

**ESCUELA POLITECNICA DEL EJÉRCITO**

**FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA**

**“ANÁLISIS Y DISEÑO DE UN SISTEMA INTEGRADO DE  
VOIP PARA LA ESPE”**

**Previa a la obtención del Título de:**

**INGENIERO EN SISTEMAS E INFORMÁTICA**

**POR: JESSICA CHIRIBOGA ALMEIDA  
ALEXANDRA GUEVARA CORONEL**

**SANGOLQUI, 26 de Junio del 2006**

## **RESUMEN**

Originalmente la voz y los datos se han transmitido a través de sistemas completamente separados. Sin embargo, hoy en día es posible realizar la transmisión de voz en las redes internas y externas de datos, integrándolas de una forma más eficiente y económica, a través del protocolo IP de Internet (Voz sobre IP), por lo que la ESPE y sus sedes deben aprovechar y utilizar sus recursos para usar esta tecnología, de tal forma, que se pueda ampliar y mejorar la comunicación conjuntamente con la red telefónica; ya que existen diferentes arquitecturas que están siendo propuestas para soportar la señalización de los sistemas de voz sobre IP, basadas en los estándares H.323, SIP, MGCP, entre otros.

SIP considerado como el futuro protocolo estándar para VoIP y clave en las comunicaciones convergentes de próxima generación, permite: crear, modificar o finalizar sesiones, donde se puede ubicar a una o más personas a través de medios combinados como: llamadas telefónicas, sistemas de mensajería y voz, etc.

Debido a que, con la central IP H.323 de la ESPE sólo se abastece a un 40% de los usuarios que cuentan con telefonía; para lo cual, se podría ofrecer una aplicación paralela mediante una implementación de voz sobre IP con SIP, a través de un servidor SIP (PBX software), con la finalidad de que exista un mayor número de beneficiarios.

## Capítulo I: Introducción

La Voz sobre IP (VoIP, Voz sobre 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 y teléfonos estándares. En general, servicios de comunicación: voz, fax, aplicaciones de mensajes de voz y otros, son transportados en la actualidad vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

Cuando se hace una llamada telefónica por IP, la voz se digitaliza, se comprime y se envía en paquetes de datos IP. Estos paquetes se envían a través de Internet a la persona con la que se está hablando. Cuando alcanzan su destino, son ensamblados de nuevo, descomprimidos y convertidos en la señal de voz original.

El protocolo SIP (Session Initiation Protocol, o Protocolo de iniciación de sesión) es un protocolo estándar para iniciar una sesión interactiva de usuario que involucra elementos de multimedia como video, audio, juegos y realidad virtual.

SIP trabaja en el nivel de aplicación del modelo de interconexión abierto (OSI). Este nivel es el nivel responsable de garantizar que la comunicación se puede efectuar. SIP puede establecer sesiones multimedia, o llamadas de telefonía por Internet, y modificar o terminarlas. El protocolo también puede invitar a los participantes para sesiones únicas o de multidifusión que no necesariamente involucran a un iniciador. Dado que el SIP soporta mapeo de nombres y servicios de redirección, hace posible que los usuarios inicien y terminen comunicaciones y servicios desde cualquier ubicación.

## **1.1.- Planteamiento del problema**

La Escuela Politécnica del Ejército cuenta con un sistema de telefonía IP instalado, pero que no cumple con todos los requerimientos de los usuarios, especialmente por costos.

Hoy en día la mayoría de las empresas e instituciones utilizan VoIP con el protocolo H.323 porque proporciona una base para las comunicaciones de audio, vídeo y datos a través de una red IP como Internet. Sin embargo, en la actualidad, una de las mejores alternativas es usar el protocolo SIP porque, está contemplado dentro de la base de datos RFC siendo un protocolo libre y abierto a nuevas modificaciones y no ligado a ninguna empresa ni entidad privada; además, SIP presenta ventajas para la transmisión de tráfico multimedia.

Actualmente, para la toma de decisiones gerenciales el señor rector de la ESPE, debe convocar a reuniones presenciales a los directores de sedes y departamentales o él debe trasladarse a cada una de las sedes a solucionar problemas que se presenten, lo que conlleva a una pérdida de tiempo y de eficiencia de los directivos de la escuela.

Los resultados de los procesos administrativos que se realizan en los vicerrectorados, facultades y direcciones son enviados mediante memorandos adjuntando los informes respectivos al rectorado y a los departamentos que los hayan solicitado, lo que constituye un problema pues en la mayoría de los casos estos son entregados a destiempo y generan un retraso en la toma de decisiones.

## 1.2.- Justificación

En los últimos años la ESPE ha destinado gran cantidad de su presupuesto al mejoramiento de la infraestructura tecnológica de networking.

Algunas de las acciones más relevantes en este campo han sido:

- Disponer de un canal de banda ancha HDSL de 4 Mbps.
- Contratar una red propia de enlace para datos.
- Dividir e implementar un anillo de fibra óptica entre los edificios de la ESPE matriz.
- Instalar cableado estructurado para la red de datos de la ESPE – Sangolquí y sus sedes.
- Diseñar el portal WAP de la ESPE.

La ESPE en caso de realizar el Análisis y Diseño de VoIP con el Protocolo de Iniciación de Sesiones (SIP) para su Intranet y extranet, solucionaría sus problemas de comunicación telefónica principalmente y proporcionaría un valor agregado a la optimización de los procesos administrativos, pues SIP facilita enormemente las videoconferencias, que podrán ponerse en marcha con un simple clic de ratón, o permitirá redirigir las llamadas para que una conferencia entre Quito y Latacunga se establezca desde esta última. Además, desde el punto de vista de inversión, la ESPE ya dispone de la red de datos y la incorporación del SIP solo la optimizaría y no se haría necesario adquirir equipos e infraestructura tecnológica adicional a la existente.

La tecnología SIP permite configurar para cada usuario de la red VoIP los servicios que va a disponer y las sesiones que puede ejecutar. Esto se resume en el hecho de que gracias a SIP y a otras tecnologías complementarias, es posible transformar la información en un mensaje de voz, un correo electrónico, un mensaje traducido al inglés y un mensaje de texto para móviles.

A diferencia del protocolo H.323 que es más complicado de utilizar, puesto que es un estándar del mundo de la telefonía (la ITU), el protocolo SIP procede del entorno informático, (el IETF) que lo hace mucho más sencillo y extensible y por tanto es probable que crezca más su uso que H.323 y termine desplazándolo.

## **1.3.- Objetivos**

### **1.3.1.-Objetivo General**

- Analizar y Diseñar un Sistema Integrado de VoIP para la Escuela Politécnica del Ejército.

### **1.3.2.-Objetivos Específicos**

- Analizar la infraestructura de comunicaciones que dispone la ESPE.
- Realizar un estudio comparativo de las tecnologías que permitan proponer una solución al problema de comunicaciones de la ESPE y escoger la que técnica y económicamente sea la más apropiada.
- Analizar la calidad de servicio de las comunicaciones IP que tiene la ESPE, con el objeto de diseñar un sistema integrado que permita la transmisión de audio, video y cualquier otra información multimedia entre las sedes.
- Realizar el análisis y diseño para la implementación de VoIP en cada sede de la ESPE.
- Implementar un prototipo del Sistema diseñado en un ambiente de laboratorio para el campus Sangolquí.

## **1.4.- Alcance**

La Tesis a Desarrollar presentará un estudio de VoIP, tecnología empleada para enviar información de voz en forma digital en paquetes discretos a través de los protocolos de Internet en vez de hacerlo a través de la red de telefonía habitual. Luego se realizará un análisis del Protocolo escogido para el diseño del sistema en el que se profundizarán sus características y especificaciones. Igualmente, se analizará la infraestructura de comunicaciones del Campus Sangolquí, lo que permitirá definir los requerimientos que el sistema integrado deberá cumplir. A continuación se realizará el Diseño del Sistema Integrado de VoIP para la ESPE, tomando en cuenta el aspecto técnico y económico.

Finalmente se realizarán pruebas del Sistema diseñado en un ambiente de laboratorio, implementando solamente un prototipo, debido a que es muy difícil disponer de los equipos requeridos para que el mismo funcione en todo el campus Sangolquí y sus sedes.

## Capítulo II: Marco Teórico

### 2.1.- Voz sobre IP

#### 2.1.1.-Introducción

La voz sobre redes IP<sup>1</sup> (VoIP<sup>2</sup>), es un tema que ya tiene unos años de existencia como tecnología pero es muy actual en cuanto a su diseminación y popularización. 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<sup>3</sup> e Internet. Con posterioridad se migró de la LAN (aplicaciones privadas) a la WAN<sup>4</sup> (aplicaciones públicas) con la denominada Telefonía IP.

La voz, los datos y las imágenes han dado la posibilidad técnica de hacer converger a los servicios de telecomunicaciones en una sola red multimedia capaz de dar toda una gama de servicios avanzados a los usuarios y que dominará los flujos de tráfico con un cambio de su forma de entrega que pasará de conmutación de circuitos, a paquetes.

La aparición de VoIP junto con los DSP<sup>5</sup> (Procesador Digital de Señal), los cuales son claves en la compresión y descompresión de la voz, son los elementos que han hecho posible el despegue de estas tecnologías. La voz sobre IP es básicamente una señal de audio digitalizada y paquetizada, de manera que estos paquetes pueden ser enviados, junto a otros paquetes (datos, correo, video, etc.), a través de una red de conmutación de paquetes utilizando el protocolo IP. En el extremo receptor los paquetes son ensamblados de nuevo para constituir una comunicación de voz.

---

<sup>1</sup> Véase en el glosario de términos

<sup>2</sup> Véase en el glosario de términos

<sup>3</sup> Véase en el glosario de términos

<sup>4</sup> Véase en el glosario de términos

<sup>5</sup> Véase en el glosario de términos



## **2.1.2.-Generalidades**

### **2.1.2.1.- Qué es VoIP?**

La telefonía IP conjuga: la transmisión de voz y datos. Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y desarrollar una única red convergente que se encargue de cursar todo tipo de comunicación, ya sea voz, datos, video o cualquier tipo de información.

La voz IP, es una tecnología que permite encapsular la voz en paquetes para poder ser transportados sobre redes de datos sin necesidad de disponer de los circuitos conmutados convencionales PSTN<sup>6</sup> (Red de Telefonía Pública Conmutada).

En cambio, la telefonía IP no utiliza circuitos para la conversación, sino que envía múltiples de ellas (conversaciones) a través del mismo canal codificadas en paquetes y flujos independientes. Cuando se produce un silencio en una conversación, los paquetes de datos de otras conversaciones pueden ser transmitidos por la red, lo que implica un uso más eficiente de la misma.

Las características principales que proporciona por su estructura el estándar son las siguientes:

- Permite el control del tráfico de la red, por lo que disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento de las redes de datos.
- Proporciona el enlace a la red telefónica tradicional.
- Al tratarse de una tecnología soportada en IP presenta las siguientes ventajas adicionales:
  - Es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales.
  - Es independiente del hardware utilizado.

---

<sup>6</sup> Véase en el glosario de términos

- Permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.
- Las llamadas tienen el mismo costo, por lo que el costo no se ve incrementado si se realiza una llamada de larga distancia.

### 2.1.2.2.- Funcionamiento

Las funciones básicas que debe realizar un sistema de voz sobre IP son:

1. Digitalización de la voz.
2. Paquetización de la voz.
3. Enrutamiento<sup>7</sup> de los paquetes.

VoIP funciona digitalizando la voz en paquetes de datos, enviándola a través de la red y reconvirtiéndola a voz en el destino. Básicamente el proceso comienza con la señal análoga del teléfono que es digitalizada en señales PCM<sup>8</sup> (pulse code modulation) por medio del codificador/decodificador de voz (codec<sup>9</sup>). Las muestras PCM son pasadas al algoritmo de compresión, el cual comprime la voz y la fracciona en paquetes que pueden ser transmitidos para este caso a través de una red privada WAN. En el otro extremo de la nube se realizan exactamente las mismas funciones en un orden inverso, como se puede observar en la figura 2.1.

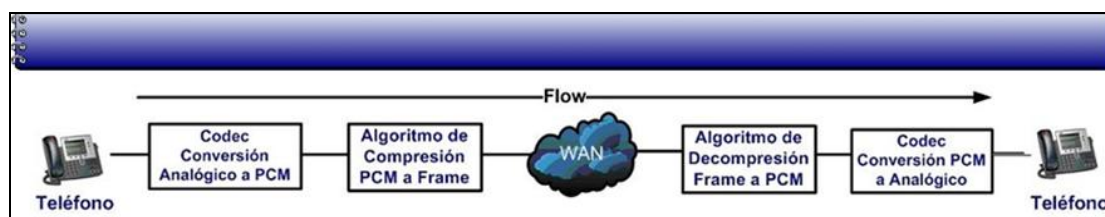


Figura 2.1: Flujo de un circuito de voz comprimido

<sup>7</sup> Véase en el glosario de términos

<sup>8</sup> Véase en el glosario de términos

<sup>9</sup> Véase en el glosario de términos

Dependiendo de la forma en la que la red este configurada, el enrutador o el gateway<sup>10</sup> puede realizar la labor de codificación, decodificación y/o compresión.

Es importante tener en cuenta también que todas las redes deben tener de alguna forma las características de direccionamiento, enrutamiento y señalización. El direccionamiento es requerido para identificar el origen y destino de las llamadas, también es usado para asociar clases de servicio a cada una de las llamadas dependiendo de la prioridad. El enrutamiento por su parte encuentra el mejor camino a seguir por el paquete desde la fuente hasta el destino y transporta la información a través de la red de la manera más eficiente, la cual ha sido determinada por el diseñador. La señalización alerta las estaciones terminales y a los elementos de la red su estado y la responsabilidad inmediata que tienen al establecer una conexión.

En la actualidad la voz sobre IP tiene tres tipos de redes IP: (Vease la figura 2.2)

- **Internet.** El estado actual de la red no permite un uso profesional para el tráfico de voz.
- **Red IP pública.** Los operadores ofrecen a las empresas la conectividad necesaria para interconectar sus redes de área local en lo que al tráfico IP se refiere. Se puede considerar como algo similar a Internet, pero con una mayor calidad de servicio y con importantes mejoras en seguridad. Hay operadores que incluso ofrecen garantías de bajo retardo y/o ancho de banda, lo que las hace muy interesante para el tráfico de voz.
- **Intranet.** La red IP implementada por la propia empresa. Suele constar de varias redes LAN (Ethernet conmutada, ATM<sup>11</sup>, etc.) que se interconectan mediante redes WAN tipo Frame Relay<sup>12</sup> / ATM, líneas punto a punto (PPP<sup>13</sup>), RDSI<sup>14</sup> (Red Digital de Servicios Integrados) para el acceso remoto, etc.

---

<sup>10</sup> Véase en el glosario de términos

<sup>11</sup> Véase en el glosario de términos

<sup>12</sup> Véase en el glosario de términos

<sup>13</sup> Véase en el glosario de términos

<sup>14</sup> Véase en el glosario de términos

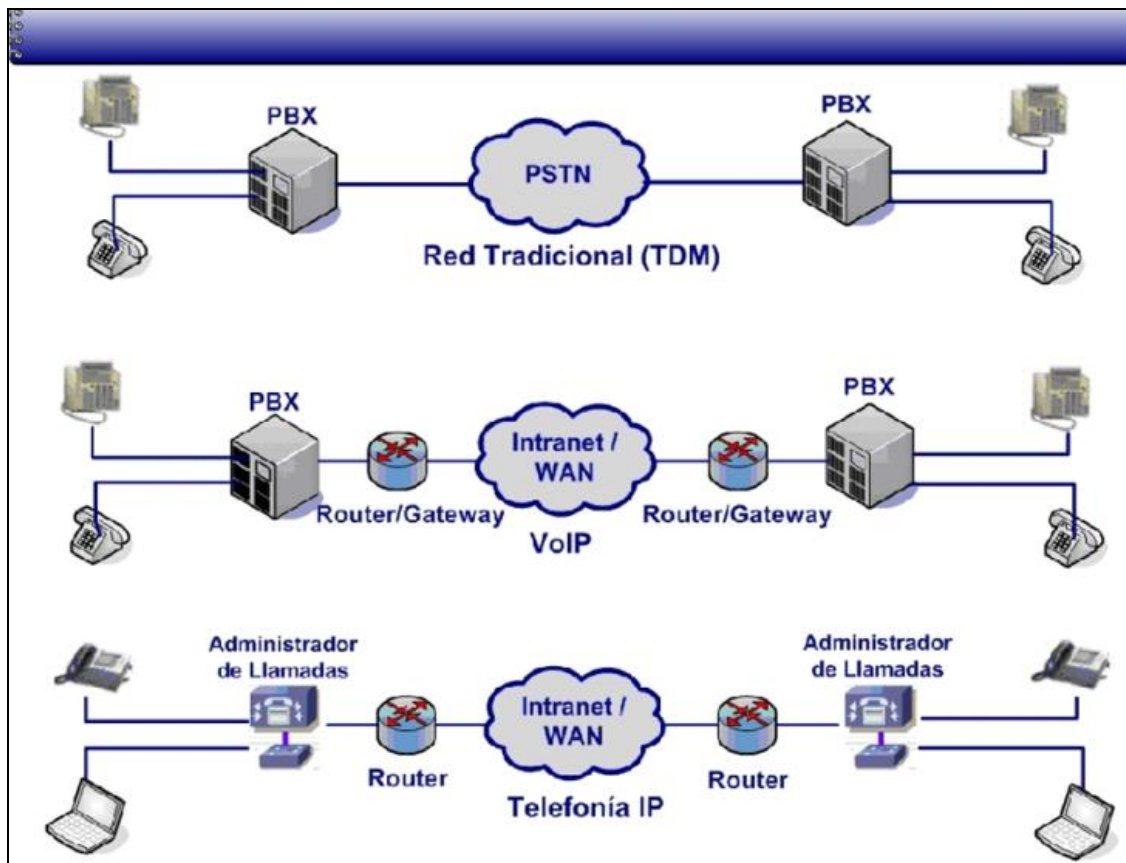


Figura 2.2: Tipos de Redes IP

Actualmente podemos partir de una serie de elementos ya disponibles en el mercado y que, según diferentes diseños, nos permitirán construir las aplicaciones VoIP. (Vease la figura 2.3) Estos elementos son:

- Teléfonos IP.
- Adaptadores IP para PC.
- Adaptadores IP telefónicos
- Hubs Telefónicos.
- Gateways IP
- Servidores de red.
- Servidores de aplicaciones.
- Unidades de audioconferencia múltiple. (MCU Voz).
- Servicios de Directorio.

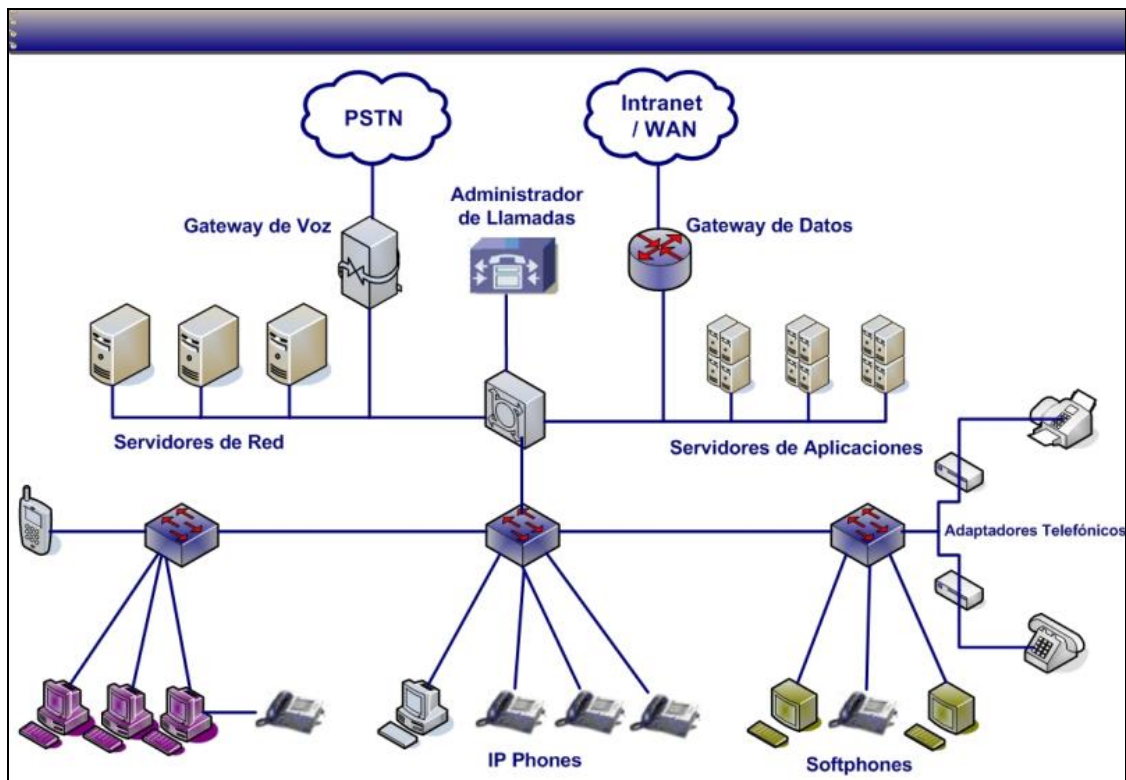


Figura 2.3: Red VoIP

#### 2.1.2.2.1.- Compresión de voz

Los algoritmos de compresión usados en los enrutadores y en los gateways analizan un bloque de muestras PCM entregadas por el codificador de voz (voice codec), estos bloques tienen una longitud variable que depende del codificador.

