Linux Red Hat Enterprise.

- **Asterisk.**

  Es el núcleo de telefonía. Cuando hablamos de Asterisk incluimos también los controladores de Zapata Telephony (zaptel) y la biblioteca para soporte RDSI (libpri).

- **FreePBX.**

  Es el entorno gráfico que facilita la configuración de Asterisk, no a través de la edición de archivos de texto, sino a través de interfaces web amigables.

- **Flash Operator Panel (FOP).**

  El FOP es una aplicación de monitorización de Asterisk tipo operadora accesible desde la Web.

- ***Web Meet Me Control.***

  El administrador de salas de conferencias múltiples o MeetMe, accesible desde la Web.

- ***A2Billing.***

  Una plataforma para llamadas prepagadas compatible con Asterisk y con Trixbox.

- **SugarCRM.**

  SugarCRM es un software que implementa la administración de las relaciones con el cliente (Customer Relationship Management), permitiendo básicamente facilitar tres procesos en los cuáles se ven involucradas la mayoría de la empresas con sus clientes: marketing, ventas y soporte. Además, sirve para almacenar todos los datos y actividades con el cliente, como reuniones, llamadas, correos, etc.

Ediciones de Trixbox.

Trixbox posee dos tipos de versiones:

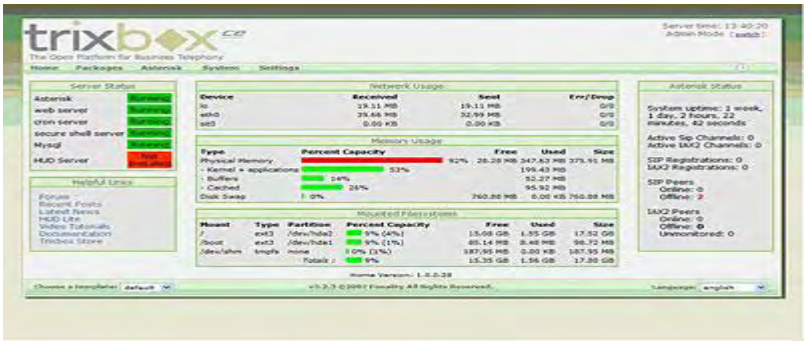


Fig. No. 23
Trixbox CE.

1) TrixBox CE (Community Edition).

Comenzó en el año 2004 como un proyecto popular IP-PBX denominado Asterisk@Home. Desde ese momento se convirtió en la distribución más popular, con más de 65.000 descargas al mes. Dicha versión se caracteriza por dos pilares importantes: su flexibilidad para satisfacer las necesidades de los clientes y, sobre todo, por ser gratuita.

¿Por qué utilizar TrixBox CE?

Tal como se dijo anteriormente TrixBox CE es una versión muy flexible, que no solo permite configurar funciones y módulos parametrizables para las necesidades de cada cliente, sino que también es posible acudir a la comunidad de TrixBox para ayudar o ser ayudado. Esta es una de las más grandes y más activas del mundo y sus miembros trabajan entre ellos día a día con el fin de responder consultas, resolver problemas, fallos y en seguir desarrollando la herramienta.

¿Quién utiliza TrixBox CE?

Empresas de todo el mundo, desde aquellas que posen muy pocas estaciones de trabajo, hasta medianas compañías que poseen cientos de empleados.

2) TrixBox Pro (Versión comercial pagada).

Es una solución denominada "hibrid-hosted", que significa que el cliente puede realizar una monitorización 24 horas al día los 7 días de la semana, administrar la central desde cualquier lugar y recibir actualizaciones del software de manera automática.

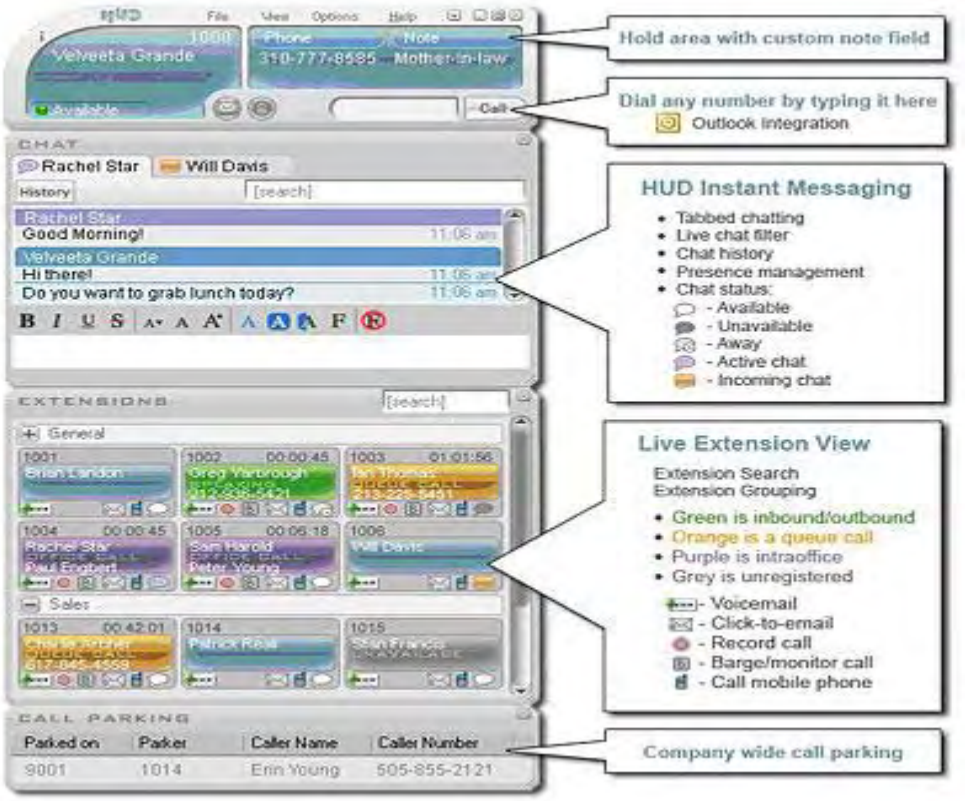


Figura No. 24

Captura de pantalla de la Herramienta HUD

Trixbox Pro es una versión empresarial que se ejecuta sobre tecnologías PBXtra, comercializada desde el 2004 permitiendo enviar/recibir más de 120 millones de llamadas por día. La familia trixbox Pro posee 3 versiones:

- Standard Edition (SE) (Gratis).
- Enterprise Edition (EE) (Bajo costo).
- Call Center Edition (CCE) (Bajo costo).

Códecs que soporta.

- ADPCM
- G.711 (A-Law & μ-Law)
- G.722

- G.723.1 (pass through)
- G.726
- G.729 (through purchase of a commercial license)
- GSM
- iLBC

Protocolos con los que trabaja.

- IAX™ (Inter-Asterisk Exchange)
- IAX2™ (Inter-Asterisk Exchange V2)
- H.323
- SIP (Session Initiation Protocol)
- MGCP (Media Gateway Control Protocol)
- SCCP (Cisco® Skinny®)
- Traditional Telephony Interoperability
- FXS
- FXO
- DTMF support
- PRI Protocols

9.- IpCop como seguridad perimetral.

IPCop es un proyecto GNU/GPL. Se trata de un firewall basado en Linux y su interface de usuario es totalmente Web.

Requiere de hardware dedicado y permite gestionar el acceso a Internet, la seguridad y la interacción da hasta cuatro redes distintas, que se denominan GREEN, BLUE, ORANGE y RED.

GREEN: Esta es la interfase de red de nuestra LAN o red de área local. Aquí es donde conectaremos todos nuestros equipos que necesiten mayor protección, como servidores que no tengan que tener presencia en Internet y puestos de trabajo. Los

dispositivos que se encuentren conectados a esta interfase tendrán acceso irrestricto a las interfases RED, BLUE y ORANGE, o sea que podrán salir a Internet (y conectarse a los equipos que se encuentren en cualquiera de estas otras tres redes) por cualquier puerto, pero a su vez los equipos de la interfase RED (equipos en Internet) no pueden iniciar conexiones a ningún equipo que se encuentre en las interfases GREEN, BLUE y ORANGE. En otras palabras, estarán protegidos del exterior, en el sentido que no son accesibles desde Internet.

BLUE: Es la interfase que se asigna normalmente para conectar un access point de modo que se puedan conectar dispositivos inalámbricos. De todas maneras sirve para conectar cualquier otra red que se necesite sea esta inalámbrica o no. Los dispositivos que se encuentren en esta red, no podrán iniciar una conexión a los dispositivos que se encuentren en la interfase GREEN, pero salvo esta excepción, contarán con el mismo nivel de acceso y protección que cuentan los dispositivos conectados a la interfase GREEN. No es necesario activar esta interfase en una instalación de IPCop si no se cuenta con más de una red, o no se va a utilizar un router inalámbrico.

ORANGE: Esta es la interfase que se utilizará para montar una DMZ o zona desmilitarizada. Principalmente se utiliza para montar servidores web, de correo, de ftp, etc. que deban tener presencia en Internet; o sea que sean accesibles desde Internet, pero que en el caso que se produzca alguna intrusión a algún equipo de esta red, eso no comprometa la seguridad de nuestra red interna (GREEN). Los equipos que formen parte de la red ORANGE no podrán iniciar conexiones a ninguno de los dispositivos que se encuentren en las interfases GREEN y BLUE. No es necesario activar esta interfase en una instalación de IPCop si no se piensa utilizar una DMZ.

RED: Es la interfase de red que nos conectará directamente a nuestro proveedor de Internet. Puede ser una conexión ADSL, cablemodem, una línea dedicada o hasta inclusive un modem telefónico común. Obviamente que por razones de ancho de

banda esta última opción es desaconsejable, pero es perfectamente factible tenerla configurada para una contingencia en la cual nuestro proveedor de Internet tenga inconvenientes para brindarnos nuestro vínculo habitual, pero si este operativo el acceso dialup. Cualquier instalación de IPCop contará con esta interfase habilitada. (Soporta tanto dispositivos ethernet como USB).

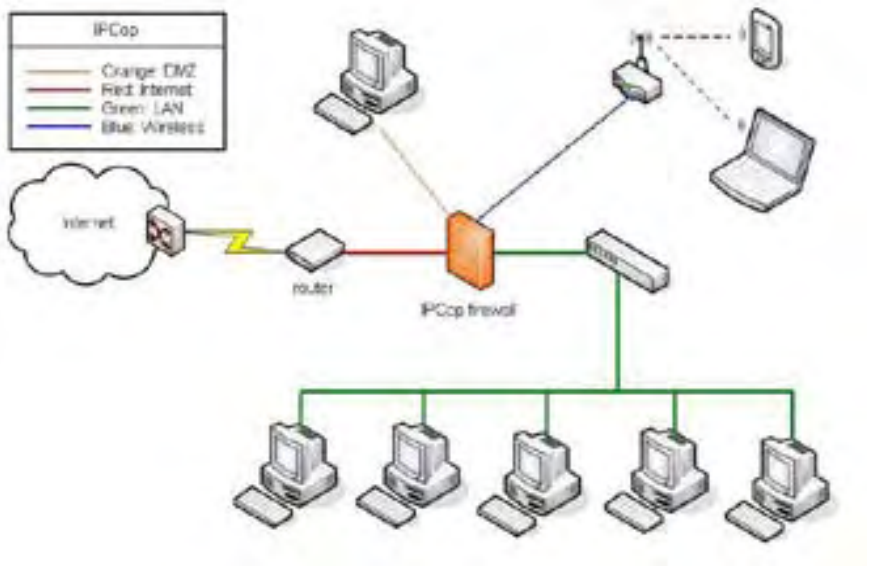


Figura No. 25 – Cuatro redes protegidas por IPCop.

Estas cuatro posibles redes, no son más que cuatro placas (tarjetas) de red instaladas en la misma computadora. No es necesario utilizar las cuatro, sino que se puede configurar de diferentes maneras, dependiendo de las necesidades que se tengan.

Funcionalidades. IPCop brinda una amplia gama de funcionalidades:

- Acceso seguro por SSL a la interfase de administración web.
- DHCP cliente / servidor.
- DNS dinámico.
- Lista de hosts seteable desde la interfase web.

- HTTP / FTP proxy (squid).
- IDS (snort) en todas las interfases.
- Log local o remoto.
- NTP cliente / servidor.
- Servidor SSH (PSK o con password).
- Traffic shaping (en la interfase RED).
- “Statefull” Firewall.
- Módulos “nat helper” para h323, irc, mms, pptp, proto-gre, quake3.
- Port forwarding (redireccionamiento de puertos).
- DMZ pin holes.
- Activar o desactivar ping en todas las interfases.
- VPN (IPSEC).
- Gráficos de monitoreo de CPU, RAM, swap, HD, tráfico de RED, etc.

Existen varios desarrolladores que han desarrollado paquetes con funcionalidad adicional, que se denominan **Addons**, estos permiten una amplia gama de funcionalidades no incluidas originalmente en el producto.

Zerina. Si bien IPCop nos permite trabajar con una VPN (Virtual Private Network) por medio de IPSEC (Internet Protocol SECurity), este excelente addon nos da la posibilidad de agregar además OpenVPN. De esta manera es posible tener un excelente y robusto entorno de trabajo remoto, accediendo por cualquiera de estas dos alternativas de VPNs, que permiten que trabajemos en cualquiera de los equipos internos de nuestra red tal como si estuviéramos dentro de nuestra red GREEN, pero trabajando desde la red BLUE como desde la RED.

10.- Seguridad en Comunicación VoIP (Open VPN).

A medida que crece la popularidad de VoIP, aumentan las preocupaciones por la seguridad de las comunicaciones y la telefonía IP. VoIP es una tecnología que ha de apoyarse necesariamente en las capas y protocolos ya existentes de las redes de

datos. Por eso en cierto modo la telefonía IP va a heredar ciertos problemas de las capas y protocolos ya existentes, siendo algunas de las amenazas más importantes de VoIP problemas clásicos de seguridad que afectan al mundo de las redes de datos. Por supuesto, existen también multitud de ataques específicos de VoIP.

Figura No. 26 – VoIP y su relación con las diferentes capas.

La seguridad de VoIP se construye sobre muchas otras capas tradicionales de seguridad de la información. En la siguiente tabla se detallan algunos de los puntos débiles y ataques que afectan a cada una de las capas.

Capa	Ataques y Vulnerabilidades
Políticas y Procedimientos	• Contraseñas débiles. • Mala política de privilegios. • Accesos permisivos a datos comprometidos.
Seguridad Física	• Acceso físico a dispositivos sensibles. • Reinicio de máquinas. • Denegación de servicio.
Seguridad de Red	• DDoS. • ICMP unreacheable. • SYN floods.

	• Gran variedad de floods.
Seguridad en los Servicios	• SQL injections. • Denegación en DHCP. • DoS.
Seguridad en el S.O.	• Buffer overflows. • Gusanos y virus. • Malas configuraciones.
Seguridad en las Aplicaciones y Protocolos de VoIP	• Fraudes. • SPIT (SPAM). • Vishing (Phising) • Fuzzing. • Floods (INVITE, REGISTER, etc.). • Secuestro de sesiones (Hijacking). • Interceptación (Eavesdroping).

Se puede apreciar que algunos de estos ataques tendrán como objetivo el robo de información confidencial y algunos otros degradar la calidad de servicio o anularla por completo (DoS). Para el atacante puede ser interesante no solo el contenido de una conversación (que puede llegar a ser altamente confidencial) sino también la información y los datos de la propia llamada, que utilizados de forma maliciosa permitirán al atacante realizar registros de las llamadas entrantes o salientes, configurar y redirigir llamadas, grabar datos, utilizar información para bombardear con SPAM, interceptar y secuestrar llamadas, reproducir conversaciones, llevar a cabo robo de identidad e incluso realizar llamadas gratuitas a casi cualquier lugar del mundo. Los dispositivos de la red, los servidores, sus sistemas operativos, los protocolos con los que trabajan y prácticamente todo elemento que integre la infraestructura VoIP podrá ser susceptible de sufrir un ataque.

Clasificación de los ataques.

Las amenazas de las redes de telefonía IP las podemos clasificar en las siguientes categorías:

- Accesos desautorizados y fraudes.
- Ataques de denegación de servicio.
- Ataques a los dispositivos.
- Vulnerabilidades de la red subyacente.
- Ataques a nivel de aplicación.

Asegurando la red Voip.

Es esencial que VoIP se asiente sobre una infraestructura de red segura, protegida por **cortafuegos** bien administrados. Es muy recomendable la existencia en la red de sistemas de **antivirus** actualizados que la protejan de ataques de virus, gusanos y troyanos. La detección de muchos ataques se puede realizar instalando sistemas de detección de intrusos (**IDS**) o de prevención (**IPS**) en los lugares estratégicos de la red. Serán capaces de detectar y prevenir ataques contra los protocolos (fuzzing), ataques contra servicios (exploits y vulnerabilidades), escaneos y ciertos tipos de ataques DoS. Es evidente que el IDS/IPS requerirá de una configuración apropiada, adaptada a la red en la que funcione para conseguir que su fiabilidad sea la adecuada.

OpenVPN.

En el ámbito de la seguridad VoIP, el uso de una Red Virtual Privada (VPN) es una metodología muy recomendada para incrementar la seguridad en la red.

OpenVPN es un software libre utilizado para crear redes virtuales privadas, que implementa conexiones de capa 2 o 3 y usa los estándares de la industria SSL (Secure Sockets Layer)/TLS (Transport Layer Security) para cifrar.

OpenVPN tiene dos modos considerados seguros, uno basado en claves estáticas pre-compartidas y otro en SSL/TLS usando certificados y claves RSA. SSL/TLS es

una de las mejores tecnologías de cifrado para asegurar la identidad de los integrantes de la VPN. Cada integrante tiene dos claves, una pública y otra privada, la clave privada debe permanecer secreta mientras la clave pública debe ser intercambiada para que nos puedan enviar mensajes.

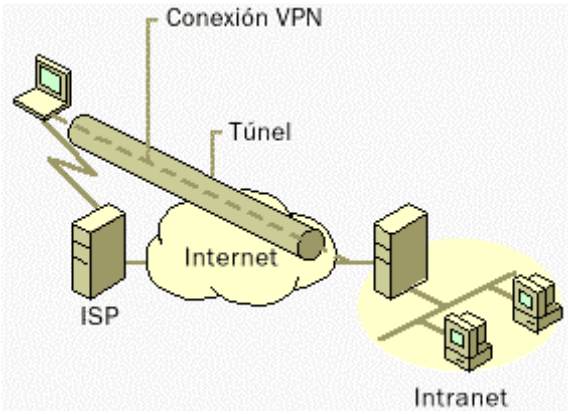


Figura No. 27 – Arquitectura de una VPN.

Conexiones OpenVPN pueden ser realizadas a través de casi cualquier firewall. Si se tiene acceso a Internet y se puede acceder a sitios HTTPS, entonces un túnel OpenVPN debería funcionar sin ningún problema.

ZERINA es una implementación de OpenVPN para el firewall IPCop, una combinación de software libre muy potente para la configuración de VPNs.

Todas las configuraciones y características de ZERINA son realizadas y controladas a través de la interfaz Web proporcionada por IPCop.

11.- Marco Legal sobre Telefonía IP en El Salvador.

El aspecto legal de la tecnología de voz sobre Internet “VoIP”, es un tema gris y que lleva a disputas doctrinarias, ya que la legislación salvadoreña no define en ninguna parte lo que es la transmisión de voz sobre el protocolo de Internet “VoIP”, ni tampoco la regula, la limita o la prohíbe.

Tampoco establece que la transmisión de datos utilizando el protocolo de Internet "VoIP" constituyan llamadas internacionales, o que su aplicación este expresamente prohibida.

En El Salvador la institución que tiene atribuciones para aplicar las normas, en las leyes que rigen los sectores de Electricidad y de Telecomunicaciones, es la Superintendencia General de Electricidad y Telecomunicaciones (SIGET).

En el sector de telecomunicaciones, la SIGET, cuenta con las siguientes normas:

a) Ley de Telecomunicaciones Reformada. 13/ 12/ 2006.

b) Reglamento de Telecomunicaciones. 06/ 10/ 2008.

Documentos que se encuentran en su sitio de Internet: www.siget.gob.sv, en el sector de Telecomunicaciones: Legislación.

En las dos normas, hay un artículo donde se dan las definiciones y términos técnicos utilizados parar facilitar la interpretación de la Ley y su Reglamento, articulo 6 de la Ley de Telecomunicaciones y articulo 3 del Reglamento de Telecomunicaciones.

En ambos artículos no se definen los términos Internet, voz sobre Internet "VoIP" ni telefonía IP.

Basándonos en los antecedentes indicados, podemos concluir lo siguiente:

- De acuerdo a la legislación vigente en El Salvador, la forma en la que se está brindando acceso al Internet y a sus distintas aplicaciones entre las que se encuentra la transmisión de datos mediante el protocolo de voz sobre Internet VoIP, es absolutamente apegada al derecho.

- Como el Internet no puede ser dividido en función de sus aplicaciones y tecnologías, de ninguna manera debe considerarse que la aplicación de una de estas tecnologías, que es la transmisión de datos mediante el protocolo de voz sobre Internet VoIP, constituye telefonía, ya que se ser así, debería considerase que el Internet mismo es telefonía.

- Como la forma en la que los usuarios acceden al Internet es absolutamente apegada al derecho, no existe impedimento legal alguno para que estos utilicen los servicios vinculados con el Internet.

- De ninguna manera puede considerarse que transmisión de datos mediante el protocolo de voz sobre Internet VoIP constituye telefonía pública.
- La transmisión de datos mediante el protocolo de voz sobre Internet VoIP, como se indica por definición, es transmisión de datos y no de voz.

.

CAPITULO II
ANALISIS DEL PROBLEMA.

1.- Situación Actual.

La Fuerza Armada de El Salvador, como una Institución histórica al servicio de la nación Salvadoreña, además de mantener la soberanía nacional y la integridad del territorio, también se le es encomendada misiones de colaboración en el mantenimiento de la paz en otros países, así como también mantener buenas relaciones con países amigos, a través del intercambio cultural o misiones de tipo protocolarias. En ese sentido para poder cumplir con estas tareas en el extranjero, se ve en la necesidad de enviar elementos de la misma hacia diferentes países del mundo, en donde se requiere que este personal mantenga comunicación de forma permanente o eventual, hacia nuestro país, con la finalidad de mantener informado al Mando, sobre el cumplimiento de las misiones asignadas.

Esta comunicación en el presente es realizada a través de medios como son: Llamadas telefónicas Internacionales, correo electrónico, telefonía satelital, telefonía IP de terceros (Operadoras locales que brindan servicio de telefonía IP enrrutandolas hacia telefonía fija y celular), y en algunos casos a través de conexión punto a punto por medio de Chat o video llamada (servicios de Internet a través de Yahoo, Hotmail y otros). Sin embargo aquellas alternativas que de alguna manera ofrecen una comunicación completa, tienden a generar costos elevados en el pago de estos servicios (Llamadas internacionales, telefonía satelital y telefonía IP de Operadoras), lo cual afecta el presupuesto asignado al Ministerio de la Defensa Nacional, obligando de esta forma a utilizar estos servicios en forma limitada.

Esta situación viene a generar limitantes, en lo relacionado a coordinaciones que son necesarias efectuar con el personal de la Fuerza Armada, que se encuentra en el Extranjero cumpliendo misiones oficiales, ya que si bien es cierto se mantiene comunicación, pero ésta es en forma limitada, a fin de evitar el pago excesivo en llamadas telefónicas.

Otra de las limitantes o vulnerabilidad, es lo relacionado a la seguridad de la comunicación, ya que debido a que se utiliza el servicio de un tercero, no es posible garantizar la confidencialidad de las mismas. En tal sentido se esta expuesto a que las llamadas puedan ser interceptadas o grabadas. Esta situación podría limitarse o reducirse, si la Institución contara con su propia plataforma que brinde servicios de comunicaciones de voz desde el Extranjero hacia nuestro país.

Tomando en cuenta el problema planteado, este trabajo pretende ofrecer una alternativa de bajo costo para la Fuerza Armada, a través de la implementación de una plataforma basada en voz sobre IP, que permita a los elementos de la Fuerza Armada en misiones en el extranjero, comunicarse a través de la red publica de Internet hacia un servidor PBX basado en software y que éste a su vez enrute las llamadas hacia la red telefónica privada de la Fuerza Armada.

2.- Justificación.

En la actualidad el personal de la Fuerza Armada que se encuentra en misiones oficiales en el Extranjero, para poderse comunicar al Ministerio de la Defensa Nacional y/o Unidades Militares del país, lo realizan a través de llamadas telefónicas Internacionales, lo cual genera costos elevados en el pago de las mismas.

Con el incremento de personal destacado en el extranjero, y con un lineamiento de reducción de gastos por parte del Ministerio de la Defensa Nacional, reducir la facturación en el rubro de llamadas internacionales es un factor que ayudará en gran medida a una política de austeridad.

Con el uso de una PBX basada en Software, la factura de llamadas internacionales casi desaparecerá, ayudando a que todas las comunicaciones se realicen por enlaces de Internet de alta velocidad, utilizando medios como lo son el e-mail y el VoIP entre otros.

El personal en el extranjero se podrá comunicar con cualquier unidad militar en el país, en cualquier momento y no importando su ubicación geográfica, dándole una mayor movilidad, necesitando solamente una conexión a Internet en el lugar en que

se encuentre, factor de importancia si consideramos la variedad de misiones que cumple el personal en el extranjero.

El poder comunicarse con sus familiares en el país, sin incrementar sus gastos y cuando lo necesite, incentivará la moral de todo el personal, que es uno de los objetivos que busca el Ministerio de la Defensa Nacional.

Con un servicio de VoIP, se tiene otra alternativa de comunicaciones, no estando limitados a utilizar los canales tradicionales, ofreciendo una redundancia en lo que respecta las llamadas al extranjero.

El futuro de las comunicaciones esta orientándose a la Internet y al uso de VoIP, con lo cual la implementación de una PBX basada en Software estaría preparando al Ministerio de la Defensa Nacional para adoptar las nuevas tecnologías.

CAPITULO III

PROPUESTA DE SOLUCION.

1.- Definición de la Propuesta.

La propuesta de solución esta orientada a la implementación de una alternativa comunicación de bajo costo para el personal de la Fuerza Armada de El Salvador, que se encuentra en misiones oficiales en el extranjero, utilizando para ello, la tecnología ASTERISK (TrixBox), de tal forma que permita al personal de la Institución, comunicarse a través de la red publica de Internet hacia el sitio central en las oficinas centrales del Ministerio de la Defensa Nacional y enrutar las llamadas telefónicas hacia los diferentes abonados de la red privada de la Fuerza Armada. Así como también realizar pruebas el enrutamiento a teléfonos de la red publica comercial. Para la presente solución, se pretende establecer la siguiente infraestructura de comunicación, tal como se muestra en el siguiente diagrama, **Ver figura No. 28.**

DIAGRAMA ESQUEMÁTICO PARA EL SERVICIO DE VOZ IP PARA LA FUERZA ARMADA A TRAVÉS DE ASTERISK

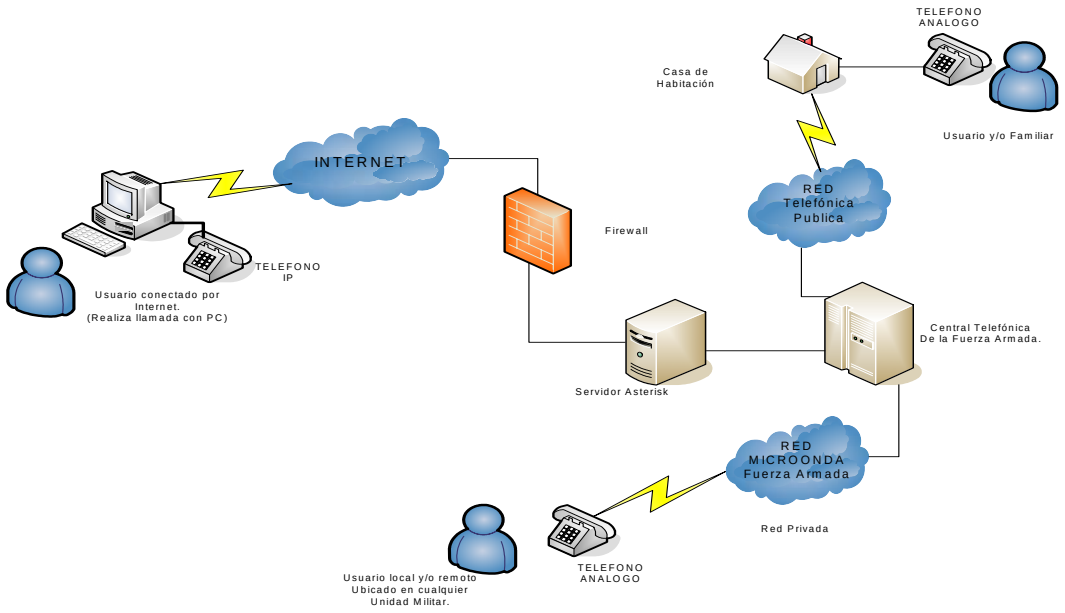


Figura No. 28 Esquema General de Conexión.

2.- Objetivo General.

Implementar un servicio de comunicación de voz sobre IP para el personal de la Fuerza Armada de El Salvador en el extranjero hacia las Oficinas Centrales del Ministerio de la Defensa Nacional, a través de la tecnología TrixBox (ASTERISK).

3.- Objetivos Específicos.

a.- Investigar sobre tecnologías de voz sobre IP de estándar libre (software libre).

b.- Establecer los mecanismos y/o procedimientos que garanticen un canal seguro entre el usuario remoto y sitio central.

c.- Seleccionar las características del hardware necesario para la implementación de la alternativa de comunicación.

d.- Configurar los diferentes servicios que permitan el adecuado funcionamiento de la plataforma Trixbox (Asterisk).

e.- Establecer el enlace que permita la comunicación y enrutamiento de llamadas telefónicas entre el servidor Asterisk y la central telefónica del Ministerio de la Defensa Nacional.

f.- Configurar el canal seguro en el cliente remoto utilizando software libre.

g.- Realizar pruebas de conexión entre el cliente remoto y el usuario local.

4.- Alcances y Limitaciones.

a.- Alcances.

1) Implementar un servicio de voz sobre IP que permita establecer una comunicación entre usuarios remotos (personal en el extranjero) y locales (Ministerio de la Defensa Nacional y Unidades Militares).

2) Ofrecer un medio alterno de comunicación entre el personal de la F.A que se encuentra en el extranjero hacia las Oficinas Centrales del Ministerio de la Defensa Nacional y Unidades Militares.

3) Reducir los costos relativos a pagos de llamadas Internacionales que actualmente son canceladas por el personal que se encuentra en misiones oficiales.
4) Asegurar las comunicaciones entre los miembros de la F.A, mediante el empleo de un servidor de Voz IP propio de la Institución.
5) Aprovechar la red publica de Internet para materializar las comunicaciones entre las misiones oficiales y el Ministerio de la Defensa.

b.- Delimitaciones.

1) Debido a limitantes de Hardware, la solución solo será implementada mediante una infraestructura previamente montada y configurada para que funcione en iguales condiciones a la pretendida para la conexión Internet – Ministerio de la Defensa Nacional.

2) Para fines prácticos y evaluar el tráfico de la señal de voz desde una conexión de Internet al servidor Trixbox, se montará un servidor alterno en el Ministerio de la Defensa Nacional, con las mismas configuraciones del que será utilizado en la demostración local.

c.- Limitaciones.

1) No podrá habilitarse el servicio de correo de voz, para usuarios o abonados, que dependan de la Central Telefónica del MDN, debido a que una vez las llamadas son enrutadas, Trixbox considera que el usuario ha respondido la llamada y si en todo caso el usuario final no responde la llamada, no podrá devolverse el control al servidor Trixbox.

5.- Herramientas Tecnológicas a Utilizar.

Para la implementación del servicio de Voz IP para el personal de la Fuerza Armada, se empleara la siguiente tecnología:

a.- Software.

1) Versión gratuita de TrixBox basada en distribución de Linux Centos Release 5.

2) Programas de SoftPhone (Teléfonos virtuales).
3) Sistema operativo Windows Xp para clientes y para administración de TrixBox.
4) Open VPN (Software para VPN), clientes remotos con Windows Xp o Linux.
5) Ipcop distribución de Linux, la cual será usada para configurar un Firewall y router por software, a fin de proteger el servidor TrixBox (si es necesario, sino se empleara un router físico).

b.- Hardware de telefonía.

1) Gateway para VoIP con interfaces Ethernet y puertos FXS para enlazarse a central telefónica y/o Tarjeta E1 tipo PCI con puertos tipo BNC (soportada para Linux y Windows).
2) Teléfono IP Cisco 7912 (para pruebas).
3) Teléfono análogo (abonado de red interna).
4) Central telefónica (para enrutar llamadas hacia red interna de la F.A).

c.- Equipo Informático.

1) Computadora Pentium IV 512 MB RAM, 40 GB en disco duro, con tarjeta de red.
2) Switch de 8 puertos para simular red externa (a este equipo se conectara PC cliente, el firewall IpCop y teléfono IP).
3) Router con 1 puerto WAN y 4 puertos LAN, con Wireless (a este equipo se conectara el Firewall IPCop a través de la interfaz Interna, el Trixbox y el resto del equipo de la red interna).
4) Computadora Pentium de 32 MB en RAM, 2 GB en disco duro, con dos tarjetas de red, para ser utilizada como Firewall y router (de ser necesario).

d.- Otros.