#### 2.1.2.2.2.- Estándares de Compresión

Los estándares para la compresión tanto de audio como de video han sido establecidos por el Grupo de Expertos en Imágenes en Movimiento (MPEG<sup>15</sup>) bajo los auspicios de la Organización Internacional para la Estandarización.

**MPEG-1** (ISO/IEC-11172), enfocado a aspectos relacionados con el almacenamiento y recuperación tanto de video como de audio. El estándar ha sido utilizado primordialmente para el almacenamiento en CD-ROMs y audio.

<sup>15</sup> Véase en el glosario de términos

**MPEG-2** (ISO/IEC-13818), que incluye al estándar MPEG-1 (tradicionalmente los estándares MPEG son compatibles con sus ancestros de forma de no hacer que tanto el soporte lógico informático como los equipamientos físicos queden obsoletos), tiene un componente el cual "define PSs (program streams) apropiados para aplicaciones sobre un medio confiable y TSs (transport streams) apropiadas para su distribución". MPEG-2 se ha popularizado bastante y es utilizado para la transmisión digital por satélite y para el almacenamiento de video en medios como el DVD.

MPEG es utilizado en una importante cantidad de aplicaciones comerciales, entre las que se incluyen la reproducción de contenido desde unidades de almacenamiento, difusión de programación audiovisual sobre variedad de canales, conexiones punto a punto conmutadas para entregar material audiovisual digital, televisión de alta definición y aplicaciones multimedia.

**MPEG-4** (ISO/IEC-14496) difiere en forma significativa con MPEG-1 y MPEG-2. MPEG-4 da un salto de la pasividad a la actividad ya que se definen objetos audiovisuales con los que se puede interactuar, mezclando sonido, imagen real, texto y gráficos en dos y tres dimensiones. La compresión y descompresión son diferentes dado que las imágenes están divididas en "componentes de vídeo-objetos (VOC) y componentes de audio-objetos (AOC)" que son tratados de forma independiente y donde deben definirse relaciones entre los mismos. En lugar de comprimir un marco (imagen) de forma completa, MPEG-4 utiliza un enfoque basado en capas, donde se separa el primer plano de la escena de su ambientación.

**MPEG-7** (ISO/IEC-15938) ya se encuentra en desarrollo y es denominado como una interfaz de descripción de contenido multimedia "preocupada con la interpretación de la información de tal forma que pueda ser usada o buscada por dispositivos o computadoras".

El equipamiento necesario para codificar la señal en un extremo y decodificarla en el otro es el mismo que debe poder empaquetar la señal antes de ser enviada y desempaquetarla antes de ser vista. Las figuras 2.4 y 2.5 muestran de forma simplificada la estructura de los codificadores y decodificadores MPEG respectivamente.

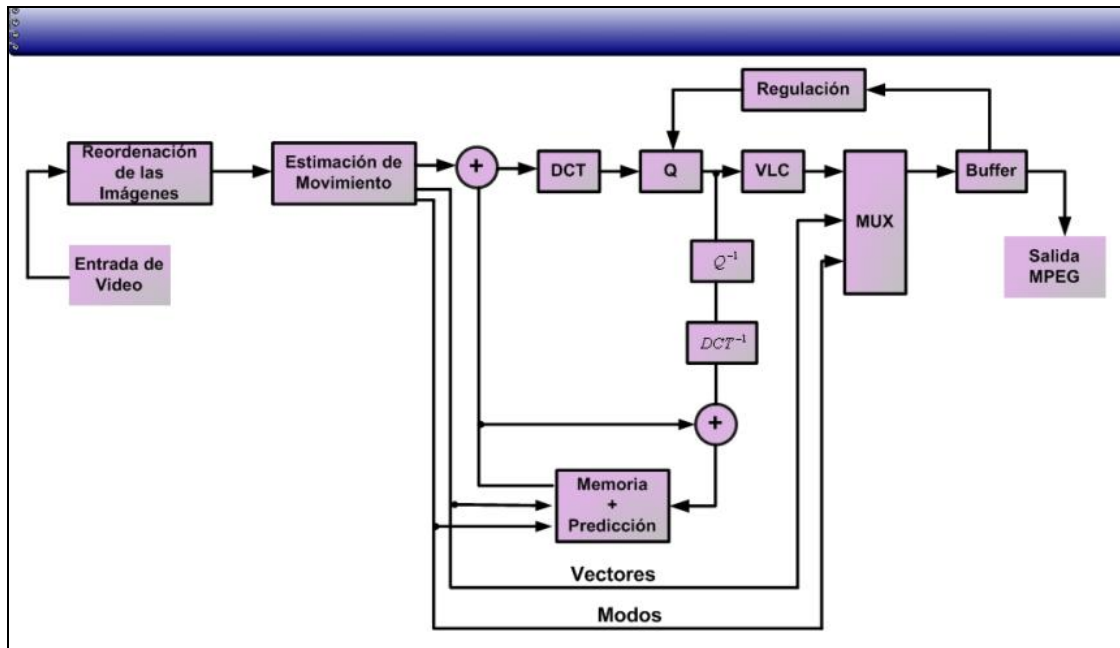


Figura 2.4: Codificador MPEG simplificado

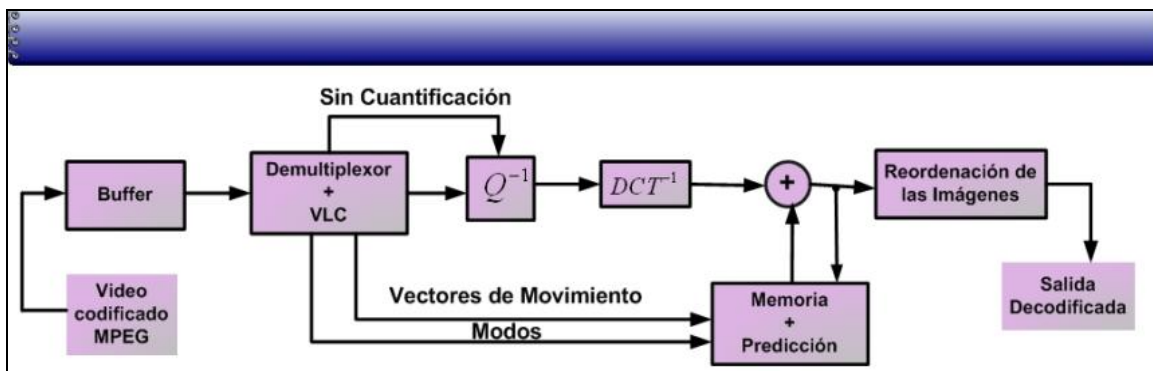


Figura 2.5: Decodificador MPEG simplificado

Para que el sistema funcione, tanto el codificador como el decodificador deben ser compatibles. Quienes diseñaron originalmente el formato MPEG aseguraron dicha compatibilidad por medio de una definición de la señal entre los dispositivos en lugar de definir los dispositivos en sí.

MPEG-4 difiere mucho de MPEG-1 en términos de complejidad y tipos de objetos que puede manejar. MPEG-4 puede comprimir y transmitir objetos virtuales en tres dimensiones como entramados, los cuales pueden ser recreados del lado del usuario usando un mapa de la superficie o textura del objeto. Al mismo tiempo el objeto puede ser reproducido desde determinado punto de vista, el cual puede ser el

punto de vista del usuario, creando un sistema interactivo. Finalmente, el diseño de MPEG-4 permite que el mismo sea distribuido utilizando UDP<sup>16</sup> sobre IP, PSTN, ATM y corrientes de MPEG-2.

#### **2.1.2.2.3.- Señalización**

La señalización VoIP tiene 3 áreas distintas: señalización del PBX<sup>17</sup> (Private Branch eXchange) al enrutador, señalización entre enrutador y señalización del enrutador al PBX.

En una arquitectura de red no orientada a la conexión (como IP), la responsabilidad del establecimiento de la comunicación y de la señalización es de las estaciones finales (end stations). Para prestar exitosamente servicios de voz a través de una red IP, es necesario realizar mejoras en la señalización.

Un protocolo confiable orientado a la conexión, TCP<sup>18</sup> (Transmission Control Protocol), es utilizado entre estaciones terminales para transportar los canales de señalización.

RTP (Protocolo de Transporte en Tiempo Real) el cual esta soportado en UDP (User Datagram Protocol), es usado para el transporte del caudal de audio en tiempo real. RTP usa UDP como mecanismo de transporte porque posee un menor retardo que TCP, y además porque el tráfico de voz en la actualidad, sin importar que sean datos o señalización, toleran menos niveles de perdida y no tienen la facilidad de retransmisión.

#### **2.1.2.2.4.- Direccionamiento**

Tomando como ejemplo una intranet con direccionamiento IP, podríamos ver que las interfaces de voz aparecerían como anfitriones IP adicionales, como extensiones del esquema de numeración existente o como nuevas direcciones IP.

---

<sup>16</sup> Véase en el glosario de términos

<sup>17</sup> Véase en el glosario de términos

<sup>18</sup> Véase en el glosario de términos



La traducción de los dígitos marcados del PBX al host IP se realizan por medio del plan de numeración. El número de teléfono de destino o alguna parte de este será vinculado a la dirección IP de destino. Cuando el número es recibido del PBX el enrutador lo compara con los que ya han sido vinculados con alguna dirección IP y están relacionados en la tabla de enrutamiento, si hay alguna coincidencia la llamada será enrutada al host IP al cual este relacionada, después de que la conexión es establecida, el enlace de la intranet es transparente hacia el suscriptor.

#### **2.1.2.2.5.- Enrutamiento**

Una de las fortalezas de IP es la sofisticación y gran desarrollo de sus protocolos de enrutamiento. Un protocolo de enrutamiento moderno, como el EIGRP<sup>19</sup> (Enhanced Internal Gateway Routing Protocol), es capaz de tener en consideración el retardo por cada uno de los caminos posibles que puede tomar el paquete y determinar la mejor ruta que puede seguir. Características avanzadas como el uso de políticas de enrutamiento y uso de listas de acceso (access lists), hacen posible crear esquemas de enrutamiento altamente seguros para el tráfico de voz.

RSVP<sup>20</sup> (Resource ReSerVation Protocol o Protocolo de Reserva) puede ser utilizado por los gateways de VoIP, de tal manera que se asegure que el tráfico ira a través de la red por el mejor y más corto camino, esto puede incluir segmentos de redes como ATM o LAN's conmutadas. Algunos de los desarrollos más importantes del enrutamiento IP son, el desarrollo del llamado tag switching y otras técnicas de conmutación IP.

El tag switching (Etiqueta de Conmutación de paquetes) muestra una manera extendida del enrutamiento IP, políticas y funcionalidades del RSVP sobre ATM y otros transportes. Otro de los beneficios del tag switching es la capacidad de manejo de tráfico, la cual es necesaria para un uso eficiente de los recursos de la red. El manejo de tráfico (traffic engineering) puede ser usado para cambiar la carga de este en diferentes sectores de la red basado en diferentes predicciones dependiendo del momento del día.

---

<sup>19</sup> Véase en el glosario de términos

<sup>20</sup> Véase en el glosario de términos

#### **2.1.2.2.6.- Consumo de ancho de banda**

Lograr transportar voz de alta calidad telefónica sobre IP en tiempo real no es una tarea nada fácil de alcanzar ya que tal labor requiere manejo de las capacidades de la red que permita el control del tráfico, protocolos de tiempo real (TCP/IP no lo son) y anchos de banda “dedicados” durante el tiempo que tome la realización de la llamada.

Sin embargo, día a día las limitaciones en los servicios de voz basados en IP, están siendo superadas gracias a dos factores: mejoras en los algoritmos de compresión (que permiten la optimización de la utilización del ancho de banda) y la sofisticación y gran desarrollo de los actuales protocolos de enrutamiento (capaces de tener en consideración el retardo por cada uno de los caminos posibles que puede tomar el paquete para así determinar la mejor ruta que puede seguir, proveer reservas de ancho de banda mientras que dura la conversación y dar preferencia al procesamiento de los paquetes dentro de los límites del enrutador, de manera que aquellos de alta prioridad son procesados primero).

#### **2.1.3.-QoS (Calidad de Servicio) en las comunicaciones**

La calidad de servicio (QoS) es el rendimiento de extremo a extremo de los servicios electrónicos tal como lo percibe el usuario final. Los parámetros de QoS son (Véase en la tabla 2.1): el retardo, la variación del retardo y la pérdida de paquetes. Una red debe garantizar que puede ofrecer un cierto nivel de calidad de servicio para un nivel de tráfico que sigue un conjunto específico de parámetros.

Tabla 2.1: Parámetros de Calidad en Telefonía IP

<b>Latencia</b>	La latencia afecta el ritmo de la conversación (se refiere al retardo entre el tiempo en que una de las partes habla y el tiempo en que la otra parte escucha lo hablado), y constituye el resultado de retardos en la pasarela o en la red. Una latencia que excede 250 ms se vuelve molesta para una conversación normal.
<b>Pérdida de Paquetes</b>	Este tema tiene relación con la Telefonía de Internet que se da en el internet público más que aquella que se produce en las redes privadas. La pérdida de paquetes ocurre cuando los routers que encaminan los paquetes sobre la red IP se sobrecargan. La respuesta de un router es la de desechar intermitentemente algunos paquetes. Es poco probable que en una conversación de voz aceptable se noten pérdidas de paquetes menores al cinco por ciento. Cualquier pérdida de paquetes que excedan el cinco por ciento tiene probabilidades de resultar en conversaciones entrecortadas.
<b>Interpolación</b>	Se refiere a qué tan bien (con qué grado de fidelidad) armoniza la voz transmitida con la voz natural de la persona que habla.
<b>Inestabilidad (Jitter)</b>	La inestabilidad resulta cuando una conversación telefónica es descompuesta en paquetes que viajan luego a través de las redes IP posiblemente a velocidades diferentes. Cuando los paquetes llegan a diferentes velocidades, el usuario escucha un poco de conversación seguida de silencio hasta que arriba el siguiente paquete.
<b>Compresión</b>	Hay una interacción entre la compresión y la calidad. Mientras más se comprime la señal de voz en el codec, menor es la calidad. Es posible comprimir la señal de voz de los 64 Kbps convencionales a tasas menores a 10 Kbps.

La implementación de políticas de calidad de servicio se puede enfocar en varios puntos según los requerimientos de la red, los principales son:

- Asignar ancho de banda en forma diferenciada.
- Evitar y/o administrar la congestión en la red.
- Manejar prioridades de acuerdo al tipo de tráfico.
- Modelar el tráfico de la red.

La comunicación sobre IP (al igual que la telefonía convencional) debe tener características de tiempo real, desafortunadamente TCP/IP no puede garantizar este tipo de particularidad siempre, de modo que se deben introducir algunas políticas que puedan manejar el flujo de paquetes en todos los enrutadores que deban intercambiar paquetes. Estas son:

- Campos en el protocolo IP para describir el tipo de servicio: los altos valores indican poca urgencia, mientras que los más bajos indicaran urgencia, es decir que se solicita respuesta en tiempo real.
- Métodos de solución para paquetes en cola:
  - FIFO (first in first out), es el método más común, donde sale primero el paquete que llegó en primer lugar.
  - WFQ (weighted fair queuing), consiste en un paso justo de paquetes en consideración con el ancho de banda disponible (por ejemplo, FTP<sup>21</sup> (File Transfer Protocol) no puede consumir todo el ancho de banda disponible del enlace en cuestión), dependiendo del tipo de flujo de datos que se esté dando, por ejemplo en un ambiente justo, por cada paquete UDP habrá uno TCP.
  - CQ (custom queuing), donde los usuarios deciden la prioridad del paquete.
  - PQ (priority queuing), se establece un número de colas (típicamente 4), cada una con un nivel de prioridad diferente: se comienza enviando los paquetes de la primera cola y luego (cuando la primera cola está vacía) se envían los paquetes de la segunda cola y así sucesivamente.
  - CB-WFQ (class based weighted fair queuing), es muy similar a WFQ pero se adiciona el concepto de clases (hasta 64) y además un valor de ancho de banda es asociado.
- Capacidad de limitación, la cual permite restringir a la fuente llegar a un ancho de banda determinado para:
  - Descarga (download).
  - Carga (upload).
  - Prevención de congestión.

### **2.1.3.1.- Retardo**

El retardo causa dos problemas: eco y traslape del habla. El eco es causado por las señales reflejadas por el equipo telefónico del extremo distante que regresan al oído del hablante. El eco llega a ser un problema significativo cuando el retardo del

---

<sup>21</sup> Véase en el glosario de términos

viaje redondo llega a ser más de 50 milisegundos. A medida que el eco se incrementa, los sistemas de paquetes se ven en la necesidad de utilizar controles como la cancelación de eco. El traslape del habla (cuando en una llamada dos personas hablan casi al mismo tiempo) es significativo si el retardo en una sola vía es mayor de 250 milisegundos (Véase la tabla 2.2). Por lo tanto el retardo completo llega a ser mayor.

Una de las fuentes de retardo es lo que se conoce como retardo acumulado o retardo algorítmico, el cual es causado por la necesidad de recolectar un número de muestras de voz para que sean procesados por el codificador de voz. Esto está relacionado con el tipo de codificador usado y varía de una sola muestra en el tiempo.

Otra fuente de retardos es el causado por el procesamiento de codificación y recolección de las muestras codificadas en paquetes para la transmisión sobre una red de paquetes (que se conoce como retardo de procesamiento).

Por último, existe lo que se conoce como retardo de red, que es causado por el medio físico y los protocolos usados para transmitir los datos de voz y por los buffers usados para remover el jitter en el lado receptor.

Tabla 2.2: Tiempos de retardo de extremo a extremo (un sentido).

Retardo total de una dirección	Recomendación para el uso
0 – 150 ms	Aceptable
50 – 400 ms	Aceptable para ciertas aplicaciones, se requiere cuidado para garantizar la satisfacción del usuario.
+ 400 ms	Inaceptable para la planificación de redes generales.

### 2.1.3.2.- Jitter

Es la variación de tiempo entre los paquetes causada por la red. Remover el jitter requiere la recolección de paquetes y retención de estos el tiempo suficiente para que el paquete más lento llegue a tiempo para ser interpretado en la secuencia correcta.

Una buena opción en redes IP para adaptar el tamaño del buffer de jitter es contar el número de paquetes que llegan tarde y crear una relación de estos paquetes al número de paquetes que son procesados exitosamente. Esta relación es usada para ajustar el buffer de jitter a una relación permisible de paquetes tardíos predeterminada.

Además de estas técnicas, la red debe estar configurada y gestionada para que tenga retardos y jitter mínimos, permitiendo así un alto QoS.

### **2.1.3.3.- Pérdida de paquetes**

En redes IP actuales, todos los marcos de voz son tratados como datos. Bajo congestión, los marcos de voz serán descartados al igual que los de datos, estos últimos sin embargo no son sensibles al tiempo, y los paquetes descartados pueden ser recuperados con la retransmisión, mientras que los paquetes de voz no pueden ser tratados de esta manera. Una forma de corregir este problema, es enviar información redundante a expensas de la utilización del ancho de banda.