1) IP publica, para enlazar servidor de Voz IP hacia Internet.

6.- Descripción de la Solución.

Para la implementación de la solución propuesta se desarrollará de acuerdo a las fases siguientes:

FASE I: Instalación, configuración y puesta en servicio del servidor de Voz IP, utilizando el software PBX TrixBox 2.6 CE, basado en la distribución de Linux Centos Release 5.

- Instalación de distribución de TrixBox.
- Selección y configuración de módulos.
- Pruebas de módulos.
- Instalación de software SIP Phone en PC de pruebas.
- Pruebas de acceso a servidor de Voz IP desde Internet.
- Pruebas con extensiones IP (Teléfono IP y PC con SIP Phone).

FASE II: Establecer enlace entre servidor TrixBox y Central Telefónica, a través de Gateway de VoIP y/o tarjeta de Interfaz E1.

- Conexión entre servidor TrixBox y Gateway de VoIP y/o Instalación y configuración de Interfaz PCI tipo E1 en servidor TrixBox.
- Pruebas de comunicación entre servidor TrixBox y Central telefónica.
- Pruebas de enrutamiento de llamadas desde red local-TrixBox-Central telefónica-Teléfono análogo.
- Pruebas de conexión desde Internet a teléfono de central telefónica.

FASE III: Configuración de canal seguro, el cual se implementará entre el cliente remoto y el servidor de Voz IP:

- Configuración de router físico y/o del servidor IpCop de Linux, para que funcione como Firewall y router hacia la red pública.
- Instalación de software en cliente y configuración de canal seguro.
- Prueba de canal seguro (VPN) entre PC en Internet y servidor de Voz IP.

FASE IV: Pruebas de conexión entre usuario remoto y local, para esta fase se establecerá una conexión entre un usuario remoto en Internet hacia un usuario de la red privada de la Fuerza Armada; Asimismo, de ser posible se tratara de establecer una conexión entre un usuario remoto en Internet hacia un teléfono comercial de las operadoras en el país.

CAPITULO IV
METODOLOGIA DE DESARROLLO.

El desarrollo de la propuesta de solución para la implementación del servicio de voz sobre IP para el personal de la Fuerza Armada, que se encuentra cumpliendo misiones en el exterior, a través de la herramienta Asterisk, será ejecutada de acuerdo a los siguientes procesos:

1.- Instalación, Configuración e Implementación de Servidor TrixBox.

a.- Requisitos de Hardware y Software.

Se requiere una PC con procesador Pentium IV a 3.06 Ghz., memoria RAM 512 Mb o superior, disco duro de 6 GB o superior, una tarjeta de Red 10/100 Mbps y una unidad de CD-ROM.

Poseer o descargar la imagen ISO de TRIXBOX y grabarla en un CD en blanco, esta puede descargarse desde el sitio de descargas de TRIXBOX http://www.trixbox.org/downloads/.

b.- Instalación de TrixBox.

Una vez se posea el Hardware necesario y el Software para instalar TrixBox Edición Comunitaria (TrixBox CE), podemos iniciar la instalación de TrixBox, siempre y cuando tomemos en cuenta que el disco duro donde se instalará, no se poseen datos de importancia para nuestra Organización, ya que una vez se inicie el proceso de instalación, **Linux Centos de manera automática formatea el disco duro y crea sus sistemas de archivos por default.**

Bueno si estamos listo, solo tenemos que introducir el disco de inicio (BOOT) de Centos y en nuestro computador se presenta la siguiente pantalla, **Ver figura No. 29.**

Figura No. 29 Pantalla de Inicio de Instalación.

Una vez, se encuentre en esta pantalla, podrá presionar ENTER para iniciar la instalación de TrixBox CE (La plataforma abierta para la telefonía del negocio), seguidamente solicitará, que seleccione el tipo de teclado, tal como se muestra en la siguiente pantalla, **Ver figura No. 30.**

Figura No. 30 Selección de idioma para el Teclado.

Asegúrese de seleccionar el idioma para el teclado, de acuerdo al que este instalado en su computador, para esto ayúdese de las teclas del cursor y una vez seleccionado, podrá utilizar la tecla TAB, para saltar el botón de OK y continuar.

Seguidamente, le solicitara la Zona Horaria, tal como se muestra en la siguiente pantalla, **Ver figura No. 31.**

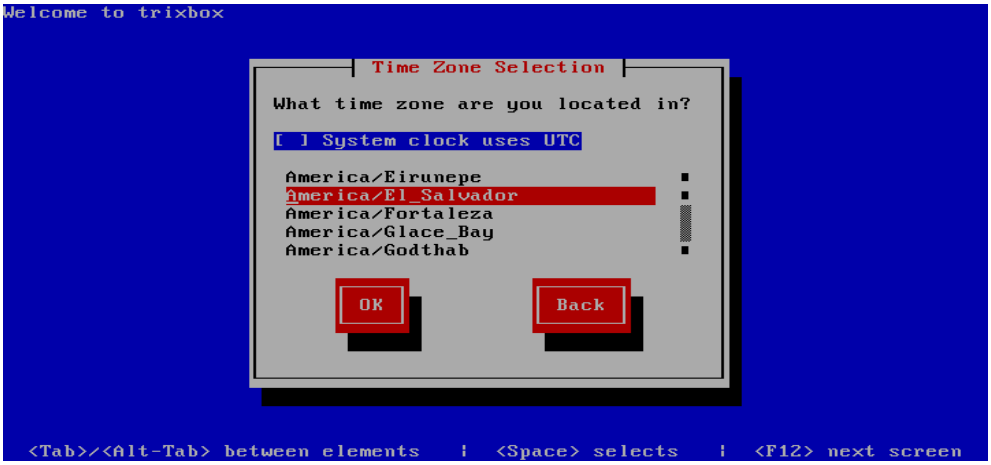


Figura No. 31 Selección de Zona Horaria.

Para nuestro caso seleccionaremos AMERICA/EL SALVADOR, y nuevamente utilizamos la tecla TAB, para saltar al botón de OK y continuar. Seguidamente, espere a que en el mismo proceso de instalación le solicite la clave del administrador ROOT, por omisión la clave es **PASSWORD**, (se recomienda cambiar la clave inicial proveída por el proveedor), ingrese la clave nueva, luego confirme la nueva contraseña (copiarla en algún lugar para efectos de recordatorio), pasada esta fase iniciará el proceso de formateo del disco duro, transferencia de archivos y seguido la instalación de todos los paquetes, **Ver figura No. 32.**

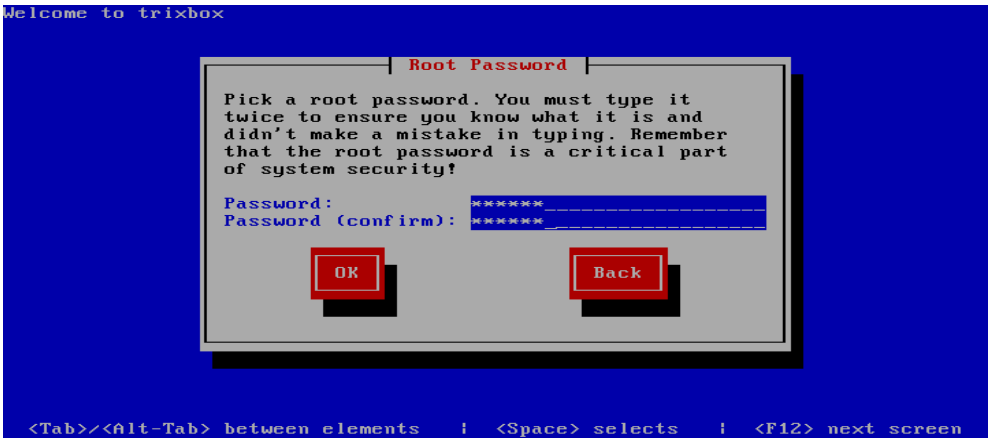


Figura No. 32 Password para root.

Posterior a la confirmación del password de ROOT, se iniciara el proceso de formateo, tal como se muestra a continuación, **Ver figura No. 33.**

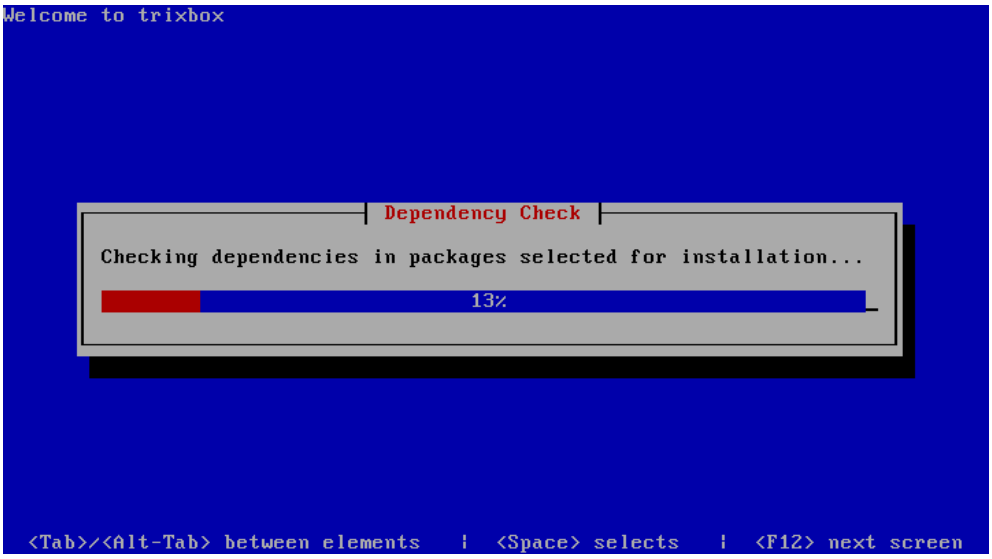


Figura No. 33 Chequeo de Dependencias.

El tiempo de duración de la instalación tendrá que ver con la capacidad de su máquina (PC), y esto no solo depende del procesador, sino también del tipo de disco duro y velocidad del CD-ROM que posea, y la capacidad de la memoria RAM.

Durante la instalación verá una pantalla similar a la siguiente en la que se muestra la instalación de cada paquete. **Ver figura No. 34.**

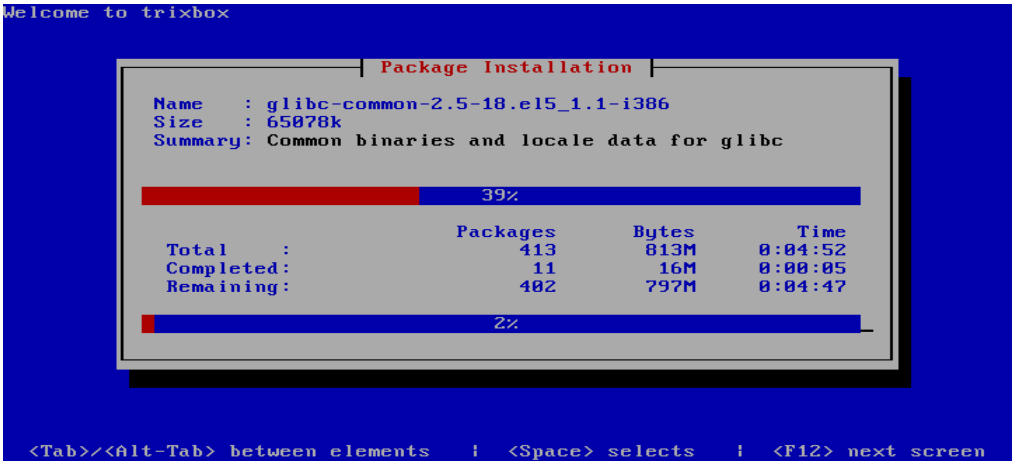


Figura No. 34 Proceso de Instalación.

Cuando Linux Centos, haya finalizado la instalación, realizara la expulsión del CD de instalación de manera automática y se reiniciará el computador, seguidamente se mostrara la pantalla de Inicio de Sistema de GRUB, tal como se muestra en la siguiente pantalla, **Ver figura No. 35.**

Figura No. 35 Pantalla Inicio de Sistema GNU GRUB.

Seguidamente, cuando el sistema inicie, TrixBox mostrará las siguiente pantalla de inicio de comando en línea, donde solicitará un nombre de Usuario, **Ver figura No. 36.**

Figura No. 36

Cuando haya introducido el nombre de Usuario, en este caso **root** y el **password**, se mostrará la versión de Linux Centos y el Kernel que esta utilizando, de igual forma visualizarán las interfaces de red, que se estén utilizando con sus respectivas direcciones IP`s, para nuestro caso, muestra una dirección IP por default. **Ver figura No. 37.**

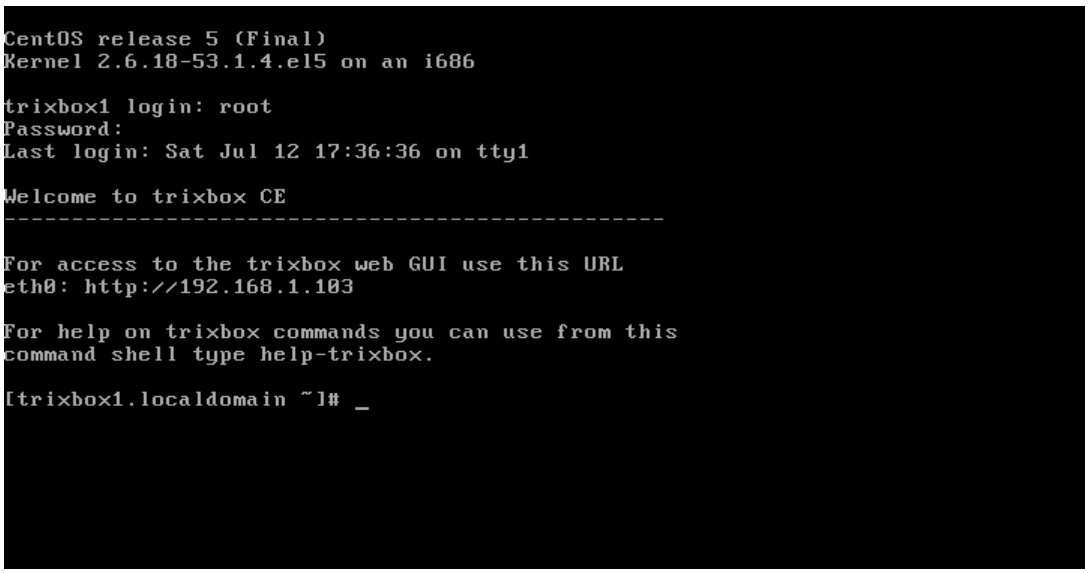


Figura No. 37 Pantalla de inicio para línea de comando.

Una vez, se haya ingresado al sistema en modo administrador, para obtener ayuda en el uso de comandos en línea, puede digitar el comando **help-trixbox** y mostrará la siguiente pantalla, **Ver figura No. 38.**

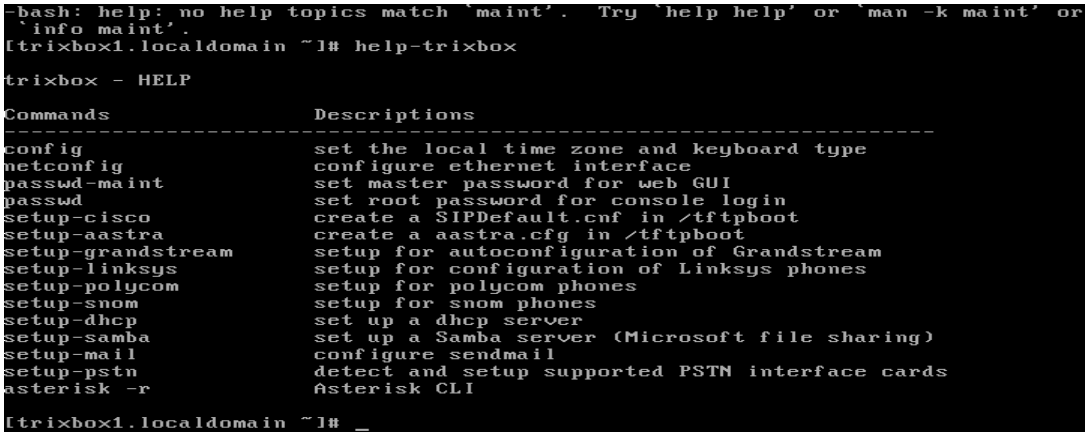


Figura No. 38 Pantalla con comandos de ayuda, para TrixBox.

Para nuestro caso, utilizaremos el comando **netconfig** para configurar la tarjeta de Red y el comando **passwd-maint**, para cambiar el password, para el usuario **maint**, el cual es utilizado para administrar la interfaz Web de TrixBox.

CONFIGURACIÓN DE INTERFAZ DE RED (INTERNA).

Como siguiente paso, procederemos a configurar la interfase de red, para nuestro caso, debido a que el servidor TrixBox, estará conectado a la red interna (LAN), se tendrá que configurar con una dirección estática (a menos que deseé utilizar DHCP), sin embargo en nuestro caso para un mejor control de servidor de Voz IP, serán de tipo estática. Para lo siguiente utilizaremos el comando **netconfig**, el cual nos desplegará la siguiente pantalla, **Ver figura No. 39a.**

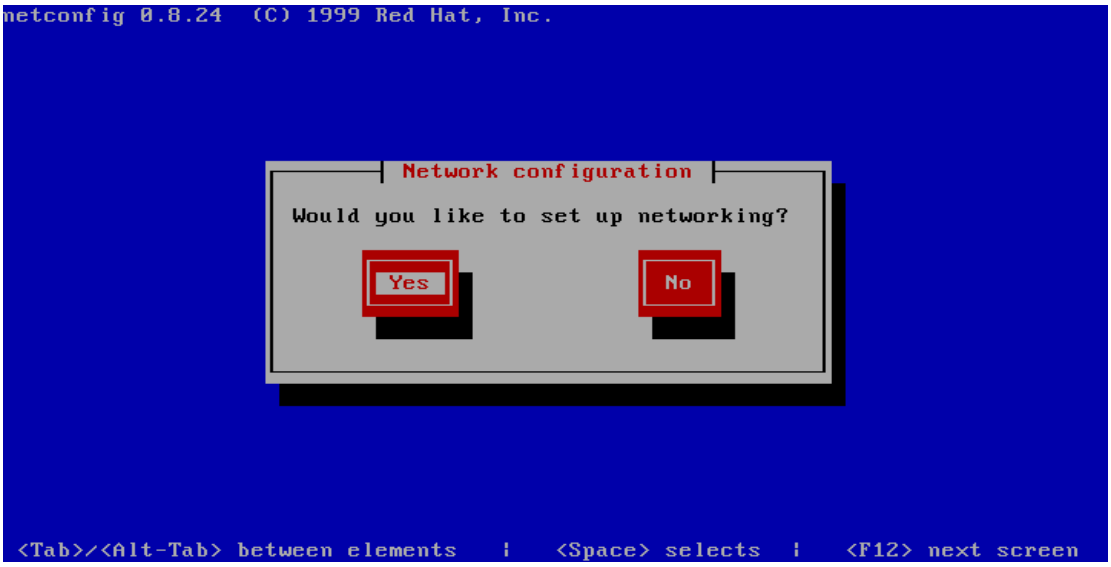


Figura No. 39a.

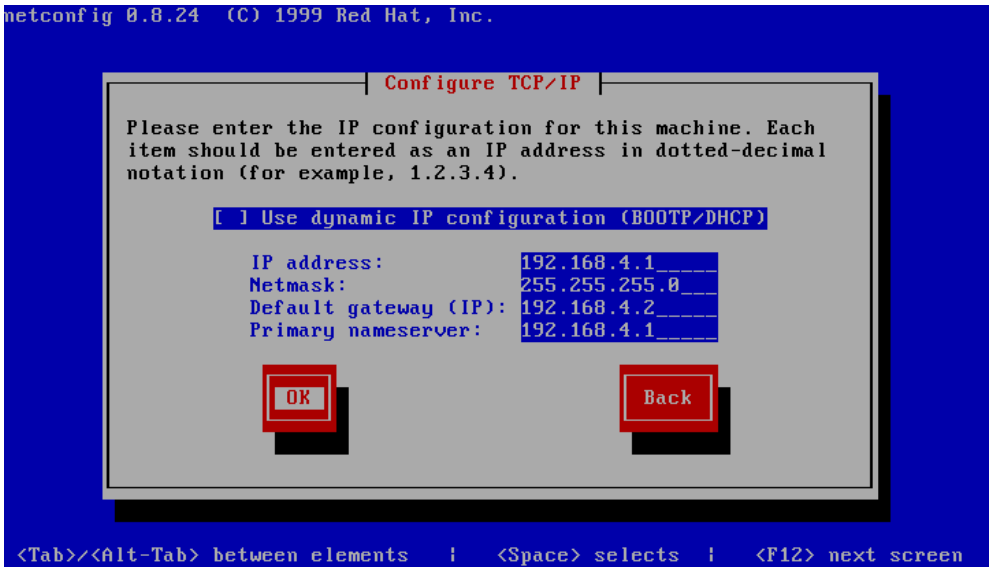


Figura No. 39b Pantalla para configurar Interfaz de red.

Como se muestra en la figura No. 39b, se deben introducir los valores correspondientes a IP address, Netmask, default gateway y primary nameserver, en nuestro caso se configurará la interfaz Eth0, con los siguientes valores, ya que esta tendrá una conexión a la red interna (LAN), para lo cual utilizaremos los siguientes valores:

IP address	:	10.1.0.60
Netmask	:	255.255.0.0
Default gateway	:	10.1.0.62 (Firewall IPCop).
Primary nameserver	:	(ninguno).

Nota: En algunos casos, no se pueda realizar la asignación de los valores de la red, a través del comando **netconfig**, por lo que habrá que configurar en forma manual a través de línea de comando, en el archivo ubicado en:

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

Con la anterior configuración, solo se requiere que se reinicien los valores de la interfase, con el comando ***service network restart*** y nuestro servidor TrixBox,

se encuentra listo, para ser administrado y configurado, en los fines que desea la Institución.

c.- Plan de marcado por Defecto de TrixBox.

Trixbox, por default trae un plan de marcado conocido como DIAL PLAN; así como también es necesario definir nuestro plan de marcado interno, para las extensiones dentro de la Institución, según el siguiente cuadro:

Plan de Marcado.

Numero	Función
Extensiones por Default para TrixBox	
#	Directorio Telefónico del Sistema
*43	Prueba de Echo de llamadas
*52	Extensión no Disponible Activo
*53	Extensión no Disponible Desactivo
*60	Hora del Sistema
*65	Escuchar su extensión.
*69	Ultimo numero que ha llamado (Call-Trace)
*70	Llamada en espera ON
*71	Llamada en espera OFF
*72	Desvió de llamada ON
*73	Desvió de llamada OFF
*77	Grabar Mensaje de IVR
*78	Opción de "No Molestar" ON
*79	Opción de "No Molestar" OFF
*90	Teléfono Ocupado No disponible ON
*91	Teléfono Ocupado No disponible OFF
*97	Acceso a mi buzón de voz.
*98	Marcar buzón de voz.
*99	Oír la Grabación de mensaje de IVR
666	Llamar al sistema de Fax
7777	Simular llamada de entrada
Extensiones de Internas	
8000	Operadora
8301	Jefe de Informática
8302	Teléfono IP Mantenimiento.
8303	Operador PBX
8304	Teléfono análogo
8305	Usuario No.1
8306	Usuario No.2
8307	Usuario No.3

Este plan de marcado, será posteriormente adaptado a un ambiente de producción a disposición de los diferentes usuarios de la Institución.

d.- Parametrización de la Herramienta Trixbox.

Antes de iniciar la administración de TrixBox desde el acceso Web, es importante considerar, las siguientes configuraciones:

- Configuración de Lenguaje de Operadora.
- Contraseñas de TrixBox.

Configuración de Lenguaje de Operadora.

El lenguaje de la operadora interna, por defecto viene con lenguaje en el idioma Inglés. En ese sentido se tiene que realizar los siguientes cambios para que nos conteste en el idioma Español:

TrixBox, por defecto trae cargados los archivos de voz tipo GSM y a la altura del sistema de archivos: **/var/lib/asterisk/sounds.**

Lo primero que se tiene que realizar es la descarga desde Internet, de los archivos de voces en español, la cual lo podemos encontrar en las siguientes direcciones:

http://www.voipnovatos.es/voces/	voipnovatos-core-sounds-es-gsm-1.4.tar voipnovatos-extra-sounds-es-gsm-1.4.tar
http://asterio.com.ar/	ThaisaC-core-sounds-gsm-1.4.12.1.tar.gz(1,23Mb) ThaisaC-core-sounds-gsm ThaisaC-extra-sounds-gsm-1.4.12.tar.gz(2,77Mb)

Una vez, se tengan los archivos de voz, solo tienes que copiarlos a la altura del sistema de archivo: **/var/lib/asterisk/sounds**, en este caso es recomendable renombrar el directorio original de **sounds**, por ejemplo con **sounds.ori**, para poder copiar los archivos de voz descargados, en el nuevo directorio sounds.

El comando para descomprimir los archivos a la altura de /var/lib/asterisk/sounds, es como se muestra en el siguiente ejemplo:

```
tar -xzvf ThaisaC-core-sounds-sln-1.4.12.tar.gz
tar -xzvf ThaisaC-extra-sounds-sln-1.4.12.tar.gz
```

Si es la primera vez que se instalan sonidos en castellano, es necesario configurar el parámetro "language" en el archivo /etc/asterisk/zapata.conf en "es".

```
;
; Zapata telephony interface
;
; Configuration file
[trunkgroups]
[channels]

language=es
defaultzone=es
context=from-zaptel
signalling=fxs_ks
...
```

Luego de haber editado zapata.conf, reiniciar Asterisk, se debe cambiar los parámetros al archivo: **/etc/asterisk/asterisk.conf.**

```
.
        .
        [general]
        Languageprefix=yes


        /etc/asterisk/sip.conf     ; aquellos que uséis FreePBX debéis
        poner esto en el sip_custom.conf
        .
        .
        [general]
        language=es
```

Básicamente modificamos los archivos:

zapata.conf, asterisk.conf y sip.conf.

Lo anterior hace que nuestros canales SIP escuchen locuciones en español. Si queremos que se utilicen en todos los canales, deberemos poner *language=es* en los ficheros zapata.conf, iax.conf, etc.

Contraseñas de TrixBox.

Trixbox por defecto utiliza las siguientes cuentas:

Administrador de FreePBX:

Usuario: admin.

Password: amp111 (lo cambiamos a trixbox).

Administrador de MYSQL.

Usuario: root

Password: passw0rd (lo cambiamos a trixbox).

Usuario de MYSQL.

Usuario: asteriskuser

Password: amp109 (lo cambiamos a trixbox).

Para cambiar el password en los usuarios de MySql, utilizamos el siguiente comando:

Mysqladmin –u root -p password trixbox

Mysqladmin –u asteriskuser –p password trixbox

Para ambos casos, una vez introducida la sentencia, solicitara el password actual, para poder aceptar el cambio.

En resumen los archivos que deben ser editados son los siguientes:

/ect/amportal.conf

/etc/asterisk/asterisk.conf

/etc/asterisk/sip.conf

/etc/asterisk/zapata.conf

/etc/asterisk/manager.conf

/var/www/html/panel/op_server.cfg

/var/www/html/maint/modules/phpmyadmin/config.inc.php

Con la edición de los archivos anteriores, se logra evitar que las claves de acceso, queden por default y de esta forma mejorar la seguridad en la administración del TrixBox.

Una vez realizadas los cambios anteriores, podemos iniciar la administración remota a través de un acceso Web, desde un equipo diferente. Para caso práctico y considerando que estamos en nuestra red privada (Interna), lo haremos a través de la IP 10.1.0.60, utilizando nuestro Internet Explorer:

http://10.1.0.60, luego de digitar esta dirección se mostrara la pagina de Inicio de Trixbox, tal como se muestra en la figura No. 40

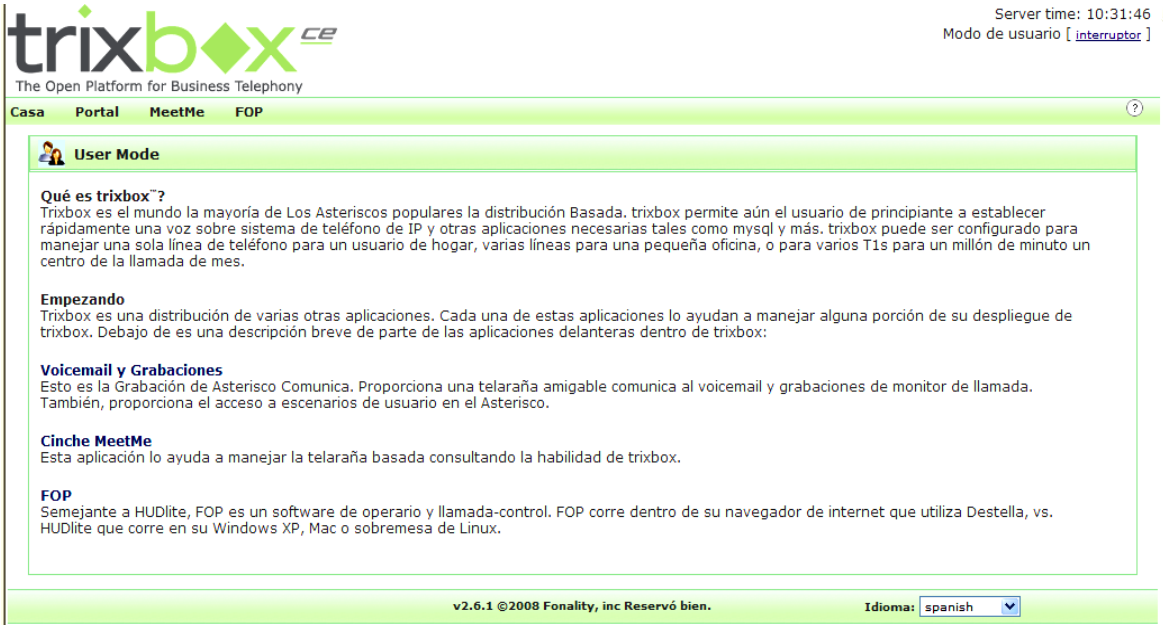


Figura No. 40 Página de Inicio de TrixBox CE.

Este portal esta compuesto de las siguientes opciones:

- Casa (Home).
- Portal.
- Meetme.
- FOP.

Ahora bien, para nuestro proyecto necesitamos ingresar al TrixBox, como Administrador, para lo cual realizamos a través de la opción (Switch o Interruptor), que aparece en la parte superior derecha de la página de inicio, tal como se muestra en la figura No. 41.

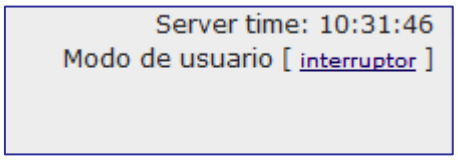


Figura No. 41 Interruptor de acceso.

Una vez seleccionada, desplegara la siguiente ventana de acceso, ver figura No. 42.

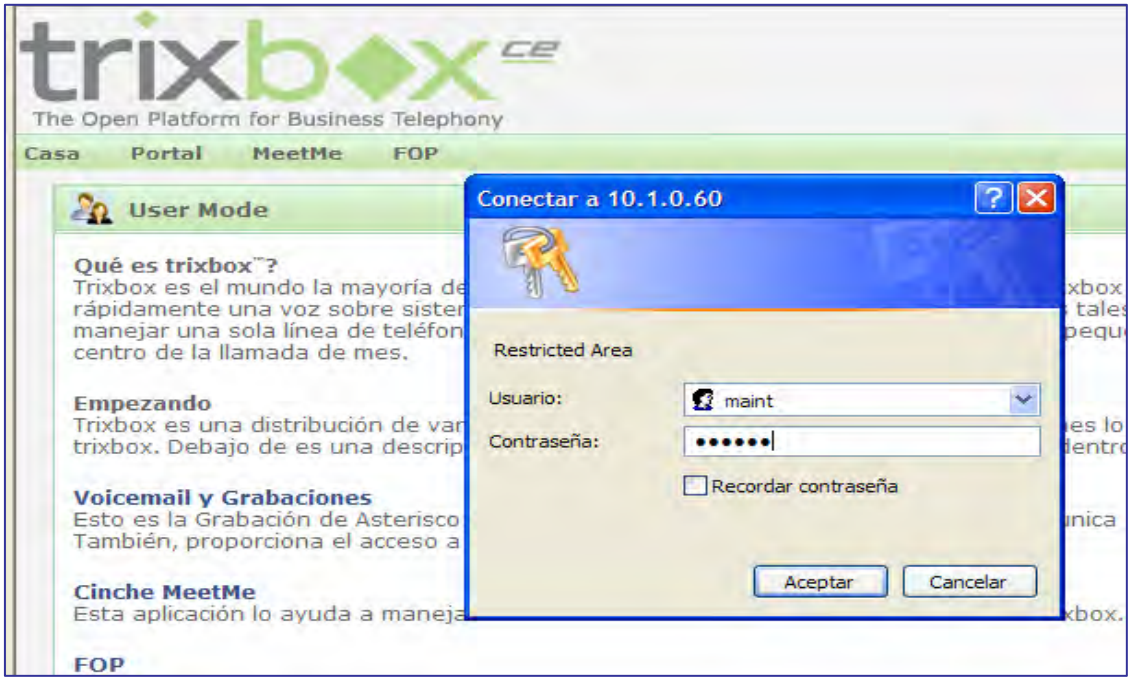


Figura No. 42 Ventana de acceso al panel de administración de TrixBox.

Seguidamente se desplegará, la siguiente página. En este acceso es de considerar que TrixBox, puede ser administrado para nuestro caso, desde nuestra red privada o a través de una conexión desde la red publica de Internet, ver figura No. 43.

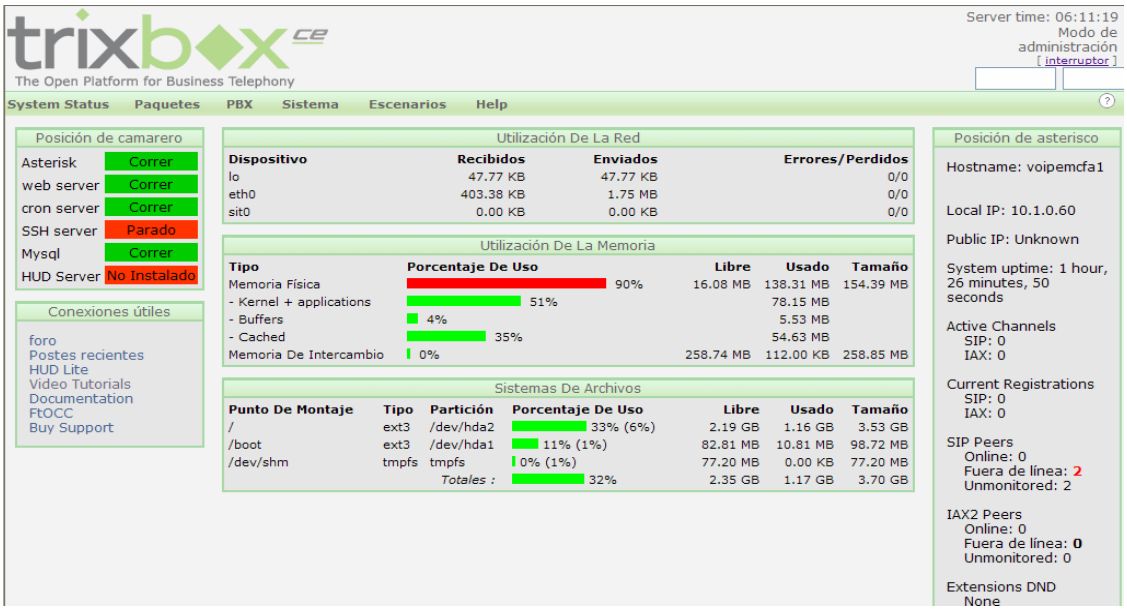


Figura 43 pantalla de Estatus del Sistema.

En esta pantalla nos despliega información relacionada a:

- Interfaces de red conectadas.
- IP local conectada (10.1.0.60).
- IP publica (desconocida).
- Canales activos (SIP o IAX).
- Canales SIP activos.
- Canales IAX activos.
- Información del sistema de archivos del servidor.
- Uso de memoria y otros valores.

Si observamos el menú, principal encontramos las siguientes opciones:

- System Status.
- Paquetes.
- PBX.
- Sistema.
- Escenario.
- Help.

En nuestro caso particular no centraremos en la opción PBX, que es la que nos interesa. Esta opción una vez es seleccionada, nos muestra el siguiente submenú, ver figura No. 44.

Figura No. 44 Opciones del menú PBX.

Al seleccionar el menú, nos muestra, opciones como son:

- PBX Settings.
- Config File Editor.
- PBX Status.
- Director Endpoint.
- Bulk Extensions.
- CDR Report.

Para casos de nuestro estudio, nos concentraremos en la opción de BPX Settings, la cual nos muestra la siguiente pantalla, ver figura No. 45.

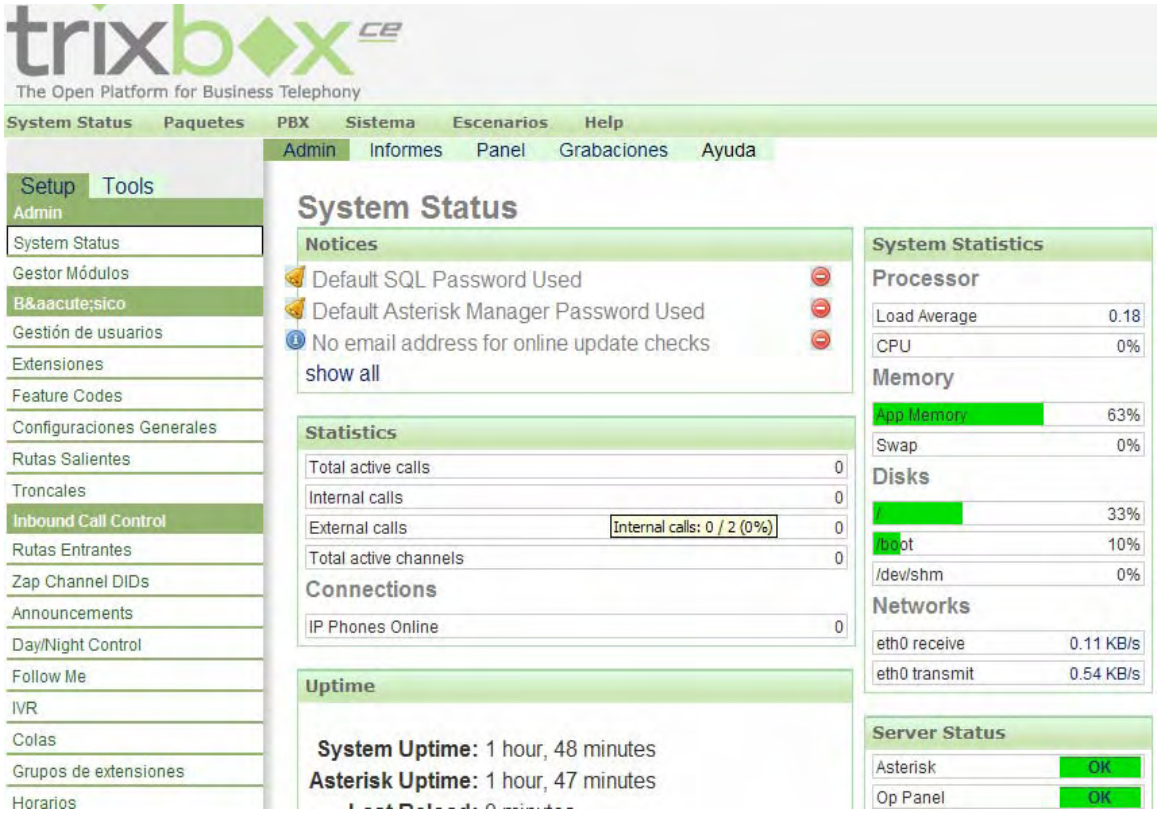


Figura No. 45 Menú principal de PBX Settings.

Con la opción PBX Settings, se puede configurar los siguientes servicios:

- System Status: muestra el status del servicio de TrixBox.
- Gestor de Módulos: administra los diferentes módulos que emplea TrixBox.
- Gestión de Usuarios: nos permite administrar usuarios.
- Extensiones: se utiliza para la creación y configuración de extensiones.
- Feature Codes: es el Plan de marcado por defecto.
- Configuraciones Generales: donde configuramos, valores como el tiempo para que una llamada pase a buzón de voz, el

digito o numero que se antepondrá antes del número de la extensión para depositar un correo de voz y otros valores.

- Rutas Salientes: administra las rutas de llamadas salientes del sistema.
- Troncales: define troncales para conexión a la red telefónica pública.
- Rutas Entrantes: especifica a donde enviar las llamadas que vienen del exterior.
- Follow me: es una opción que se crea como una extensión, de tal forma que si nadie contesta, sea redireccionado a una extensión alternativa.
- Horarios: nos permite condicionar las llamadas basándonos en el horario, fecha, semana, día.
- IVR: operadora automática, crea menús de voz que escucharan los usuarios que llaman.
- Grupos de Extensiones: agrupa extensiones para timbre simultáneo.

Estas opciones serán descritas y configuradas en los siguientes numerales.

e.- Configuración general de módulos.

Esto administra los módulos que se usaran para configurar el TrixBox. Permite activar, desactivar y actualizar módulos con las últimas versiones disponibles en el sitio oficial de TrixBox. Ver figura No. 46.

Figura No. 46 Pantalla de Gestor de Módulos.

Nota importante: cuando se instala TrixBox, coloca habilitados los módulos que vienen por defecto, sin embargo algunos módulos como por ejemplo: para realizar respaldos y otros módulos de administración no aparecen. En todo caso basta con seleccionar en link ***Check for updates online***, y esto nos mostrara todos aquellos módulos que permiten ser actualizados y cuales no están instalados para poder descargar los que se requieran.

f.- Configuraciones Generales del PBX.

Antes de iniciar con el proceso para crear extensiones, es necesario completar algunos parámetros para TrixBox. Estos parámetros son los siguientes:

- ❖ Opciones de marcado.
- ❖ Correo de voz.
- ❖ Directorio de la Empresa.
- ❖ Maquina de Fax.

- ❖ International settings.
- ❖ Security settings.

Opciones de marcado.

Esta opción habilita diferentes opciones que el usuario podrá utilizar para las llamadas que reciba. Las opciones más comunes son "**Tr**", que significa "La persona que esta recibiendo la llamada puede transferirla usando #" y "Generar tonos de llamado cuando una extensión esta llamando". Otras opciones que se pueden utilizar son:

- A(x): reproducir un anuncio a la parte llamada utilizando "x" como archivo.
- C: no guarda registro de las llamadas en la base de datos.
- D ([llamado] [llamante]): enviar las líneas DTMF (Dual-Tone Multi-Frequency) especificadas después de que la parte llamada haya contestado, pero antes la llamada es puenteada. La denominada línea DTMF es enviada al llamado, y la denominada línea DTMF es enviada a la parte llamante. Ambos parámetros pueden ser utilizados solos.
- h: permite a la parte llamada cortar mediante el envió del dígito "*" DTMF.
- H: permite a la parte llamada cortar presionando el dígito "*" DTMF.
- r: indica llamado a la parte llamada. No transmite audio a la parte llamada hasta que el canal del llamado haya contestado.
- t: permite a la parte llamada transferir a la parte llamante mediante el envió de la secuencia DTMF definida en la configuración de presentaciones.
- T: permite a la parte llamante transferir la parte llamada mediante el envió de la secuencia DTMF definida en la configuración de presentaciones.

- w: permite a la parte llamada iniciar la grabación de la llamada mediante el envió de la secuencia DTMF definida para la grabación por un botón en la configuración de presentaciones.
- W: permite a la parte llamante iniciar la grabación de la llamada mediante el envió de la secuencia DTMF definida para la grabación por un botón en la configuración de presentaciones.

Correo de voz.

En esta opción, existen varios parámetros, pero los más utilizados son:

- Segundos que los teléfonos llamaran antes de pasar la llamada al correo de voz.
- Prefijo de extensión para acceder directamente al correo de voz.

Directorio de la Empresa.

Esta opción posee tres (3) principales parámetros:

- Buscar usuarios en el Directorio de la empresa.
- Reproducir número de extensión al llamante antes de transferir la llamada.
- Extensión del operador.

Maquina de Fax.

La maquina de Fax, de igual forma posee tres (3) opciones, siendo éstas las siguientes:

- Extensión de maquina de fax para recibir faxes.
- Dirección de correo electrónico a la cual serán enviados los faxes.
- Dirección de correo electrónico de donde los faxes parecen llegar.

International settings.

Son los tonos de ocupado, tono de llamada, llamada en espera adaptables a distintos formatos internacionales. Simplemente se tendrá que seleccionar el país donde se encuentre.

Security settings.

Este apartado, es para configurar si se desea llamadas anónimas SIP, lo cual si se coloca “Si”, permitirá que cualquier persona pueda llamar dentro de su servidor TrixBox utilizando el protocolo SIP.

A continuación se muestra la figura No. 47, en la cual se presenta un formulario para completar los parámetros. Para esto seleccionamos la opción CONFIGURACIONES GENERALES del menú de PBX SETTIGNS.

Figura No. 47a. Configuraciones Generales.

Figura No. 47b. Configuraciones Generales.

Descripción de llenado de parámetros de configuraciones generales:

1.- Opción de marcado= tr.

2.- Buzón de voz (se ha colocado 15 segundos antes de enviar al buzón de voz y el digito que se antepondrá para ingresar directamente al buzón de voz será 9).

3.- Opciones de IVR.

4.- Directorio de la Empresa (se ha seleccionado que realice búsqueda por apellido).

5.- Maquina de Fax (se ha dejado el valor para “sistema”).

6.- International settings (se ha seleccionado France y formato de 24 horas).

7.- Security settings (se ha dejado “no” para que no acepte llamadas de otras extensiones SIP).

g.- Configuración de extensiones.

Este apartado explica la forma de accesar y configurar los números de extensiones que utilizará TrixBox, para tal efecto seleccionamos la opción EXTENSIONES del menú de PBX SETTINGS. Luego nos mostrará la pantalla siguiente, ver figura No. 48 Configuración de Extensiones.

Figura No. 48 Configuración de Extensiones.

Para crear una extensión seleccionamos en tipo de dispositivo, el cual puede ser Generic SIP Device, Generic AIX2 Device, Generic ZAP Device y Other, para nuestro caso seleccionaremos GENERIC SIP DEVICE y presionamos el botón ENVIAR, seguidamente desplegara la siguiente pantalla, ver figura No. 49 Parámetros de configuración de extensión.

Antes de iniciar la creación y configurar los parámetros, debemos explicar cada uno de ellos, para un mejor entendimiento:

- Extensión: el valor ingresado en este campo debe ser único. Este es el número que puede ser marcado desde otra extensión cualquiera o directamente desde la recepcionista digital (IVR), si está activado este modulo. Este número puede tener cualquier largo, pero convencionalmente es utilizado un número de tres o cuatro dígitos.

- Nombre asociado: Este es el texto de identificación de la llamada que se presenta a los que son llamados.
- Cid Num Alias: El valor colocado en este campo, sobrescribe el ya configurado en “nombre asociado”, solo cuando se realizan llamadas internas. Por ejemplo, puede colocarse como alias el número de la cola a la que pertenece el interno y así, las llamadas devueltas, serán hacia la cola y no directamente al interno.
- Direct DIC: Aquí se coloca el numero directo (PSTN o VoIP) tal como es recibido por la central, al que se requiere asociar con este interno. Por ejemplo, si tenemos una línea con el numero 11-5555-1234 y las llamadas a este que suenen directamente en este interno, debemos colocar 1155551234.
- DID Alert info: Esta función es para configurar los ringtones de los teléfonos IP. No tiene efecto si no se configura un número en Direct DID.
- Music on Hold: Esta opción especifica que categoría de música usara este interno cuando necesite enviar música en espera a la parte llamante. Las categorías se configuran previamente en el modulo “Music Hold”.
- Outbound CID: Debe ingresarse un valor con el formato “Nombre” <##########>. Este valor sobrescribirá el Caller ID de la línea cuando este interno realice una llamada al exterior.
- Ring Time: Aquí se configuran los segundos de espera antes de derivar al llamante al voicemail. La opción default toma el valor ingresado en el modulo “Configuraciones Generales”.
- Call Waiting: Permite activar o desactivar la función de llamada en espera para el interno que se está creando. Esta función puede activarse o desactivarse posteriormente utilizando *70 o *71.
- CID de emergencia: El valor que se ingresa en este campo, sobrescribirá todos los ajustes anteriores referentes a la identificación

de llamada cuando se utilice una ruta saliente marcada como “Llamadas de emergencia”.

- Contraseña (secret): Esta es la contraseña (password), utilizada por el dispositivo telefónico para autenticarse al servidor de TrixBox cuando se crea una extensión SIP o IAX2. Esto es generalmente configurado por el administrador antes de dar el teléfono al usuario, y comúnmente no conocida por el usuario. Si el usuario esta utilizando un softphone, entonces necesita saber esta contraseña para configurar el programa, se recomienda que la contraseña sean números, ya que el usuario lo ingresara desde un teléfono.
- Extensión del Fax: Puede seleccionarse el interno donde se harán llegar las llamadas originadas desde un Fax. Si se selecciona FreePBX default, se utilizarán los valores indicados en el modulo “Configuraciones Generales”. Si en cambio, es seleccionado “sistema”, los faxes recibidos serán enviados por email.
- Email del Fax: En este campo se indica el mail de destino de los faxes recibidos por el interno que se esta creando. Esta función tiene efecto solo si el parámetro “Extensión del Fax” es configurado a “sistema”.
- Pausa después de responder: Ajustar el tiempo en segundos que desea reproducir el sonido de señal del fax a la parte llamante.
- Aplicar privacidad: Si la persona que llama no tiene identificador de llamada (numero privado), se le pedirá que ingrese los números de su número telefónico.
- Language Code: Aquí puede especificar el idioma de los paquetes de sonido que TrixBox utilizará para este interno. Por ejemplo, “en” para ingles, “es” para español, “it” para italiano, etc.
- Grabación entrante: Opciones para grabar las llamadas recibidas en la extensión. Existen tres opciones: **Siempre, nunca, a pedido** (el usuario puede presionar “*” 1 para activarlo durante cualquier llamada).

- Grabación saliente: Funciona de la misma manera que el anterior, pero con llamadas salientes.
- Buzón de voz: Al seleccionar “habilitado”, se activa la casilla de mensajes para el interno que se está creando. Si la casilla ya estaba habilitada y se la deshabilita, se borrarán todos los valores de configuración ingresados.
- Contraseña del correo de voz: Esta es la contraseña para acceder al sistema de correo de voz (voicemail). Puede ser cambiada por el usuario cuando ingresa en su buzón de voz marcando *98. Para hacer esto, luego de ingresar, debe presionar cero y luego cinco.
- Dirección de e-mail: Las direcciones a las que el correo de voz, enviará las notificaciones cuando haya un nuevo correo almacenado.
- Dirección de e-mail pager: Esta es la dirección de e-mail a la que se enviara una pequeña notificación al momento de registrarse un nuevo mensaje en la casilla (voicemail), adaptable para un servicio de e-mail a pager.
- Reproducir CID: Reproduce el numero que llamó antes de reproducir el mensaje, e inmediatamente después anuncia la fecha y la hora en la que fue grabado el mensaje.
- Reproducir fecha y hora (envelope): Esta opción controla si el sistema reproducirá o no la fecha y hora del mensaje antes de reproducir el mensaje. Esta configuración no tiene efecto sobre la operación de la opción de envelope en el menú “advance” del buzón de voz (voicemail).
- Borrar buzón de voz (voicemail): Si esta seleccionada en “yes” el mensaje será borrado de la casilla de correo de voz (voicemail), después de que se haya enviado por e-mail. Esta función provee la funcionalidad que le permite al usuario recibir su correo de voz, únicamente por e-mail, en lugar de recuperar el mensaje desde la web o la extensión.

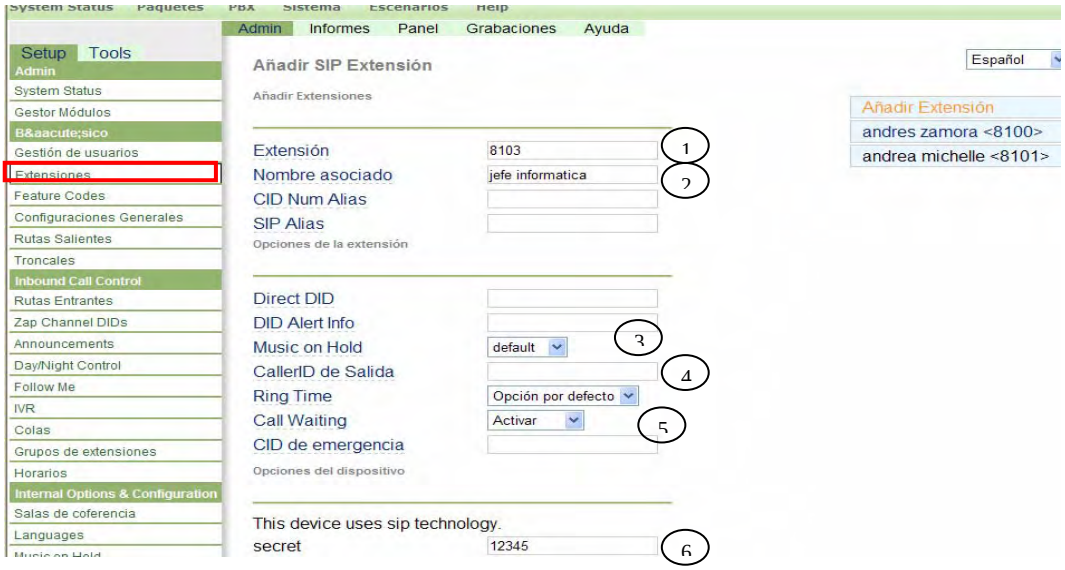


Figura No. 49a. Parámetros para configurar Extensión.

Los valores que se han tomado para el ejemplo, son los siguientes:

1.- extensión: 8301.

2.- nombre asociado: jefe de informática.

3.- Music on Hold: default.

4.- Ring Time: opción por defecto.

5.- Call Waiting: Activar.

6.- secret: 12345.

Figura No. 49 b. Parámetros Extensión.

7.- extensión de fax: sistema.

8.- Aplicar privacidad: No.

9.- Language code: es.

10.- Grabaciones entrantes: Bajo demanda.

11.- Grabaciones salientes: Bajo demanda.

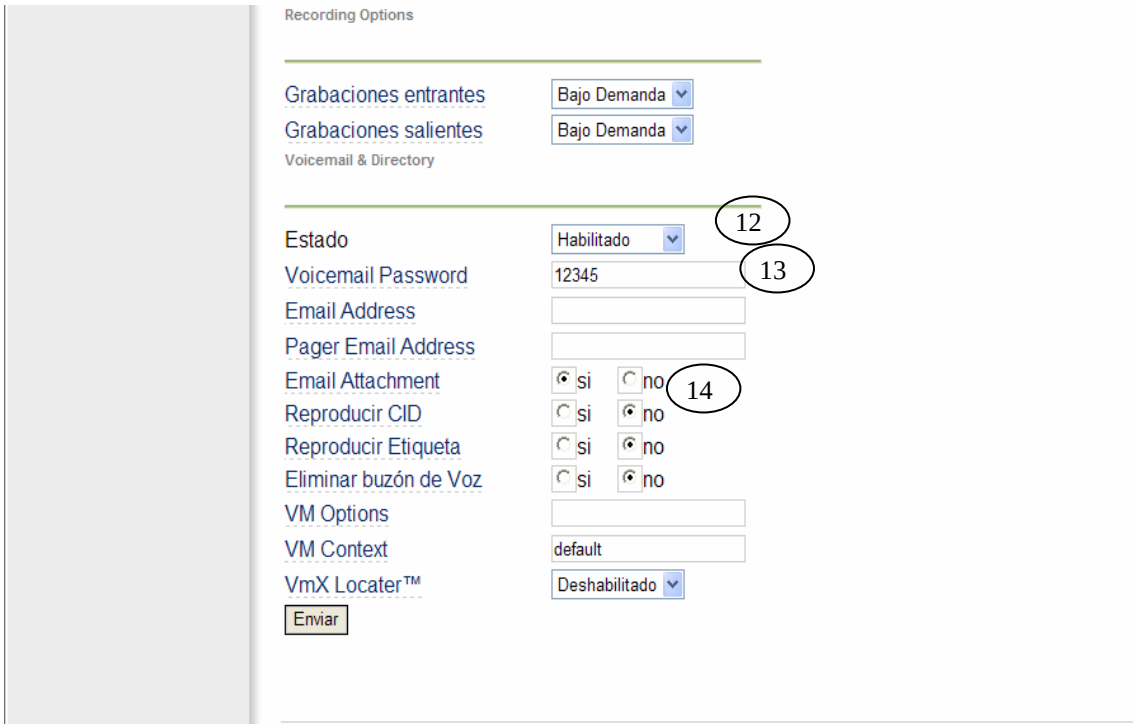


Figura 49 c. Parámetros de extensión.

12.- Estado: Habilitado.

13.- Voicemail password: 12345.

14.- Email attachment: si.

Finalmente una vez introducidos los parámetros, según se mostraron en el ejemplo, se procede a salvar los datos presionando el botón **Enviar** y seguidamente se activara una etiqueta color naranja, solicitando aplicar los cambios. Ver figura No. 50 y 51.

Figura No. 50 Aplicar cambios.

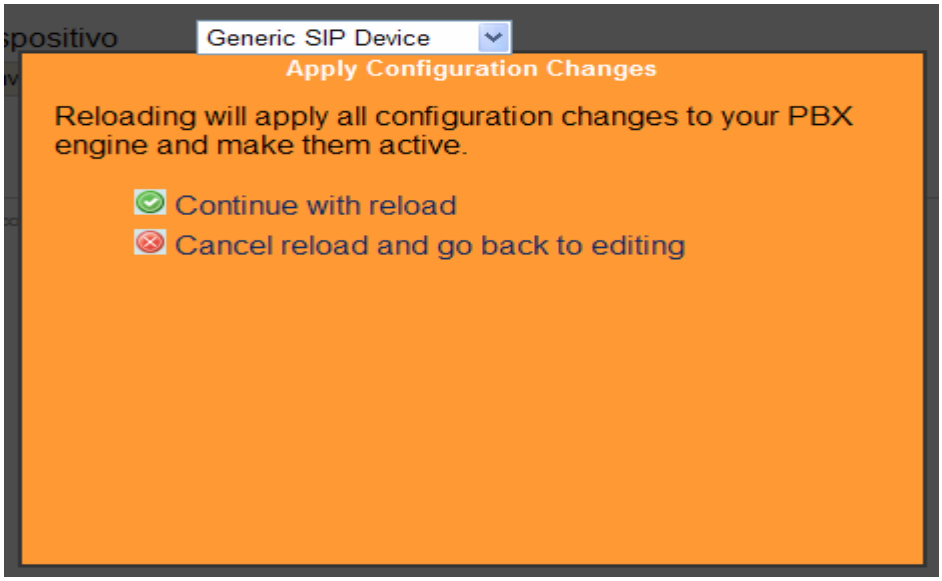


Figura No. 51 Continue with reload.

Una vez salvado los parámetros, la extensión ha sido creada y agregada a la Base de Datos. (Extensión No. 8103, asociada a Jefe de Informática, tipo SIP).

h.- Grupos de extensiones.

TrixBox posee lo que se denomina Grupo de Extensiones o Grupo de Timbre, lo cual significa que agrupa dos o más extensiones que sonaran o timbraran cuando alguien marque el numero asignado al grupo, en este caso el primero que contesta se queda con la llamada.

Para crear un Grupo de Extensiones, es necesario conocer cada uno de los parámetros a introducir, siendo éstos los siguientes:

- Numero de grupo: este es el número que es marcado desde cualquier extensión para que todos los teléfonos del grupo llamen.
- Descripción del grupo: una descripción que ayuda a identificar el grupo. Existen tres (3) estrategias de timbrado:

  Ringall: llama a todos los canales disponibles hasta que alguno conteste.

  Hunt: toma turnos llamando a cada extensión disponible.

  Memoryhunt: llama a la primera extensión, luego a la primera y a la segunda, luego la primera y a la segunda y a la tercera, y así sucesivamente.
- Listado de extensiones: lista las extensiones que serán agrupadas, una por línea. Se puede incluir una extensión en un sistema remoto o un numero externo mediante el sufijo de un numero con un numeral (#). Ejemplo 22500000#, marcara 22500000 en la troncal apropiada.

  Nota: no deben incluirse extensiones propias del sistema.
- Nombre de prefijo CID: se tiene la opción de colocar un prefijo al nombre del identificador de llamadas cuando llamen las extensiones en este grupo.
- Tiempo de llamada (máximo 60 segundos): cuanto tiempo (en segundos) el grupo llamará antes de fallas y tomar la opción “destino nadie contesta”.
- Destino si nadie contesta: Esto da una serie de opciones a tomar, cuando la llamada excede el tiempo de llamado especificado en “tiempo de llamada”. Si nadie contesta se puede asignar a otro grupo o a una extensión única denomina BASICO, este puede ser la recepcionista, IVR.

Ahora que se conocen los parámetros, se procede a crear el Grupo de Extensiones, para lo cual seleccionamos la opción Grupo de extensiones del menú PBX SETTINGS, ver figura No. 52 Configuraciones de Grupo de Extensiones.

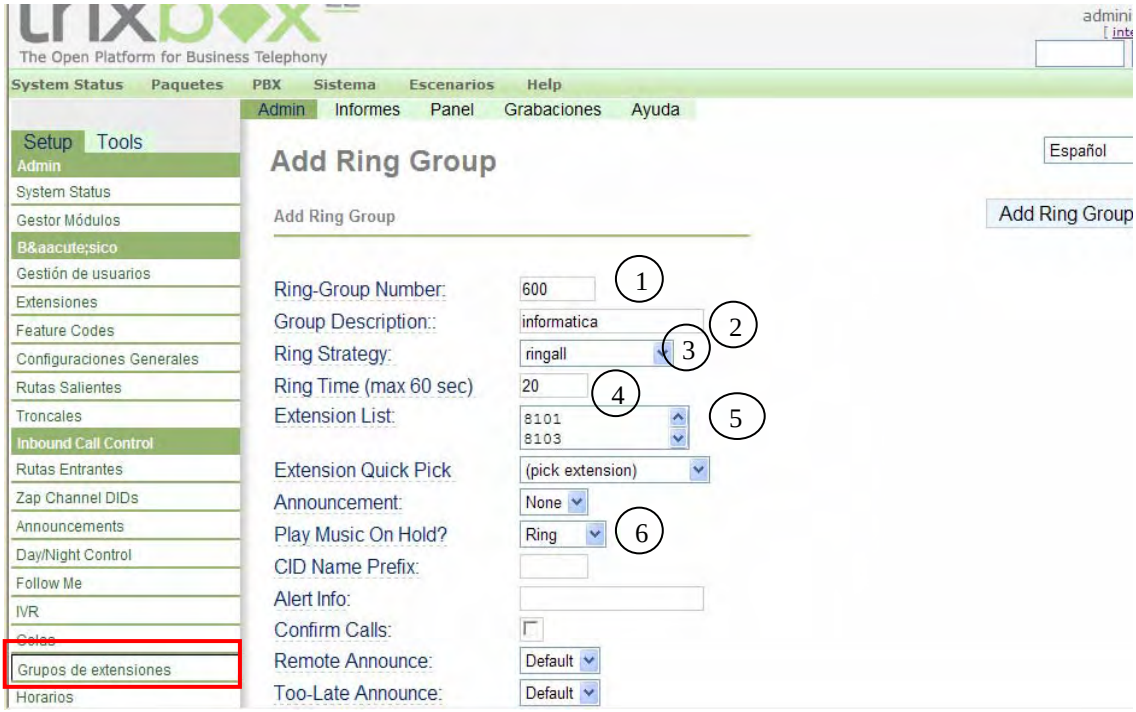


Figura No. 52 Configuración de Grupo de Extensiones.

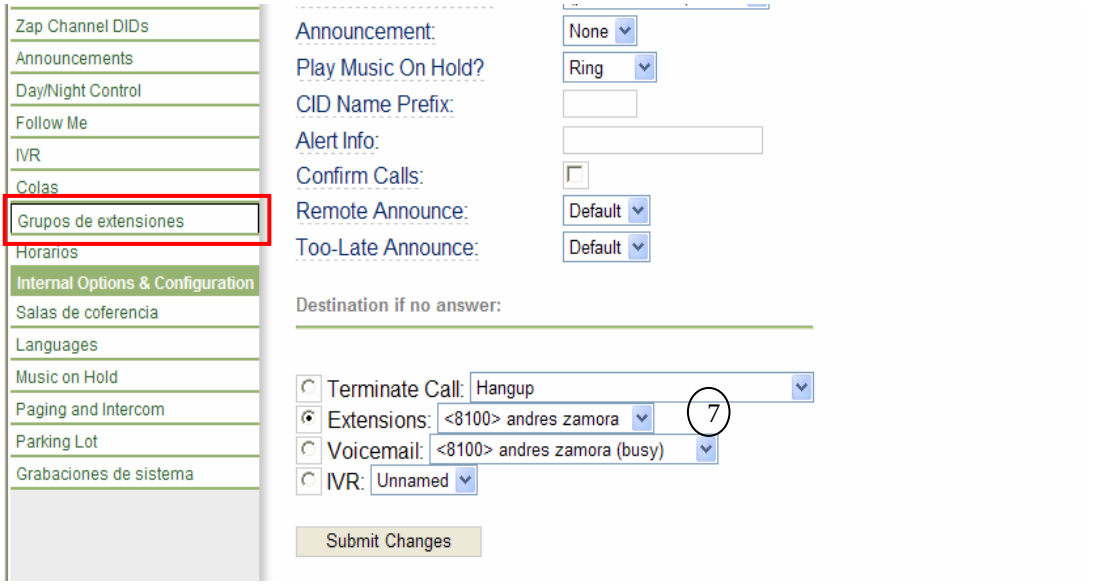


Figura No. 52a. Configuración de Grupo de Extensiones.

Los parámetros que se ha tomado en cuenta para la creación del Grupo de Extensiones son los siguientes:

1.- Ring Group Number = 600.

2.- Descripción de grupo= informatica.

3.- Estrategia de timbrado = ringall.