La pérdida de paquetes también afecta a la calidad de la voz, pero el tanto por ciento admisible depende tanto de los algoritmos de compresión usados como de la percepción subjetiva de los usuarios. El límite generalmente aceptado como máximo se sitúa alrededor del 8-10%.

La realidad es que el asegurar estos parámetros, esta calidad de servicio, a lo largo de una red IP con los niveles de calidad habituales en una red de voz, sólo es posible, y con limitaciones, cuando se realiza dentro de una red IP privada con los equipos y el ancho de banda necesarios y siendo gestionada centralizadamente (Véase la tabla 2.3). Habitualmente un canal de voz necesita un ancho de banda garantizado de 12-15 Kb/s por lo que proporcionar o asegurar en una red como Internet ese ancho de banda no es posible en general. La utilización de las nuevas redes IP por los operadores puede hacer posible la disponibilidad, dentro de esas redes IP, de ancho de banda garantizado; pero sin duda, con el costo asociado de reserva de ese ancho de banda.

La compartición de las conexiones tanto para datos como voz sobre IP reducirá los costos globales, pero no se puede suponer que si se desea obtener una calidad

comparable a la que la red de voz tiene, los costos se reduzcan muy significativamente.

La tendencia a la reducción del precio del ancho de banda, así como la integración de servicios reducirán los costos de las conexiones, pero el aseguramiento de calidades de servicio tendrá su costo, aunque menor.

Tabla 2.3: Requerimientos básicos de características de voz para aplicaciones de voz sobre datos.

CARACTERÍSTICA	REQUERIMIENTO
<b>Compresión:</b> La compresión sub-PCM reduce significativamente la cantidad de ancho de banda usada para una conversación de voz manteniéndose a la vez una alta calidad.	Debe tener
<b>Supresión de silencio:</b> Habilidad de recuperar ancho de banda durante periodos de silencio en una conversación, poniendo a disposición ese ancho de banda para otros usuarios de la red.	Debe tener
<b>QoS:</b> Asegurar la prioridad para la transmisión de voz es crítico. Esto mantiene el retardo, la variación del mismo y la pérdida a niveles mínimos tolerables.	Debe tener. Cuenta con poco apoyo (Tipo de Servicio (ToS) no es generalmente implementado en nodos).
<b>Señalización para tráfico de voz:</b> El apoyo a pbs tradicionales y señales asociadas es crítico.	Debe tenerse para aplicaciones en tiempo real.
<b>Control de eco:</b> El eco es molesto y problemático. El control es clave.	Debe tenerse para aplicaciones en tiempo real.
<b>Conmutación de voz:</b> Los equipos de red de datos generalmente soportan aplicaciones en red. Fuera de red es también crítico. Como mínimo los equipos adjuntos deben decidir si se debe encaminar una llamada sobre la red de datos internos o encaminarla a la RTPC (red telefónica pública conmutada).	La capacidad de enrutamiento fuera de red es indispensable para aplicaciones en tiempo real.

#### 2.1.4.-Seguridad

La información sobre una llamada es tan valiosa como el contenido de la voz. Las llamadas son también vulnerables al "secuestro" debido a que un atacante puede interceptar una conexión y modificar los parámetros de la llamada. Las posibilidades

incluyen diversas técnicas como robo de identidad, y redireccionamiento de llamada, haciendo que la integridad de los datos estén bajo un gran riesgo.

La enorme disponibilidad de las redes VoIP es otro punto sensible. En PSTN, la disponibilidad era raramente un problema. Una pérdida de potencia puede provocar que la red se caiga por lo que es mucho más sencillo hackear una red VoIP. Los efectos demolidores de los ataques traen como consecuencia la denegación de servicio. Si se dirigen a puntos clave de la red, podrían incluso destruir la posibilidad de comunicación vía voz o datos.

Los teléfonos y servidores son en base a ordenadores con software. Obviamente, este software es vulnerable con los mismos tipos de falencias de seguridad que pueden hacer que un sistema operativo pueda estar a plena disposición del intruso. El código puede ser insertado para configurar cualquier tipo de acción maliciosa.

En los esquemas iniciales y en diseños de hardware para voz, software y protocolos, la seguridad no es su punto fuerte.

Internet, generalmente es poco confiable para transportar voz de alta calidad telefónica, porque los actuales protocolos TCP/IP no proveen reservas de ancho de banda ni garantizan la calidad del servicio. Por consiguiente, la calidad de las llamadas sobre IP serán adversamente afectadas por la congestión de la red que origina que los paquetes se tarden o se pierdan. Un ambiente como una red pública Internet, está marcada por una incontrolable fluctuación de carga, razón por la cual no puede garantizar una conexión de voz aceptable.

La encriptación es la única manera de prevenirse de un ataque, desafortunadamente se consume ancho de banda. Existen múltiples métodos de encriptación: VPN<sup>22</sup> (virtual personal network), SRTP<sup>23</sup> (secure RTP). La clave, de cualquier forma, es elegir un algoritmo de encriptación rápido, eficiente, y emplear un procesador dedicado de encriptación. Otra opción podría ser QoS; los requerimientos para QoS asegurarán que la voz se maneja siempre de manera oportuna, reduciendo la pérdida de calidad.

---

<sup>22</sup> Véase en el glosario de términos

<sup>23</sup> Véase en el glosario de términos



Estas limitaciones de los servicios de VoIP, están siendo solucionadas por nuevos protocolos que proveen diferentes clases de servicios o prioridades de paquetes y la habilidad de reservar ancho de banda a través de la red para la duración de una llamada telefónica. Nuevos protocolos para tráfico, otorgan la habilidad, no sólo de destinar ancho de banda por prioridad de paquetes, sino que también dan preferencia al procesamiento de los mismos dentro de los límites del enrutador de manera que los paquetes de alta prioridad son procesados primero. Estas mejoras a los algoritmos y protocolos en los enrutadores y conmutadores están reduciendo la tenencia y la pérdida de paquetes para lograr una mejor calidad de servicio, y estos avances han comenzado a permitir a los proveedores de servicios de VoIP encontrar los estándares necesarios para servicios de voz.

Se necesita además configurar cada uno de esos dispositivos con acceso a las listas de control y a los filtros y también asegurarse de que están en línea con las demandas en términos de seguridad. Los servidores pueden tener pequeñas funciones trabajando y sólo abiertos los puertos que sean realmente necesarios. Todos los dispositivos deben estar actualizados. Se trata del mismo tipo de precauciones que es necesario tomar cuando se añaden nuevos elementos a la red de datos; únicamente habrá que extender este proceso a la porción que le compete a la red VoIP.

Es posible emplear un firewall y un IDS<sup>24</sup> (intrusion detection system) para ayudar a proteger la red de voz. Está diseñado para detener ataques antes de que tengan éxito. Actualmente existe IPS<sup>25</sup> (Intrusion Prevention System) que es un sistema que combina las capacidades de bloqueo de un cortafuego y las de análisis de un IDS. Los firewalls de VoIP son complicados de manejar y tienen múltiples requerimientos. Los servidores de llamada están constantemente abriendo y cerrando puertos para las nuevas conexiones. Este elemento dinámico hace que su manejo sea más complicado. No obstante, el costo es equiparable la cantidad de beneficios. Se debe prestar especial atención al perfeccionamiento los controles de acceso. Un IDS puede monitorizar la red para detectar cualquier anomalía en el servicio o un abuso potencial, pero no toma ninguna acción correctiva; por lo tanto se debe utilizar IPS.

Las redes de conmutación por paquetes pueden transportar llamadas de voz eficientemente, utilizando un ancho de banda de 8 kbps que provee de alta calidad

---

<sup>24</sup> Véase en el glosario de términos

<sup>25</sup> Véase en el glosario de términos

telefónica, comparadas a las redes de conmutación de circuitos (tradicionales) que hacen uso de un ancho de banda de 64 kbps. Además, los costos de infraestructura, asociados a la implementación de redes de conmutación por paquetes, son mucho más bajos que las alternativas tradicionales. Como resultado, nuevos proveedores de servicios telefónicos, están utilizando cada vez más este tipo de arquitecturas.

### 2.1.5.-Protocolos

Para soportar el servicio de VoIP se requiere, además de los protocolos para el transporte de la información de usuario en tiempo real, también los de señalización, es decir, los protocolos necesarios que garanticen el establecimiento, mantenimiento - modificación y terminación de las llamadas de voz sobre las redes IP, lo que quiere decir que es necesario la señalización de control de las llamadas. De igual forma se requiere señalización para: QoS, control de medios, etc.

El conjunto de protocolos de VoIP se descompone en dos categorías:

- a. **Protocolos del plano de control:** es el tráfico necesario para conectar y mantener el tráfico actual de usuario. Es también responsable de mantener toda la operación de toda la red (comunicaciones router<sup>26</sup> - router).
- b. **Protocolos del plano de datos (Voz):** es el protocolo necesario para llevar el tráfico de un usuario a otro.

Un usuario puede navegar en la web (HTTP<sup>27</sup> - HyperText Transfer Protocol) o enviar correo electrónico (SMTP<sup>28</sup> - Simple Mail Transport Protocol) a través de la red. Esto constituye el plano de datos, el tráfico de usuario. Por otro lado, los routers en la red también necesitan comunicación sobre la misma LAN utilizando OSPF<sup>29</sup> (Open Shortest Path First) o RIP<sup>30</sup> (Router Information Protocol). Este tráfico siempre es invisible al usuario, pero es necesario para enrutar el tráfico del mismo. Esto constituye el plano de control.

---

<sup>26</sup> Véase en el glosario de términos

<sup>27</sup> Véase en el glosario de términos

<sup>28</sup> Véase en el glosario de términos

<sup>29</sup> Véase en el glosario de términos

<sup>30</sup> Véase en el glosario de términos

### 2.1.5.1.- Pila de protocolos de VoIP

Como su nombre indica, VoIP utiliza IP. VoIP puede utilizar tanto UDP como TCP sobre IP. En la figura 2.6 se muestra la pila de protocolos de VoIP. Es importante destacar que VoIP trabaja sobre cualquier pila de protocolos IP. Los usuarios de VoIP pueden añadir esta tecnología de forma fácil y rápida a la red ya existente de datos.

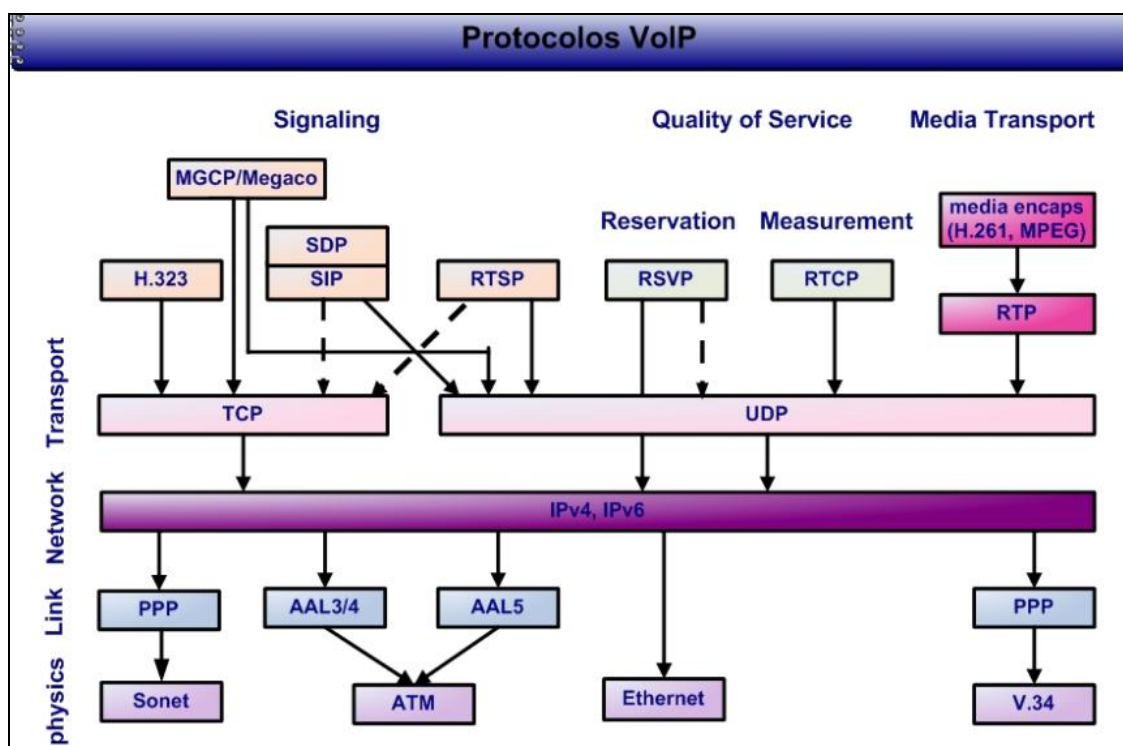


Figura 2.6: Protocolos VoIP

### 2.1.5.2.- Protocolos del Plano de datos

RTP y cRTP Ambos, Real-Time Protocol (RTP) y Compressed Real-Time Protocol (cRTP) están normalmente disponibles en cualquiera de las arquitecturas de VoIP. El tráfico propio de VoIP a veces va por caminos diferentes a la señalización, esto significa que pueden viajar de forma independiente. RTP es el protocolo que soporta la voz del usuario. Cada paquete RTP contiene una muestra pequeña de la conversación de voz. El tamaño del paquete y el tamaño de la muestra de voz, dentro de dicho paquete, dependerán del CODEC utilizado. En la figura 2.7 se muestra la pila de protocolos RTP.

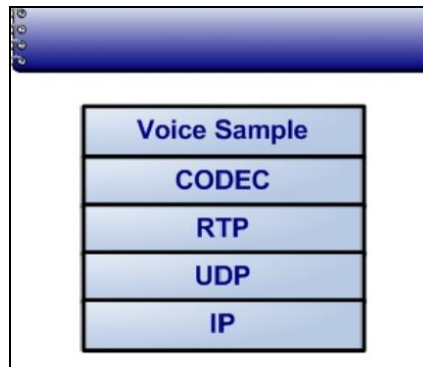


Figura 2.7: Protocolo RTP

Si un paquete RTP se pierde o es descartado por la red, no será retransmitido, esto es debido a la conveniencia de evitar largas pausas en la conversación telefónica. La red debería diseñarse para que tan sólo unos pocos paquetes sean perdidos en la transmisión. En la cabecera RTP se incluye información para identificar y gestionar cada llamada, de forma individual, desde un extremo a otro.

#### **2.1.5.2.1.- RTP Comprimido**

Una variante de RTP es RTP comprimido (cRTP). RTP Comprimido elimina mucha de la información de la cabecera del paquete. Eliminando estos bytes, la red se optimiza disminuyendo la información añadida al paquete. Utilizando cRTP, un usuario puede doblar el número de llamadas que al utilizar RTP estándar. Compressed RTP se utiliza en enlaces WAN, especialmente en enlaces punto-punto. Como la cabecera de UDP y RTP se reduce a un máximo de 4 bytes, no hay lugar para añadir en la cabecera la dirección IP. Por lo tanto, el paquete no puede ser enrutado y sólo puede ser utilizado en enlaces donde no resulte necesario direccionamiento IP. La consecuencia de cRTP, similar a cualquier forma de compresión, es que necesita más ciclos de procesado en el router para tratar el paquete. El router debe recrear cada cabecera tan pronto llegue el paquete IP, y de esta forma, la información es enrutada a través de la LAN hasta el teléfono IP.

### **2.1.5.2.2.- RTCP**

Real-Time Control Protocol (RTCP) es un protocolo del plano de datos. Este protocolo permite a los usuarios finales ajustar en tiempo real la calidad de la llamada. También contribuye a detectar los posibles problemas. Con RTCP habilitado, cualquier analizador puede visualizar la calidad de la llamada en los dos extremos, analizando los paquetes que envían los dos equipos de comunicación. Se puede detectar la sección donde está la incidencia de una forma mucho más rápida. De cualquier modo, aunque la información que aporta es muy útil, también añade ancho de banda, por esta razón es el usuario quien tiene que decidir si quiere o no utilizarlo.

### **2.1.5.2.3.- RTCP XR**

RTP Control Protocol Extended Reports (RTCP XR) es una versión más nueva de RTCP. Define una serie de medidas que pueden ser añadidas de forma económica a gestores, pasarelas y teléfonos IP para el análisis de las llamadas de voz. Los mensajes RTCP XR se intercambian de forma periódica entre los teléfonos IP y las pasarelas. Estos mensajes también pueden ser gestionados por peticiones SNMP<sup>31</sup> (Simple Network Management Protocol) y formar parte de un sistema superior de calidad.

### **2.1.5.2.4.- CODECs**

Hay varios tipos de CODECs (coder/decoder) para la implementación de VoIP, como por ejemplo los que se muestran en la tabla 2.4:

---

<sup>31</sup> Véase en el glosario de términos

Tabla 2.4: Tipos de Codec's

CODEC'S	TIPO	VELOCIDAD BINARIA Kbps	TAMAÑO DE TRAMA	RETARDO TOTAL	OTROS DATOS
G.711	PCM	64	Depende del tamaño de los paquetes		Códec elegido para servicio vocal de alta calidad, equivalente a RTPC.
G.726	ADPCM	32	Depende del tamaño de los paquetes		Usado frecuentemente para multiplexaje en canales de 64 kbps y se especifica para muchos sistemas inalámbricos de baja potencia. Generalmente considerado un límite más bajo de la gama de calidad "interurbana".
G.729	CSACELP	8	10 ms	25 ms	Norma de codificación de 8 kbps de la UIT. Buenas características de retardo (debido a trama corta) y calidad vocal aceptable. Ha sobrepasado el G.723.1 como códec preferido para aplicaciones que requieren compresión.
G.729a	CSACELP	*	*	*	Versión de G.729 de complejidad reducida. La calidad vocal es equivalente a la G.729. Los descodificadores idénticos permiten que los dos códecs interfundan sin transiciones.
G.723.1	MPMLQ	6,3/5,3	30 ms	67,5 ms	Norma predeterminada para clientes de derivación interurbana de fabricación en serie. La calidad vocal básica es generalmente inadecuada para aplicaciones comerciales. El retardo total compromete el cálculo del retardo.
GSMEFR	ACELP	12.2	20 ms	40 ms	Códec inalámbrico

### 2.1.5.3.- Protocolos del Plano de Control

Son los protocolos de señalización que permite a los usuarios interconectar sus teléfonos de VoIP. Hay muchos tipos de protocolos de señalización diferentes, H.323, SIP, SCCP<sup>32</sup>, MGCP, MEGACO, SIGTRAN<sup>33</sup>.

<sup>32</sup> Véase en el glosario de términos

<sup>33</sup> Véase en el glosario de términos

## **2.1.5.3.1.- H.323**

### **2.1.5.3.1.1. Introducción**

El estándar H.323 proporciona una base para las comunicaciones de audio, video y datos a través de una red IP como Internet. Los productos que cumplen con el estándar H.323 pueden interoperar con los productos de otros, permitiendo de esta manera que los usuarios puedan comunicarse sin preocuparse con problemas de compatibilidad.

H.323 es un estándar bajo el amparo de la ITU<sup>34</sup>, es un conjunto de estándares para la comunicación multimedia sobre redes que no proporcionan QoS. Estas redes son las que predominan hoy en todos los lugares, como redes de paquetes conmutadas TCP/IP e IP sobre Ethernet, Fast Ethernet y Token Ring<sup>35</sup>. Por esto, los estándares H.323 son bloques importantes de construcción para un amplio rango de aplicaciones basadas en redes de paquetes para la comunicación multimedia y el trabajo colaborativo.

El estándar tiene amplitud e incluye desde dispositivos específicos hasta tecnologías embebidas en ordenadores personales, además de servir para comunicación punto-punto o conferencias multi-punto. H.323 habla también sobre control de llamadas, gestión multimedia y gestión de ancho de banda, además de los interfaces entre redes de paquetes y otras redes.

H.323 forma parte de una gran serie de estándares que permiten la videoconferencia a través de redes. Conocidos como H.32X, esta serie incluye H.320 y H.324, que permiten las comunicaciones RDSI y PSTN respectivamente.