4.- Tiempo de timbrado = 20 segundos.

5.- Lista de extensiones = 8100, 8101, 8103.

6.- Play music on Hold = ring.

7.- Destino si nadie contesta = 8100.

Una vez introducidos los parámetros se presiona el botón submit changes, para enviar los datos y finalmente el grupo es adicionado con el numero de identificación 600.

i.- Follow me.

Follow me es como un mini grupo de extensiones, pero esta ligada directamente a una extensión. Se configura de la misma manera en la que se configura un grupo de extensiones, incluyendo la presentación de anunciar a la persona que llama que esta siendo transferida a otra parte.

Para efectos de este documento utilizaremos el Follow me, para direccional a un IVR, los parámetros necesarios para configurar el Follow me, son los siguientes:

- Disable: si se marca, se deshabilitará la función de follow me para la extensión seleccionada.
- Initial Ring Time: en este campo se elige la cantidad de segundos que sonará el primer numero de la lista follow me, si aplica a la estrategia de llamada seleccionada.
- Listado de extensiones: aquí se agregan uno por línea, los números que se quiere hacer sonar. Si ingresa un numero externo, debe agregarse el signo # al final.
- Estrategia de ring:

  - ringallv2: llama al primer numero de la lista durante el tiempo establecido en "Initial Ring Time". Luego llama a los demás números ingresados por el tiempo fijado en "Ring Time".
  - Ringall: llama a todos los canales disponibles al mismo tiempo hasta que alguno conteste.
  - Hunt: toma turnos llamando a cada extensión disponible.
  - Memoryhunt: llama a la primera extensión, luego a la primera y a la segunda, luego a la primera y a la segunda y a la tercera, y así sucesivamente.
- Extensión Quick Pick: aquí puede elegirse una extensión que se incluirá al final de la lista Follow me.
- Announcement: el sonido seleccionado de este lista (previamente cargado en el modulo de grabaciones del sistema), será reproducido antes de marcar los números de la lista.
- Play music on hold: puede seleccionar una categoría de música en espera, ninguna o tono de llamada, que será escuchado por el llamante.
- CID name prefix: el texto introducido en este campo, se antepondrá el CID especificado en las extensiones que figuren en la lista follow me.
- Sonido de alerta: la información de la alerta puede ser usada para un tono de llamada distintivo con ciertos dispositivos SIP.
- Confirm Calls: activar esta opción si se ingresaron a la lista follow me números que necesitan ser confirmados. La persona llamante deberá presionar 1 para que la llamada pueda ser realizada.
- Remote announce: el sonido seleccionado será reproducido a la persona que recibe la llamada, si **confirm calls** esta activado.
- Destino si nadie contesta: se configura similar al grupo de extensiones.

Ahora bien, el siguiente paso es selecciona del menú de PBX SETTINGS, el menú con la opción Follow me, tal como se muestra en la figura No. 53.

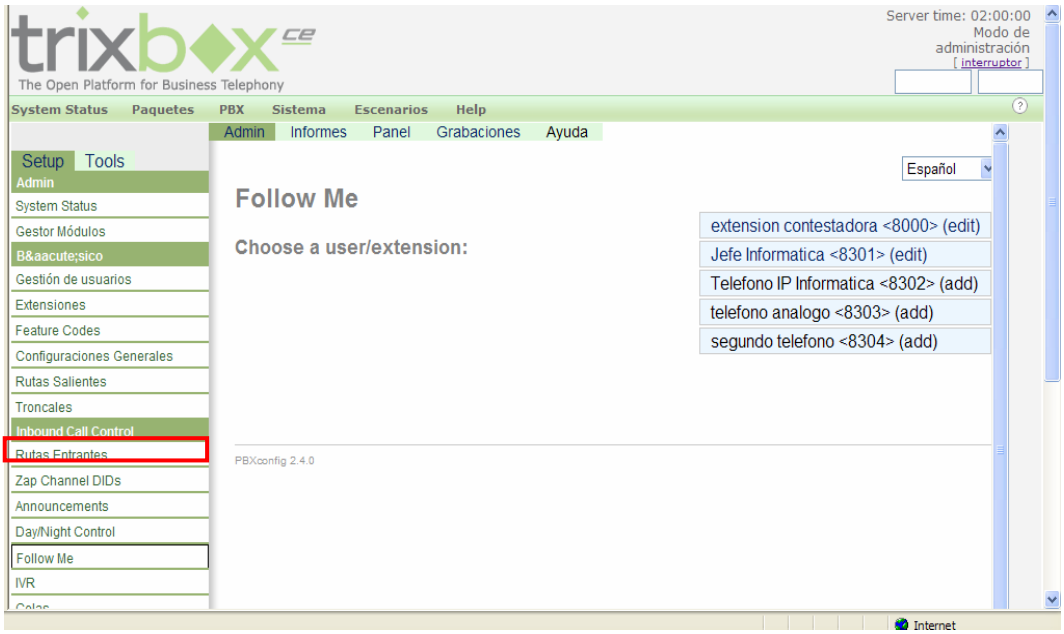
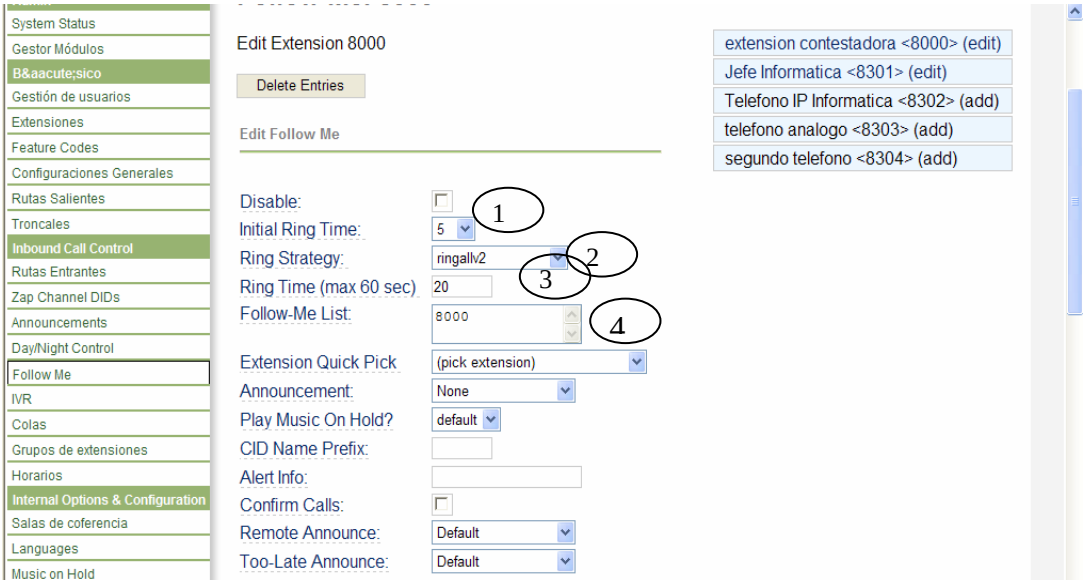


Figura No. 53 Follow me.

Para nuestro caso seleccionaremos una extensión previamente creada, siendo esta la extensión 8000, la cual se denomina “extensión contestadora”, y posteriormente se desplegara la siguiente ventana, ver figura No. 54.



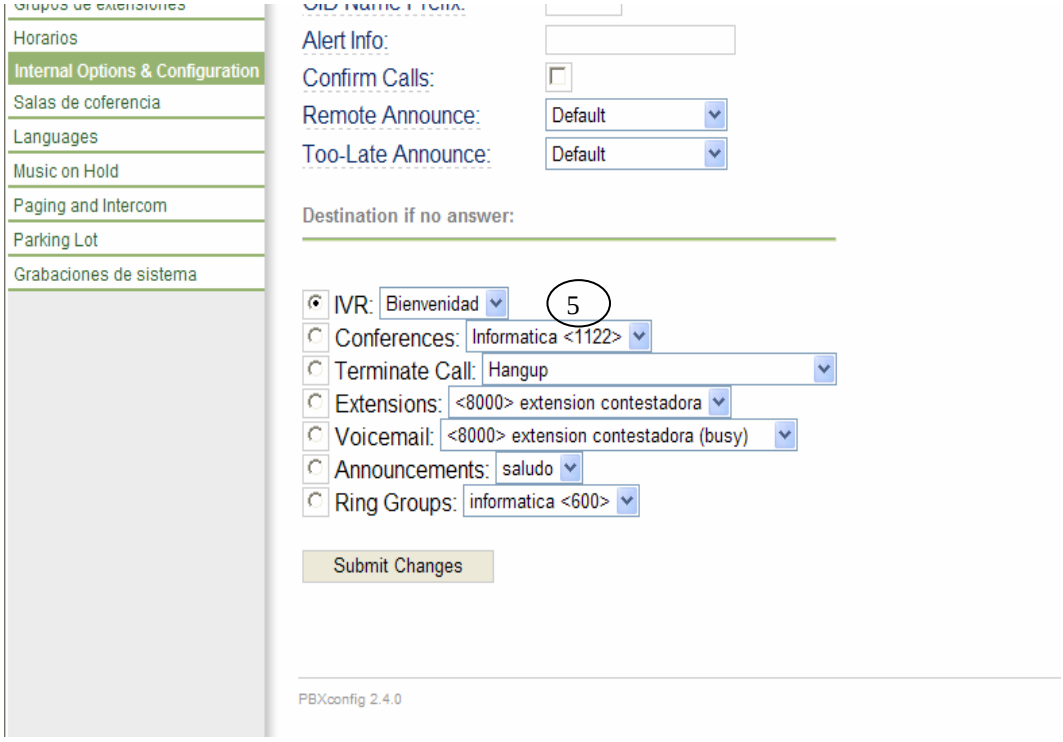


Figura No. 54 Configuración de Follow me.

Los valores que se ha configurado son los siguientes:

1.- initial ring time = 5.

2.- estrategia de ring = ringallv2.

3.- ring time = 20.

4.- listado de extensiones = 8000.

5.- destino si nadie contesta = IVR “Bienvenida”.

j.- Grabaciones del sistema.

Las grabaciones del sistema son utilizadas para los grupos de llamados y conferencias, para hacer anuncios.

Para generar una grabación, se deberá seguir los pasos que se indican en el panel. Para nuestro caso se generaron archivos con formato MP3, para los

anuncios, ya que si se utilizaban formato wav, éstos no se podían ser reproducidos por TrixBox. Ver figura No. 55 Carga de archivos de grabaciones.

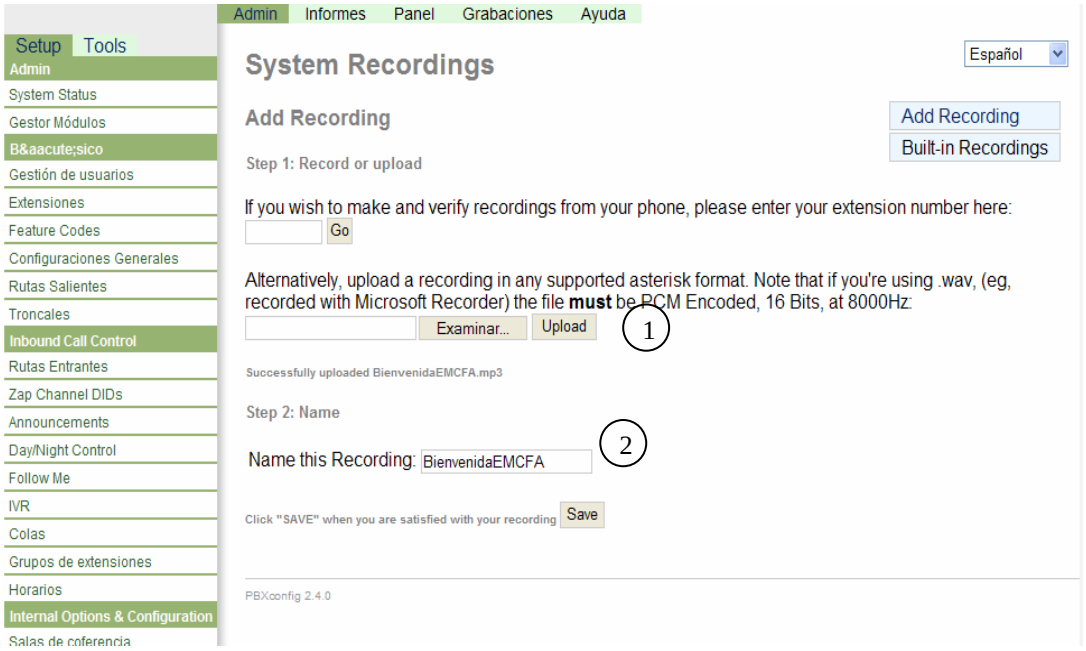


Figura No. 55 Grabaciones del Sistema.

En este caso, para cargar una grabación al sistema seleccionamos la opción “Grabaciones del Sistema” de menú PBXSetting, y posteriormente seleccionamos “Add Recording”. En la opción Examinar (1), presionamos y abre una ventana de nuestro explorador de Windows, seleccionamos el archivo tipo MP3 y luego presionamos el botón “Upload”, posterior a ese paso, la casilla “Name this Recording, es llenada con el nombre del archivo que cargamos, para el ejemplo es: Bienvenida (2), finalmente presionamos el botón “Save” y el archivo es guardado y podrá ser utilizado en los IVR o Anuncios de nuestro TrixBox.

k.- IVR.

El IVR es la recepcionista digital de TrixBox, normalmente se escucha un mensaje, el cual proporciona al llamante una guía u orientación sobre las opciones

de la recepcionista digital. Para la creación de un IVR, seguimos los pasos siguientes, ver figura No. 56 Adición de IVR.

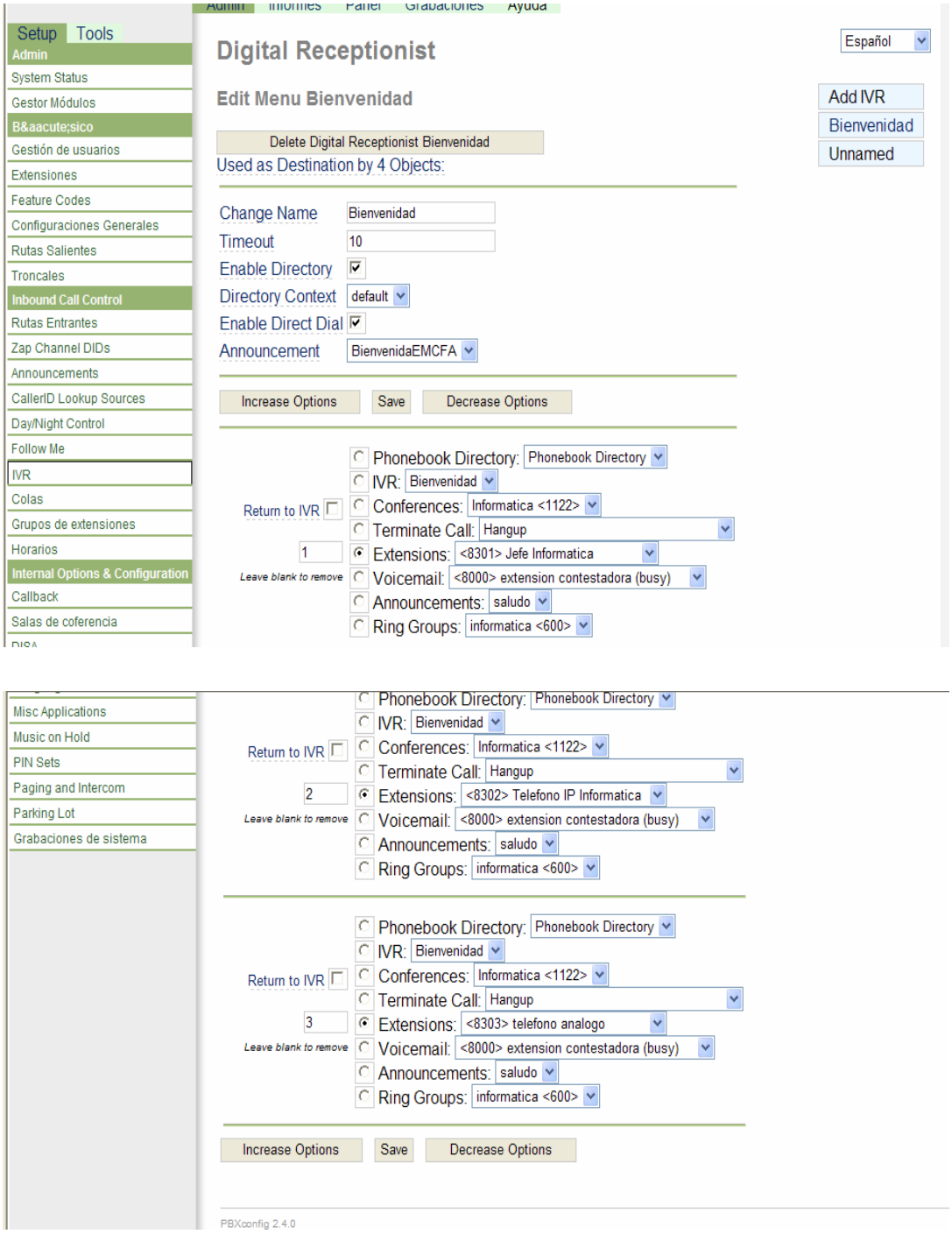


Figura No. 56 Adición de IVR.

Para esta herramienta seleccionamos del menú PBXSetting, la opción IVR y posteriormente nos muestra la imagen anterior, en donde podremos ingresar los valores siguientes:

1- Change name = Bienvenida (nombre del IVR).
2- Timeout = 10 (tiempo que espera antes de enviar la llamada al destino "t").
3- Announcement= Bienvenida (nombre del archivo MP3, que será reproducido al ingresar a la recepcionista digital).
4- Opciones del IVR = 1 (significa que al marcar la opción "1", la llamada será desviada a la extensión 8301), y así sucesivamente para las demás opciones se desviara la llamada entrante a la extensión que este preconfigurada.

Posterior a introducir los respectivos valores, procedemos a salvar los datos.

I.- Salas de Conferencia.

Las conferencias son una facilidad preestablecida que esta disponible como un destino.

Para adicionar una sala de conferencia en TrixBox, se deben seguir los siguientes pasos:

- Numero de sala: este el numero que los usuarios locales pueden marcar para incluirse en la conferencia. Ejemplo: 1122
- Nombre de la sala: esto es usado como un identificador, junto con el número, cuando se selecciona una conferencia como destino. Ejemplo: Informática.
- PIN de usuario: si cualquiera de estas opciones están activadas, cualquiera que llame a la conferencia le será requerida una contraseña PIN. Ejemplo: 123.

- PIN de administrador: este campo es opcional, en cuyo caso si es activada, se solicitara el PIN del administrador, para que pueda iniciarse la conferencia. Ejemplo: 12345.
- Opciones de la Sala:
  - Mensaje de entrada (join message): puede seleccionar YES o NO.
  - Esperar administrador (leader wait): puede seleccionar YES o NO.
  - Modo silencio (Quit mode): puede seleccionar YES o NO.
  - Cuenta de usuarios (User count): puede seleccionar YES o NO.
  - Aviso entrada/salida (User join/leave): puede seleccionar YES o NO.
  - Música en espera (Music on Hold): puede seleccionar YES o NO.
  - Permitir menú (allow menú): puede seleccionar YES o NO.

    En este caso si selecciona YES, podrá acceder a las opciones del menú desde su teléfono, con * más la opción:

    1: Silenciar.

    2: Bloquear o desbloquear conferencia.

    Ver figura No. 57 Agregar Sala de Conferencia.

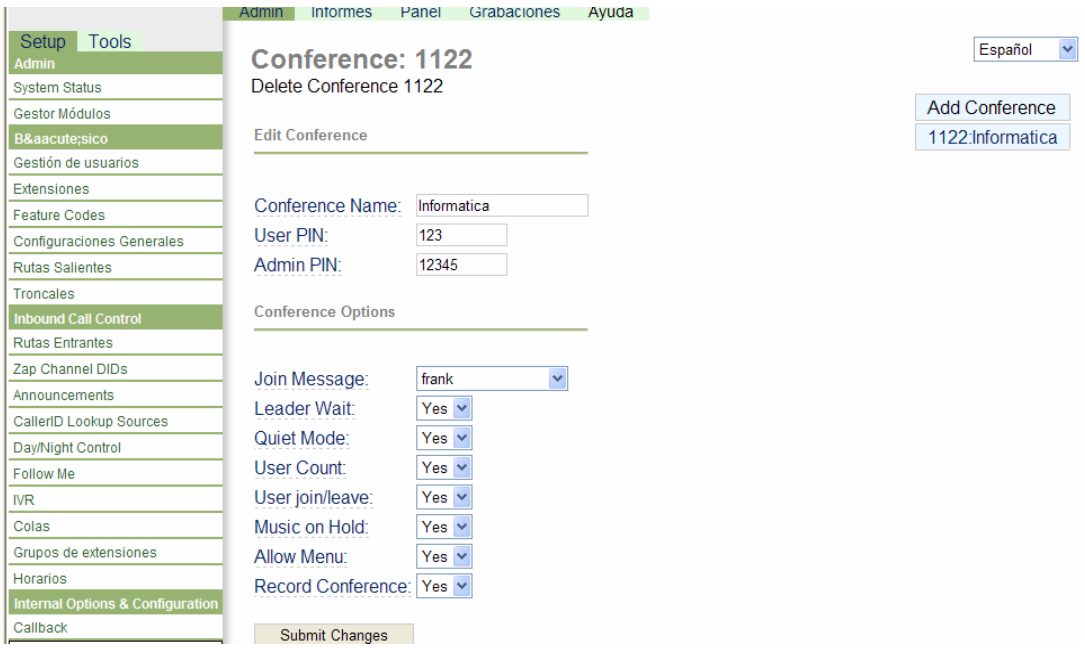
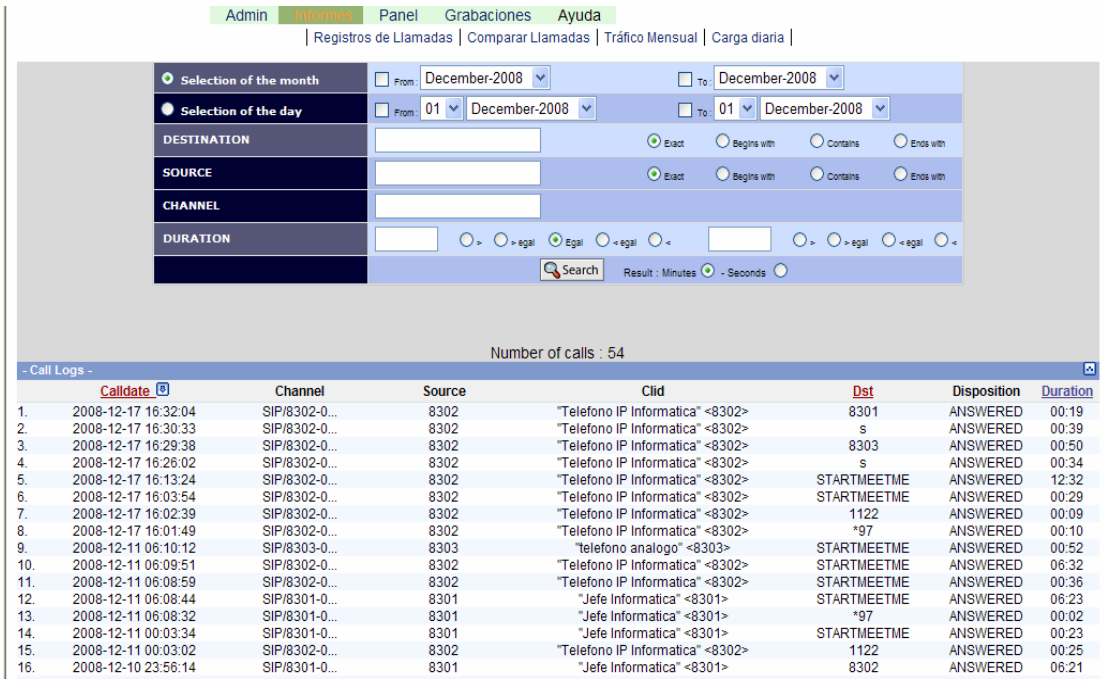


Figura No. 57 Agregar Sala de Conferencia.

Para el caso anterior, se puede observar que los valores de cada parámetro han sido completados, con los datos de ejemplo que se mencionaron en el párrafo anterior.

m.- Informes.

TrixBox guarda un registro llamado CDR (Call Detail Record), de todas las comunicaciones efectuadas a través del sistema, en la base de datos. Dentro de las opciones que muestra PBXSetting, existe la opción de informes, la cual una vez seleccionada nos muestra lo siguiente:



	Calldate	Channel	Source	Clid	Dst	Disposition	Duration
1.	2008-12-17 16:32:04	SIP/8302-0...	8302	"Telefono IP Informatica" <8302>	8301	ANSWERED	00:19
2.	2008-12-17 16:30:33	SIP/8302-0...	8302	"Telefono IP Informatica" <8302>	s	ANSWERED	00:39
3.	2008-12-17 16:29:38	SIP/8302-0...	8302	"Telefono IP Informatica" <8302>	8303	ANSWERED	00:50
4.	2008-12-17 16:26:02	SIP/8302-0...	8302	"Telefono IP Informatica" <8302>	s	ANSWERED	00:34
5.	2008-12-17 16:13:24	SIP/8302-0...	8302	"Telefono IP Informatica" <8302>	STARTMEETME	ANSWERED	12:32
6.	2008-12-17 16:03:54	SIP/8302-0...	8302	"Telefono IP Informatica" <8302>	STARTMEETME	ANSWERED	00:29
7.	2008-12-17 16:02:39	SIP/8302-0...	8302	"Telefono IP Informatica" <8302>	1122	ANSWERED	00:09
8.	2008-12-17 16:01:49	SIP/8302-0...	8302	"Telefono IP Informatica" <8302>	*97	ANSWERED	00:10
9.	2008-12-11 06:10:12	SIP/8303-0...	8303	"telefono analogo" <8303>	STARTMEETME	ANSWERED	00:52
10.	2008-12-11 06:09:51	SIP/8302-0...	8302	"Telefono IP Informatica" <8302>	STARTMEETME	ANSWERED	06:32
11.	2008-12-11 06:08:59	SIP/8302-0...	8302	"Telefono IP Informatica" <8302>	STARTMEETME	ANSWERED	00:36
12.	2008-12-11 06:08:44	SIP/8301-0...	8301	"Jefe Informatica" <8301>	STARTMEETME	ANSWERED	06:23
13.	2008-12-11 06:08:32	SIP/8301-0...	8301	"Jefe Informatica" <8301>	*97	ANSWERED	00:02
14.	2008-12-11 00:03:34	SIP/8301-0...	8301	"Jefe Informatica" <8301>	STARTMEETME	ANSWERED	00:23
15.	2008-12-11 00:03:02	SIP/8302-0...	8302	"Telefono IP Informatica" <8302>	1122	ANSWERED	00:25
16.	2008-12-10 23:56:14	SIP/8301-0...	8301	"Jefe Informatica" <8301>	8302	ANSWERED	06:21

Figura No. 58 Informe de Registro de Llamadas.

La ventana desplegada para informes, permite obtener datos relativos a:

- Registro de llamadas.
- Comparación de llamadas.
- Trafico mensual.

- Carga diaria.

Por defecto al cargarse la opción de Informes, muestra el Registro de llamadas, en la cual obtenemos datos tales como:

- Hora y fecha de la llamada.
- Canal SIP.
- Fuente (source) extensión que llamó.
- ID del llamante.
- Destino (extensión llamada).
- Disposición (si fue contestada o no).
- Tiempo de la llamada.

De igual forma estos datos pueden ser exportados a dos tipos de formato, ya sea en archivo PDF o archivo CSV para ser cargado desde Excel de Microsoft.

La opción de comparación de llamadas, nos permite establecer el numero de llamadas realizadas por día y el tiempo en el cual se ejecutaron y compararlas con uno, dos, tres y/o los últimos cuatro días, lo cual es mostrado en dos tipos de gráficos (un cuadro con barras de progresión por día y un grafico de línea), tal como se muestra en la figura No. 59 Comparación de llamadas.

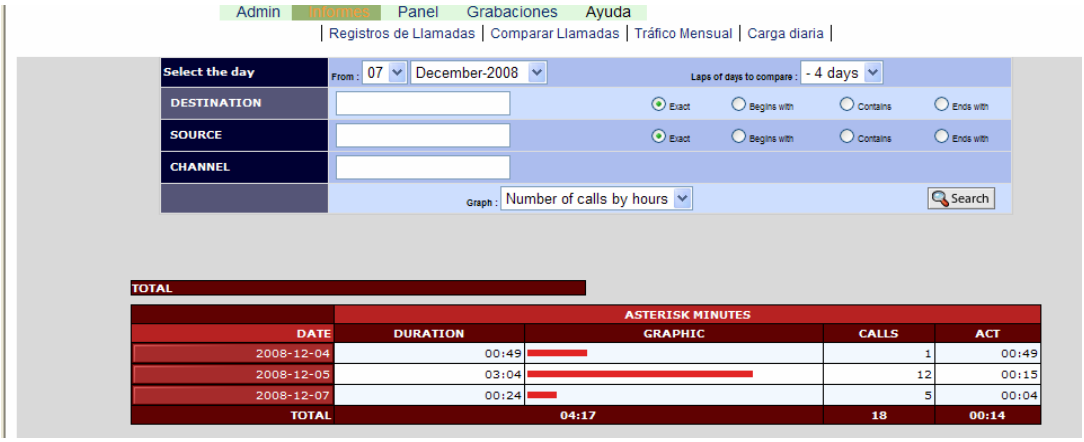


Figura No. 59 Comparación de Llamadas.

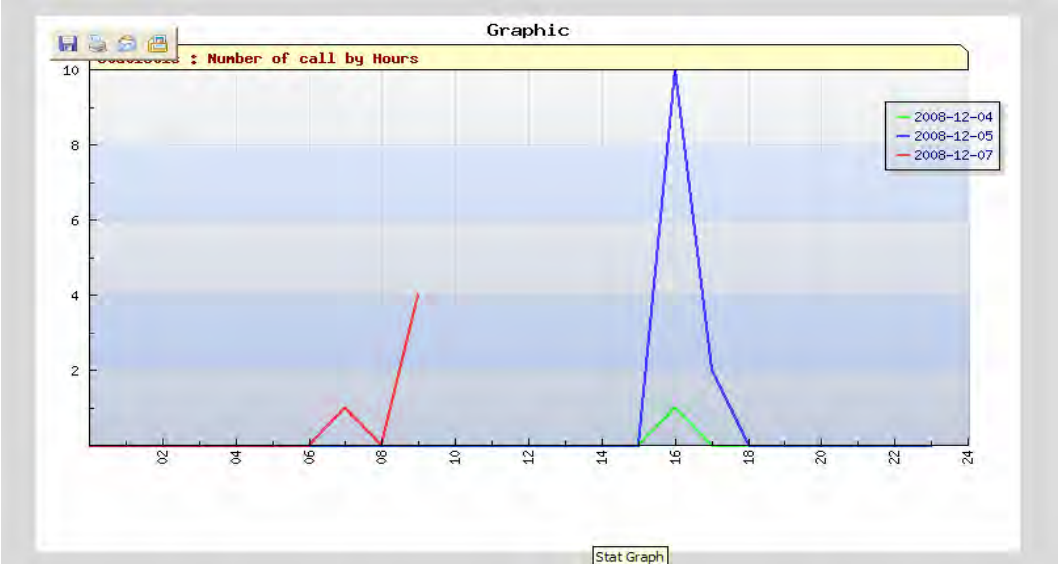


Figura No. 59a Grafica Comparación de Llamadas.

La opción trafico mensual, nos permite visualizar en forma grafica el comportamiento que ha tenido el trafico de llamadas por mes, tal como se muestra en la figura No. 60 Grafica de Trafico por Mes.

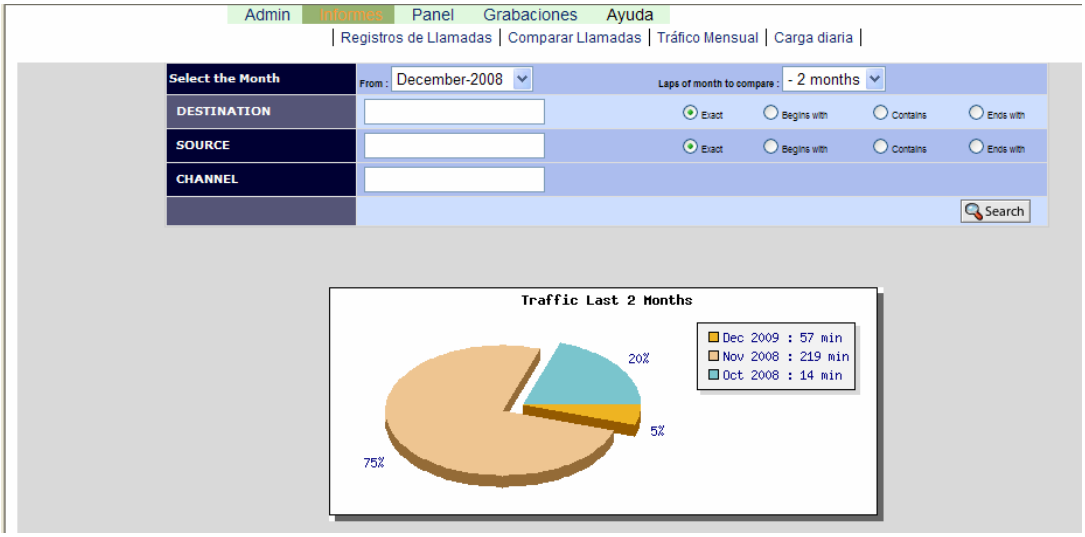


Figura No. 60 Tráfico Mensual.