### **2.1.5.3.1.2. Protocolos incluidos en H.323**

H.323 es en realidad una recomendación paraguas que engloba un conjunto de protocolos (Véase la figura 2.8). Especifica los codecs que se deben emplear, tanto para manejar voz como video, además de los protocolos necesarios para el transporte

---

<sup>34</sup> Véase en el glosario de términos

<sup>35</sup> Véase en el glosario de términos

de la información (ya sea audio, video o datos) o el intercambio de señalización de control entre los terminales y el órgano encargado del control de la red.

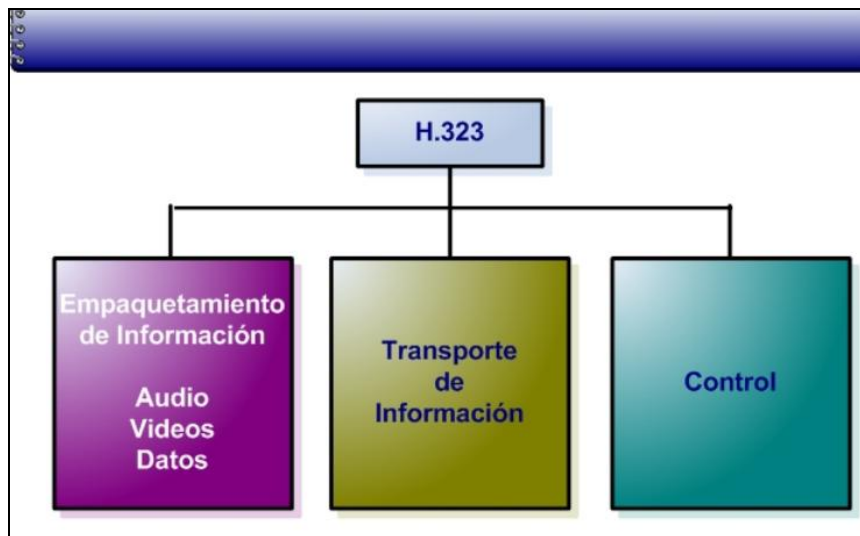


Figura 2.8: Protocolos incluidos en H.323

Este protocolo permite dotar a la red de mecanismos avanzados de control y de gestión, tales como control de admisión, gestión de ancho de banda, autorización de llamadas o traducción de direcciones entre la PSTN y las redes de paquetes.

Aunque se trate de un protocolo maduro que ya se emplea en ciertas soluciones comerciales, tiene una serie de limitaciones e inconvenientes, como su elevada complejidad, o ciertas ineficiencias debidas a su orientación a la compatibilidad con la PSTN, que justifican los esfuerzos que se están realizando en la especificación de otros protocolos con propósitos similares.

VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

- Direccionamiento:
  1. *RAS (Registration, Admission and Status)*. Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través de el Gatekeeper.



2. *DNS (Domain Name Service)*. Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

- Señalización:

1. *Q.931*: Señalización inicial de llamada
2. *H.225*: Control de llamada: señalización, registro y admisión, y paquetización / sincronización del stream (flujo) de voz
3. *H.245*: Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz

- Compresión de voz:

1. *Requeridos*: G.711 y G.723
2. *Opcionales*: G.728, G.729 y G.722

- Transmisión de voz:

1. *UDP*. La transmisión se realiza sobre paquetes UDP, aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.
2. *RTP (Real Time Protocol)*. Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

- Control de la transmisión:

1. *RTCP (Real Time Control Protocol)*. Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

Se puede observar en la tabla 2.5 los estándares de H.323 ubicados en la capa a la que correspondiente dentro del modelo OSI<sup>36</sup>.

---

<sup>36</sup> Véase en el glosario de términos

Tabla 2.5: Modelo de referencia OSI y estándar h.323

CAPA SEGÚN EL MODELO OSI	ITU H.323 ESTÁNDAR
Presentación	G.711, G.729, G.729a, etc.
Sesión	H.323, H.245, H.225, RTCP
Transporte	RTP, UDP
Red	IP, RSVP, WFQ
Enlace	RFC 1717 (PPP/ML), Frame, ATM, etc

### 2.1.5.3.1.3. Arquitectura

En la figura 2.9 se muestra que H.323 es un conjunto de protocolos “multi capa”, que tocan con casi todos los niveles (capas) superiores del modelo OSI. Se puede usar cualquier protocolo de red y de enlace de datos de los que usa TCP/IP, que son muy diversos para usarla como capa de transporte.

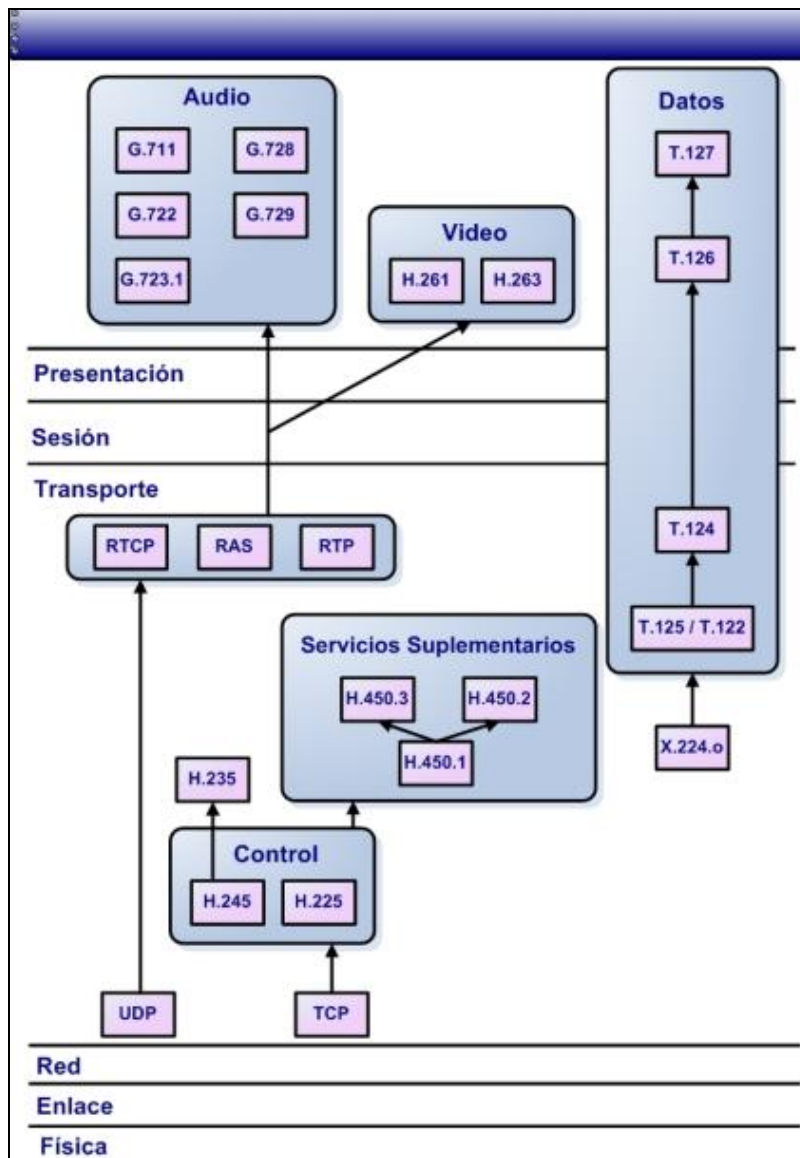


Figura 2.9: Arquitectura H.323 dentro del modelo OSI

H.323 formatea y empaqueta a la información de audio y video para transmitirla sobre la red. Los Codecs estándar de audio y video codifican y decodifican las entradas/salidas de las fuentes de comunicación entre nodos. H.323 también usa el protocolo T.120<sup>37</sup>, que especifica los servicios para comunicación de datos y conferencias dentro de una sesión H.323 o adjunto a ella y lo más importante es que este soporte. T.120 significa que el manejo de datos puede ocurrir conjuntamente con video y audio H.323 o de manera separada.

<sup>37</sup> Véase en el glosario de términos

La figura 2.10 muestra la arquitectura H.323. Esta arquitectura define un grupo de funciones específicas para el entramado y el control de llamadas, para los codecs de audio y video y para las comunicaciones de datos T.120, presenta también las interfaces con la red, con los usuarios y con los equipos de audio y video.

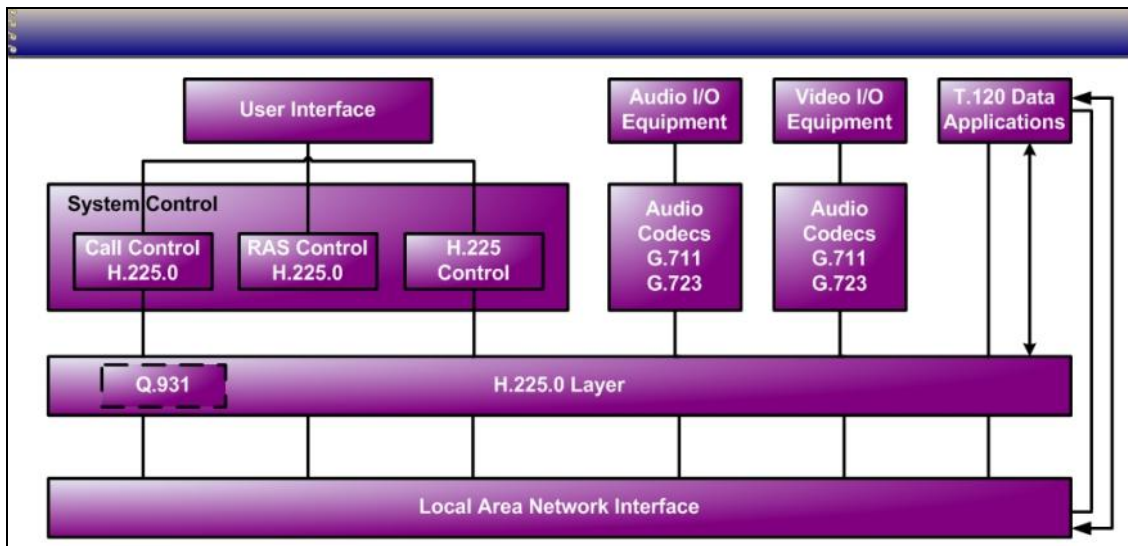


Figura 2.10: Arquitectura H.323

#### 2.1.5.3.1.4. Entramado (framing) y control de llamadas

Los siguientes estándares constituyen la Unidad de Control del Sistema (System Control Unit) y proveen las capacidades de control de llamada y entramado (como se forman las tramas):

**H.225.0:** este estándar define una capa que formatea los flujos de video, audio, datos y control que serán transmitidos a la red y recibidos de ella.

Como una parte de las transmisiones de audio y video, H.225.0 realiza el formateo de paquetes especificado por IETF<sup>38</sup> y por los protocolos RTP y RTCP para las siguientes tareas:

- **Entramado local:** Define como el protocolo entrama los datos de audio y video en bits (paquetes) para transportarlos sobre un canal de comunicación seleccionado.

<sup>38</sup> Véase en el glosario de términos

- **Secuencia de Numeración:** Determina el orden de los paquetes de datos, transportados sobre un canal de comunicación.
- **Detección de errores:** Después de iniciar una llamada, una o más conexiones RTP o RTPC se establecen. Múltiples flujos le permiten a H.225.0 enviar y recibir diferentes tipos de medios simultáneamente, cada uno con su propia secuencia de tramas y calidad de servicio. Con el soporte de RTP y RTCP el nodo receptor sincroniza los paquetes recibidos en el orden adecuado, para que el usuario oiga o vea la información correctamente.

El H.225.0 también incluye el control de Registro, Admisión y Estado (RAS), el cual es usado para comunicarse con el Gatekeeper y es el soporte para RTP/RTCP para secuenciar paquetes de audio y video. Un canal RAS hace las conexiones entre el Gatekeeper y los componentes H.323 disponibles. El Gatekeeper controla el terminal H.323, el Gateway y el acceso MCU (Unidad de control Multipunto) a la LAN, permitiendo o negando el acceso a conexiones H.323.

**Q.931:** Este protocolo define como interactúan cada una de las capas con sus correspondientes en el otro extremo. Este protocolo reside con el H.225.0. Como parte del control de llamada de H.323, Q.931 es un protocolo de capa de enlace para establecer conexiones y entramado de datos. Provee un método para definir canales lógicos dentro de un gran canal. Los mensajes Q.931 contienen un discriminador de protocolo que identifica cada mensaje con un valor de referencia de llamada y un tipo de mensaje. La capa H.225.0 luego especifica como son recibidos y procesados estos mensajes.

**H.245:** Este estándar provee el mecanismo de control de llamadas que le permite a los terminales compatibles H.323 interconectarse. H.245 provee los medios para conexiones de audio y video. Define la serie de comandos y requerimientos que debe seguir un componente para comunicarse con otro. Especifica la señalización, el control de flujo y la asignación de los canales para mensajes, requerimientos y comandos.

La estructura de H.245 permite la selección de codec y la negociación de capacidades con H.323. La velocidad de bits y de trama, el formato de la figura y la selección del algoritmo son algunos de los elementos negociados por H.245.

**Codecs de Audio y Video:** Los codecs definen el formato de la información de audio y video y representan la manera en que esta es comprimida y enviada a través

de la red. H.323 provee una variedad de opciones para codificación. Dos codecs, el G.711 para audio y el H.261 para video son requeridos (obligatorio el G.711) por la especificación H.323. Los terminales H.323 son capaces de enviar y recibir con algoritmos de codificación del tipo ley-A y ley- $\mu$  (G.711). Codecs adicionales de audio y video proveen una variedad de velocidades, retardos y opciones de calidad que se acomodan a las selecciones de red.

A continuación se describen los codec de audio y video requeridos (G.711 y H.261), así como los dos codec preferidos para conexiones NetMeeting (G.723 and H.263), que ofrecen las conexiones de baja velocidad, necesarias para transmisión de audio y video sobre Internet.

- G.711: este codec transmite audio a 48, 56 y 64 Kbps. Es apropiado para audio sobre conexiones de alta velocidad.
- G.723: este codec especifica el formato y algoritmo usado para enviar y recibir comunicaciones de voz sobre la red. Es un codec de alta velocidad que transmite audio a 5.3 y 6.3 Kbps, reduciendo el ancho de banda.
- H.261: este codec transmite imágenes de video a 64 Kbps (calidad VHS). Es apropiado para video sobre conexiones de alta velocidad.
- H.263: este codec especifica el formato y algoritmo usado para enviar y recibir imágenes de video sobre la red. Soporta codificación con cuantización por compresión, pero es acompañado de predicción y estimación de movimiento. Ofrece muy buen desempeño para transmisión sobre conexiones de baja velocidad como las de los modem de 28.8 Kbps.

**Aplicaciones de Datos:** H.323 usa a T.120 como el mecanismo para empaquetar y enviar datos. T.120 puede usar la capa de H.225.0 para enviar y recibir los paquetes de datos o simplemente crear una asociación con la sesión de H.323 y usar sus propias capacidades de transporte para transmitir datos directamente a la red. Los datos de los programas de conferencia, como la transferencia de archivos y la compartición de programas, usan el soporte de T.120 para operar en unión con las conexiones H.323. Los productos compatibles H.323 ínteroperan con productos de conferencias de datos desarrollados bajo la especificación T.120.

### 2.1.5.3.1.5. Componentes H.323

Los principales componentes son (Véase la figura 2.11): Terminales, Gateways, Gatekeepers, Controladores Multipunto (MC), Procesadores Multipunto (MP) y Unidades Controladoras Multipunto (MCU).

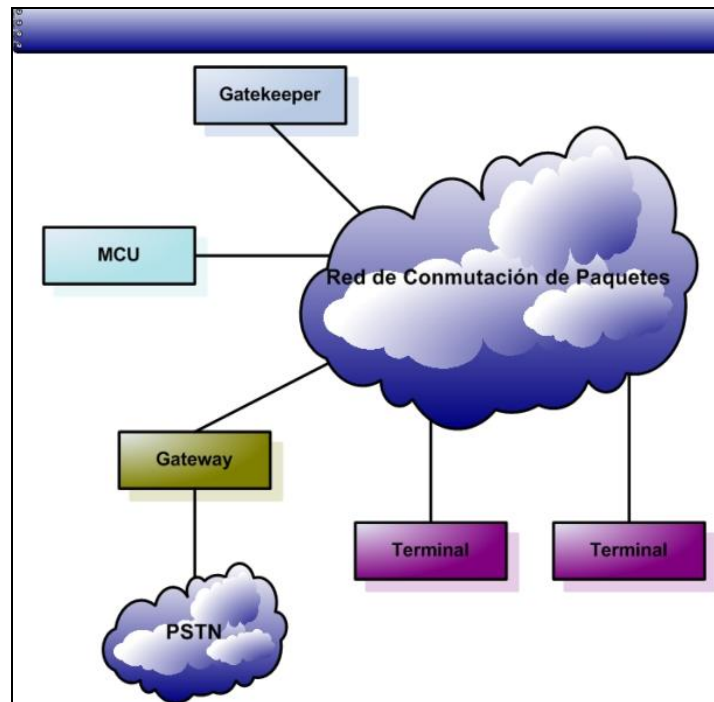


Figura 2.11: Componentes de la Arquitectura H.323

**Terminal:** es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y/o datos entre los dos terminales. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.

**Gatekeeper:** es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs. Puede también ofrecer otros servicios a los terminales, gateways y MCUs, tales como gestión del ancho de banda y localización de los gateways o pasarelas.

Los Gatekeepers proporcionan importantes funciones obligatorias:

- *Traducción de Direcciones:* traducción de alias a direcciones de transporte, usando para ello una tabla que es modificada con mensajes de registro. Se permiten otros métodos de modificar la tabla.
- *Control de Admisión:* el Gatekeeper debe autorizar el acceso a la red usando mensajes H.225.0 (ARQ<sup>39</sup>, ACF<sup>40</sup> o ARJ<sup>41</sup>). Esto puede basarse en autorización de llamada, ancho de banda, o algún otro criterio que es dejado al fabricante. También puede ser una función nula que admita todas las peticiones.
- *Control de Ancho de Banda:* el Gatekeeper debe soportar mensajes BRQ<sup>42</sup>, BRJ<sup>43</sup> y BCF<sup>44</sup> para gestión del ancho de banda. También puede aceptar todas las peticiones de ancho de banda.
- *Gestión de Zona:* el Gatekeeper debe suministrar las funciones anteriores a todos los terminales, MCU's y Gateways que se encuentren registrados en su zona de control.

**Gateway:** es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. En general, el propósito del gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa.

Las principales aplicaciones de los Gateways son:

- Establecer enlaces con terminales telefónicos analógicos conectados a la PSTN.
- Establecer enlaces con terminales remotos que cumplen H.320 sobre redes RDSI basadas en conmutación de circuitos.
- Establecer enlaces con terminales remotos que cumplen H.324 sobre la red telefónica básica conmutada.

---

<sup>39</sup> Véase en el glosario de términos

<sup>40</sup> Véase en el glosario de términos

<sup>41</sup> Véase en el glosario de términos

<sup>42</sup> Véase en el glosario de términos

<sup>43</sup> Véase en el glosario de términos

<sup>44</sup> Véase en el glosario de términos



**Unidad de Control Multipunto (MCU):** es un extremo que proporciona la capacidad para que tres o más terminales y gateways participen en una conferencia multipunto. Una MCU se forma de dos partes: un controlador multipunto (MC) que es obligatorio y un procesador multipunto (MP) opcional. En el caso más simple, una MCU puede estar formada por un MC únicamente.

### **2.1.5.3.2.- SIP**

El protocolo de inicio de sesiones (SIP, Session Initiation Protocol) es un protocolo de control de nivel de aplicación para crear, modificar y terminar sesiones con uno ó varios participantes. Estas sesiones incluyen llamadas de teléfono a través de Internet, distribución de contenidos multimedia y conferencias.

SIP es únicamente un protocolo para introducir en el modelo Internet el nivel de sesión que le falta frente al modelo OSI. En dicho modelo (OSI), el nivel de sesión realiza básicamente cinco funciones:

- Gestión de diálogos.
- Gestión de la sincronización.
- Intercambio de datos.
- Gestión de actividades.
- Notificación de excepciones.