La opción carga diaria, nos muestra datos relativos a las llamadas realizadas en un día determinado a través de una grafica de barras, ver figura No. 61 Carga Diaria.

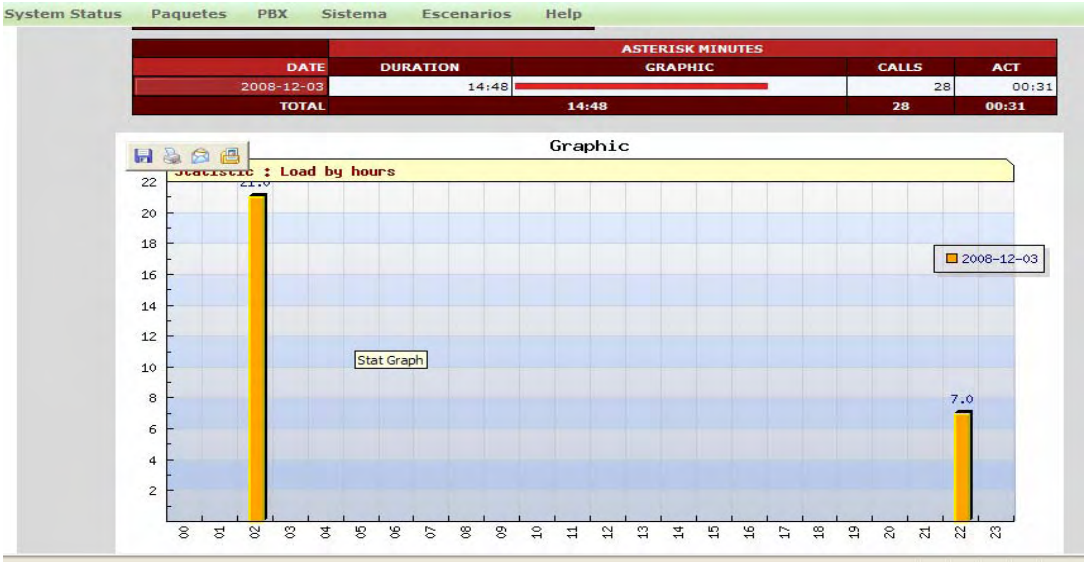


Figura No. 61 Carga Diaria.

n.- Flash Operador Panel.

El panel de operador es una aplicación que funciona en ambiente Web, y puede ser accesada a través de un explorador de Internet, éste funciona en tiempo real y nos permite visualizar la siguiente información.

- Extensiones que están ocupadas, llamando o disponibles.
- Quien esta hablando y con quien.
- El registro y disponibilidad en SIP e IAX.
- Estado de las salas de conferencia.
- Estado de las colas.
- Indicador de mensajes en espera.
- Agentes presentes en el sistema.

Ver figura No. 62 Consola del Operador.

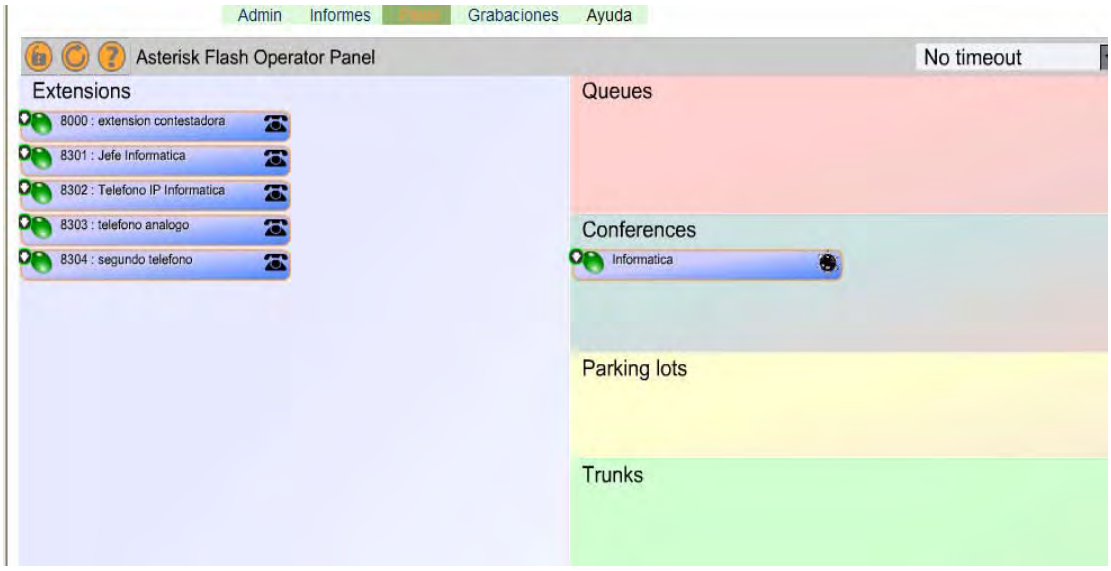


Figura No. 62 Panel del Operador de TrixBox.

Por defecto la el código de seguridad para acceder es **passw0rd**, una vez introduciendo el código de seguridad respectivo, el administrador podrá cancelar llamadas, unir dispositivos a una conferencia y/o cola. Editar el archivo **/etc/amportal.conf**

Para nuestro caso lo cambiamos por: **trixbox.**

Es importante mencionar en este punto, que el acceso remoto a través de la Web, presenta algunas vulnerabilidades, y esta son que un usuario, fácilmente puede digitar: http://10.1.0.60/panel, y sin mayor restricción podrá visualizar los diferentes dispositivos y usuarios que utilizan TrixBox. Así como las Conferencias, Colas y Troncales que existen. En este sentido es conveniente tomar las medidas seguridad pertinentes, para asegurar el acceso al Panel del Operador.

Esto lo podemos lograr, si colocamos restricción de acceso a la ruta siguiente: /var/www/html/panel.

Se tendrá que agregar un usuario al archivo ubicado en:

```
htpasswd /usr/local/apache/passwd/wwwpasswd  nombreUsuario
New password:
Re-type new password:
Apache confirma el usuario agregado:
```

Adding password for user nombreUsuario
Para nuestro caso usaremos:
Usuario : trixemcfa
Clave : trixemcfa

Para versiones de TrixBox 2.0 en adelante, se modificara el siguiente archivo:
vi /etc/trixbox/httpdconf/trixbox.conf
se Adicionaran las siguientes Líneas:

```
#Password protect the Asterisk@Home Splash Page /var/www/html/panel
<Directory /var/www/html/panel>
AuthType Basic
AuthName "Restricted Area"
AuthUserFile /usr/local/apache/passwd/wwwpasswd
Require user maint trixemcfa
</Directory>
```

Para eliminar un usuario de apache, basta con digitar la siguiente sentencia, para que sea removido de httpd.conf.

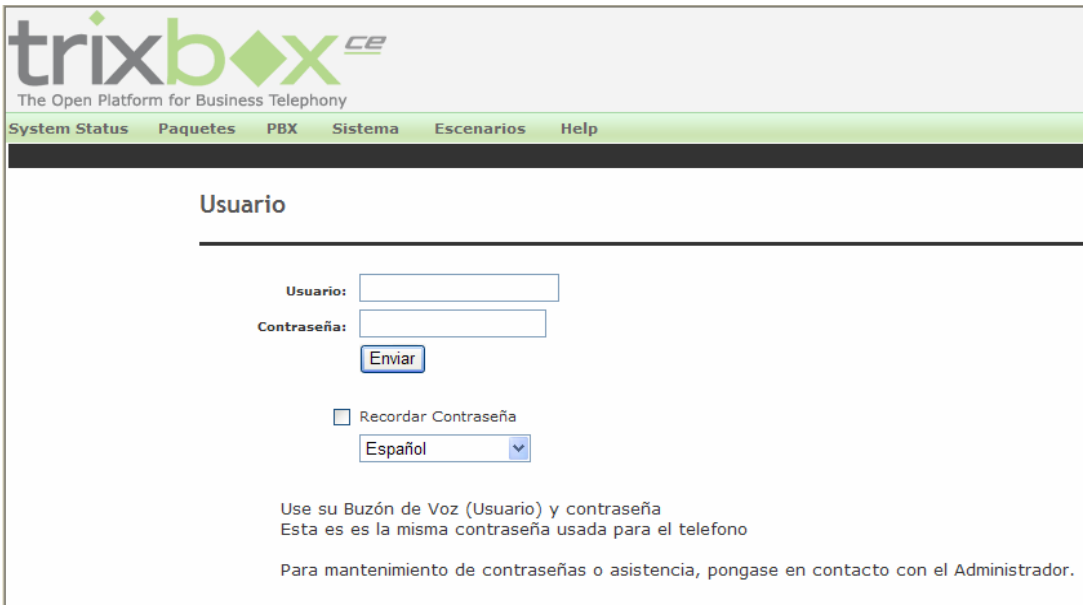
```
htpasswd -D /usr/local/apache/passwd/wwwpasswd NewUserName
```

Para re-iniciar APACHE, basta con digitar la siguiente sentencia:

```
/etc/init.d/httpd restart
```

o.- Grabaciones.

ARI (Asterisk Recording Interface), es un portal de usuario central para el programa de Asterisk PBX. Proporciona una interfase simple para el correo de voz (voicemail), y las grabaciones de monitoreo de las llamadas. Asimismo, proporciona el acceso a configuraciones de usuario Trixbox.



Para acceder a este portal, solamente debe ingresarse el nombre de usuario y la contraseña, para nuestro caso el nombre de usuario será el número de la extensión y la contraseña será el PIN secreto de acceso a la misma. La página de acceso es la siguiente:

Una vez se ingrese la validación respectiva, se mostrara la siguiente ventana, ver figura No. 63 Buzón de Voz.

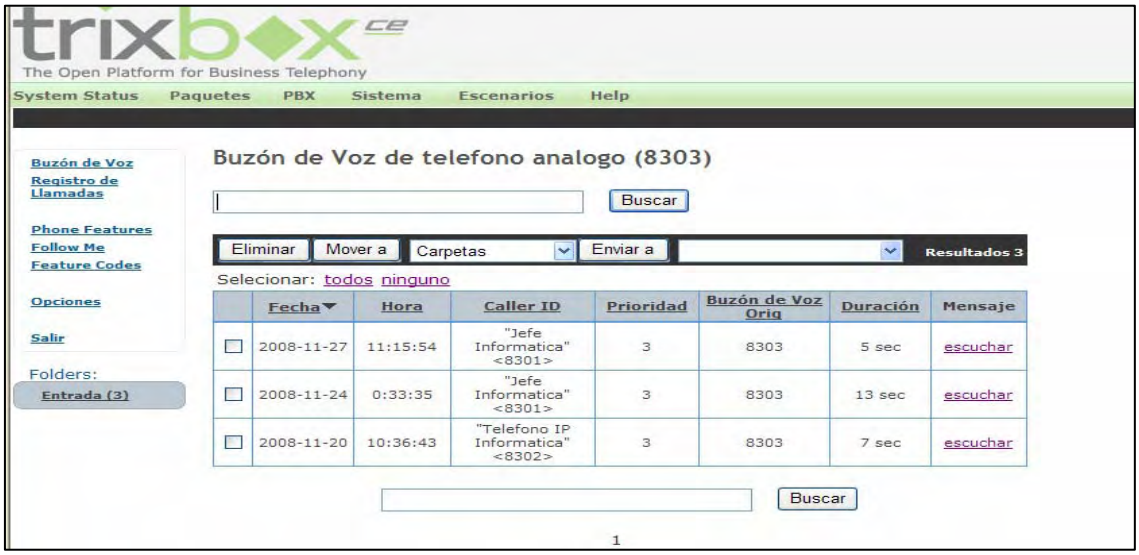
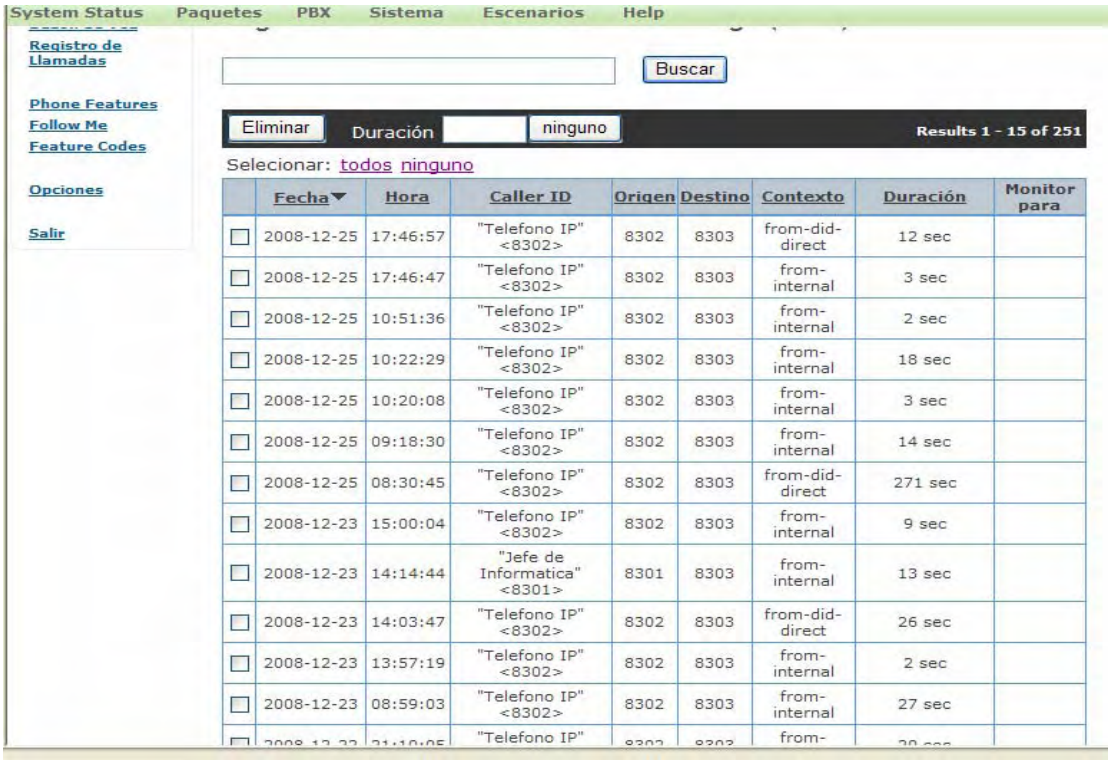


Figura 63 Buzón de Voz

En este buzón se almacena todos los mensajes de voz, que han sido depositados para la extensión, 8303 para nuestro caso. En dicho buzón se pueden obtener datos relativos a:

- Fecha de llamada.
- Hora la llamada.
- Caller ID del llamante.
- Prioridad.
- Duracion del mensaje.
- Mensaje de voz (para reproducirlo).

De igual forma dentro de las opciones de esta interfaz, puede tenerse acceso al registro de llamadas, como se muestra en la figura No. 64 Registro de llamadas.



	Fecha	Hora	Caller ID	Origen	Destino	Contexto	Duración	Monitor para
☐	2008-12-25	17:46:57	"Telefono IP" <8302>	8302	8303	from-did-direct	12 sec	
☐	2008-12-25	17:46:47	"Telefono IP" <8302>	8302	8303	from-internal	3 sec	
☐	2008-12-25	10:51:36	"Telefono IP" <8302>	8302	8303	from-internal	2 sec	
☐	2008-12-25	10:22:29	"Telefono IP" <8302>	8302	8303	from-internal	18 sec	
☐	2008-12-25	10:20:08	"Telefono IP" <8302>	8302	8303	from-internal	3 sec	
☐	2008-12-25	09:18:30	"Telefono IP" <8302>	8302	8303	from-internal	14 sec	
☐	2008-12-25	08:30:45	"Telefono IP" <8302>	8302	8303	from-did-direct	271 sec	
☐	2008-12-23	15:00:04	"Telefono IP" <8302>	8302	8303	from-internal	9 sec	
☐	2008-12-23	14:14:44	"Jefe de Informatica" <8301>	8301	8303	from-internal	13 sec	
☐	2008-12-23	14:03:47	"Telefono IP" <8302>	8302	8303	from-did-direct	26 sec	
☐	2008-12-23	13:57:19	"Telefono IP" <8302>	8302	8303	from-internal	2 sec	
☐	2008-12-23	08:59:03	"Telefono IP" <8302>	8302	8303	from-internal	27 sec	

Figura No. 64 Registro de Llamadas.

p.- Instalación de un Softphone.

Un Softphone es un programa que emula un teléfono convencional para ser usado en una computadora. En general, utiliza protocolos SIP o IAX2 de la misma manera que los utiliza Trixbox, a la hora de crear extensiones.

Primero debe instalar el programa  BOL SIPPhone_EN.msi , el cual le desplegará la siguiente pantalla, ver figura No. 65 Pantalla de Bienvenida.

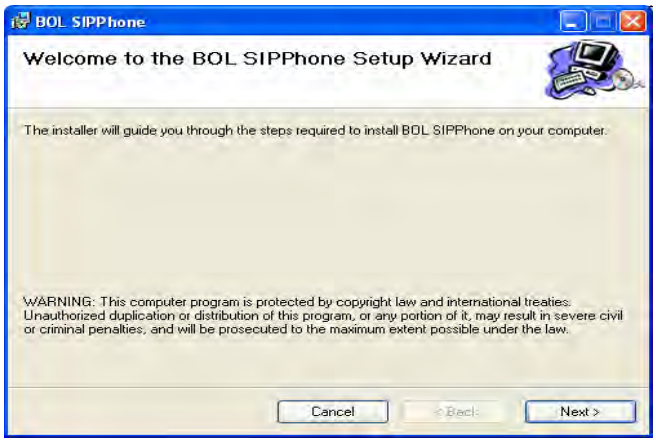
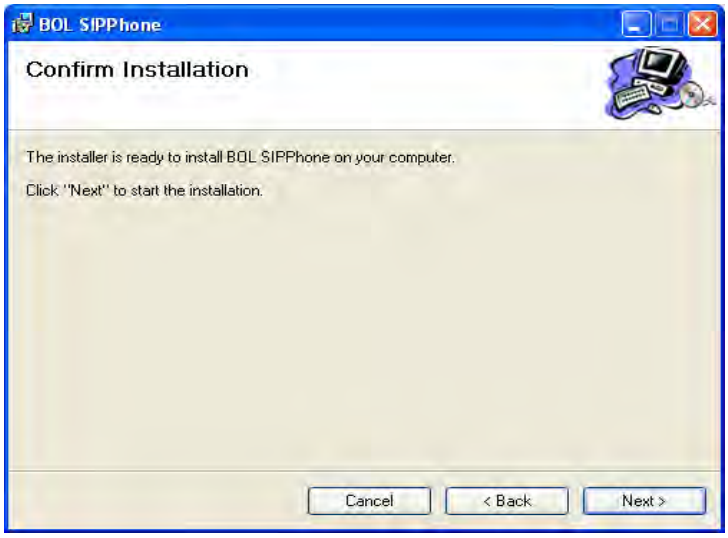


Figura No. 65 Pantalla de Bienvenida.

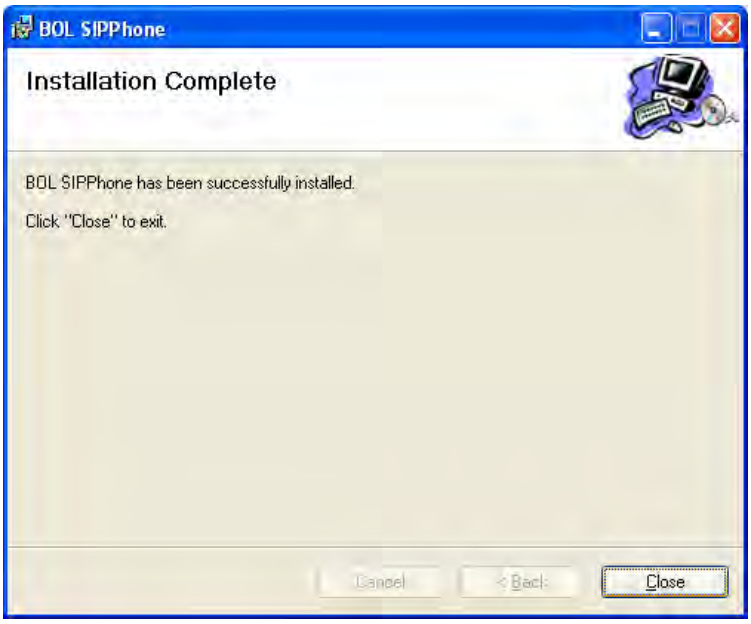
Presione NEXT para que muestre la pantalla donde será ubicado el programa:

Presione el botón NEXT>, el cual mostrara la pantalla siguiente:



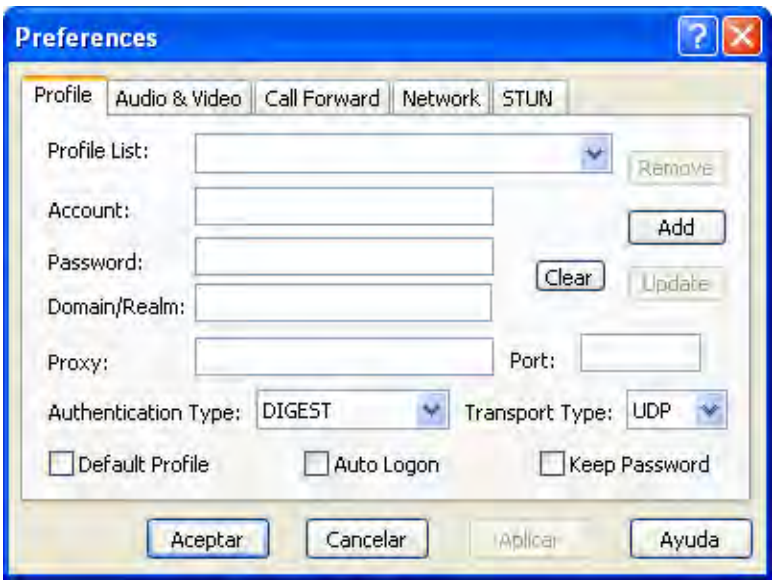
Presione el botón NEXT>, para ejecutar el proceso:

Una vez instale los archivos necesarios mostrara la pantalla de instalación exitosa, luego presione el botón cerrar (close).



Una vez instalado el software se requiere configurarlo para que este funcione, para ello debe de localizar el icono de acceso directo denominado BOL SIP Phone, se activa con doble click y se Cargara el programa para poderlo configurar.

Esta herramienta permitirá utilizar su máquina para hacer llamadas vía extensión a otro usuario en la red, posee varios iconos de los cuales se hará énfasis en el de configuración mostrado como un martillo,  al presionarlo con el Mouse, mostrará la siguiente pantalla:



De las pestañas Profile, Audio&Video, Call Forward, Network, Stun, se configuraran Profile, Audio&Video, Network, las demás no se tocaran.

Pestaña PROFILE

ACOUNT: Debe indicar el número de extensión que será utilizado para realizar las llamadas.

PASSWORD: Indica la clave de acceso a la cuenta, por definición se sugiere el numero de extensión más un juego de caracteres, estos deben de coincidir con los asignados en la creación de la extensión. Sin embargo deben ser de tipo numérico, ya que al usar teléfono solo acepta números.

DOMAIN/REALM: no se utiliza

PROXY: se ingresa la dirección IP del servidor Trixbox.

PORT: Por definición se asigna el numero de puerto escucha del servidor este es 5060.

AUTHENTICATION TYPE: Siempre será DIGEST.

TRANSPORT TYPE: Se refiere al protocolo a utilizar UDP.

DEFAUL PROFILE: Debe indicar si este será la extensión por omisión, es decir la primera que aparecerá al momento de activar el programa de llamada.

AUTO LOGON: Auto conexión con el servidor.

KEEP PASSWORD: Guarda la clave encriptada en la máquina.

ADD: sirve para adicionar una nueva extensión utilizando el mismo programa. Hasta 5 extensiones.

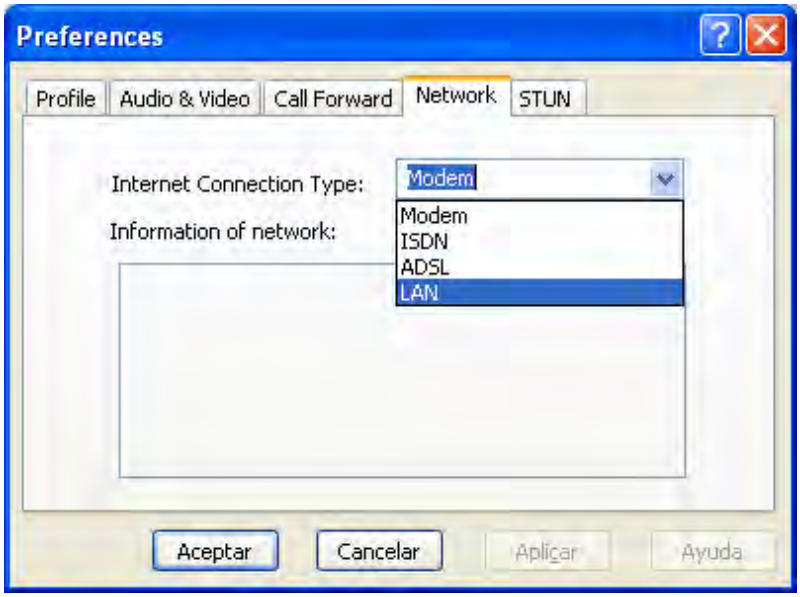
UPDATE: Permite guardar los cambios hechos en el profile.

REMOVE: Permite remover una extensión determinada.

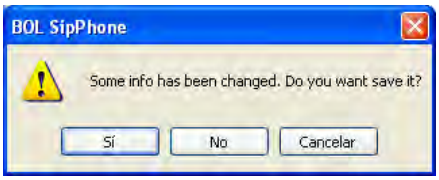
Pestaña Audio&Video

Por ser intuitivo, se utiliza el TUNING WIZARD, para efectuar dicha configuración, luego se activan los check Auto Send Video, Auto Receive Video, los cuales sirven para enviar y recibir una imagen con cámaras digitales conectadas a la PC, de no activar esta función no será posible utilizar.

Pestaña Network



Esta pestaña permite indicarle al programa cual será la vía de comunicación a utilizar, para nuestro caso, se selecciona LAN y se presiona la tecla ACEPTAR, el cual activara un box, para confirmar los cambios, presione el botón Si.



Ahora ya tiene configurada el software para la transmisión de voz por medio de la IP, para una prueba haga una llamada interna desde su teléfono, por ejemplo *98 llama al sistema de correo de voz para probar que este funciona. (Se requiere por supuesto que cuente con el softphone configurado correctamente para conectarse a su sistemaTrixbox).

Con estos pasos usted debe tener ahora una extensión SIP funcional en su sistema TrixBox.

2.- Enlace entre servidor TrixBox y Central Telefónica.

En este apartado se explicará la forma de conexión desde el servidor Trixbox hacia una central telefónica análoga. Para nuestro caso se ha empleado un equipo Gateway de VoIP, el cual cuenta con los siguientes puertos:

1 puerto RJ-45 para WAN.

4 puertos RJ-45 para LAN.

2 puertos FXS.

Este equipo a través de los puertos FXS, entrega un tono, el cual puede ser recibido por un teléfono normal o entregárselo como tono de entrada a una troncal de una central telefónica, para este caso solo podrá entregarse tono a dos (2) troncales, es decir solo podrán haber dos (2) llamadas concurrentes.

De igual forma para las pruebas realizadas en el presente trabajo, se empleará una central telefónica análoga marca SIEMENS, la cual posee troncales análogas.

Nota: Si se hubiera utilizado una tarjeta E1 en el servidor Trixbox, en este caso se hubiera configurado una Troncal, para que ésta se conectara hacia un puerto E1 de la Central Telefónica (si ésta tuviera esa característica), y de esa forma tener hasta un máximo de 30 llamadas concurrentes.

Su forma de funcionamiento se explica a continuación:

Para conectar una central analógica convencional a VoIP, la solución más sencilla es conectar un ATA o Gateway FXS a Ethernet como línea entrante. La configuración es la siguiente: Ver figura No. 66.

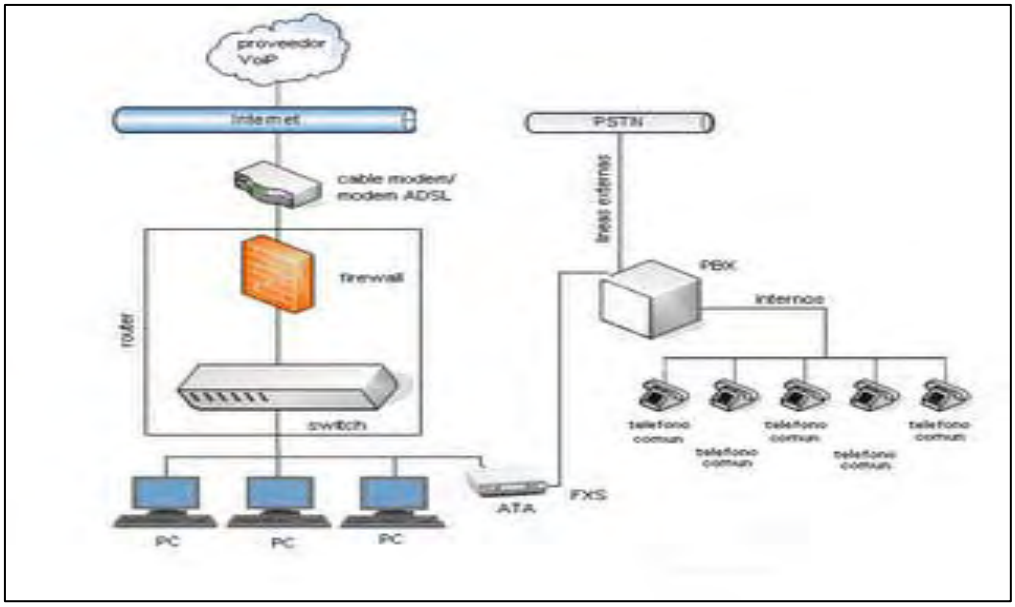


Figura No. 66 Configuración Básica de la Infraestructura.

Esta configuración solo es posible si su central telefónica cuenta con entradas para líneas externas que no están siendo usadas. Se conecta el cable desde el puerto FXS a una entrada de línea externa libre.

Para obtener tono VoIP los internos (abonados de la central telefónica), deben marcar la línea externa donde esta conectado el Gateway. Las llamadas VoIP entrantes serán respondidas con el atendedor de la central telefónica.

La configuración realizada para que el Gateway realice un enrutamiento desde la re LAN hacia la troncal de la central telefónica, es la siguiente:

Configuración Inicial:

El Gateway por defecto trae asignada la dirección 192.168.15.1, a través de la cual permite el acceso al equipo por medio Web y poder administrarlo y configurar los servicios necesarios:

Al accesar a la dirección 192.168.15.1, nos presenta la siguiente pagina, ver figura No. 67 Pantalla Home Wizard.

http://192.168.15.1

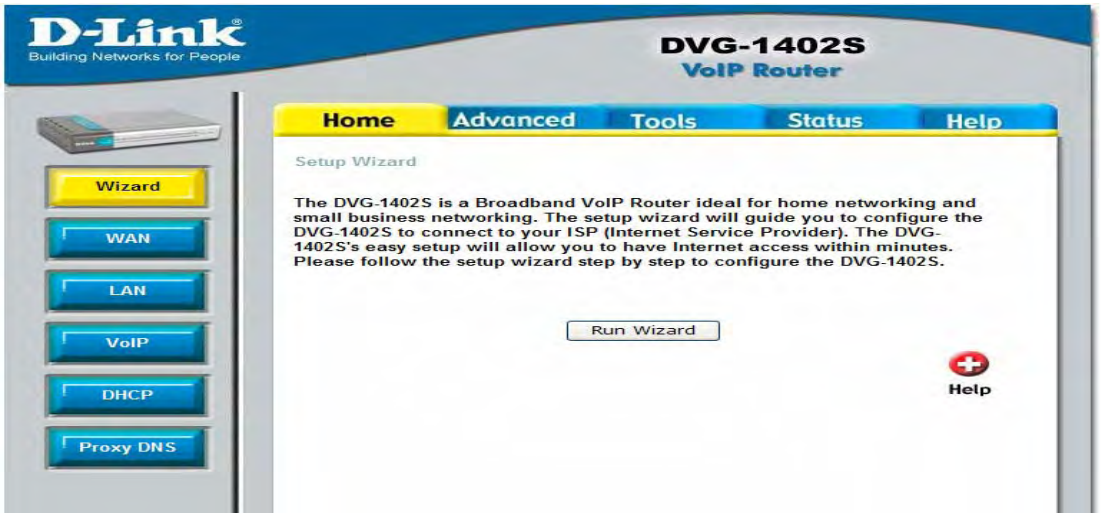


Figura No. 67 Home Wizard.

Generalmente estos equipos utilizan el puerto No. 80 para su administración, en la siguiente opción, seleccionamos TOOLS, el cual nos permite actualizar la clave de acceso: Ver figura No. 68 Tools (cambio de password).

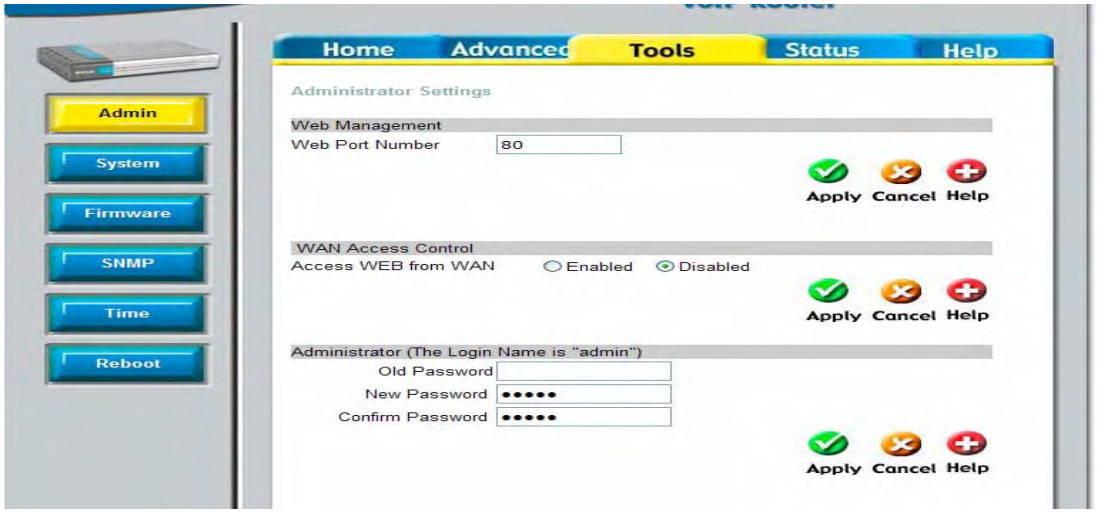


Figura No. 68 Tools.

Para nuestro caso se utilizan los siguientes valores:

User: admin.

Password: admin.

(Son los valores por defecto que trae el Gateway VoIP).

CONFIGURACIÓN WAN:

En este apartado seleccionamos WAN, para configurar la conexión a la red pública o en su defecto este puerto se utiliza para conexión a la red Local, la cual puede ser: Dinámica o Estática. Para efectos prácticos, seleccionamos de tipo Estática y asignamos con dirección IP 10.1.0.63, mascara 255.255.0.0. Tal como se muestra en la figura No. 69 Pantalla de configuración WAN.

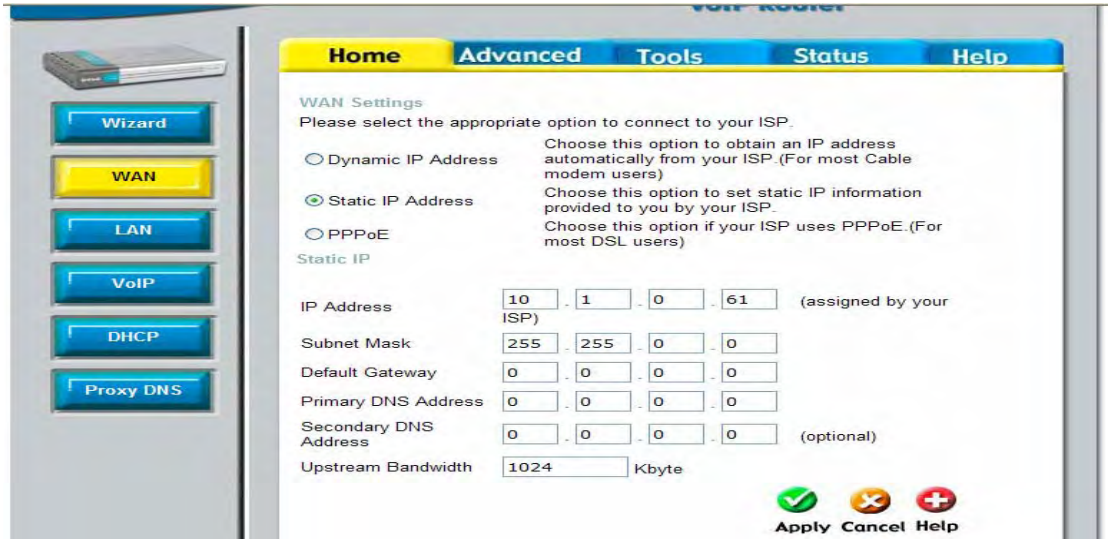
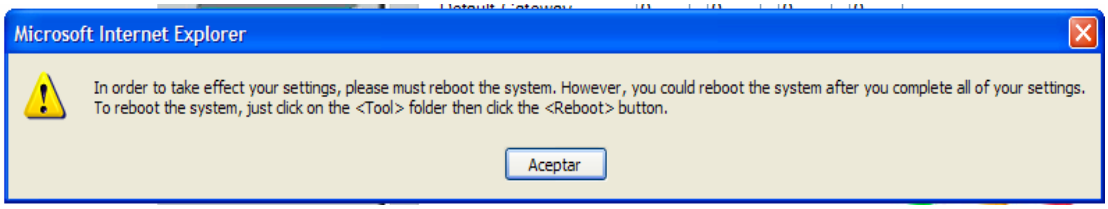


Figura No. 69 Configuración WAN.

Posteriormente se aplican los cambios. Después de cada cambio, envía un mensaje para que se seleccione el menú TOOLS y luego REBOOT para aceptar las modificaciones.



CONFIGURACION LAN:

Una vez seleccionada la opción LAN, aparece la siguiente pantalla, ver figura No. 70 Configuración LAN. Para nuestro caso se mantiene la IP por defecto 192.168.15.1, mascara 255.255.255.0.

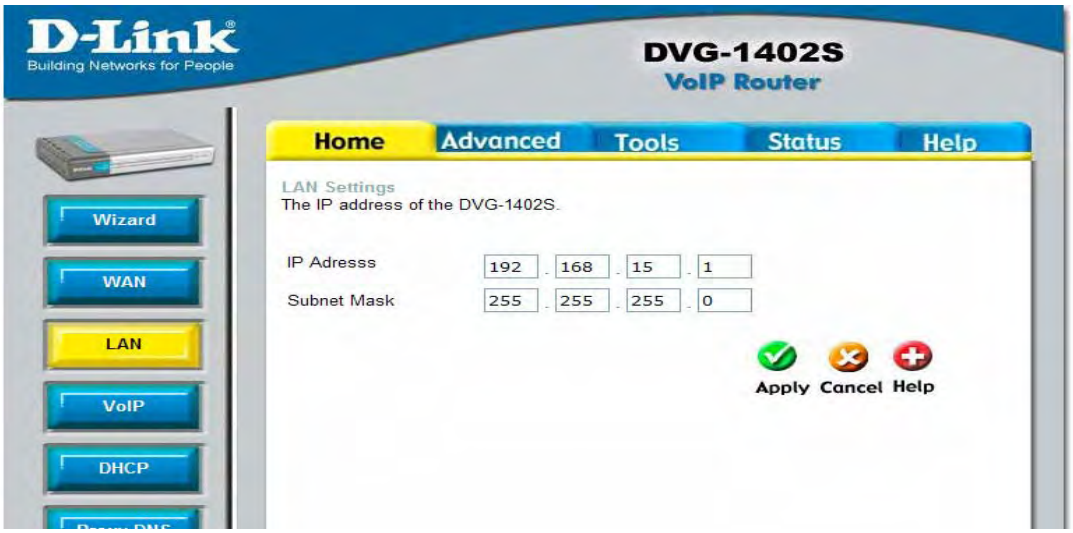


Figura No. 70 Configuración LAN.

La siguiente opción, seleccionada es Status del GW, la cual nos proporciona información general sobre el dispositivo, ver figura No. 71 Status Gateway.

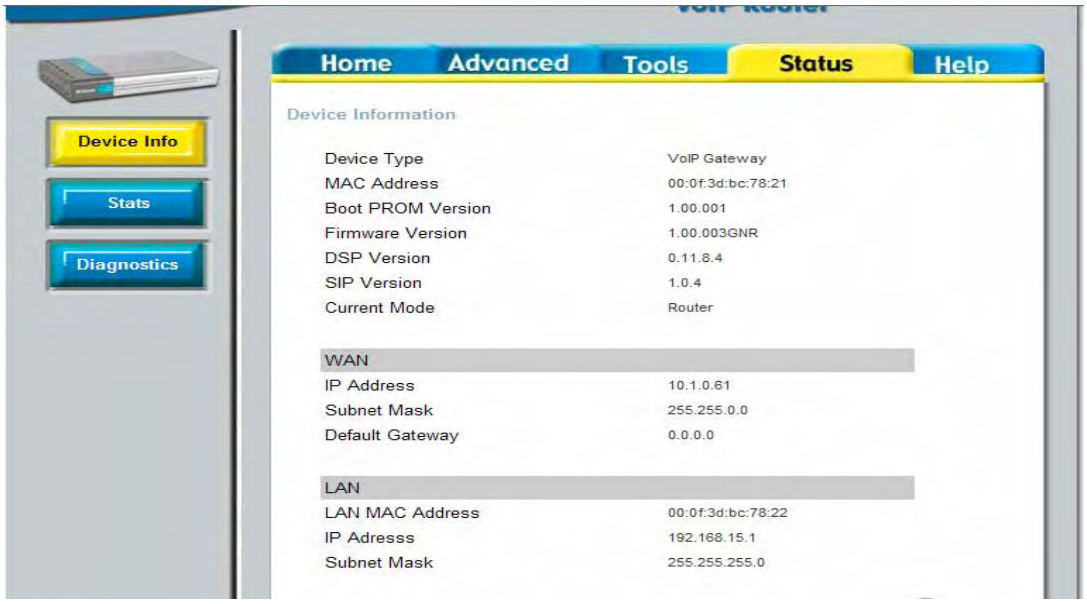


Figura No. 71 Status del Gateway.

Una vez configurados los valores anteriores, volvemos a la opción HOME y del menú de la izquierda, seleccionamos VoIP, como se muestra en la Figura No. 72.

CONFIGURACION DE VoIP

Figura No. 72 Configuración de VoIP.

Esta pantalla nos muestra ciertas opciones, de las cuales para nuestro caso práctico, solo configuraremos: Server Configuration y User Agent, ya que solamente utilizaremos el Gateway, para enrutar las llamadas desde la red LAN y/o de la red pública de Internet hacia la Central Telefónica análoga.

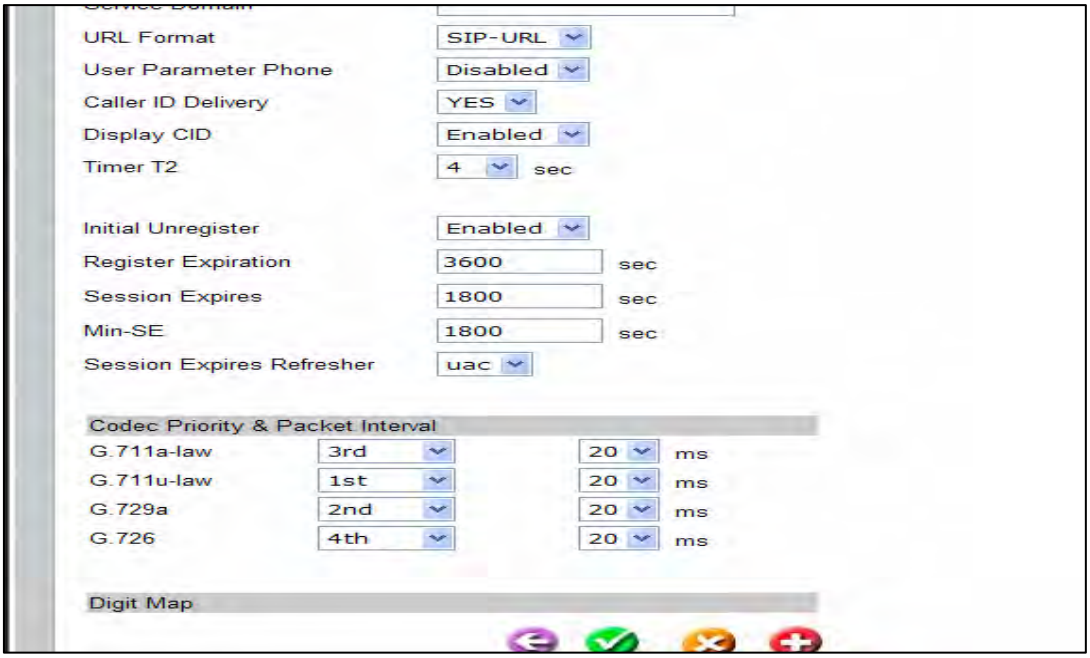
Server Configuration.

Figura No. 73 Configuración de Server Voip.

Los valores introducidos serán los siguientes:

- Server FQDN = Disable.
- IP Addresss = 10.1.0.60 (que es la IP de Trixbox).
- Port = 5060.
- Secundary FQDN = Disable.
- Secundary IP Address = sin llenar.
- Secundary port = sin llenar.
- Outbound Proxy State = Enable.
- Outbound Proxy FQDN = Disable.
- Outbound Proxy IP Address = 10.1.0.60
- Outbound Proxy Domain Name = sin llenar.
- Outbound Proxy Port = 5060.

Los siguientes valores, se dejan los que están por defecto.



Posteriormente, aplicamos los cambios y seguimos las instrucciones del mensaje que brinde el Gateway.

User Agent.

En este apartado se configurará, las números de extensiones, que le serán asignados a cada uno de los puertos FXS, estos números de extensión tiene que ser creados previamente en el servidor Trixbox como una Extensión SIP, con el propósito que una vez se conecte un teléfono normal o troncal, puedan ser reconocidos y serán vistos como extensiones de Trixbox. Ver figura No. 74 Configuración de extensiones.

Figura No. 74 Configuración de Extensiones o Agentes.

En este caso como el GW posee dos (2) puertos FXS, el Index posee capacidad para dos conexiones a teléfonos análogos. De esa forma se han configurado las dos extensiones para Trixbox 8303 y 8304, los valores configurados son los siguientes:

- Same phone number = disable.
- Index = 1
- Phone number = 8303.
- Display name = pbx análoga.
- User Agent Port = 5060.
- Autenticación Name = 8303 (el mismo numero de extensión).

- Password = 12345.
- Repyte Password = 12345.

Para la segunda extensión, el llenado es similar, solo cambia en numero de extensión, el index, el nombre y el password.

De esta manera, ya tenemos configurado nuestro Gateway de Voz IP, el cual permitirá enrrutar las llamadas, ya sea a un teléfono normal o hacia una troncal de nuestra PBX análoga.

Para efectos de funcionamiento, el ejemplo es el siguiente:

Teléfono normal:

Si el abonado desea llamar a cualquier extensión de las definidas en el servidor Trixbox, solamente tiene que levantar el auricular y marcar la extensión deseada, ya que ese puerto, el servidor Trixbox lo ve como una extensión más conectada.

Extensión de la PBX.

Si el abonado de la central PBX, desea llamar a una extensión de Trixbox, deberá hacer lo siguiente:

1.- Primero marcar Cero, para que la PBX le de tono de marcado desde la troncal.

2.- Una vez reciba el tono, deberá marcar el numero de extensión asignada a la troncal de la PBX, en nuestro caso 8303.

3.- Posteriormente el abonado recibirá un tono, el cual indicara que puede marcar la extensión requerida y poder comunicarse a un numero de extensión de Trixbox.

Si un abonado de Trixbox, desea realizar una llamada a una extensión de la PBX, deberá marcar el número de extensión asignado a la troncal y en nuestro caso el operador del panel, recibe la llamada y la transfiere a la extensión deseada.

Nota: Si la PBX contara con un sistema de IVR, no habría necesidad que un operador transfiriera la llamada, ya que el llamante, podría marcar la extensión deseada, siguiendo las instrucciones del IVR.

3.- Implementación de Canal Seguro VPN.

Para nuestro proyecto, se empleará software Open Source, como es la distribución de Linux IpCop versión 1.4.20 y Open VPN Zerina. El primero será configurado como un servidor de seguridad perimetral (Firewall) y el segundo será instalado como una herramienta de IpCop, para habilitar un canal seguro, que permita asegurar las comunicaciones entre usuarios remotos (personal de la Fuerza Armada en el extranjero), y los usuarios de nuestra red local.

a.- Instalación y configuración de IpCop.

Para la instalación de IpCop, se requerirá lo siguiente:

Hardware:

PC con procesador Pentium III o superior.

128 en RAM o superior.

Disco duro de 6 GB o superior.

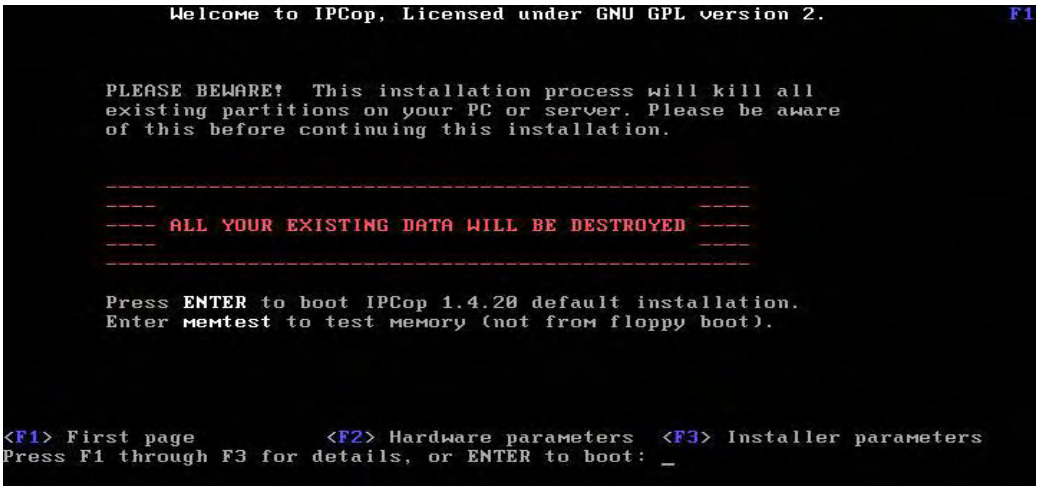
Dos Tarjetas de Red.

Unidad de CD-ROM.

Software:

La imagen ISO de la versión más reciente de IPCOP puede ser bajada (download) del sitio http://www.ipcop.org, el tamaño del archivo ISO es de aproximadamente de 40 a 60 Mbyte. Para nuestro caso usaremos la versión 1.4.20.

1) Para la instalación de IpCop, debe tenerse en cuenta las siguientes consideraciones, debe configurarse la PC para que inicie desde la Unidad de CD-ROM, asimismo es tomar en cuenta que la distribución de IpCop, al iniciar su proceso de instalación, destruye todos los datos contenidos en el disco duro, al insertar el CD, presentara la siguiente pantalla:



Solamente deberá presiona ENTER, para iniciar el proceso.

2) En la siguiente pantalla, deberá seleccionar el modo de instalación, por defecto se toma desde la Unidad de CD-ROM.

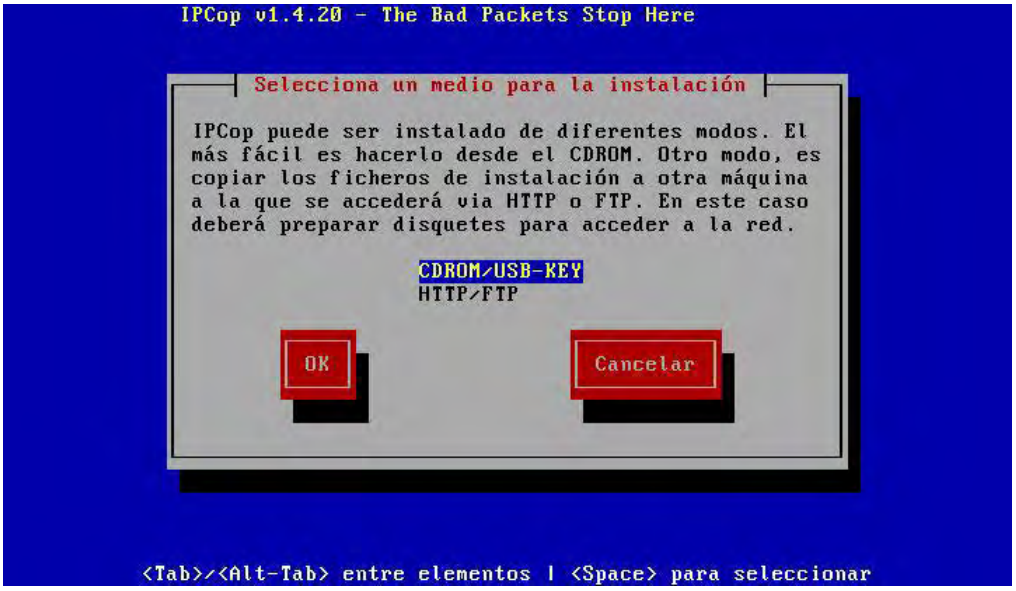


Figura No. 75 Selección de medio para instalación.

3) Seguidamente solicitara el idioma de instalación.

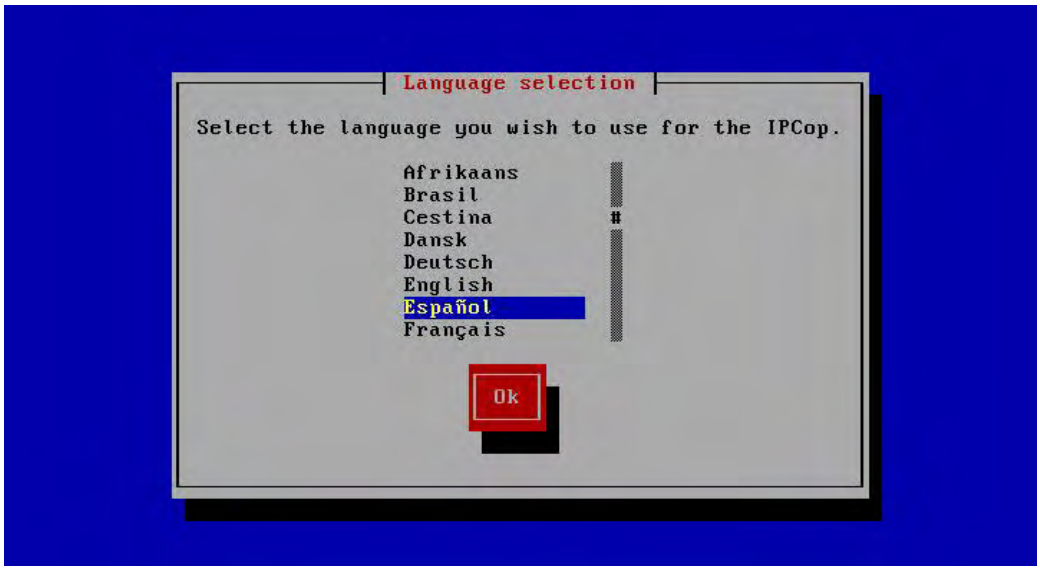


Figura No. 76 Selección de Lenguaje.

4) Posteriormente IpCop, iniciara en forma automática, un reconocimiento de tarjetas de red:

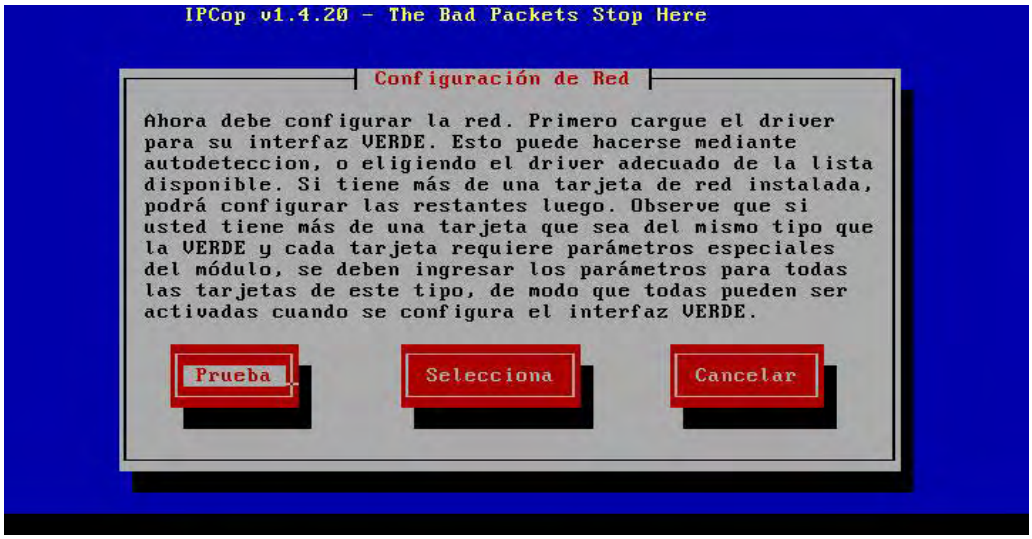


Figura No. 77 Reconocimiento de Tarjetas de red.

5) Seguidamente deberá seleccionar la configuración de tarjetas de red a utilizar:

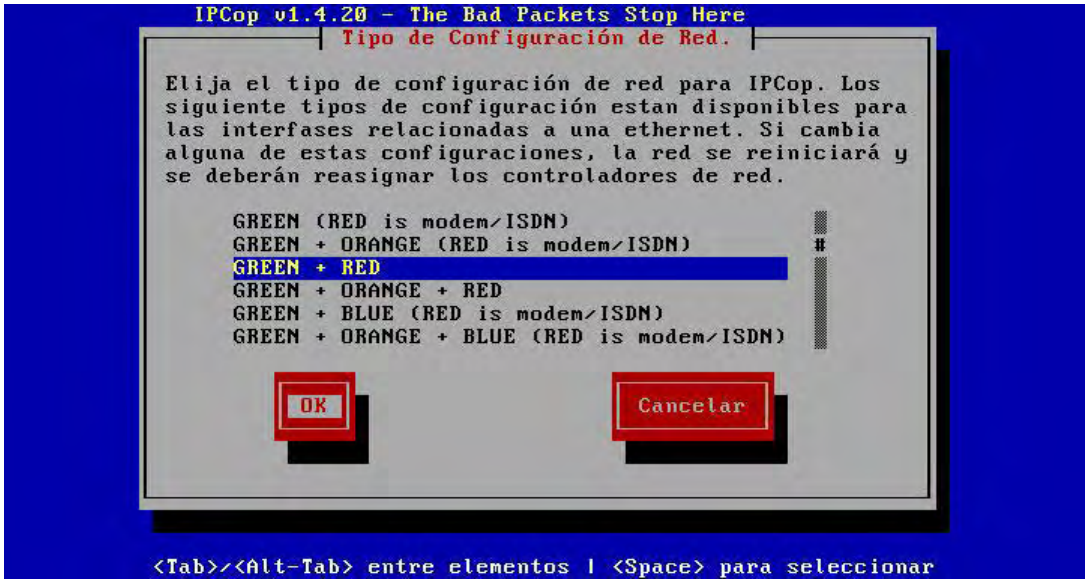


Figura No. 78 Selección de tipo de configuración de red.

Las redes implementadas por IPCOP se detallan a continuación:

GREEN: Red Lan Interna de la empresa.

ORANGE: Red de DMZ o Red de Servidores Corporativos que deben ser consultados por Internet.

RED: Red de acceso a Internet, normalmente es la Red del proveedor de servicios.

BLUE: Red de usuarios de acceso inalámbricos.

Para los aspectos prácticos del presente proyecto se definirá solo dos redes, una Red GREEN o red local y una Red RED o red de acceso a Internet.

Configuración preseleccionada para las interfases:

Nombre del Host	ipcopvoip
IP interfase Green	10.1.0.62 / 255.255.0.0
IP interfase RED	200.31.162.125/255.255.255.240
Gateway	200.31.162.113
DNS	200.31.160.210.

6) Configuración de Tarjeta GREEN.

Figura No. 79 Interfaz GREEN.

7) Configuración de Tarjeta RED.

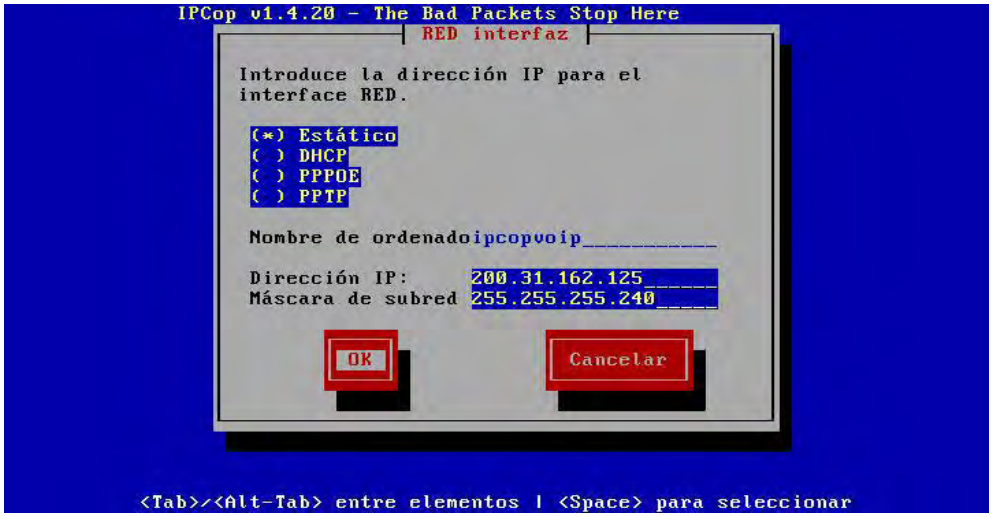


Figura No. 80 Interfaz RED.

8) Ingreso de Clave de Root.

Figura No. 81 password de root.

Ipcop, utiliza dos tipos de cuentas: root para el administrador en línea de comando y la cuenta ADMIN, para acceso Web.

Usuario : root password: copernico (Ejemplo).

Usuario : admin Password: copernico2485 (Ejemplo).

La esquematización de funcionamiento del IpCop, como parte de la solución será la siguiente:

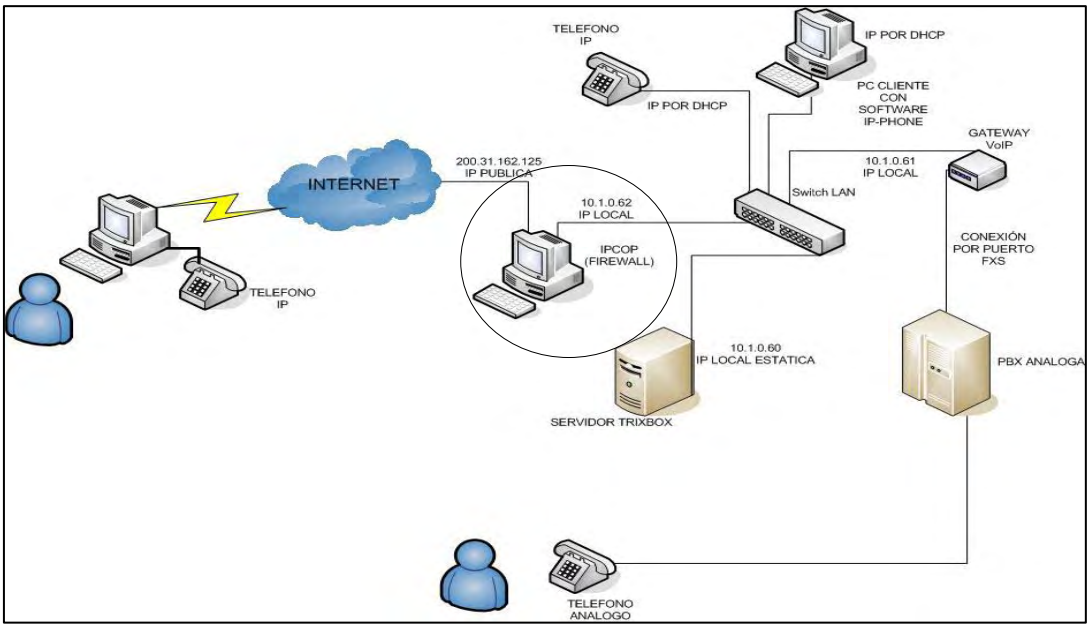


Figura No. 82 Esquema de conexión de IPCop.

b.- Configuración de Reglas de Ruteo en IpCop.

Una vez instalado y configuradas las interfaces de red, que tendrá el Firewall Ipcop (Para nuestro caso se han configurado una interfaz GREEN para la red local y una interfaz RED para la red publica). Podemos iniciar la administración del Ipcop a través de ambiente WEB, digitando https://10.1.0.62:445, el puerto 445 es el utilizado por Ipcop y https para modo seguro. Tal como se muestra en la siguiente figura:

Figura No. 83 Pantalla inicio de Ipcop (interfaz Web).