### **Integración con Protocolos IETF**

SIP no es un protocolo integrado verticalmente, puede utilizar otros protocolos estándares para construir las sesiones de una aplicación basada en SIP. Por ejemplo (Véase la figura 2.12):

- TCP/UDP – para transportar la información de señalización.
- TLS<sup>45</sup> – para establecer sesiones seguras.
- DNS – para resolver nombres de servidores de acuerdo a la dirección de destino.
- RSVP, DiffServ - para asegurar la calidad de servicio de la sesión.

---

<sup>45</sup> Véase en el glosario de términos

- RTP – para transportar las comunicaciones interactivas de voz, datos y video.
- RTSP – para controlar el envio de streaming media.
- SAP Session Advertisement Protocol – para publicar sesiones multimedia via multicast.
- SDP Session Description Protocol – para describir sesiones multimedia.
- MIME – Multipurpose Internet Mail Extension – estándar para describir contenido en Internet.
- HTTP – toma parte de la sintaxis y semantica, los mecanismos de autenticación, etc.
- SMTP – reutiliza headers, mecanismos de enrutamiento, modo de direccionamiento, etc.
- COPS – Common Open Policy Service – para establecer políticas de calidad y seguridad.
- OSP – Open Settlement Protocol. – para automatizar el provisioning de los usuarios.
- XML – eXtensible Markup Language – para crear servicios y transmitir información de eventos.

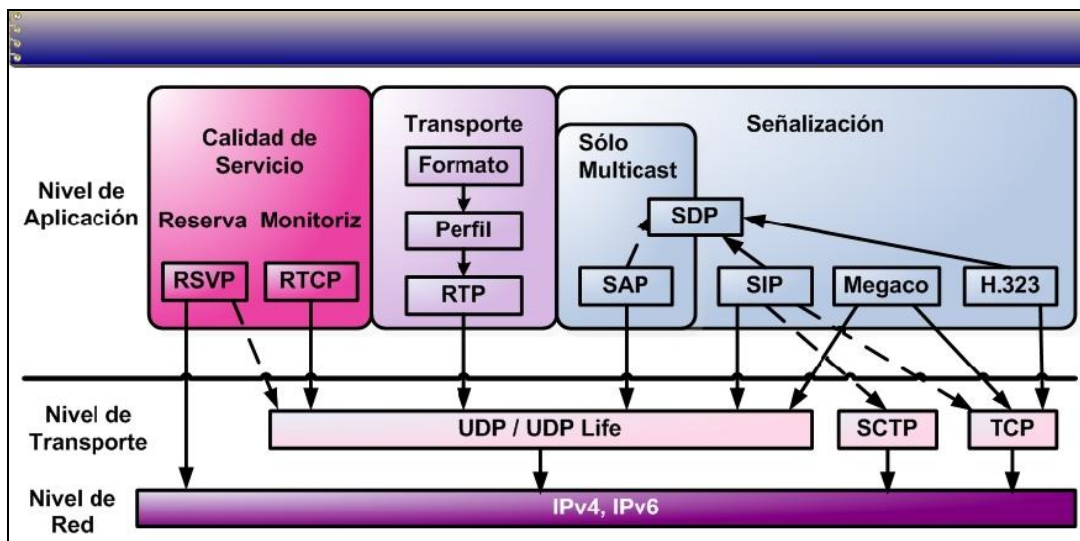


Figura 2.12: Pila de Protocolo SIP según IETF

### 2.1.5.3.2.1. Características

SIP posee a grandes rasgos, características que lo hacen interesante, lo cual está motivando un creciente interés en la industria y en la comunidad tecnológica:

- *Generalidad*: permite acceder a servicios Web transmitiendo SOAP<sup>46</sup> (Simple Object Access Protocol) sobre SIP, lo que proporciona el concepto de 'estado', del que carece HTTP (que es el protocolo tradicional para servicios Web usando SOAP). También se puede realizar una llamada de audio contra otro usuario SIP ó enviar un mensaje de texto junto con una imagen. SIP no especifica la aplicación: toma las funcionalidades de nivel de transporte y proporciona primitivas a los niveles superiores, implementando una capa de sesión genérica.
- *Simplicidad*: SIP pertenece al modelo Internet, y como tal, busca realizar la mayor cantidad posible de operaciones de la forma más sencilla. Por ejemplo, codificando los mensajes en texto plano: aumentará el ancho de banda necesitado para la señalización, pero simplificará el protocolo tanto para su desarrollo como para su depuración.
- *Localización global de usuarios*: comparando con las implementadas por otros sistemas (H.323, ICQ<sup>47</sup> y otros sistemas de señalización y mensajería), SIP es un diseño potente y escalable.
- Establece la comunicación entre dos aplicaciones junto con unas reglas para el diálogo.
- Se trata de un nivel orientado a conexión: establecimiento, transferencia de datos y liberación de sesiones.
- Permite una liberación de las sesiones de forma ordenada, impidiendo la pérdida de datos.
- Suministra primitivas a los niveles superiores (en este caso al de aplicación) para establecer sesiones.

#### **2.1.5.3.2.2. Arquitectura SIP**

SIP se creó como un protocolo de inicio de sesiones, ha ido evolucionando, mediante la definición de nuevas funciones y servicios en forma de módulos complementarios basados en un núcleo de funciones básicas flexibles y ampliables, hasta constituirse en el protocolo de señalización y control propuesto por el IETF como

---

<sup>46</sup> Véase en el glosario de términos

<sup>47</sup> Véase en el glosario de términos

base para los servicios de telefonía y comunicación multimedia en general en Internet, así como el protocolo de señalización de la red telefónica de tercera generación y la base de algunos de los sistemas de mensajería instantánea más extendidos.

SIP es un protocolo de señalización cliente-servidor de nivel de aplicación válido para redes unicast y multicast. Generalmente, los mensajes SIP constan de un conjunto de cabeceras y un cuerpo que contiene descripciones de sesiones multimedia, siendo SDP el formato utilizado en la actualidad.

Puesto que el formato de los mensajes SIP es textual, basado en HTTP y SMTP, y sigue principios similares a los de HTTP, es posible desarrollar servicios SIP mediante los procedimientos extendidos en la Web.

SIP cumple las siguientes funciones: establecimiento, modificación y finalización de sesiones multimedia, registro y localización de participantes, gestión del conjunto de participantes y de los componentes del sistema, así como descripción de las sesiones y negociación de capacidades.

Los tipos de elementos presentes en la arquitectura SIP son (Véase la figura 2.13):

- Puntos Terminales SIP
  - Teléfonos, Gateways, PC.
  - Entiende los protocolos SIP
  - Pueden hacer comunicación directa
  
- Servidores SIP
  - Redirección, Proxy, Movilidad, Presencia, Registra y Localización de Base de Datos.
  
- Agente de usuario
  - AU Cliente (UAC), Inicia la sesión
  - AU Servidor (UAS), Recibe la sesión

- Modelo Peer to Peer<sup>48</sup>
- Pueden ser hallados de diferentes formas
  - IP Configurada, DNS Lookup(proxy)
  - IP Multicast<sup>49</sup> (Registra)

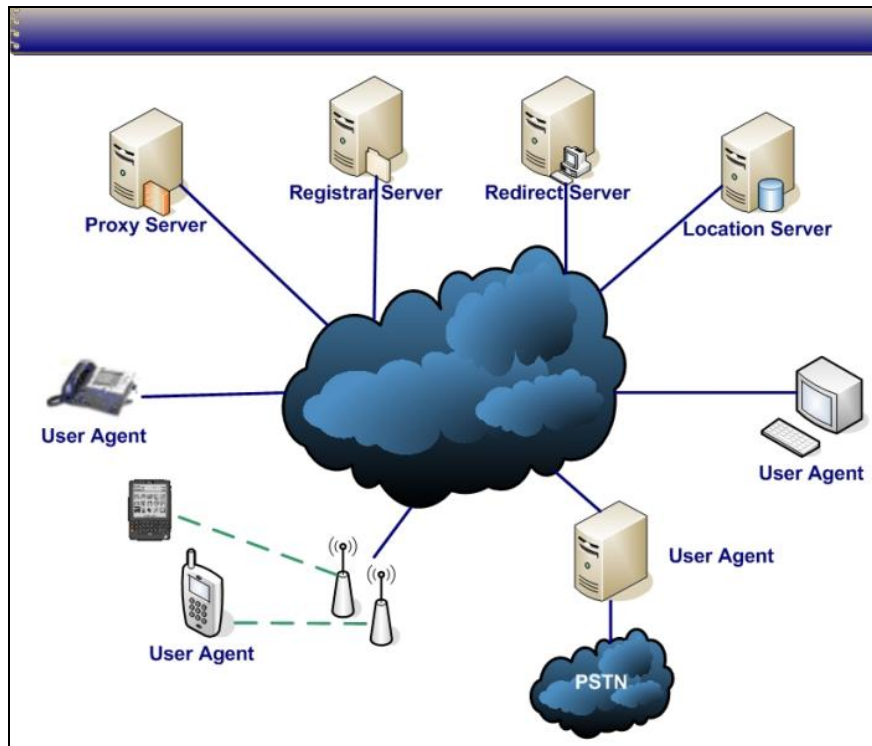


Figura 2.13: Arquitectura SIP

- Los *agentes de usuario (UA)*

Los UA constan a su vez de dos componentes: los *agentes de usuario clientes (UAC)* y los *agentes de usuario servidores (UAS)*. Ambos se encuentran en todos los agentes de usuario, permitiendo la comunicación entre diferentes agentes de usuario mediante peticiones y respuestas de tipo cliente/servidor.

<sup>48</sup> Véase en el glosario de términos

<sup>49</sup> Véase en el glosario de términos

Los UAC tienen como misión el envío de peticiones SIP, mientras que los UAS están encargados de atender tales peticiones y remitir las correspondientes respuestas.

- Los *servidores*.

Las funciones básicas de los servidores SIP son la localización de usuarios y la resolución de nombres. Puesto que generalmente los agentes de usuario clientes no conocen la dirección IP del destinatario de una llamada, sino su nombre de usuario o un número de teléfono al que habrá que acceder a través de un gateway, necesitan enviar en primer lugar un mensaje de invitación al servidor correspondiente al nombre o número para que localice al destinatario. El servidor puede conocer la dirección del destinatario o recurrir a otros servidores para continuar la búsqueda. Cuando las llamadas se redirigen, la ruta seguida se registra en los mensajes SIP, de modo que a la hora de generar respuestas se pueda conocer el camino de retorno hasta el origen del mensaje inicial.

Los servidores SIP actúan generalmente como varios tipos de servidores de forma simultánea. Gracias a una infraestructura de servidores SIP, es posible gestionar las llamadas de forma distribuida entre equipos personales, equipos de proveedores de servicios y pasarelas corporativas, con la consiguiente flexibilidad y control por parte del usuario, que puede mantener la privacidad de sus datos personales en todo momento. Asimismo, un mensaje SIP puede pasar por un número indeterminado de servidores desde que un agente de usuario cliente lo envía hasta que llega al agente de usuario servidor destinatario.

Los tipos de servidores SIP definidos hasta el momento son los siguientes:

- Servidores de registro. El uso más común de estos servidores es registrar un dispositivo después de su arranque, de modo que cuando lleguen invitaciones destinadas a él, los servidores SIP puedan proporcionar su dirección. Se contempla la existencia de un tiempo máximo de validez de cada registro, definible por el servidor, tras el cual se debe renovar el registro. Asimismo, existen mecanismos para cancelar todos los registros contenidos en un servidor.

- Proxys. Su función es similar a la de los proxys HTTP: recibir solicitudes y decidir a qué otro servidor se deben remitir, alterando además algunos campos de la solicitud. Por tanto, actúan como intermediarios en las transacciones que procesan. Normalmente, los proxys actúan como servidores de registro para todos los dispositivos representados por ellos. Para ello, aceptan y procesan peticiones de registro (método REGISTER).

La figura 2.14 esquematiza el funcionamiento de estos servidores. Téngase en cuenta que el elemento al que el proxy reenvía la petición sólo es el agente de usuario servidor destinatario en el caso más simple, pudiendo ser tanto otro servidor proxy como un servidor de redirección.

Asimismo, el proxy puede recurrir a un servidor de localización para determinar la dirección en la que actualmente está disponible el destinatario.

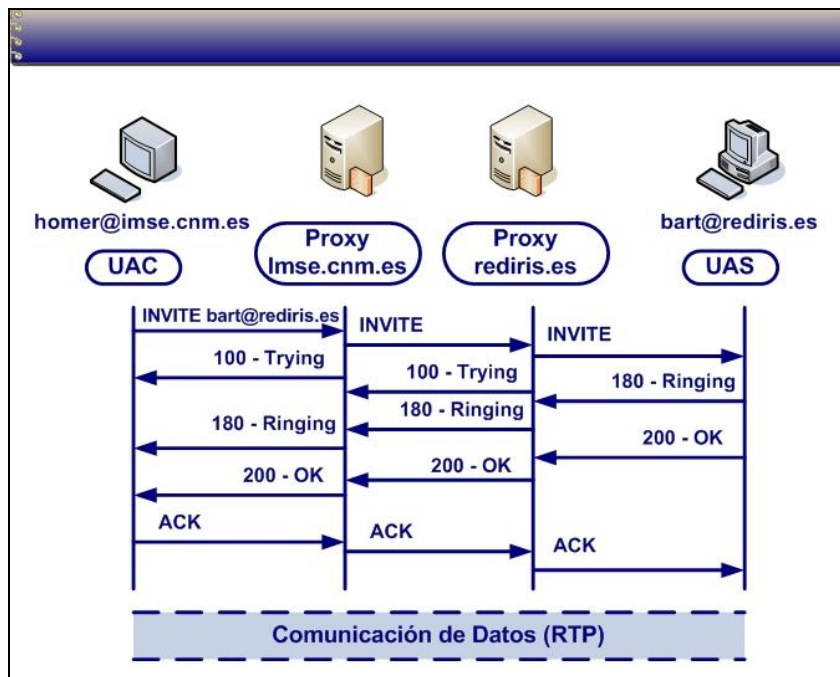


Figura 2.14: Ejemplo de establecimiento de llamada mediante Proxys SIP

Los proxys son, al igual que los proxys HTTP, particularmente útiles como representantes de salida/entrada de y a redes corporativas, proporcionando servicios de búsqueda de direcciones, control de

cortafuegos y gestión de normas de administración corporativas. Asimismo, pueden cumplir funciones de control de salida a pasarelas para redes telefónicas tradicionales.

- Servidores de redirección. A diferencia de los proxys, no inician transacciones, sino que, cuando reciben solicitudes desde un agente de usuario cliente, remiten al mismo agente un mensaje indicando el o los servidores con los que debe ponerse en contacto, en un procedimiento similar al de búsqueda iterativa del sistema DNS. Asimismo, a diferencia de los agentes de usuario servidores, no aceptan llamadas.

Normalmente, los servidores de redirección gestionan mayor número de mensajes que los proxys, pero con menores necesidades de procesamiento. Nótese que, puesto que en sesiones controladas por SIP la redirección se realiza mediante mensajes SIP, las respuestas se pueden generar con flexibilidad y adecuación a servicios de conferencia multimedia, modificándose en función de parámetros tales como la hora del día, el origen o urgencia de la llamada, o cualquier otro criterio específico aplicado por el servidor SIP.

Los servidores pueden mantener el estado de las llamadas a dos niveles de detalle o no mantener estado alguno. Al igual que en la red telefónica convencional, pueden mantener el estado completo de cada llamada; sin embargo, este comportamiento es opcional, puesto que limitaría la escalabilidad de los sistemas SIP.

El modo de funcionamiento recomendado y más frecuente es que los servidores mantengan únicamente el estado de cada transacción por separado. Las transacciones SIP se pueden definir como el conjunto de peticiones y respuestas intercambiadas desde que un agente de usuario cliente envía una petición hasta que recibe una respuesta definitiva originada en el agente de usuario servidor que recibió la petición inicial. Por este motivo, si los servidores sólo mantienen el estado de cada transacción por separado, no tienen conocimiento de las llamadas existentes en un cierto instante. Por tanto, los servidores no tienen que mantener una máquina de estados para cada llamada, constituyendo así un sistema altamente escalable. Asimismo, el comportamiento de los servidores SIP en cuanto al mantenimiento de estados se puede modificar de forma dinámica en función de las circunstancias.



Aunque una llamada básica se puede realizar con SIP sin que intervengan servidores, las funciones avanzadas del protocolo no se pueden llevar a cabo sin su participación.

La interacción entre UAC, UAS y servidores se realiza mediante el intercambio de mensajes SIP cuyo cuerpo contiene generalmente descripciones de sesiones multimedia.

## Mensajes

Los mensajes SIP, solicitudes (métodos) y respuestas (códigos de estado), emplean el formato de mensaje genérico establecido en la RFC 822<sup>50</sup> (Véase la figura 2.15), esto es:

- Una línea de inicio
- Uno o más campos de cabeceras (header)
- Una línea vacía (indica final del campo de cabeceras)
- Cuerpo del mensaje (opcional)



Figura 2.15: Mensaje genérico (RFC 822)

### Solicitudes (Métodos) SIP:

La solicitud tiene la siguiente estructura:

Request-Line \*(general-header | request-header | entity-header) CRLF [message-body]

La línea "Request-Line" tiene la estructura siguiente:

---

<sup>50</sup> Véase en el glosario de términos

*Method SP Request-URI SP SIP-Version CRLF* donde: “SP” es el carácter “espacio” y “CRLF” es la secuencia “retorno del carro” y “nueva línea”.

### **Componentes de la línea “Request-Line”**

**Método (Method):** son seis los métodos básicos definidos en SIP, en su núcleo (RFC 2543<sup>51</sup>), a saber:

- INVITE  
Invita a un usuario, o servicio, a participar en una sesión. El cuerpo del mensaje contiene, generalmente, una descripción de la sesión.
- ACK  
Confirma que el cliente solicitante ha recibido una respuesta final desde un servidor a una solicitud INVITE, reconociendo la respuesta como adecuada. Solo para reconocer solicitudes INVITE, y no otros mensajes de solicitud.
- BYE  
Finaliza una llamada, o una solicitud de llamada. Puede ser enviado por el agente llamante o por el agente llamado.
- CANCEL  
Cancela una solicitud pendiente, pero no afecta una solicitud ya completada. Este método finaliza una solicitud de llamada incompleta.
- OPTIONS  
Posibilita “descubrir” las capacidades del receptor.
- REGISTER  
Se utiliza este método como un servicio de localización que registra la localización actual de un usuario.

Los métodos que no sean soportados por servidores, proxy o de redirección, son tratados por éstos como si se tratase de un método OPTION, y en consecuencia reenviados los métodos que no sean soportados por los servidores UAS o Registrar, provocan el mensaje de respuesta 501, “no implementado”.

De ellos, los cuatro primeros intervienen en el establecimiento de llamadas. El método OPTIONS permite intercambiar información sobre las capacidades de los

---

<sup>51</sup> Véase en el glosario de términos

componentes de un sistema SIP y el método REGISTER es la base para los servicios de localización.

**Request-URI:** es un SIP-URL o un URI (Uniform Resource Identifier).

Indica el usuario o servicio al que la solicitud está siendo dirigida. A diferencia de la cabera “To”, el “Request-URI” puede ser re-escrito por servidores proxy. Típicamente, el UAC establece el “Request-URI” y la cabecera “To” al mismo SIP-URL, pero puede no ser así.

Los servidores proxy o de redirección pueden usar la información en los campos Request- URI y cabeceras de solicitud para manejar la solicitud, y posiblemente re-escribir el Request- URI. Los servidores proxy son responsables del procesamiento del Request-URI.

**SIP-Version:** da cuenta de la versión del protocolo SIP en uso, y se incluye tanto en mensajes de solicitud (métodos) como en mensajes de respuesta (códigos de estado).

Obsérvese los tres campos de cabeceras, que se muestran en la figura 2.16 y 2.17.

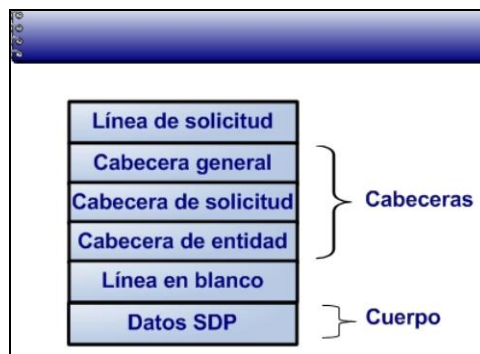


Figura 2.16: Formato general de los mensajes de solicitudes o métodos SIP.

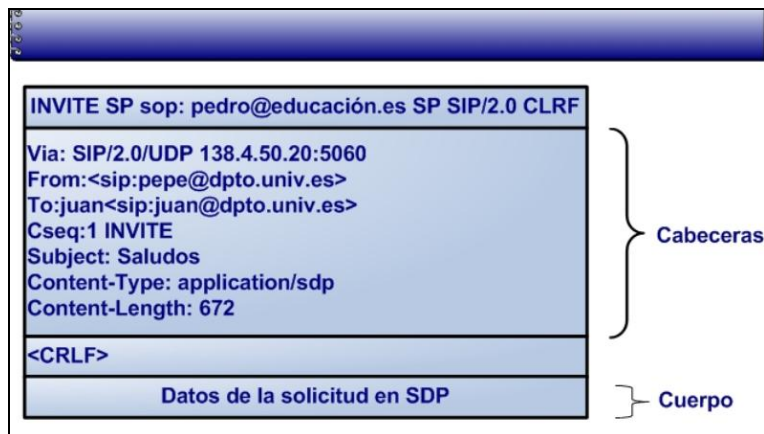


Figura 2.17: Ejemplo de un mensaje de solicitud SIP.

**Respuestas (Códigos de estado) SIP:** Después que se recibe e interpreta un mensaje de solicitud SIP, el receptor del mismo (servidor SIP) responde con un mensaje (o varios) de respuesta (código de estado). El formato de los mensajes de respuesta es como sigue:

Status-Line \*(general-header | response-header | entity-header) CRLF [message-body]

La línea “Status-Line” comprende:

SIP-Version SP Status-Code SP Reason-Phrase CRLF donde: “SP” es el carácter “espacio” y “CRLF” es la secuencia CRLF.

- *SIP-Version*: versión del protocolo SIP.
- *Status-Code*: código de tres enteros para ser interpretado por máquinas. Indica el resultado de comprender y satisfacer o no una solicitud. Hay seis tipos diferentes de Status-Code:
  - 1xx: Informativo. Solicitud recibida, se continua para procesar la solicitud. Por ejemplo, 180, RINGING.
  - 2xx: Solicitud exitosa. La solicitud (acción) fue recibida de forma adecuada, comprendida y aceptada. Por ejemplo, 200, OK.
  - 3xx: Re direccionado. Más acciones deben ser consideradas para completar la solicitud. Por ejemplo, 302, MOVED TEMPORARILY.
  - 4xx: Error de cliente. La solicitud contiene mal la sintaxis o no puede ser resuelta en este servidor. Por ejemplo, 404, NOT FOUND.
  - 5xx: Error de servidor. El servidor ha errado en la resolución de una solicitud aparentemente válida. Por ejemplo, 501, NOT IMPLEMENTED.

- 6xx: Fallo global. La solicitud no puede ser resuelta en servidor alguno. Por ejemplo, 600, BUSY EVERYWHERE.

Los mensajes respuestas 2xx, 3xx, 4xx, 5xx y 6xx son “respuestas finales”, y terminan la transacción SIP. En cambio, los mensajes de respuestas 1xx’s son “respuestas provisionales”, y no terminan la transacción SIP.

- *Reason-Phrase*: explicación textual muy breve del Status-Code, para ser interpretada por humanos.

En la figura 2.18 se muestra el formato general de los mensajes de respuestas SIP. Obsérvese la similitud en cuanto a los campos de cabeceras en relación con los métodos SIP.

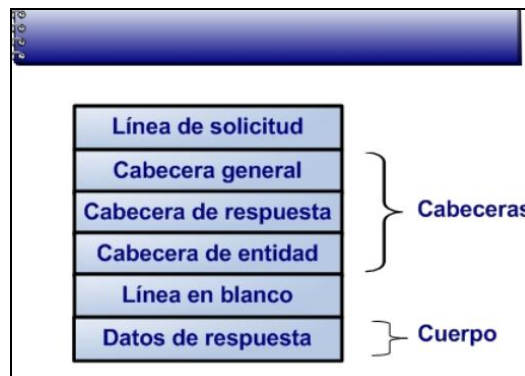


Figura 2.18: Formato general de los mensajes de respuesta SIP.

Por otra parte, la figura 2.19 muestra un ejemplo de mensaje de respuesta SIP correspondiente al código de estado 200, OK.



Figura 2.19: Ejemplo de un mensaje de respuesta SIP.

## Modo de Operación de SIP

Ya antes se planteó que los UAs pueden, por si solos y sin los servidores de red, ser capaces de soportar una comunicación básica, esto es, directamente entre endpoints. Pero también se dejó establecido que la potencialidad de SIP se aprovecha con el empleo de los servidores de red.

Entonces, la señalización SIP puede desarrollarse por intermedio de servidores proxy, o servidores de redirección, a través de los cuales se llevan a efecto las transacciones SIP. De manera muy resumida, la operatividad SIP es la siguiente:

- un UAC emite una solicitud,
- un servidor proxy interviene en la localización de la parte llamada,
- un UAS acepta (o rechaza) la llamada,
- un UAC emite una solicitud,
- un servidor de redirección notifica la dirección de la parte llamada,
- un UAS acepta (o rechaza) la llamada,

Por lo que se requiere la localización de servidores y usuarios SIP, invitaciones SIP, servicios de registro SIP, transacciones SIP, direcciones SIP, etc.

**Direcciones SIP:** los “objetos” direccionados a través del protocolo SIP son usuarios en hosts, que se identifican mediante SIP– URL´s del tipo user@host, donde:

- user: nombre de usuario o número telefónico.

- host: nombre de dominio o dirección numérica de red.

Los SIP- URL's son utilizados en los mensajes SIP para indicar, en relación con una solicitud: origen (from), destino actual (request-URI) y destino final (to). También para especificar direcciones de "redirección".

Por otra parte, los campos de cabeceras SIP pueden no contener SIP-URL's, por ejemplo, en el caso que una llamada desde un teléfono convencional se trasvase por Internet con el empleo del protocolo SIP, entonces la cabecera "from" puede contener un URL telefónico.

**Localización de un servidor SIP:** cuando un cliente SIP desea enviar una solicitud, debe:

- enviar ésta a un servidor proxy configurado localmente, o
- enviar dicha solicitud a la dirección IP y puerto que corresponda, por lo que es evidente que el software cliente debe disponer de una, o de un conjunto de direcciones SIP relativas a servidores SIP.

**Transacciones SIP:** una vez efectuada la localización de un servidor SIP, tienen lugar las transacciones, entendiendo como tal el conjunto de solicitudes (o solicitud) enviadas por el cliente al servidor, y las respuestas (o respuesta) retornadas por éste al cliente. Se trata de solicitudes y respuestas relacionadas, o lo que es lo mismo, con determinados parámetros idénticos (por ejemplo, call-ID, Cseq, to, from).

Si se emplea TCP como protocolo de transporte, la solicitud (o solicitudes) y la respuesta (o respuestas) de una transacción usan la misma conexión TCP. Varias solicitudes desde el mismo cliente y al mismo servidor pueden emplear la misma conexión TCP, o para cada transacción una conexión TCP diferente. Esto es, una conexión TCP puede soportar una o varias transacciones entre un cliente y un servidor.

**Invitaciones SIP:** una invitación SIP consta de dos solicitudes, por tanto corre a cargo de un cliente. Estas parejas de solicitudes son INVITE y ACK, o INVITE y BYE, según el caso.

La solicitud INVITE contiene, generalmente, la descripción de la sesión, descrita con formato SDP. Esta descripción informa a la parte llamada qué tipo de medios el solicitante puede aceptar, y dónde éste desea le sean enviados los datos.

**Localización de usuarios SIP:** dado que el usuario llamado puede desplazarse entre diferentes terminales, con un Servidor de Localización estas localizaciones pueden registrarse dinámicamente. Para esto puede usarse uno de diferentes protocolos, por ejemplo, finger, LDAP<sup>52</sup>, etc.

Un Servidor de Localización puede retornar varias localizaciones, bien porque el usuario esté “loggeado” en diferentes hosts al mismo tiempo, o porque el Servidor de Localización tenga temporalmente información no actualizada.

Con esta información, y según el tipo de servidor SIP, proxy o de redirección, se procede así:

- Servidor de redirección: retorna dicha información de dirección al cliente solicitante, y éste procede a direccionar a la parte llamada.
- Servidor proxy: secuencialmente, o en paralelo, intenta éste direccionar a la parte llamada.

**Servicio de registro SIP:** posibilita que el cliente, mediante una solicitud REGISTER, notifique a un servidor, proxy o de redirección, su ubicación. Ya se ha comentado antes que usualmente en la práctica un servidor de localización o registro acompaña a los servidores proxy y redirección. Nótese que, tanto uno como otro, debe consultar a un servidor de localización para poder desarrollar su tarea.

## Implementación mínima

Una implementación mínima de SIP debe cumplir, en relación con los elementos funcionales clientes y servidores, lo siguiente:

CLIENTES: deben ser capaces de generar las solicitudes INVITE y ACK, así como las cabeceras Call-Id, Content-Length, Content-Type, Cseq, Require, From y To.

---

<sup>52</sup> Véase en el glosario de términos



También deben “entender” el protocolo SDP y ser capaces de reconocer las clases 1 hasta la 6 de los status code.

SERVIDORES: deben “entender” las solicitudes INVITE, ACK, OPTIONS y BYE. De tratarse de servidores proxy, también la solicitud CANCEL...

También deben ser capaces de generar de manera apropiada las cabeceras Call-Id, Content-Lenght, Content-Type, CSeq, Expires, From, Max-Forwards, Require, To y Via.

## **Aplicaciones del protocolo SIP**

La arquitectura que propone SIP, y que se ha perfilado en los apartados anteriores, ofrece muchas posibilidades para el desarrollo de servicios en un entorno convergente. Partiendo de los ingredientes básicos (voz, vídeo y datos) podemos componer infinidad de servicios nuevos de valor añadido para el entorno corporativo, e incluso doméstico; no hay que olvidar que el desarrollo está en manos tanto de los proveedores de servicio como de los departamentos de tecnologías de la informática, o de los propios usuarios finales.

La incorporación de la voz como un servicio vía Web ofrece muchas posibilidades para el comercio electrónico: se puede incluir un servicio de 'click para marcar en un sitio Web para poner en contacto al usuario (que en Internet puede ser el cliente final del banco) con un experto de producto, con una línea de atención al cliente. Se puede pensar en un verdadero centro de contactos Web en el que el cliente pueda contactar con un agente por cualquier medio: voz, correo electrónico, mensajería instantánea (IM), videoconferencia.

En el escenario de convergencia del que se habla, han surgido todo tipo de terminales móviles, con capacidades muy heterogéneas que exigen la disponibilidad de medios que permitan el acceso a servicios asociados al usuario concreto que los demanda, y no a los requisitos propios de cada sistema o plataforma. Una vez más parece que **SIP** se perfila como el candidato perfecto, puesto que permite a los terminales negociar el medio de comunicación y las capacidades y recursos de cada uno. Además los clientes **SIP** son lo suficientemente ligeros como para residir en prácticamente cualquier dispositivo, ya sea un teléfono celular, una agenda portátil digital (PDA), una *notebook* o lo que sea; en una **arquitectura** basada en **SIP** se pueden ofrecer servicios de red inteligente (IN) a un PC de la misma forma que se

hace con un teléfono fijo. Evidentemente a nadie se le escapa que habrá limitaciones relacionadas con el ancho de banda y las dimensiones de las pantallas de los diferentes dispositivos.

Se ha planteado que **SIP** era un candidato; pero es mucho más que eso, puesto que el 3GPP lo ha seleccionado como protocolo de señalización para los sistemas móviles de tercera generación 3G.

La **arquitectura** que propone SIP permite también tener los perfiles de los usuarios en una base de datos centralizada a la que accedan los dispositivos. De esta forma cualquier actualización que se haga en esos perfiles será recogida por el dispositivo que utilicen aquellos en cada caso para el acceso a los servicios.

Precisamente esta capacidad para tener la información de usuario asociada al usuario y no al dispositivo, resulta crucial para las aplicaciones de mensajería unificada; además las similitudes que ya hemos comentado con SMTP y la utilización del DNS hacen que la integración de la voz con el correo electrónico sea prácticamente inmediata.

También podemos pensar en **SIP** para el lanzamiento de servicios asociados a la localización de usuarios móviles. Todas las posibilidades que se han mencionado nos llevan a la integración de todo tipo de comunicación en el “escritorio” del puesto de cada empleado, posibilitando la gestión conjunta de todos los medios de comunicación a disposición de aquellos, con un 'repositorio' único de contactos a mantener. Este aspecto resulta de un interés indudable en el entorno empresarial, puesto que redundará de forma directa en el incremento de la productividad de los empleados, permitiendo el despliegue de servicios de valor añadido como cualquier otro servicio sobre una **arquitectura** SIP apoyada en una red IP multiservicio.

## **QoS del SIP**

- SIP no asegura el cumplimiento de la QoS.
- SIP pretende asegurar que los recursos estén disponibles antes de establecer la comunicación.

### 2.1.5.3.3.- MGCP

MGCP es un protocolo de control de Media Gateway definido por la IETF (RFC 2705<sup>53</sup>) para su uso en ambientes de conmutación distribuidos. En estos ambientes, la lógica de la señalización está localizada en el Controlador de Gateways de Media (MGC) también conocidos como Softswitches y la lógica de media en los Media Gateways (MG). Usando MGCP, los MGC pueden controlar los MG para la inicialización de caminos de media a través de redes distribuidas, por lo que es un protocolo que define una arquitectura de control centralizada para la creación de aplicaciones multimedia incluyendo VoIP.

La pasarela de medio es, típicamente, un elemento de la red que proporciona la conversión entre señal de audio de un teléfono conmutado por circuito y la señal de paquete que se puede transportar a través de Internet o sobre la red de conmutación de paquete como ATM y Frame Relay.

Los Gateways de los medios de comunicación pueden ser:

- Trunking gateways: Interfaz entre la red telefónica y la red de Voz sobre IP.
- Voice over ATM gateways: Es igual al Trunking gateways pero que es para interfaz de red ATM.
- Residencial gateways: Proporcionan una interfaz (RJ11) a una de Voz sobre IP.
- Access gateways: Proporcionan una interfaz desde PBX digitales en una red de Voz sobre IP.
- Business gateways: Proporcionan una interfaz de PBX digital tradicional o un PBX a una red de Voz sobre IP.

Los Servidores de Acceso a red pueden ser conectados a través de un módem a una red telefónica de circuito y pueden proporcionar el acceso a Internet. Se espera que, en el futuro, las mismas pasarelas combinaran servicio de VoIP y servicios de Acceso a Red. Además, la Conmutación por circuito o paquete puede ofrecer una interfaz de control a elementos de control externo.

---

<sup>53</sup> Véase en el glosario de términos

El protocolo MGCP presenta una arquitectura de control de llamada donde la “inteligencia” está fuera de las pasarelas y es manejado por elementos de control de llamada externos, conocidos como Agentes de Llamada.

El MGCP presupone que estos elementos del control de llamada, o Agentes de Llamada, se sincronizan entre sí para enviar órdenes coherentes y respuesta a las pasarelas. Si esta suposición se viola, debe esperarse una conducta incoherente. No define un mecanismo para sincronizar a los Agentes de Llamada.

Para la implementación de una buena señalización de la llamada, el Agente de Llamada debe guardar huella del estado del Equipo Terminal, y la entrada debe asegurarse que se notifiquen los eventos apropiadamente al Agente de Llamada. Las condiciones especiales existen cuando la entrada o el Agente de Llamada se reinician. La entrada debe remitirse a un nuevo Agente de Llamada durante los procedimientos de “fallas”, el mismo debe tomar la acción cuando la entrada se desconecta, o hay que reiniciar.

Los mensajes MGCP viajan sobre UDP, por la misma red de transporte IP. El formato de trabajo genera una inteligencia externa a la red (concentrada en el MGC) y donde la red de conmutación está formada por los router de la red IP. El gateway solo realiza funciones de conversión vocal (analógica o de velocidad digital) y genera un camino RTP entre extremos. La sesión de MGCP puede ser punto-a-punto o multipunto. MGCP entrega al gateway la dirección IP, el puerto UDP y los perfiles de RTP; siguiendo los lineamientos del Protocolo de Descripción de Sección (SDP).

Los comandos disponibles en MGCP son los siguientes:

- **NotificationsRequest**, indica al gateway de eventos como puede ser la señalización DTMF en el extremo.
- **Notification Command**, confirma las acciones del comando NotificationsRequest.
- **CreateConnection**, usado para crear una conexión que se inicia en el gateway.
- **ModifyConnection**, usado para cambiar los parámetros de la conexión existente.
- **DeleteConnection**, usado para cancelar la conexión existente.
- **AuditEndpoint**, usado para requerir el estado del extremo al gateway.

- **AuditConnection**, usado para requerir el estado de la conexión.
- **RestartInProgress**, usado por el gateway para notificar que un grupo de conexiones se encuentran en falla o reinicio.
- **EndpointConfiguration**, usado para indicar al gateway las características de codificación esperadas en el extremo final.

#### **2.1.5.3.4.- MEGACO**

H.248, también conocido como MEGACO (Media Gateway Control protocol ), es el resultado de la cooperación entre la UIT (Unión Internacional de Telecomunicaciones) y la IETF (Internet Engineering Task Force) y se podría contemplar como un protocolo complementario a los dos anteriores.

MEGACO/H.248 especifica los procedimientos que se deben seguir para llevar a cabo la comunicación entre la pasarela física y su controlador. Se trata de una evolución de MGCP (Media Gateway Control Protocol), que ya está empezando a ser soportado por bastantes equipos.

El modelo MEGACO tiene los siguientes elementos funcionales (Véase la figura 2.20):

- Pasarelas de medios (MG, Media Gateway).
- Controlador de las pasarelas de medios (MGC, Media Gateway Controller), también llamado Call Agent (CA).
- Endpoints (físicos y virtuales).
- Protocolo MGCP.

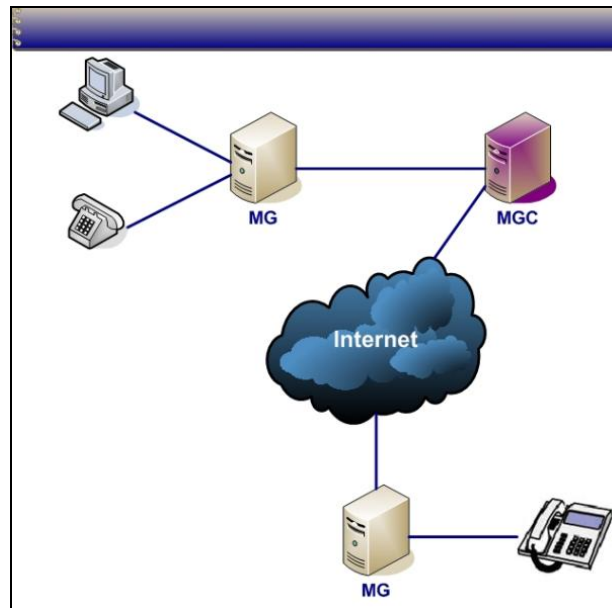


Figura 2:20: Red MEGACO

**Media Gateway:** recibe los streams de medios desde un origen no IP, paquetiza los datos y los entrega a la red de paquetes IP. Realiza la operación inversa cuando los streams de medios fluyen desde la red IP.

Según su función específica o su ubicación, los media gateways se pueden clasificar en:

- MG's residenciales (entre telefonos y red IP)
- MG's troncales (entre redes PSTN y red IP)
- MG's de acceso (entre PBX's y red IP).

**Media Gateway Controller:** controla el registro y control de recursos de los MG's pudiendo incluso disponer de la capacidad para autorizar el uso de estos recursos bajo cierta política.

El MGC puede actuar como punto de origen y terminación para protocolos de red de circuitos conmutados SCN (ISUP/SS7, Q.931/DSS1). Casi toda la "inteligencia" recae en los MGC's y una pequeña parte en los G's. Por lo tanto es adecuado cuando los terminales disponen de poca inteligencia como son los teléfonos convencionales.