Seguidamente para configurar las reglas de ruteo en el Ipcop, se accesa al menú de Firewall y se selecciona ACCESO EXTERNO y nos mostrara la siguiente pantalla:

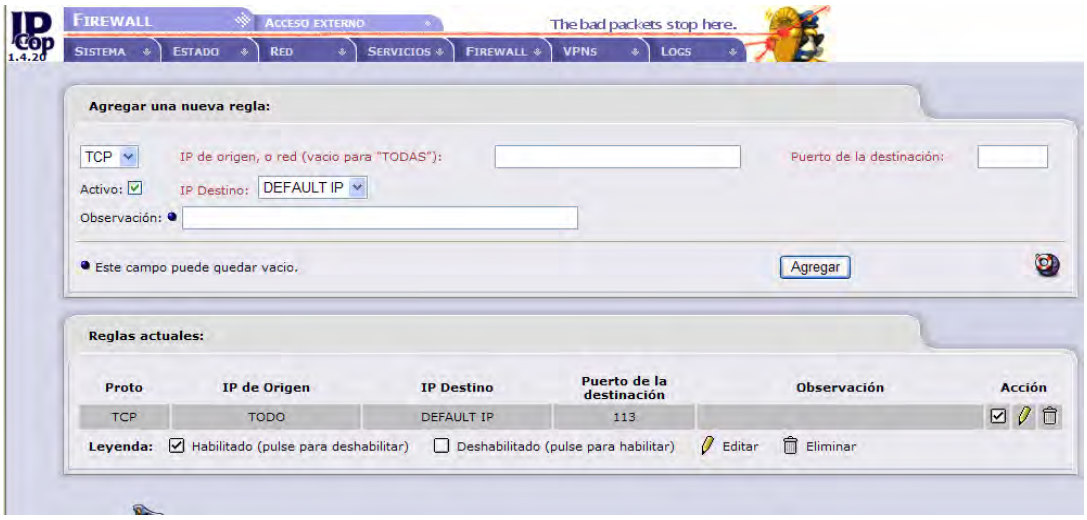


Figura No. 84 Acceso Externo

En esta parte se tiene que definir los puertos que se abrirán, para permitir el acceso de los usuarios de VoIP de la red pública, como se muestra en la siguiente tabla:

IP Origen	Puerto Destino	IP Destino (IP publica)
TODAS	2000-3000 (udp y tcp)	Defualt IP (200.31.162.125)
TODAS	4000-6000 (udp y tcp)	Defualt IP
TODAS	10000-20000 (udp y tcp)	Defualt IP

De acuerdo a la tabla anterior, permitirá el acceso a cualquier IP Publica a través de los puertos antes detallados. Estos puertos se abren para permitir la transmisión del audio de la llamada, como se muestra en la Figura No. 85.

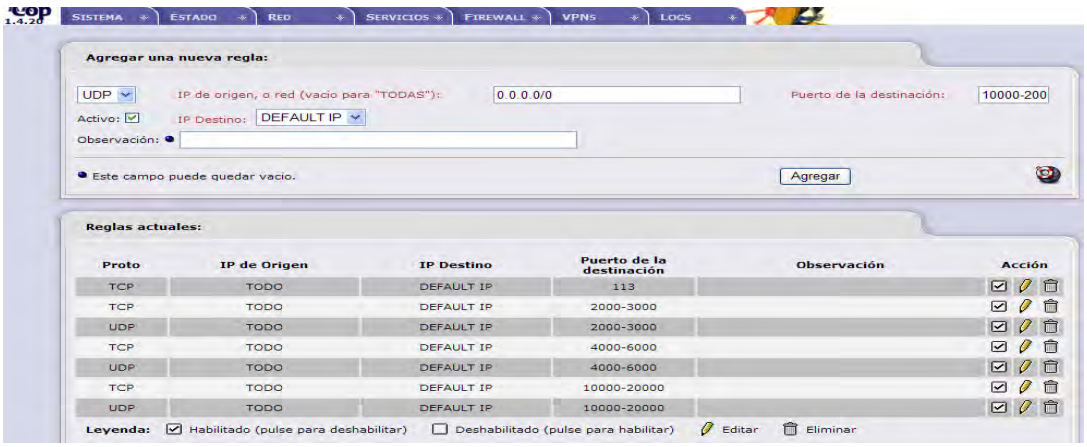


Figura No. 85 Reglas de acceso Externo.

Una vez definidas las reglas de acceso externo, se deben declarar las reglas de reenvío de puertos, según se detalla en la siguiente tabla:

IP Alias (interna Ipcop) 10.1.0.62	Puerto origen	IP destino	Puerto destino.
Defualt IP	2000-3000 (tcp – udp)	10.1.0.60 (trixbox)	2000-3000
Defualt IP	4000-6000 (tcp – udp)	10.1.0.60	4000-6000
Defualt IP	10000-20000 (tcp – udp)	10.1.0.60	10000-20000

De acuerdo a la tabla anterior, permitirá el reenvío de puertos desde la IP interna de Ipcop (10.1.0.62) hacia la IP del Servidor Trixbox (10.1.0.60), tal como se muestra en la Figura No. 86 Reglas de Reenvío de Puertos.

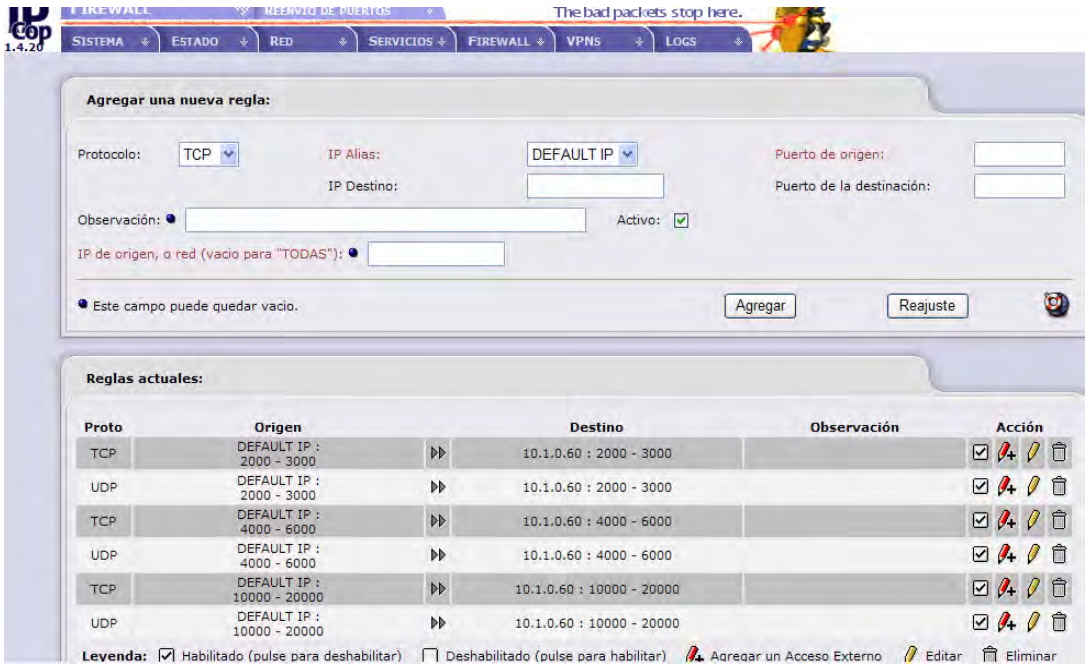


Figura No. 86 Reglas de Reenvío de Puertos.

Con la anterior configuración, se garantiza que todo paquete proveniente de un usuario remoto de VoIP, sea enrrutado por IPCop hacia nuestro servidor de VoIP TrixBox.

c.- Instalación de software Zerina en servidor IpCop.

Una vez nuestro IpCop, se encuentra instalado, configurado y con sus respectivas reglas de ruteo, el siguiente paso es instalar el software ZERINA, el cual nos permitirá habilitar una VPN. Para este procedimiento puede realizarlo accesando al servidor IpCop, con el software WinSCP, el cual permite establecer un ambiente para intercambiar datos entre un equipo Windows e IpCop.

El archivo a copiar en le raíz de IpCop, es ZERINA-0.9.5b-Installer.tar.tar. Este archivo puede ser copiado dentro de un directorio del mismo nombre, en donde se deberá descomprimir el archivo:

1) tar -xzvf ZERINA-0.9.5b-Installer.tar.tar
2) Seguidamente se debe modificar la versión de Ipcop, que evalúa Zerina antes de instalar el paquete (esto se realiza debido a que el archivo install, verifica contra la versión 1.4.18 y para nuestro caso tenemos la versión 1.4.20 de ipcop).
3) Ejecutar el comando ./install
4) Si todo se instaló sin problemas, se puede accesar el ipcop desde ambiente Web.
5) Si seleccionamos VPNs, ya aparecerá la opción OpenVPN.
6) Una vez seleccionada mostrara la siguiente pantalla:

Figura No. 87 Pantalla Inicial de OpenVPN.

d.- Configuración de OpenVPN en IpCop.

Una vez se ha ingresado a la opción OpenVPN y visualizada la pantalla anterior, la cual muestra la configuración general, se procede a colocar los valores respectivos y finalmente guardar.

En nuestro caso casi todo los valores aparecen por defecto:

- Host VPN local = 200.31.162.125 (IP publica).
- Subred VPN = 10.218.50.0/255.255.255.0 (valor por defecto).
- Dispositivo VPN = TUN
- Procolo = UDP
- Puerto destino = 1194
- MTU = 1400
- Encriptación= BF-CBC

Generando Certificado de Raiz/Anfitrion.

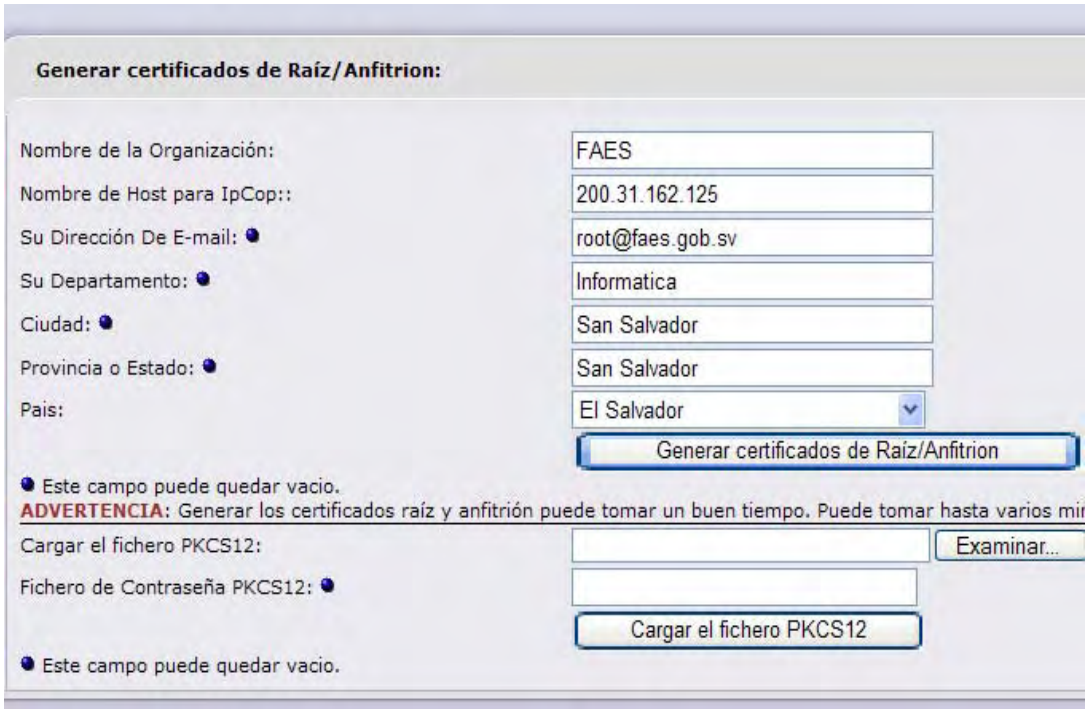


Figura No. 88 Generación de Certificado.

Una vez introducido los valores se presiona el botón, Generar certificado de Raiz/Anfitrion y posteriormente se muestra la siguiente pantalla:

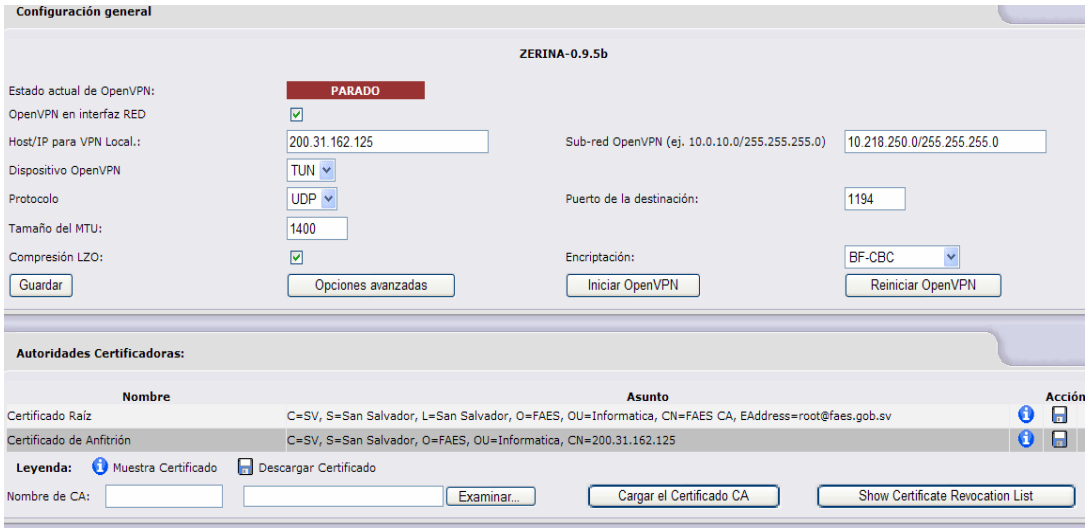


Figura No. 89 Certificado Generado.

Como puede observarse, en la parte inferior de la pantalla, aparece generado el certificado Raíz y el certificado del anfitrión.

Agregando una nueva conexión.

Seguidamente en Estado y control del cliente, se presiona el botón AGREGAR y mostrara la siguiente pantalla:

Figura No. 90 Selección de tipo de conexión.

Se seleccionara ANFITRION, ya que no es una conexión de Red a Red, sino que de cliente a un Anfitrión. Seguidamente desplegara una pantalla, en donde de

tendrá que completar los valores, que serán utilizados en nuestro caso por el cliente remoto.

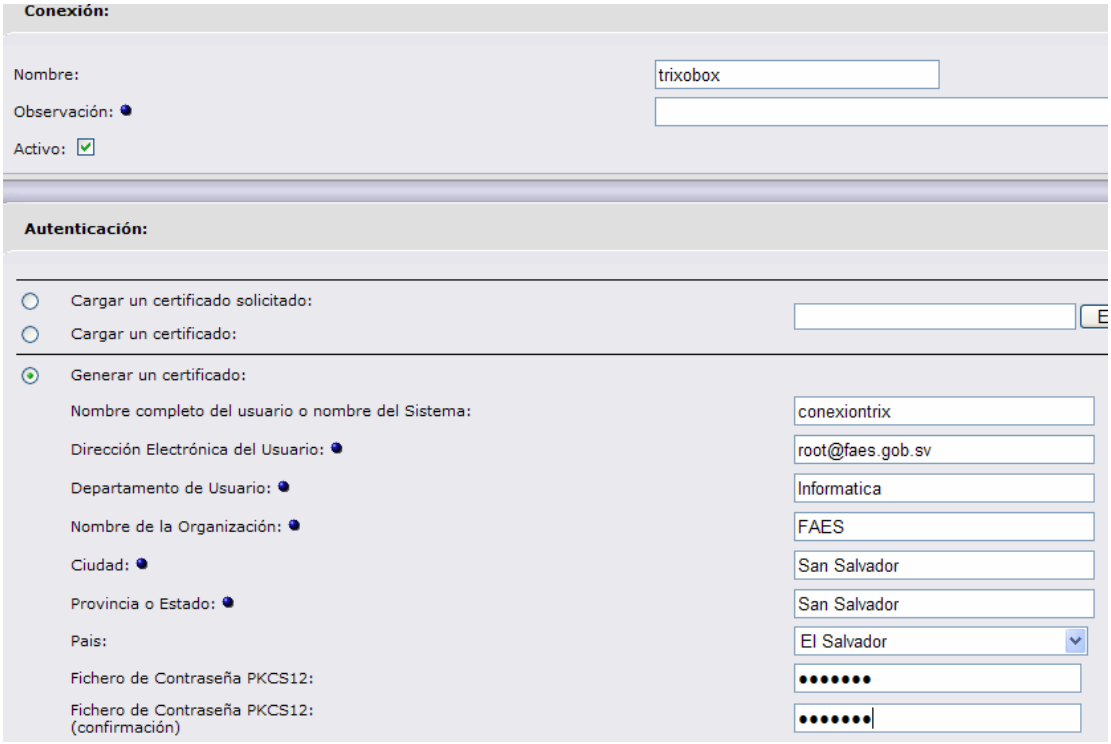


Figura No. 91 Creación de conexión para el cliente (Certificado).

Los valores acá introducidos, son los siguientes:

Nombre = trixbox.

Seleccionar el radio boton GENERAR UN CERTIFICADO.

Nombre completo del usuario = conexiontrix

Email = root@faes.gob.sv

Nombre de la organizacion = FAES

Ciudad = San Salvador.

Provincia = San Salvador.

Una vez introducidos los valores, se procede a GUARDAR.

La contraseña PKC es **trixbox.**

Posteriormente al guardar los datos, se desplegara una pantalla, la cual muestra en la parte inferior de la misma, el certificado del Cliente Remoto.

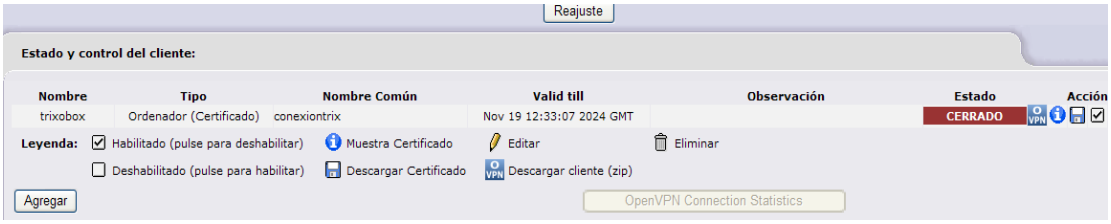


Figura No. 92 Certificado del cliente remoto.

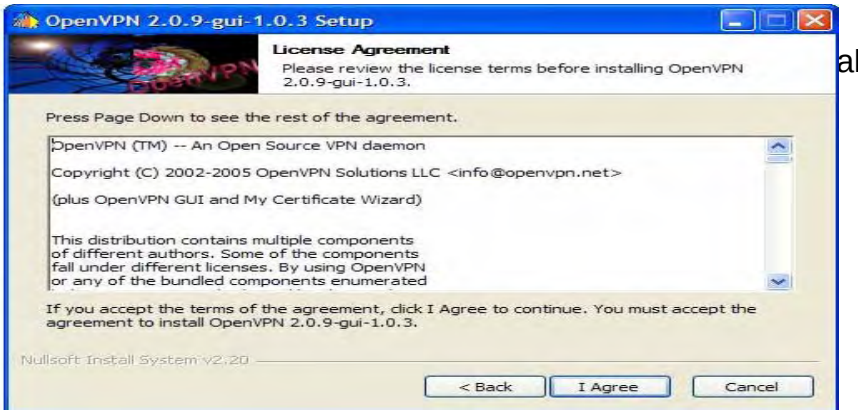
En este momento ya se puede descargar del Ipcop, el archivo .ZIP, que contiene el certificado del cliente remoto. Este archivo para nuestro caso tendrá el nombre: **trixboxToIpcop.zip**. El mismo se debe copiar en la carpeta CONFIG en donde se encuentra instalado el cliente de OpenVNP (PC de Windows), en nuestro equipo personal. El procedimiento para instalar el cliente de OpenVPN, se explicará en el siguiente literal.

e.- Instalación y Configuración VPN en Cliente Remoto.

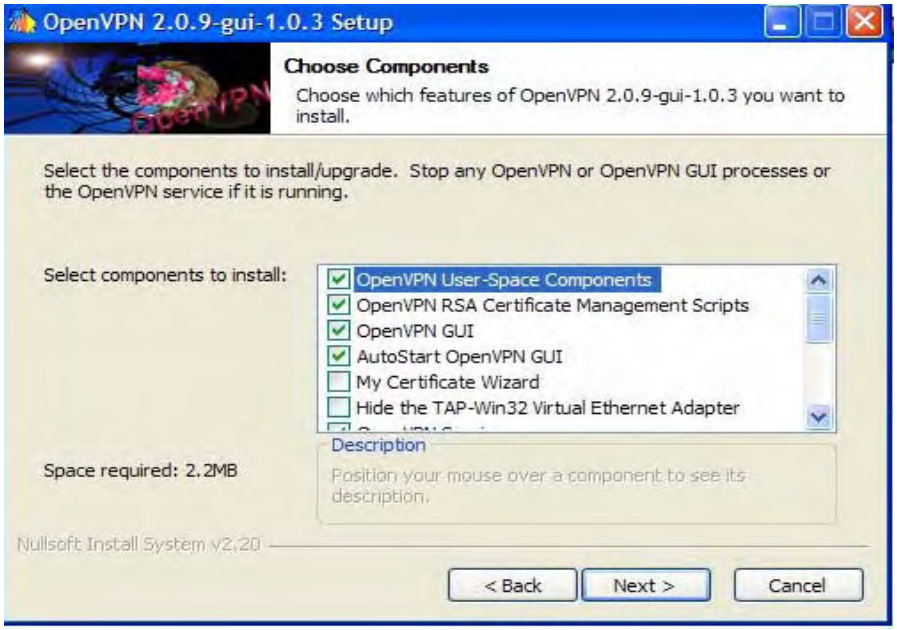
Para la configuración del cliente remoto, se utilizara el programa **openvpn-2.0.9-gui-1.0.3-install.exe,** el cual puede ser descargado del sitio http://www.openvpn.net/. (Es gratuito).

Cuando se ejecuta la aplicación presenta la pantalla de bienvenida a la instalación, ver la siguiente figura:

S alla:

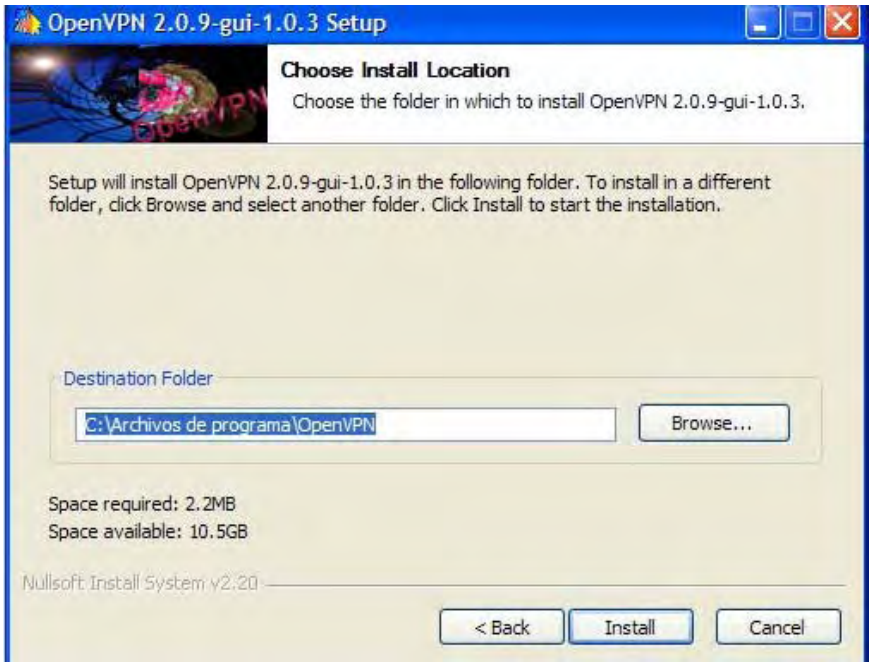


Seleccionamos I Agree para aceptar el licenciamiento y continuara con el proceso de instalación:

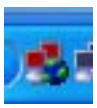


En este punto seleccionamos los componentes que se desean instalar o si solamente se desean los valores por defecto, se presionara Next.

Seguidamente nos mostrará la ubicación, donde será instalado el programa, por defecto se instala en c:\Archivos de programa\openVPN, sin embargo puede ubicarse en otro directorio.

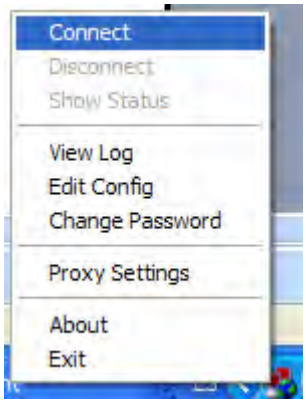


Posteriormente nos mostrara la pantalla de finalización de la instalación:

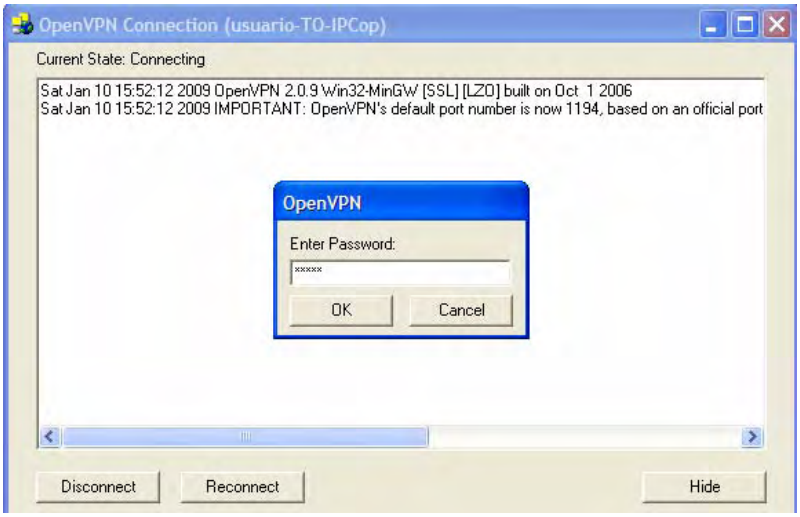
Una vez finalizada la instalación, en nuestro en la parte inferior de nuestro escritorio aparecerá el siguiente  icono: Lo anterior indica que el programa esta listo, para activar la conexión a nuestra red VPN,

que se creado anteriormente.

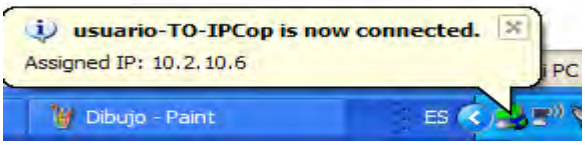
Posteriormente le damos clic derecho al icono, y nos mostrara las siguientes opciones:



De lo anterior seleccionaremos conectar, y nos pedirá una clave, sin embargo, antes de realizar la conexión, debemos copiar en el directorio **\openVPN\config** de nuestro disco C:, el certificado comprimido que descargamos del IpCop, el cual es **trixboxToIpcop.zip.** Este archivo se descomprime en esa ubicación y con son eso se esta listo para iniciar la conexión a través de nuestro canal seguro.



Una vez conectado, mostrara la IP asignada para el túnel VPN.



CAPITULO V
RESULTADOS ALCANZADOS.

Para la implementación de la propuesta, es necesario realizar la evaluación del funcionamiento del servicio de voz sobre IP para Interconectar a un usuario remoto a través de Internet hacia un servidor con TrixBox, que estará ubicado en las Oficinas del Ministerio de la Defensa Nacional, con una dirección IP publica y éste a su vez se enlazará a una central telefónica que enrutará las llamadas a los usuarios locales (abonados con teléfono). En este sentido en este capitulo se explicará los resultados alcanzados, basándonos en los siguientes procedimientos:

1.- Funcionamiento del servidor TrixBox (Asterisk).

El servidor Trixbox, instalado en el Ministerio de la Defensa Nacional y/o prototipo móvil, ha sido instalado en una PC, con las características siguientes:

Procesador Pentium IV 1.8 Ghz.
RAM 512 MB.
Disco duro de 40 GB.
Tarjeta de red 10/100 Mbps.
Unidad de CD-ROM.
Teclado y Mouse tipo USB.
Monitor LCD 15".

Su configuración es la siguiente:

Nombre del host	:	emcfaip
Versión de software IP	:	Trixbox CE 2.6 (basado en Centos).
Lenguaje de operadora	:	español.
Dirección interfaz red	:	10.1.0.60/255.255.0.0
Puerta de enlace	:	10.1.0.62 (dirección de servidor IpCop).

Dentro de la configuración básica realizada a Trxibox, se han configurado los siguientes servicios:

Configuraciones Generales.

Parámetros definidos:

15 segundos para el tono de llamada, luego automáticamente pasa a correo de voz.

El numero 9, se ha definido como prefijo de extensión, para enviar o dejar un mensaje de voz.

Módulos de administración.

Se actualizaron y se descargaron de Internet, módulos para mejorar la administración de Trixbox, siendo los siguientes:

- Modulo para llevar los log`s.
- Modulo asterisk info.
- Modulo para Backup y Restore.
- Modulo para imprimir directorio telefónico.

Extensiones creadas.

Para la realización de las pruebas, se han creado los siguientes números de extensiones:

No. extensión	Descripción
8000	Operadora
8301	Jefe de Informática.
8302	Teléfono IP
8303	PBX análoga.
8304	Teléfono análogo
8305	Casa
8306	Empresa
8307	Líbano

Cada una con su clave de acceso numérica para autenticarse en el servidor Trixbox y para acceder a su correo de voz.

Grupos de llamada.

Nombre : Grupo Informática.
Numero extensión : 600
Extensiones agrupadas : 8302, 8303, 8304
Destino si nadie contesta: 8301

Conferencias.

Se ha creado una sala de conferencia con los valores siguientes:

Nombre : Informática.
Extensión : 1122
Clave admin. : 12345
Clave usuario : sin clave (se digita #).
Música de espera: Frank Sinatra.

IVR.

Nombre : Bienvenida.
Archivo mensaje : BienvenidaIP.
Opciones : 1 = jefe de informática.
2 = teléfono IP.
3 =operador PBX análoga.

Follow me.

Debido a que no se cuenta con una troncal definida dentro de Trixbox, que permita enrrutar las llamadas a una central telefónica digital, se ha configurado una extensión como Follow me, para que una vez marcada por el usuario, lo traslade a un IVR.

No. Extensión : 8000.

Usuarios y Claves de acceso.

Acceso a trixbox : user (root) passwd (copernico).
Acceso Web : user (maint) passwd (copernico2485).
Código seguridad FOP: trixbox.

2.- Enlace entre servidor TrixBox y Central PBX análoga.

Para enlazar el servidor de voz IP Trixbox hacia la central PBX análoga, se realizó a través de un equipo de ruteo de Voz IP (Gateway).

Consideraciones:

a.- Servidor Trixbox conectado a red LAN.

b.- Gateway conectado a red LAN a través de puerto WAN.

c.- Puerto FXS No. 1 conectado a troncal de PBX análoga.

d.- Puerto FXS No. 2 conectado a teléfono análogo.

El esquema de conexión es el siguiente:

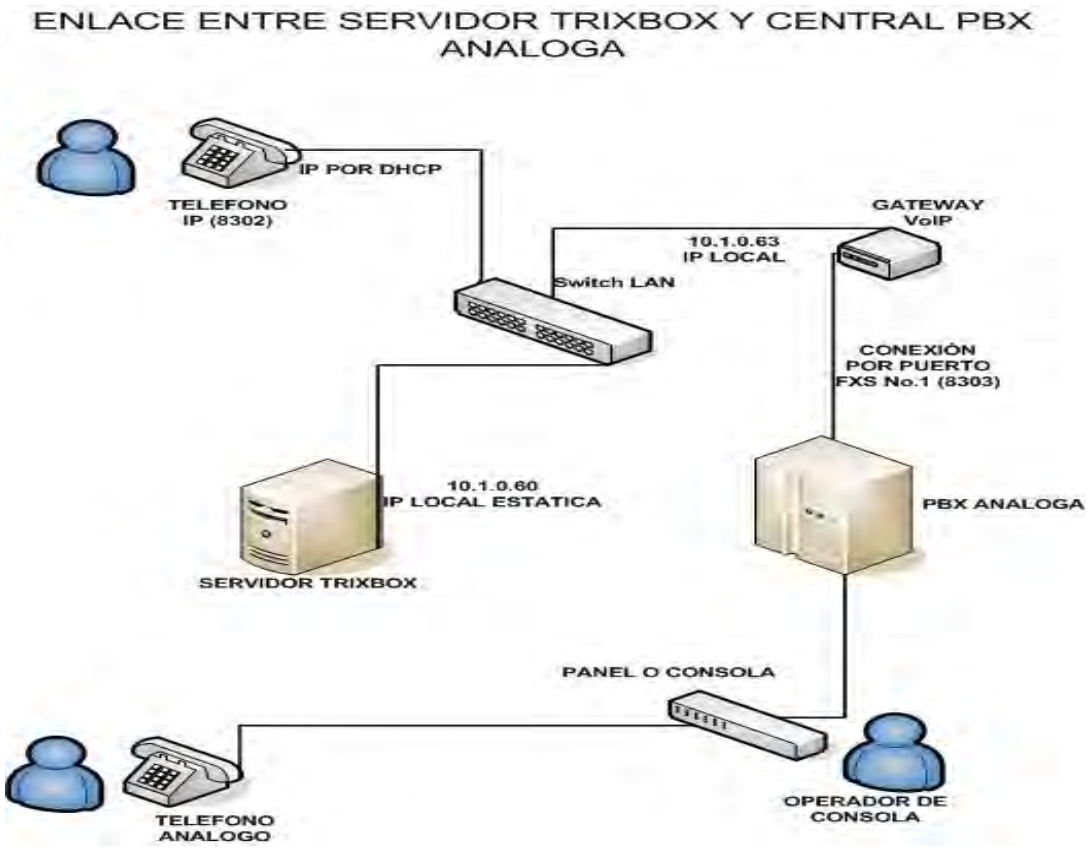


Figura No. 93 Enlace entre Trixbox y PBX Analógica.