El modelo MEGACO está basado en el modelo Maestro-Esclavo, donde los MGC's y los MG's dialogan a base del protocolo MGCP. Todo el control de la llamada

está soportado en el MGC (elemento central de control) y los MG's son los elementos funcionales que median entre las redes IP y los terminales y otras redes. Por lo tanto, si bien los MG's realizan un control muy limitado de la llamada bajo el mando del MGC, a su vez se transfieren las señales de medios, es decir, la información de usuario, de manera que le son comunes funciones tales como el cambio del formato de los datos.

**Endpoints:** Los endpoints son las fuentes y los sumideros de la información de usuario.

Hay dos tipos de endpoints:

- 1) Físicos: enlace troncal, teléfono...etc.
- 2) Virtuales: módulo software sobre un endpoint físico.

La conexión entre endpoints (teléfonos...etc.), a través de las redes IP se desarrolla bajo el control de los MGC y el MG que corresponda. Toda la información generada por los endpoints se maneja por el MGC, aunque el gateway puede desarrollar también este tipo de tareas.

La especificación define un modelo de conexión encargado de describir las entidades lógicas dentro del MG que pueden ser controladas por un MGC. Maneja dos abstracciones:

- Terminación: Es la fuente o sumidero de uno o más flujos. Hace referencia a una conexión.
- Contexto: es la asociación existente entre un número de terminaciones, que permite describir la topología (quién escucha a quién) y la mezcla de flujos y/o parámetros de conmutación en el caso de que haya más de dos terminaciones involucradas en la comunicación. Por ejemplo, en una llamada bidireccional existirá un contexto con dos terminaciones, una por cada extremo de la misma.

Las terminaciones se caracterizan por una serie de propiedades, plasmadas en descriptores que especifican parámetros como el tipo de codificador empleado o las características de los flujos de información intercambiados. También se encargan de detectar eventos en la línea de los clientes, como el hecho de que un usuario haya descolgado su teléfono para realizar una llamada o marcado el número del destino con

el que quiere establecer una comunicación, para después mandar el mensaje de notificación correspondiente al controlador, de manera que éste pueda obrar en consecuencia.

El MGC emplea una serie de comandos, incluidos en los mensajes intercambiados con la pasarela física, para manipular los contextos y las terminaciones. De esta manera se permite realizar la gestión de las conexiones, pudiendo crear nuevas terminaciones o modificar los valores de las propiedades de las existentes.

MEGACO/H.248 no sólo es compatible con H.323 y SIP, sino que además presenta funcionalidades complementarias. Así, mediante el uso del protocolo MEGACO/H.248 se puede realizar el control de la red y la provisión de algunos servicios, aunque bastante básicos. Sin embargo, desde el momento en que se pretendan ofrecer servicios más avanzados, se requiere el empleo de un protocolo con un mayor número de funcionalidades para este propósito, como SIP.

#### **2.1.5.3.5.- Comparación de Protocolos**

Se puede comparar H.323, SIP y MGCP/MEGACO para resolver un mismo problema de diversas formas de acuerdo a las necesidades de la empresa y brindar múltiples servicios. Estos emplean el protocolo RTP para el transporte de medios (audio y vídeo) pero en lo que se diferencian es en cómo desarrollan la señalización y el control de llamadas.

El entorno MEGACO se relaciona con H323 y SIP por medio del módulo MGC con los interfaces correspondientes.

En el caso del vínculo entre H.323 y SIP, éste se logra por intermedio del gateway H.323-SIP que se ocupa del mapping de señalización.

Por lo tanto, es posible la comunicación entre terminales de los tres entornos. (Véase la figura 2.21).



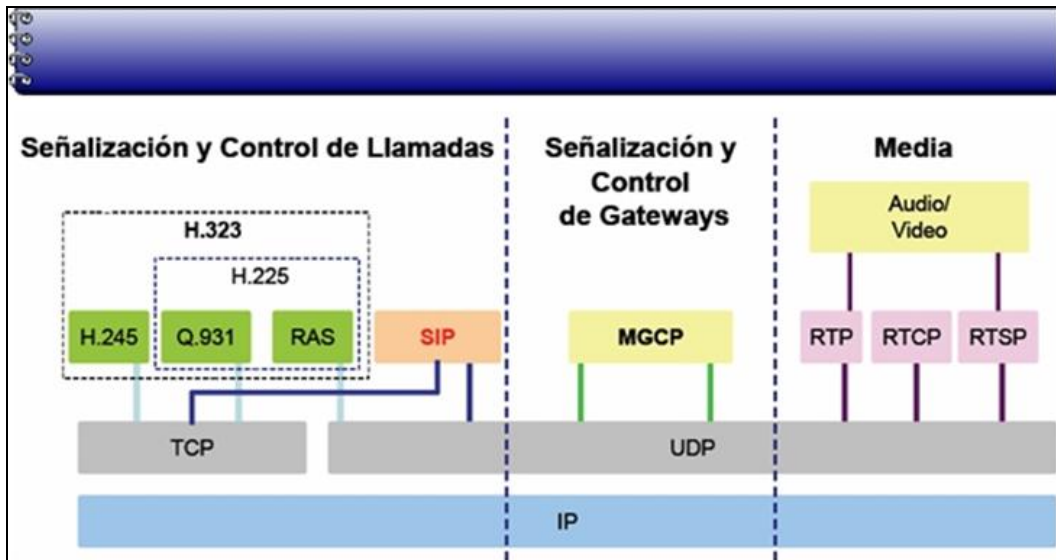


Figura 2.21: Comparación de Protocolos

- H.323 Version 1 y 2 soporta H.245 sobre TCP, Q.931 sobre TCP y RAS sobre UDP.
- H.323 Version 3 y 4 soporta H.245 sobre UDP/TCP y Q.931 sobre UDP/TCP y RAS sobre UDP.
- SIP soporta TCP y UDP.

En la tabla 2.6 se proporciona una comparación de las características entre los protocolos mencionados.

Tabla 2.6: Características de protocolos

	H.323	SIP	MGCP/MEGACO
<b>Complejidad</b>	Alto	Bajo	Alto
<b>Nuevos Servicios de Renta</b>	No	Si	No
<b>Interconexión con Internet</b>	No	Si	No
<b>Compatibilidad SS7</b>	Bajo	Bajo	Medio
<b>Costo</b>	Alto	Bajo	Medio
<b>Codificación</b>	Binaria (ASN.1)	Textual (SigComp)	
<b>Formatos</b>	Serie G.xxx y H.xxx, MPEG, GSM	Tipos MIME –IANA	
<b>Ampliabilidad</b>	Campos reservados	Métodos, cabeceras	Agentes de llamada
<b>Autenticación</b>	H.235 (puede usar TLS)	Análogo a HTTP	
<b>Localización</b>	GateKeeper (Puede usar DNS)	DNS	Gateways
<b>Transporte</b>	TCP, UDP	TCP, UDP, SCTP, DCCP	UDP
<b>Escalabilidad</b>	Compleja y limitada	Mayor escalabilidad	Moderado
<b>Mensajes</b>	Complejo (muchos mensajes codificados en binario)	Sencillo (pocos mensajes de texto)	
<b>Mecanismos de Seguridad y Gestión</b>	Implementación y mecanismos de seguridad y gestión complicados	Mecanismos sencillos de seguridad y gestión y fácil implementación	
<b>Servicios</b>	Complicado desarrollo de servicios	Fácil desarrollo de servicios	
<b>Arquitectura</b>	Arquitectura maestro/esclavo	Arquitectura cliente/servidor	Arquitectura maestro/esclavo

### 2.1.5.3.5.1. Características

- En la **codificación y formatos** se refiere al método de encapsulación que utiliza cada protocolo y al tipo de formato que se utiliza durante una llamada.
- Los **servicios** se refiere a los agentes o aplicaciones como desvío de llamadas, transferencia de sesiones de video conferencia y a las infinitas posibilidades de desarrollo de servicios de los protocolos.
- La **compatibilidad SS7** se refiere al estándar global para telecomunicaciones SS7 que se utiliza para establecer, enrutar, facturar y controlar llamadas, tanto a terminales fijos como móviles.

- En los **mecanismos de seguridad** podemos encontrar los diferentes servicios que provee, que en la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son Intercambio de autenticación, Cifrado, Integridad de datos, Firma digital, Control de acceso, Tráfico de relleno, Control de encaminamiento, Intercambio de autenticación.
- En la **interconexión con Internet** se refiere a la utilización de los protocolos de Internet y a la realización de llamadas en Internet, conferencias multimedia sobre cualquier red IP.
- La **escalabilidad y flexibilidad** se refiere al Soporte para un gran número de dominios (direcciones de área global, localización del usuario), la habilidad para manejar gran número de llamadas y el límite en el número de integrantes en multiconferencias, entre otras.
- Los **nuevos servicios de renta** se refiere a las facilidades básicas como: control por aplicaciones externas, colaboración Web, videoconferencias, picture ID, mensajes instantáneos, etc.
- La **complejidad** se refiere a la medida que se aumenta nuevas aplicaciones y la integración de componentes de varios fabricantes.
- La **arquitectura** se refiere a la manera natural en la que se adapta a un ambiente de colaboración ya que permite el uso de varios tipos de datos, aplicaciones, multimedia, etc, con una o más personas.
- La **ampliabilidad** se refiere al método que utiliza cada protocolo para realizar el envío de llamadas.

Analizando las características de la tabla podemos decir que SIP define mecanismos de señalización para establecer y terminar llamadas, así como otras funciones de control de conferencia, negociación de capacidades y servicios adicionales sobre redes de conmutación de paquetes.

SIP se ha diseñado con posterioridad con la intención de que presente dos ventajas frente a H.323:

- Mayor flexibilidad para incorporar nuevas funciones.
- Implementación más fácil de realizar y depurar.

Mientras que SIP es un protocolo ligero similar a otros desarrollados previamente por el IETF y de amplia extensión, como HTTP, H.323 sigue un esquema similar al sistema tradicional de conmutación de circuitos, basándose en la

señalización de la red digital de servicios integrados, ISDN, y otras recomendaciones de la serie H.

Las arquitecturas en las que se basan H.323 y SIP son sustancialmente distintas; sin embargo, al comparar la evolución de ambos estándares durante los últimos años, se llega a la conclusión de que, a medida que se definen nuevas ampliaciones a SIP, aparecen nuevas versiones de H.323 y cada vez se diferencian menos en cuanto a las funciones y posibilidades que ofrecen.

La arquitectura de SIP y H.323 deben tener en cuenta las siguientes características:

- Escalabilidad hasta un gran número de usuarios de todo el mundo así como un gran número de llamadas activas de forma simultánea, del orden de millones.
- Permitir gestionar la red, de modo que sea posible aplicar políticas de control y tarificación.
- Proporcionar métodos de selección de calidad de servicio.
- Interoperabilidad entre diferentes fabricantes, protocolos y versiones de protocolos.
- Facilidad de ampliación.

#### **2.1.5.3.5.2. Ventajas y Desventajas**

- Escalabilidad: SIP no es tan complejo como H.323, ya que la señalización de SIP puede ser procesada más rápidamente y, por tanto, soportar un mayor número de llamadas simultáneas.
- Movilidad: Cada usuario puede ser localizado en un conjunto de direcciones diferentes.
- Simplicidad: Mensajes estilo HTTP.
  - Simplicidad de las herramientas de desarrollo.
  - Facilidad de depuración: desarrollos más rápidos.
- SIP utiliza analizadores y generadores de mensajes mediante scripts en lenguajes como Perl o Tcl, facilitando su integración con los entornos Web; en

cambio, H.323 requiere generalmente el uso de herramientas de generación de analizadores para sintaxis ASN.

- SIP ha optado por prescindir de muchas de las opciones contempladas en H.323, ya que añaden complejidad sin aportar ventajas, y son en algunos casos redundantes.
- La ampliabilidad dentro de los protocolos de sesiones multimedia, es un factor clave para el éxito; por lo que al regular servicios de uso muy extendido, están sujetos a futuras necesidades de ampliación procedentes de muy diversas fuentes y campos, al mismo tiempo es trascendental que los dispositivos diseñados para distintas versiones y por distintos fabricantes sean compatibles entre sí en la ejecución de un conjunto mínimo de funciones.
- SIP emplea de forma estandarizada cualquier formato multimedia registrado a través de la IANA; en cambio, H.323 sólo puede emplear formatos registrados a través de una entidad central, la ITU-T, que hasta el presente sólo ha estandarizado formatos promovidos por la propia entidad, la mayoría de los cuales son de uso limitado por problemas de patentes.
- SIP no requiere mantener estados en elementos intermedios y utiliza fundamentalmente conexiones UDP o de otros protocolos que requieren menos recursos que TCP, como SCTP; por el contrario, H.323 requiere que los elementos intermedios mantengan el estado a lo largo de toda la sesión, y sólo emplea UDP a partir de la versión 3, debiendo mantener la compatibilidad con versiones previas plenamente basadas en conexiones TCP.
- Para establecer una llamada, SIP sólo requiere un intervalo de ida y vuelta de paquetes en el caso más común, puesto que se realiza mediante un mensaje transportado generalmente sobre UDP; en cambio, H.323 versiones 1 o 2 requiere establecer, previamente a la conexión H.323, conexiones TCP para H.225.0 y H.245. Por lo tanto el establecimiento de llamadas es aún así normalmente más rápido con SIP.
- H.323 especifica servicios, mientras que SIP es sólo un protocolo de señalización para dar base a servicios.
- H.323 engloba un amplio conjunto de protocolos de implementación obligatoria.

### **2.1.5.3.5.3. Conclusión**

En una leve comparación, llegamos a la conclusión que los tres protocolos son buenos, sin embargo H.323 por ahora tiene un mercado más compartido, pero SIP es

mejor protocolo, debido a su arquitectura modular de los protocolos desarrollados para aplicaciones multimedia como servicios Web, mecanismos de gestión y seguridad más sencillos de implementar como Intercambio de Autenticación y lo más importante que entrega flexibilidad, simplicidad, escalabilidad y la posibilidad de encontrar combinaciones entre ellos para entregar nuevos servicios y cubrir las necesidades de la ESPE.

## Capítulo III: Análisis y Diseño de la infraestructura de la ESPE y las Sedes para comunicaciones de VoIP

### 3.1.- Situación Actual

Actualmente, la Escuela Politécnica del Ejército tiene su matriz ubicada en Sangolquí, (Véase la figura 3.1) la misma que cuenta con 5 sedes: Idiomas, Latacunga, Héroes del Cenepa, IASA I y IASA II (Santo Domingo). Internamente la comunicación se realiza mediante redes de área local (LAN) y redes inalámbricas (WLAN) y externamente a través de redes de área extendida (WAN).



Figura 3.1: ESPE – Sangolquí

A continuación, se describe las centrales que utiliza cada una de las sedes:

- **ESPE – Sangolquí**

El modelo de la red que actualmente esta en el campus Sangolquí consiste en una red de datos y en un sistema de telefonía IP para las comunicaciones de voz.

Actualmente, el campus Sangolquí, ha adquirido un central telefónica de Voz sobre IP, 3Com NBX V5000, que es escalable para soportar 1500 dispositivos por localización (incluyendo 720 líneas PSTN); es decir, que con las 86 líneas que cuenta la ESPE se puede colocar 1414 dispositivos de su capacidad total. (Véase la figura 3.2)



Figura 3.2: Central VoIP

- **ESPE – Latacunga**

La ESPE Latacunga, tiene una central Panasonic KX-TA 308 con 3 líneas directas y 8 extensiones.

- **ESPE – Idiomas**

El Instituto de Idiomas, cuenta con una central Panasonic KX-TA 308, pero con una tarjeta adicional, es decir, con 4 líneas directas y 16 extensiones.



- **IASA I**

El Instituto Agropecuario San Antonio I, tiene una central Panasonic KX-TDA 100 BX y cuenta con un módulo adicional, es decir, con 3 líneas directas y 16 extensiones.

- **IASA II**

El Instituto Agropecuario San Antonio II, tiene una central Panasonic KX-TA 308 con 3 líneas directas y 8 extensiones en Zoila luz y en San Antonio no cuentan con una central telefónica sólo hay dos líneas directas con las que se comunican.

- **Héroes del Cenepa**

La Escuela de Ciencias Tecnológicas Héroes del Cenepa posee una central Panasonic KX-TA 308 con 32 extensiones.

Asimismo, el campus Sangolquí es el que provee el servicio de Internet, canal de datos por el cual se corren aplicaciones como correo, web, base de datos, FTP, etc. a las demás sedes; para lo cual cada sede utiliza los siguientes equipos:

Tabla 3.1: Equipos ESPE – Sangolquí

Equipo	Cantidad	Descripción
Router	2	Cisco 1700 y 2600
Firewall	1	Cisco Secure PIX 525
Switch CORE	1	3COM 4050 3C17708 (48 puertos)
Switch	3	3COM Super Stack 3 4250T 3C17302 (48 puertos)
Sistema de Almacenamiento	1	Sun 6130
Servidor Financiero	1	HP Netserver LH 6000
Active Directory	1	HP Netserver LC 2000
Servidor Web	1	Sun Fire V890
Servidor de Correo	1	DELL PowerEdge 6400
Servidor de Base de Datos	1	Sun Fire V890
Servidor DNS	1	IBM Netfinity 3500
Servidor DHCP	1	Compac Proliant ML 370

Tabla 3.2: Equipos ESPE – Latacunga

Equipo	Cantidad	Descripción
Router	1	Cisco 1700
Firewall	1	Check Point
Switch	1	3COM (48 puertos)
Servidor	1	Mail (Sendmail), Web

Tabla 3.3: Equipos ESPE – Idiomas

Equipo	Cantidad	Descripción
Router	1	Cisco 1700
Firewall	1	Red Hat Linux 7.5
Switch	1	IBM (26 puertos)
Switch	1	DLINK (24 puertos)
Switch	1	Cisco Catalyst 2950 (24 puertos)
Servidor	1	DELL (Base de Datos)

Tabla 3.4: Equipos ESPE – IASA II

Equipo	Cantidad	Descripción
Router	1	Cisco 1700
Firewall	1	Red Hat Linux 9.0
Switch	1	3COM (24 puertos)

Tabla 3.5: Equipos ESPE – IASA I

Equipo	Cantidad	Descripción
Radio Modem	1	Aix Mux - IDU
Firewall	1	Red Hat Linux 9.0
Switch	1	3COM (24 puertos)
Switch	1	3COM (48 puertos)

Tabla 3.6: Equipos ESPE – Héroes del Cenepa

Equipo	Cantidad	Descripción
Router	1	Cisco 1700
Firewall	1	HP 370 (24 puertos)
Switch	3	3COM (24 puertos)

### 3.1.1.-Análisis de la Red Área Local de la ESPE - Sangolquí

En la actualidad, la red interna de la ESPE tiene una topología tipo estrella con un Backbone de fibra óptica Gigabit Ethernet y cableado UTP dentro de los edificios, la misma que comunica a todos los departamentos y facultades; excepto en la sección de talleres la cual se enlaza a través de una red inalámbrica. Adicionalmente se dispone de Wireless en un 30% aproximadamente en el campus Sangolquí. En la figura 3.3 se muestra la distribución de la red área local e inalámbrica del campus Sangolquí.