Pruebas realizadas:

Caso No.1 “Llamada desde la red LAN a Teléfono de PBX”.

a.- Usuario de extensión 8203 (teléfono IP) conectado a la LAN, realiza llamada a la central PBX que tiene asignada la extensión 8303, la misma que esta asignada al puerto FXS No.1 del Gateway.

b.- Servidor VoIP traslada llamada al Gateway al puerto FXS No.1 (8303).

c.- El Gateway recibe llamada del usuario 8302 en puerto FXS No.1 y la traslada a troncal que espera tono del GW.

d.- Troncal de PBX recibe llamada y la traslada a la consola del operador de la PBX.

e.- Operador puede recibir la llamada y contestarla o trasladarla a una extensión de sus abonados internos.

Caso No.2. "Llamada desde abonado de Central PBX hacia extensión de red LAN".

a.- Abonado de PBX desea realizar llamada a extensión de Trixbox (8302).

b.- Abonado marca Cero "0" para recibir tono de troncal.

c.- Abonado recibe tono y marca numero asignado a la troncal 8303 y recibe nuevamente tono de marcado.

d.- Abonado marca la extensión 8203 asignada a teléfono IP.

e.- Teléfono IP 8302 recibe llamada.

RESULTADO ALCANZADO:

Tanto para el Caso No. 1 y 2, las llamadas fueran hechas de forma exitosa.

3.- Funcionamiento de software para telefonía en cliente Local.

Para verificar el funcionamiento del BOL SIPPhone, se instalo dicho software como teléfono de software en una PC Laptop, cual se le asignaron los siguientes valores:

Numero de cuenta	:	8301
Password	:	12345
Proxy	:	10.1.0.60 (LAN).
Autenticación tipo	:	DIGEST.

Puerto	:	5060.
Tipo transporte	:	UDP.
Conexión network	:	LAN

El esquema de conexión es el siguiente:

Figura No. 94 Conexión Cliente Local (Red) hacia Trixbox.

Pruebas Realizadas:

Caso No.1 "Realizar llamada desde LAPTOP hacia teléfono IP de red LAN".

a.- Usuario de laptop extensión 8301 realiza llamada a extensión 8302 (teléfono IP).

b.- Llamada ingresa a teléfono IP y ésta es contestada por el usuario de la misma.

Notas:

- La llamada es registrada en la Base de Datos de Trixbox (MySQL).

- Si pasan 15 segundos y la llamada no es contestada, ésta pasa al buzón de voz de la extensión llamada.

Caso No.2 "Realizar llamada desde teléfono IP hacia LAPTOP".

a.- Usuario de teléfono IP, marca extensión 8301 asignada a SIPPhone en la Laptop.

b.- Usuario de SIPPhone en la Laptop, contesta llamada e inicia conversación.

RESULTADO ALCANZADO:

Las llamadas fueron realizadas con éxito, tanto para el Caso No. 1 y 2.

4.- Enlace a través de canal seguro (VPN) entre cliente remoto y servidor Asterisk.

Para esta prueba, se realizará una conexión desde un cliente remoto usando SIPPhone o teléfono IP, el cual se conectará desde la red pública de Internet hacia nuestro servidor Trixobox, para realizar una llamada a una extensión conectada a la red LAN del Ministerio de la Defensa Nacional.

Para esta conexión se tendrá la siguiente configuración:

Cliente remoto (puede ser Laptop o PC)

No. extensión	:	8305
Password	:	12345
Proxy	:	10.1.0.60 (IP de la red LAN).
Conexión	:	LAN.
Puerto	:	5060
Tipo transporte	:	UDP.
IP del cliente	:	Asignada por DHCP del proveedor de Internet.

Firewall (IpCop).

User	:	root
Passwor	:	copernico
Admin Web	:	admin.

Password Web : copernico2485
IP externa : 200.31.162.125/255.255.255.240 (Red)
IP interna : 10.1.0.62/255.255.0.0 (Green)
Gateway : 200.31.162.113
DNS : 200.31.160.210
Puertos acceso externo : 2000-3000 (UDP/TCP)
4000-6000 (UDP/TCP)
10000-20000 (UDP/TCP)
Reenvío de puertos : 2000-3000 (UDP/TCP)
4000-6000 (UDP/TCP)
10000-20000 (UDP/TCP).

Nota: Todos estos puertos son abiertos, ya que de lo contrario no puede escucharse el audio de la llamada.

OpenVPN (instalado en IpCop). En MARCHA.

Certificado Raíz/Anfitrión generado en IpCop.

Servidor Trixbox.

Con los parámetros definidos en consideraciones generales.

Cliente Local.

IP asignada por DHCP de la LAN.

BOL SIPPhone (instalado y configurado).

OpenVPN (software instalado).

Certificado de cliente remoto de OpenVPN (instalado).

Extensión = 8301

Password = 12345

Proxy = 10.1.0.60

El esquema de conexión es el siguiente:

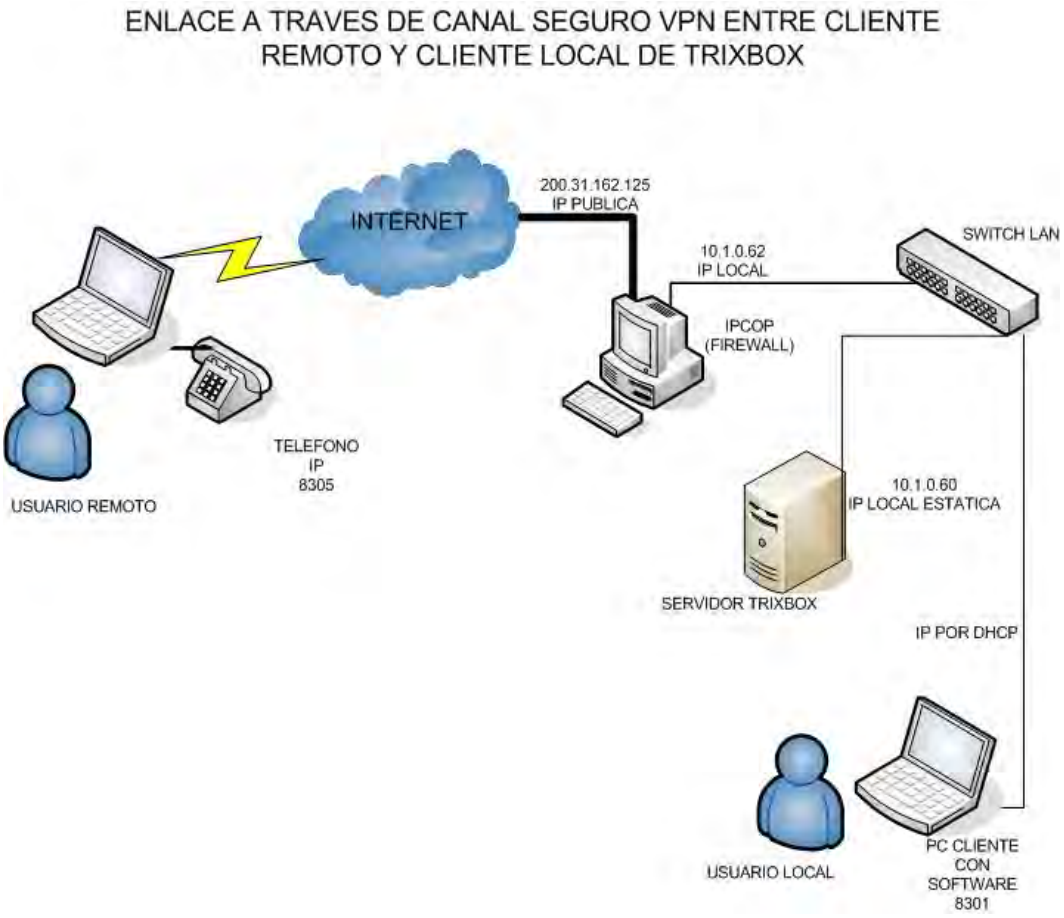


Figura No. 95 Conexión Canal Seguro hacia Trixbox (Cliente Local de LAN).

Pruebas Realizadas:

Caso No.1 "Llamada desde cliente remoto con SIPPhone hacia cliente local con SIPPhone"

a.- El cliente remoto se conecta a Internet y le es asignada una dirección IP por su proveedor.

b.- Establece la conexión a Internet.

c.- Cliente remoto abre conexión a través del software OpenVPN e introduce la clave de acceso a la VPN.

d.- Cliente remoto obtiene una dirección IP del servidor de OpenVPN y establece comunicación, a través de un canal seguro encriptado.

e..- Cliente remoto carga software SIPPhone y es validado en el servidor Trixbox a través del canal seguro, utilizando como Proxy la IP 10.1.0.60.

f.- Cliente remoto realiza llamada a la extensión 8301 de la red local del Ministerio de la Defensa Nacional.

g.- Cliente local recibe llamada y establece conversación.

Notas: Al establecer la conexión por VPN, el rendimiento de la red en el lado del cliente remoto, sufre degradación. Esto se debe a que el canal seguro por transportar paquetes encriptados, consumo más recurso de ancho de banda.

Si la conexión se establece sin usar VPN, el rendimiento de la red no se ve afectado.

RESULATADO ALCANZADO:

La conexión pudo realizarse, sin embargo el rendimiento baja notablemente.

5.- Generación de llamada desde cliente remoto (PC) hacia cliente local (abonado de Central PBX análoga).

La conexión de un cliente remoto (desde Internet), hacia un abonado de la Central PBX, se realiza de forma similar al caso anterior, la única variante es la incorporación del Router de VoIP (Gateway de voz IP) y la Central PBX analógica. La configuración adicional que se incorpora es la siguiente:

Cliente remoto.

Similar al caso anterior.

Gateway de VoIP.

Dirección IP : 10.1.0.63/255.255.0.0 (es entregada al puerto WAN del router VoIP).

Puerto FXS No.1 : 8303 (Esta misma esta definida en Trixbox).

Puerto FXS No.2 : 8304 (Esta misma esta definida en Trixbox).

Central PBX análoga.

Una troncal disponible para recibir el tono que entrega el puerto FXS (8303).

Extensiones de abonados internos de la PBX.

Servidor Trixbox.

Similar al caso anterior.

Firewall (IpCop).

Similar al caso anterior.

Cliente local.

Similar al caso anterior.

El esquema de conexión es el siguiente:

Figura No. 96 Conexión Cliente Remoto (VPN) a PBX Análoga.

Pruebas realizadas:

Caso No.1 " Cliente remoto realiza llamada por VPN a cliente local en extensión de abonado de PBX análoga).

a.- Cliente remoto se conecta a Internet y realiza conexión a OpenVPN.

b.- Enlaza PC con Red VPN, lo que permite ver los recursos de la red LAN del Ministerio de la Defensa, como si estuviera físicamente a la Red LAN del mismo.

c.- Carga software BOLSIPPhone, en su PC personal.

d.- Llamada enrutada por servidor IpCop a través de IP 10.1.0.62 hacia la 10.1.0.60 servidor Trixbox.

f.- Llamada llega a red LAN y es enrrutada hacia puerto WAN del Gateway VoIP (IP 10.1.0.63).

g.- Gateway enrruta llamada a través de puerto No. 1 FXS hacia troncal disponible en PBX análogo.

f.- Llamada llega al operador de la PBX y enruta la llamada hacia extensión de abonado de la PBX.

g.- Abonado de la PBX, recibe llamada e inicia conversación, que llega desde Internet a través de un canal seguro.

Caso No.2 "Generación de llamada desde abonado de PBX análoga hacia cliente remoto en Internet conectado a red LAN del Ministerio de la Defensa, a través de una VPN".

a.- Abonado de PBX, marca Cero para recibir tono y luego marca el número de la troncal 8303, para recibir tono por parte de Trixbox.

b.- Abonado al recibir el segundo tono, marca el número de extensión del cliente remoto 8305.

c.- Llamada llega a Gateway, la cual es enrrutada hacia el cliente remoto.

d.- Llamada es enviada a la puerta de enlace 10.1.0.62 (servidor IpCop).

e.- Servidor IpCop, re-enrruta la llamada a través de interfaz conectada a Internet (200.31.162.125).

f.- Cliente remoto conectado a Internet, recibe la llamada a través de la VPN.

g.- Cliente remoto, contesta llamada e inicia conversación.

RESULTADO ALCANZADO:

Las llamadas tanto entre cliente remoto –abonado de BPX y viceversa, fue completada de forma exitosa. Siempre se considera degradación de rendimiento de la red en la conexión.

CAPITULO VI
CONCLUSIONES.

El desarrollo del proyecto de implementación de servicio de Voz sobre IP para el personal de la Fuerza Armada que se encuentra cumpliendo misiones en el Exterior, como una herramienta alterna de comunicación para los mismos, nos ha permitido establecer las siguientes conclusiones:

1.- Es necesario implementar un servicio de voz sobre IP, para que todo el personal que se encuentra cumpliendo misiones en el Extranjero pueda contar con un medio alterno para materializar las comunicaciones en forma segura hacia el Ministerio de la Defensa Nacional.

2.- El empleo de software de código abierto para implementar una solución de comunicación de voz a través de IP, constituye una alternativa viable y económica, ya que garantiza un servicio eficiente y oportuno.

3.- La implementación de Redes Privadas Virtuales (VPN), dentro de un ambiente público, permite establecer un canal seguro de comunicación entre usuarios remotos que accedan a servicios locales de una Institución.

4.- Las soluciones de código abierto y/o propietario, para la implementación de servicios de Voz sobre IP, permiten intercomunicar usuarios o Instituciones ubicadas en cualquier sitio geográfico del mundo, ya que son factibles y garantizan una adecuada comunicación en tiempo real. Asimismo toda vez que sea empleada para uso privativo entre las diferentes dependencias de una Empresa o Institución, no se estaría afectando a las operadoras de telecomunicaciones.

5.- La implementación del servicio de voz IP, sobre infraestructura propia (red interna y servidor), garantiza la confidencialidad de los datos y diferentes registros de abonados de una Empresa, así como también permite llevar un mejor control de las comunicaciones entre los usuarios locales y/o remotos.

6.- Las soluciones de voz sobre IP, además de ofrecer el servicio de comunicaciones a los sus usuarios locales y remotos de una Empresa, también

permiten incorporar nuevos servicios como son: videoconferencias, servicios de IVR y correo de voz.

REFERENCIAS ESTUDIADAS.

REFERENCIAS BIBLIOGRAFICAS.

1. DEMPSTER, BARRIE; GARRISON, KERRY. *Trixbox made easy*. 1° ed. Birmingham, UK: Pack publishing, 2006. 166p. ISBN 1-904811-93-0.
2. GONCALVES, FLAVIO EDUARDO. *Asterisk pbx guía de configuración*. Traducido por OSCAR FUEYO ALVAREZ. 1° ed. Florianópolis, Titulo independiente, 2007. 362p. ISBN 978-85-906904-3-6.
3. GUTIERREZ GIL, ROBERTO. *Seguridad voip. Ataques, amenazas y riesgos*. [en línea]. Universidad de valencia. Disponible en: http://www.uv.es/montanan/ampliación/trabajos/seguridad%20voip.pdf. [Consulta: 14 octubre 2008].
4. IBARRACORRETGE, SAUL. *Seguridad en voip*. [en línea]. Semana ESIDE 2008. Disponible en: http://www.saghul.net/blog/documentos-cc/eside-word-08/seguridad-voip.pdf. [Consulta: 17 noviembre 2008].
5. KANELLAKIS, KELLY. *Voip security*. [en línea]. JUST-USA mayo 2003. Disponible en: http://www.just-usa-org/zipadobe/wedt1b.pdf. [Consulta: 23 noviembre 2008].
6. KELLY, TIMOTHY. *Voip for dummies*. 1° ed. Indianapolis, USA: Wiley publishing, 2005. 272p. ISBN 0-7645-8843-5.
7. MEGGELEN, JIM VAN; MADSEN, LEIF; SMITH, JARED. *Asterisk the future of telephony*. 2° ed. Sebastopol, USA: O'Reilly media, 2007. 574p. ISBN 0-596-51048-9.
8. SEIFFORT, DIRK ENRIQUE; SALINAS, EDISON J. *Asterisk telefonía voip y software libre*. [en línea]. Lintec, abril 2008. Disponible en: http://www.champetux.org/files/lintec_voip.pdf. [Consulta en: 11 enero 2009].
9. WALLACE, KEVIN. *Authorized self-study guide cisco voip over ip*. 1° ed. Indianapolis, USA: Cisco press, 2006. 504p. ISBN 1-58705-262-8.
10. YANCE, ALFREDO CERTAIN. *Trixbox al descubierto*. 1° ed. Bogota, CO: Gekco eu, 2006. 63p.

11. ZAR, JONATHAN. *Voip security and privacy threat taxonomy*. [en línea]. VOIPSA, 24 octubre 2005. Disponible en: http://www.voipsa.org/activitis/voipsa_threat_taxonomy_0.1.pdf. [Consulta en: 17 noviembre 2008].

GLOSARIO DE TERMINOS.

Access Gateway - Gateway de acceso

Un gateway (pasarela) es un elemento de la red que actúa como punto de entrada a otra red. Un access gateway es un gateway entre la red telefónica y otras redes como Internet.

Certificado Digital

Acreditación emitida por una entidad o un particular debidamente autorizada garantizando que un determinado dato (una firma electrónica o una clave pública) pertenece realmente a quien se supone. Por ejemplo, Verisign y Thawte

CGI

Common Gateway Interface. Una interfaz escrita en un lenguaje de programación (perl, c, c++,visual basic, etc) y posteriormente ejecutada o interpretada por una computadora servidor para contestar a pedidos del usuario desde una computadora con una aplicación cliente; casi siempre desde el World Wide Web. Esta interfaz permite obtener los resultados pedidos, como los que resultan al consultar una base de datos. Entre los programas más habituales encontrará gestores de formularios y de email, libros de visitas, foros de discusión, etc.

Conmutación de Paquetes

Un portador separa los datos en paquetes. Cada paquete contiene la dirección de origen, la dirección de su destino, e información acerca de cómo volver a unirse con otros paquetes emparentados. Es un "paradigma de las comunicaciones" ya que cada paquete de un mensaje recorre una ruta entre sistemas anfitriones (hosts), sin que esa ruta (path) esté previamente definida. Este proceso permite que paquetes de

distintas localizaciones se entremezclen en las mismas líneas y que sean clasificados y dirigidos a distintas rutas.

Contraseña

Password. Código utilizado para acceder un sistema restringido. Pueden contener caracteres alfanuméricos e incluso algunos otros símbolos. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario.

Criptografía

Se dice que cualquier procedimiento es criptográfico si permite a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo, luego de haberlo descifrado.

Denegación de Servicio

Incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar. Habitualmente, la pérdida del servicio supone la indisponibilidad de un determinado servicio de red, como el correo electrónico, o la pérdida temporal de toda la conectividad y todos los servicios de red. En los peores casos, por ejemplo, un sitio web accedido por millones de personas puede verse forzado temporalmente a cesar de operar. Un ataque de denegación de servicio puede también destruir programas y archivos de un sistema informático. Aunque normalmente es realizado de forma intencionada y maliciosa, este tipo de ataques puede también ocurrir de forma accidental algunas veces. Si bien no suele producirse robo de información estos ataques pueden costar mucho tiempo y dinero a la persona u organización afectada.

DNS

Servidor de Nombres de Dominio. Servidor automatizado utilizado en el Internet cuya tares es convertir nombres fáciles de entender (como www.panamacom.com) a direcciones numéricas de IP.

E1

Conexión por medio de la línea telefónica que puede transportar datos con una velocidad de hasta 1,920 Mbps. Según el estándar europeo (ITU), un E1 está formado por 30 canales de datos de 64 kbps más 2 canales de señalización. E1 es la versión europea de T1 (DS-1). Velocidades disponibles:

E1: 30 canales, 2,048 Mbps

E2: 120 canales, 8,448 Mbps

E3: 480 canales, 34,368 Mbps

E4: 1920 canales, 139,264 Mbps

E5: 7680 canales, 565,148 Mbps

Embedded System

Conjunto software y hardware que forma parte de algún sistema mayor y que se funciona sin intervención humana. Un sistema embebido típico sería una tarjeta microcomputadora con software en ROM, que realiza cierta tarea de forma ininterrumpida. Puede incluir algún tipo de sistema operativo (muy sencillo normalmente), no suele contar con periféricos (teclado, monitor o discos) y raramente tienen interfaz con el usuario. En muchos casos debe proporcionar respuesta en tiempo real.

Encriptación

Cifrado. Tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

Firewall

Combinación de hardware y software la cual separa una red de área local (LAN) en dos o más partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

Firewall, Cortafuegos

Un sistema diseñado para prevenir accesos desautorizados hacia o desde una red privada. Los cortafuegos pueden ser implementados como hardware, software o una combinación de ambos. Todos los mensajes entrantes o salientes hacia Internet deben pasar primero por el firewall, que examinara cada mensaje y bloqueara los que no alcancen el criterio de seguridad especificado en su configuración. Algunos cortafuegos deben ser especialmente configurados para que estos permitan circular el trafico VoIP.

FXO, Foreign Exchange Office

Es una interfaz en un dispositivo VoIP para conectarlo a una central telefónica PBX.

FXS, Foreign Exchange Station

Es la interfaz en un dispositivo VoIP que permite conectarlo directamente a teléfonos, faxes y puertos CO en centrales PBXs.

Firma Digital

Información cifrada que identifica al autor de un documento electrónico y autentifica su identidad.

Gatekeeper

Un componente del estándar ITU H.323. Es la unidad central de control que gestiona las prestaciones en una red de Voz o Fax sobre IP, o de aplicaciones multimedia y de videoconferencia. Los Gatekeepers proporcionan la inteligencia de red, incluyendo servicios de resolución de direcciones, autorización, autenticación, registro de los detalles de las llamadas para tarificar y comunicación con el sistema de gestión de la red. También monitorizan la red para permitir su gestión en tiempo real, el balanceo de carga y el control del ancho de banda utilizado. Elemento básico a considerar a la hora de introducir servicios suplementarios.

Gateway

En general se trata de una pasarela entre dos redes. Técnicamente se trata de un dispositivo repetidor electrónico que intercepta y adecua señales eléctricas de una red a otra. En Telefonía IP se entiende que estamos hablando de un dispositivo que actúa de pasarela entre la red telefónica y una red IP. Es capaz de convertir las llamadas de voz y fax, en tiempo real, en paquetes IP con destino a una red IP, por ejemplo Internet.

Originalmente sólo trataban llamadas de voz, realizando la compresión/descompresión, paquetización, enrutado de la llamada y el control de la señalización. Hoy en día muchos son capaces de manejar fax e incluir interfaces con controladores externos, como gatekeepers, soft-switches o sistemas de facturación.

H.323

H.323 es la recomendación global (incluye referencias a otros estándares, como H.225 y H.245) de la Unión Internacional de Telecomunicaciones (ITU) que fija los estándares para las comunicaciones multimedia sobre redes basadas en paquetes que no proporcionan una Calidad de Servicio (QoS, Quality of Service) garantizada.

Define las diferentes entidades que hacen posible estas comunicaciones multimedia: endpoints, gateways, unidades de conferencia multipunto (MCU) y gatekeepers, así como sus interacciones.

IP - Internet Protocol

La parte IP del protocolo de comunicaciones TCP/IP. Implementa el nivel de red (capa 3 de la pila de protocolos OSI), que contiene una dirección de red y se utiliza para enrutar un paquete hacia otra red o subred. IP acepta paquetes de la capa 4 de transporte (TCP o UDP), añade su propia cabecera y envía un datagrama a la capa 2 (enlace). Puede fragmentar el paquete para acomodarse a la máxima unidad de transmisión (MTU, Maximum Transmission Unit) de la red.

Dirección IP: un número único de 32 bits para una máquina TCP/IP concreta en

Internet, escrita normalmente en decimal (por ejemplo, 128.122.40.227).

IP PBX - IP Private Branch Exchange

Centralita IP. Dispositivo de red IP que se encarga de conmutar tráfico telefónico de VoIP.

IP Telephony - Telefonía IP

Tecnología para la transmisión de llamadas telefónicas ordinarias sobre Internet u otras redes de paquetes utilizando un PC, gateways y teléfonos estándar.

En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportada vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional. Los pasos básicos que tienen lugar en una llamada a través de Internet son: conversión de la señal de voz analógica a formato digital y compresión de la señal a protocolo de Internet (IP) para su transmisión. En recepción se realiza el proceso inverso para poder recuperar de nuevo la señal de voz analógica.

ISDN - Integrated Services Digital Network (RDSI, Red Digital de Servicios Integrados).

Red telefónica pensada para mejorar los servicios de telecomunicaciones a nivel mundial. Proporciona un estándar aceptado internacionalmente para voz, datos y señalización. Todas las transmisiones son digitales extremo a extremo, utiliza señalización fuera de banda, y proporciona más ancho de banda que la red telefónica tradicional.

ITU-T International Telecommunications Union – Telecommunication

Antes conocida como CCITT (Comite Consultatif Internationale de Telegraphie et Telephonie). Agencia de la Organización de las Naciones Unidas que trata lo referente a telecomunicaciones: crea estándares, reparte frecuencias para varios servicios, etc.

El grupo ITU-T recomienda estándares para telecomunicaciones y está en Génova (Suiza). También se encarga de elaborar recomendaciones sobre codecs (compresión/descompresión de audio) y modems.

Línea Conmutada.

Dial Up. Conexión de red la cual se puede crear y desechar según se requiera que se establece usando un emulador de terminal y un módem y realiza una conexión de datos a través de una línea telefónica. Los enlaces de marcado por línea telefónica son la forma más sencilla de conexiones con acceso conmutado. Los protocolos utilizados generalmente en este tipo de conexiones son SLIP y PPP.

Línea Dedicada

Línea privada que se utiliza para conectar redes de área local de tamaño moderado a un proveedor de servicios de Internet y se caracteriza por ser una conexión permanente.

Proxy

Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red. Al mismo tiempo contiene mecanismos de seguridad (firewall o cortafuegos) los cuales impiden accesos no autorizados desde el exterior hacia la red privada. También se le conoce como servidor cache.

Puente

Dispositivos que tienen usos definidos como interconectar segmentos de red a través de medios físicos diferentes (es usual ver puentes entre un cable coaxial y otro de fibra óptica). Además, pueden adaptar diferentes protocolos de bajo nivel (capa de enlace de datos y física de modelo OSI).

Red Privada Virtual.

Red en la que al menos alguno de sus componentes utiliza la red Internet pero que funciona como una red privada, empleando para ello técnicas de cifrado.

RFC

En inglés es Requests for Comments. Serie de documentos iniciada en 1967 la cual describe el conjunto de protocolos de Internet y experimentos similares. No todos los RFC (en realidad muy pocos de ellos) describen estándares de Internet pero todos los estándares Internet están escritos en formato RFC. La serie de documentos RFC es inusual en cuanto los protocolos que describen son elaborados por la comunidad Internet que desarrolla e investiga, en contraste con los protocolos revisados y estandarizados formalmente que son promovidos por organizaciones como CCITT y ANSI. El RFC 822 es el formato estándar Internet para cabeceras de mensajes de correo electrónico. El nombre viene del "RFC 822", que contiene esa especificación (STD 11, RFC 822). El formato 822 era conocido antes como formato 733.

T-1

Una línea dedicada capaz de transferir datos a 1,544,000 bits – por-segundo. Teóricamente una T-1 a su máxima capacidad de transmisión transporta un megabyte en menos de 10 segundos. Sin embargo, esto no es lo suficiente rápido para pantallas completas con movimiento general, para las cuales se requiere al menos 10,00,000 bits- por-segundo. Una T-1 es el medio más rápido comúnmente usado para realizar conexiones a Internet.

VoIP

La Voz sobre IP (VoIP, Voice over IP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways, teléfonos IP y teléfonos estándares. En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportadas

vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

ANEXOS.

ANEXO "A" REQUERIMIENTO DE EQUIPO INFORMATICO PARA PROTOTIPO.

ITEM	DESCRIPCION	CANT.	COSTO UNITARIO	TOTAL
1	PC`S	2	$ 900.00	$ 1,800.00
2	Software VoIP (Trixbox)	1	$ 0.00	$ 0.00
3	Teléfonos IP	2	$ 70.00	$ 140.00
4	Gateway VoIP	1	$ 120.00	$ 120.00
5	IP publica	1	$ 250.00	$ 250.00
6	Software para VPN	1	$ 0.00	$ 0.00
7	Software teléfono PC	1	$ 0.00	$ 0.00
8	Central PBX	1	$1,500.00	$ 1,500.00
9	Teléfonos análogos	2	$ 30.00	$ 60.00
	Total			**$ 3,870.00**

Nota: Se consideran la mayor parte de costos, ya que si bien es cierto no se cancelo por la IP Publica, pero en todo caso de no tenerla hubiera existido la necesidad de obtenerla. Así mismo con el costo de la PBX, se considera ya que era necesario adquirirla sino se hubiera tenido a disposición. De igual forma para los teléfonos, por ser costos que deben tomarse en cuenta si se monta un prototipo partiendo del supuesto que no se tiene ningún recurso.

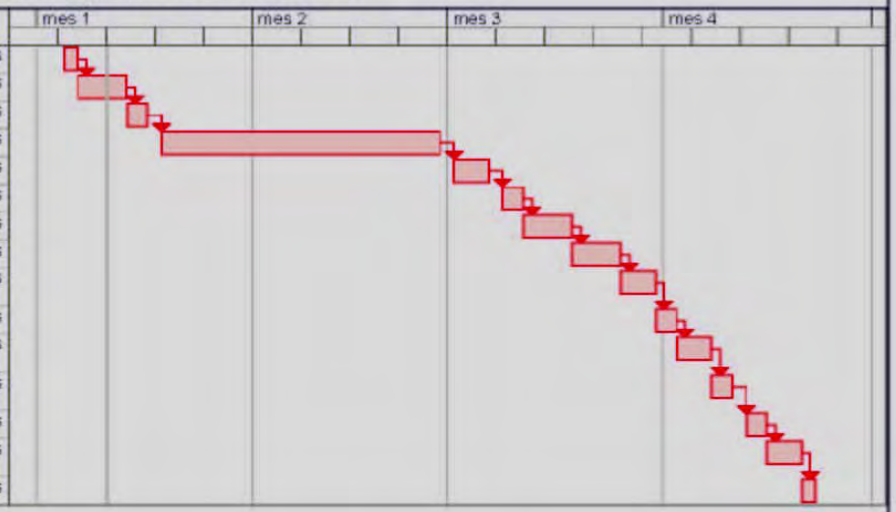
ANEXO "B" REQUERIMIENTO DE EQUIPO INFORMATICO PARA PRODUCCION.

ITEM	DESCRIPCION	CANT.	COSTO UNITARIO	TOTAL
1	Servidor	1	$4,000.00	$ 4,000.00
2	Firewall	1	$2,000.00	$ 2,000.00
3	Software VoIP (Trixbox)	1	$ 0.00	$ 0.00
4	Teléfonos IP	35	$ 70.00	$ 2,450.00
5	Tarjeta E1	1	$1,250.00	$ 1,250.00
6	IP publica	1	$ 250.00	$ 250.00
7	Software para VPN	1	$ 0.00	$ 0.00
8	Software teléfono PC	1	$ 0.00	$ 0.00
9	Central PBX	1	$ 0.00	$ 0.00
	Total			**$ 9,950.00**

Nota: A la Central PBX no se le asigna costo, considerando que se utilizara la central matriz de la Institución, así como también no existiría costo por los teléfonos análogos, ya que re-utilizarían los asignados a las dependencias.

ANEXO "C" CRONOGRAMA DE IMPLEMENTACION PARA PRODUCCION.

Id	Nombre de tarea	Duración
1	PRESENTACION DE PROPUESTA	2 días
2	ACTUALIZACION DE COTIZACIONES	5 días
3	SOLICITUD PARA AQUIRIR EQUIPO	3 días
4	PROCESO DE COMPRA	30 días
5	ELABORACION DE DIRECTIVA DE USO DE SERVICIO	5 días
6	DISEÑO DE CONFIGURACION Y CONEXIÓN DE EQUIPO	3 días
7	INSTALACIÓN Y CONFIGURACIÓN DE SERVIDOR DE VoIP	5 días
8	CONFIGURACION Y CONEXIÓN DE ENLACE E1	5 días
9	PRUEBAS DE CONEXION ENTRE TELEFONOS DE LA RED LAN HACIA CENTRAL MATRIZ	3 días
10	CONFIGURACION DE FIREWALL	3 días
11	PRUEBAS DE CONEXIÓN ENTRE FIREWALL Y SERVIDOR VoIP	3 días
12	PRUEBAS CON CLIENTES REMOTOS HACIA CENTRAL MATRIZ	3 días
13	CONFIGURACION DE VPN EN FIREWALL	3 días
14	PRUEBAS CON CLIENTES REMOTOS HACIA CENTRAL MATRIZ POR VPN	3 días
15	CREAR DIRECTORIO TELEFONICO	2 días



Proyecto: ANEXO-C
Fecha: dom 11/01/09

Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Fecha límite

Página 1