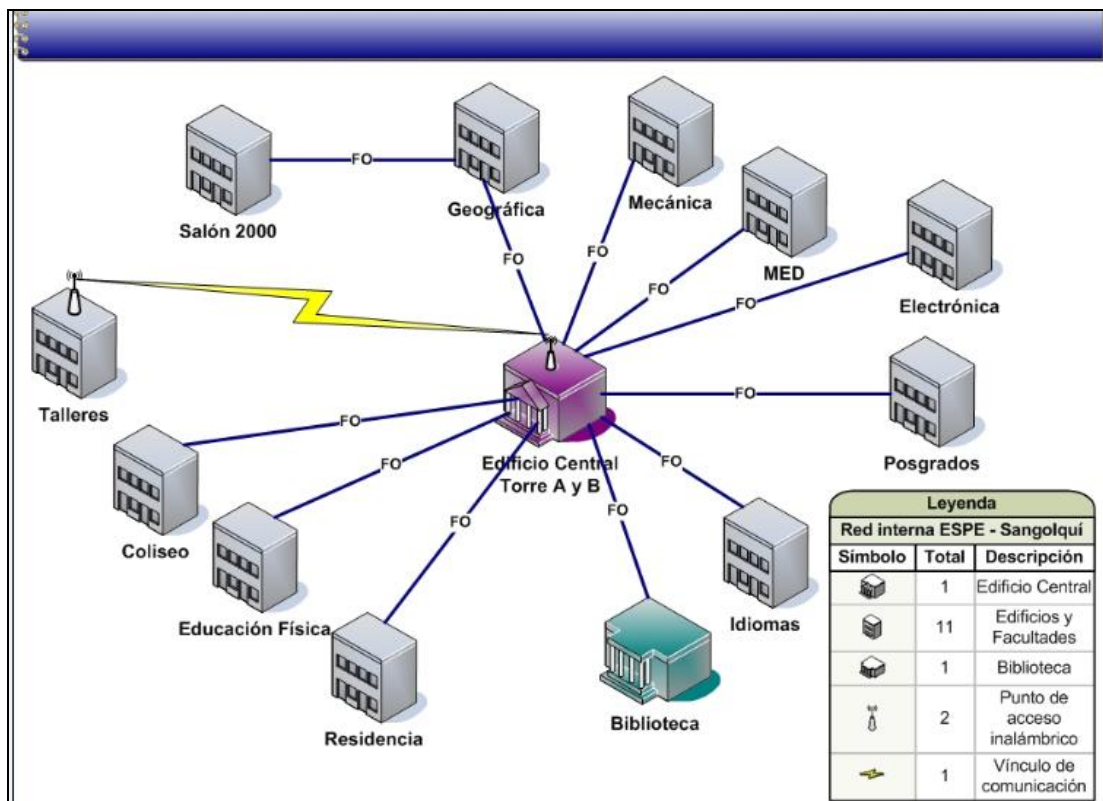


Figura 3.3: Ubicación de las redes en el campus ESPE – Sangolquí

### 3.1.2.-Análisis de la Red de Área Extendida de la ESPE y sus Sedes

Los canales de datos del campus Sangolquí con las sedes esta basada en una tecnología en HDSL<sup>54</sup>, cuyo proveedor es Andinatos. En las siguientes tablas se presenta el crecimiento que ha ido obteniendo año ha año el ancho de banda, para mejorar los diferentes servicios que brinda a los usuarios.

Tabla 3.7: Enlace WAN en el año 2001

SEDE	Ancho de Banda
Idiomas	64 kbps
Latacunga	64 kbps
Héroes del Cenepa	64 kbps
IASA I	64 kbps
IASA II	Conexión Dial-up

Tabla 3.8: Enlace WAN en el año 2002 – 2003

SEDE	Ancho de Banda
Idiomas	128 kbps
Latacunga	128 kbps
Héroes del Cenepa	128 kbps
IASA I	64 kbps
IASA II	Conexión Dial-up

Tabla 3.9: Enlace WAN en el año 2004

SEDE	Ancho de Banda
Idiomas	192 kbps
Latacunga	384 kbps
Héroes del Cenepa	128 kbps
IASA I	192 kbps
IASA II	64 kbps

---

<sup>54</sup> Véase en el glosario de términos

Tabla 3.10: Enlace WAN en el año 2005


## SEDE

Para realizar la conexión a los canales de datos, el campus Sangolquí se conecta a través de un router Cisco 1700 cuyo proveedor es Andinadatos. Para brindar el servicio de Internet se realiza una conexión al router Cisco 2600 provisto por la empresa IMPSAT, quien es el proveedor del enlace de 4Mbps de Latacunga ESPE (Véase la figura 3.4). Además, cuenta con dos enlaces adicionales independientes; uno para los laboratorios especializados de 512 Kbps (Véase la figura 3.5) y uno de 512Mbps de Internet II del proyecto Cedia proveído por TELCONET (Véase la figura 3.6).

## IASA I

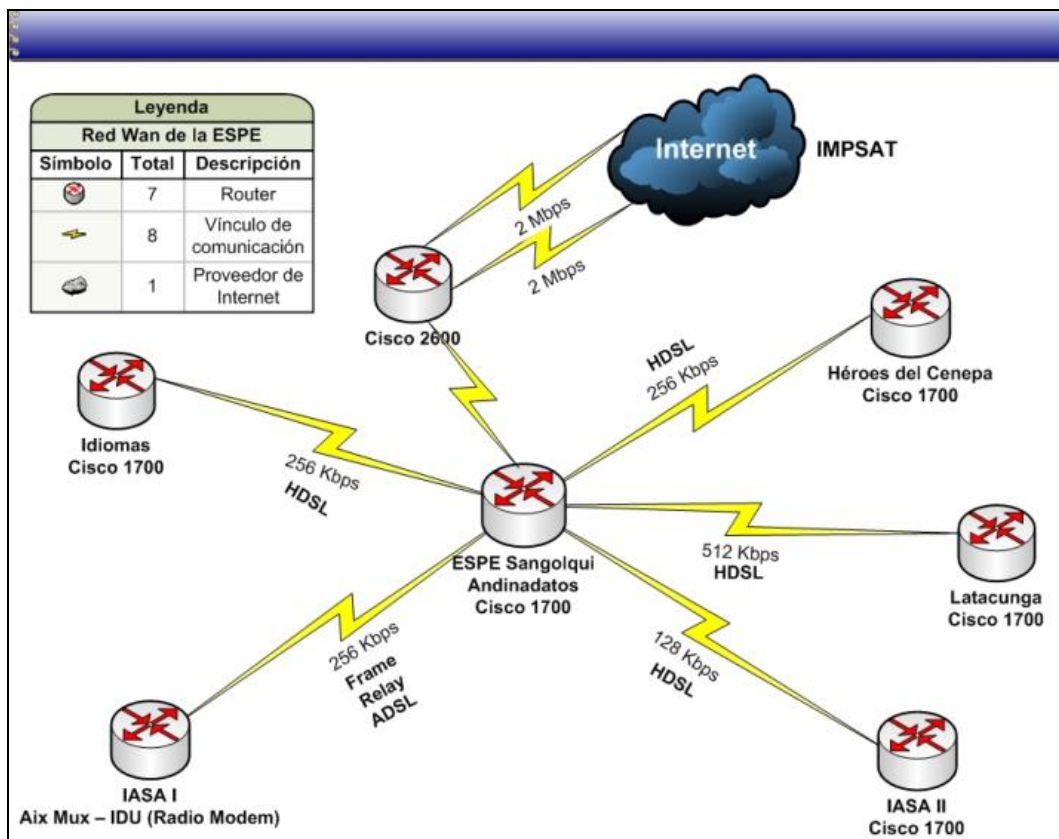


Figura 3.4: Gráfico de los enlaces WAN de la ESPE y sus Sedes

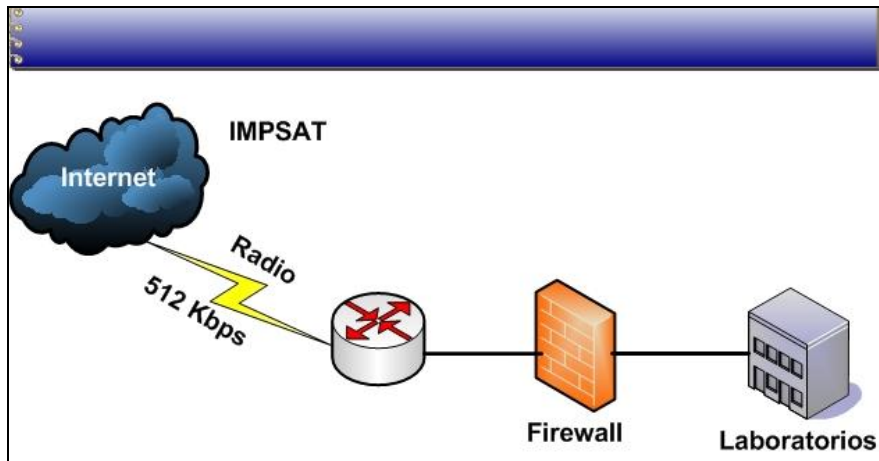


Figura 3.5: Laboratorios Especializados

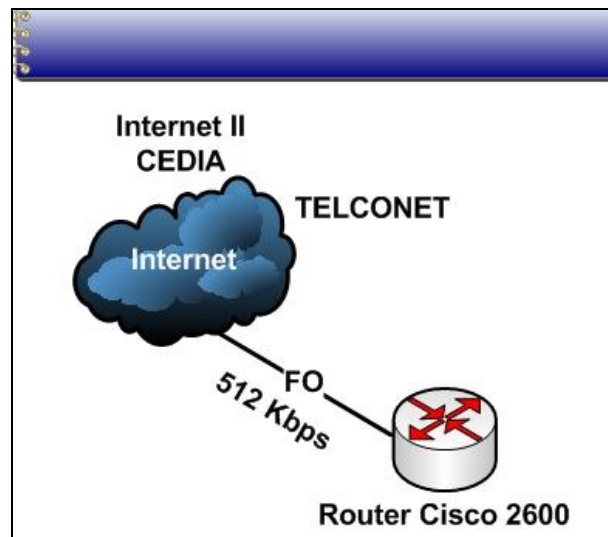


Figura 3.6: Internet II proyecto Cedia

### 3.2.- Requerimientos del enlace de la ESPE y sus Sedes

La telefonía IP aparece cada vez con mayor frecuencia, buscando herramientas que le permitan ser más rentables y le ayuden a los usuarios de la ESPE a aumentar su productividad. En especial si se tienen grandes necesidades telefónicas, es interesante integrar las comunicaciones en una sola red, económica y flexible. Hoy, la tendencia señala que en una sola red pueden transmitirse estos dos contenidos, además de video.

Una de las ventajas de voz sobre IP frente a la tradicional, es que es más barata. Como las llamadas se realizan usando una red de datos como Internet, la reducción en costos puede ser grande, especialmente para todas las sedes de la ESPE que se encuentran en diferentes ciudades, debido al ahorro en tarifas de larga distancia. Cerca del 13 por ciento de todas las llamadas de larga distancia del mundo ya se realizan mediante redes IP. Para transmitir, se utilizará el protocolo SIP, que es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet.

En la tabla 3.11 se muestra algunas de las características de los codec's de compresión que utiliza el protocolo SIP.

Tabla 3.11: Codec's de compresión audio que utiliza el protocolo SIP.

Codec	Sampling Rate	Bit Rate
G.711	8 KHz	64 Kbps
G.722	16 KHz	48, 56, 64 Kbps
G.723	8 KHz	5.3, 6.4 Kbps
G.726	8 KHz	16, 24, 32, 40 Kbps
G.728	8 KHz	16 Kbps
G.729	8 KHz	8 Kbps

A continuación, incluimos una breve descripción de cada uno:

**G.711.-** convierte la voz en una secuencia digital de 64 kbps. Es el mismo CODEC que se utiliza en TDM. Se considera el indicado para una mayor calidad.

**G.722.-** describe el uso de la modulación adaptativa diferencial de pulsos para transmitir audio de alta calidad 8 khz en 48, 56 o 64 kbps. Esta recomendación también permite la transmisión de datos a 16 kbps sobre un canal de 64 kbps, con los 48 kbps restantes para audio, el cual puede ser utilizado en una gran variedad de aplicaciones de voz de una mayor calidad.



**G.723.-** Hay dos tipos diferentes de compresión G.723.1. Un tipo utiliza el algoritmo de compresión CELP y tiene una tasa de bit de 5.3 kbps. El segundo utiliza el algoritmo MP-MLQ y proporciona una mejor calidad de sonido, la tasa de bit es de 6.3 kbps.

**G.726.** - Ofrece diferentes tasas, incluyendo 40 kbps, 32 kbps, 24 kbps y 16 kbps. Se adapta bien a interconexiones con PBX y la tasa más utilizada es 32 kbps.

**G.728.** - Proporciona una calidad de voz muy buena y está especialmente diseñado para aplicaciones de baja latencia. Comprime la voz a una tasa de 16 kbps.

**G.729.** - Ofrece una mayor calidad de voz a una tasa relativamente baja, 8 kbps. Hay dos versiones más utilizadas de este CODEC, G.729 y G.729a utiliza un algoritmo más simplificado y permite trabajar con teléfonos que aporten menos potencia de procesado, es decir, teléfonos más simples y baratos para el mismo nivel de calidad.

Los codecs G.723.1, G.729 y G.729a normalmente requieren un hardware especial, un DSP (Procesador de Señal Digital).

## **Medir la calidad**

Hay muchos métodos para medir la calidad de una llamada de VoIP, en este caso utilizaremos MOS (Mean Opinion Score).

**MOS** asigna un valor a la calidad de la llamada en toda la red. La medida tiene en cuenta tanto al Codec como los efectos de la red. Las marcaciones MOS tienen valores desde 1 (mala) a 5 (excelente). El valor de MOS real ha sido determinado en un ejercicio estadístico, un gran número de personas escuchando la misma llamada y valorándola de 1 a 5. (Véase la figura 3.7).



<b>MOS</b>	<b>Calidad voz</b>	<b>Nivel de distorsión</b>
5	Excelente	Imperceptible
4	Buena	Apenas perceptible, no desagradable
3	Regular	Perceptible, levemente desagradable
2	Pobre	Desagradable, pero aceptable
1	Insatisfactoria	Muy desagradable. Inaceptable

Figura 3.7: Valores de MOS (Mean Opinion Score)

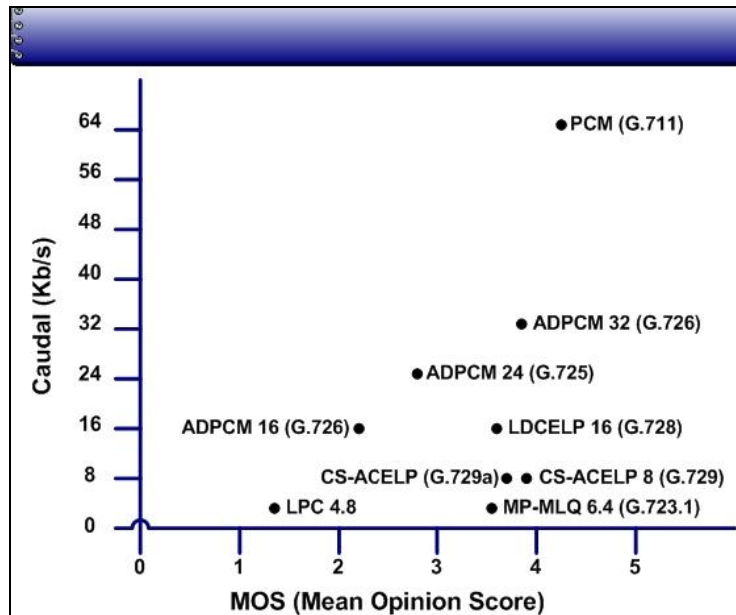


Figura 3.8: Compresión vs. Calidad

De acuerdo a la figura 3.8 podemos concluir que el codec de compresión de voz que se va a utilizar es G.711 porque la calidad de la voz es la mejor en comparación a los otros codecs con 4.2, no desagradable en base al MOS, el único limitante es que ocupa gran ancho de banda y para brindar este servicio a un grupo grande de usuarios en la ESPE, se necesitará pedir al ISP más ancho de banda. Otra opción es usar un codec que brinde un buen servicio, utilizando menor ancho de banda y que tenga un alto valor en la escala de MOS.

### 3.2.1.-Cálculo del consumo de ancho de banda con SIP para la ESPE y sus Sedes

Para el prototipo se ha considerado los siguientes puntos de voz, para lo cual los datos de ancho de banda requeridos actualmente (de 48, 56 a 64 Kbps por llamada), utilizando el codec G.711 del protocolo SIP que consume 64 Kbps, podemos decir que:

**ESPE – Sangolquí.-** con 5 llamadas concurrentes que a la vez se podrían establecer, ocupa:

$$64 * 5 = 320 \text{ Kbps de } 2\text{Mbps}$$

**ESPE – Latacunga.-** con 2 llamadas concurrentes que a la vez se podrían establecer, ocupa:

$$64 * 2 = 128 \text{ Kbps de } 512 \text{ Mbps}$$

**ESPE – Idiomas.-** con 1 llamada concurrente que se podría establecer, se ocupa:

$$64 * 1 = 64 \text{ Kbps de } 256 \text{ Kbps}$$

**ESPE – IASA II.-** con 2 llamadas concurrentes que a la vez se podrían establecer, ocupa:

$$64 * 2 = 128 \text{ Kbps de } 128 * 2 \text{ Kbps (San Antonio y Zoila luz)}$$

**ESPE – IASA I.-** con 1 llamada concurrente que se podría establecer, se ocupa:

$$64 * 1 = 64 \text{ Kbps de } 256 \text{ Kbps}$$

**Héroes del Cenepa.-** con 1 llamada concurrente que se podría establecer, se ocupa:

$$64 * 1 = 64 \text{ Kbps de } 256 \text{ Kbps}$$

**Biblioteca - MED.-** con 3 llamadas concurrentes que a la vez se podrían establecer, ocupa:

$$64 * 3 = 192 \text{ Kbps de } 1\text{Mbps}$$

### **3.3.- Levantamiento de Requerimientos de la ESPE**

#### **3.3.1.-Tamaño de la Muestra**

La muestra es el número de elementos, elegidos o no al azar, que hay que tomar de un universo para que los resultados puedan extrapolarse al mismo, y con la

condición de que sean representativos de la población. El tamaño de la muestra depende de tres aspectos:

- Del error permitido.
- Del nivel de confianza con el que se desea el error.
- Del carácter finito o infinito de la población.

La fórmula general para poblaciones finitas que permiten determinar el tamaño de la muestra es la siguiente:

$$n = \frac{Z^2 * P * Q * N}{e^2(N - 1) + Z^2 * P * Q}$$

Donde:

n = Número de elementos de la muestra

N = Número de elementos del universo.

P/Q = Probabilidades con las que se presenta el fenómeno.

Z = Valor crítico correspondiente al nivel de confianza elegido siempre se opera con valor sigma 2; pero Z también puede tomar los siguientes valores: z = 1.15 donde  $\alpha = 0.25 \equiv 75\%$ , z = 1.96 para  $\alpha = 0.05 \equiv 85\%$  y z = 2.58 para  $\alpha = 0.01 \equiv 97\%$ .

e = Margen de error permitido (a determinar por el director del estudio).

En nuestro caso, los valores que vamos a utilizar para el cálculo de la muestra son los siguientes:

N = 1500 son las personas que se va a considerar en el campus Sangolquí para el cálculo de la muestra; 500 Administrativos, 800 tiempo completo y 200 Hora clase.

P = 0.75 es la cantidad de personas que conocen acerca del tema.

Q = 0.25 es la cantidad de personas que no conocen acerca del tema.

Z = 1.15 es el valor que correspondiente al nivel de confianza elegido.

e = 0.05 es el estándar de error.

$$n = \frac{1.15^2 * 0.75 * 0.25 * 1500}{0.05^2 (1500 - 1) + 1.15^2 * 0.75 * 0.25}$$

$$n = 93.093739$$

El número de encuestas que se van a realizar es 93.

### **3.3.2.- Encuesta dirigida a los usuarios de la ESPE**

Con el resultado de los datos de la encuesta se conocerá la aceptación, el beneficio y las necesidades que tienen las instalaciones y servicios que brinda la universidad en su red.

Los datos proporcionados por los encuestados no serán publicados, se tendrá total confidencialidad en la información. Éstos serán utilizados solamente para fines de investigación y de estudio.

#### **3.3.2.1.- Objetivos**

- Obtener datos que nos permitan conocer las necesidades de la red de la ESPE.
- Saber cuanto conocimiento tiene el usuario acerca del tema de Voz sobre IP.
- Determinar los requerimientos de los usuarios para mejorar los servicios de la universidad.

#### **3.3.2.2.- Enfoque**

La encuesta esta enfocada a la obtención de información acerca del conocimiento de los usuarios referente al tema de Voz sobre IP para conseguir datos que nos permitan evaluar, optimizar y aprovechar el uso correcto de la red de la ESPE.

El tipo de encuesta es un procedimiento utilizado para obtener información mediante preguntas dirigidas cerradas.

La encuesta se realizará a todo el personal administrativo, departamento de organización y sistemas, profesores, ciencias básicas y laboratorios especializados de la ESPE.

El proceso de la encuesta se realizó la semana de 6 al 13 de Febrero de 2006.

### 3.3.2.3.- Formato de la encuesta

El formato de la encuesta se encuentra detallado en el Anexo A.

### 3.3.2.4.- Resultados

- **Pregunta 1**

¿Con que frecuencia se comunica desde la ESPE - Sangolquí a las sedes y viceversa?

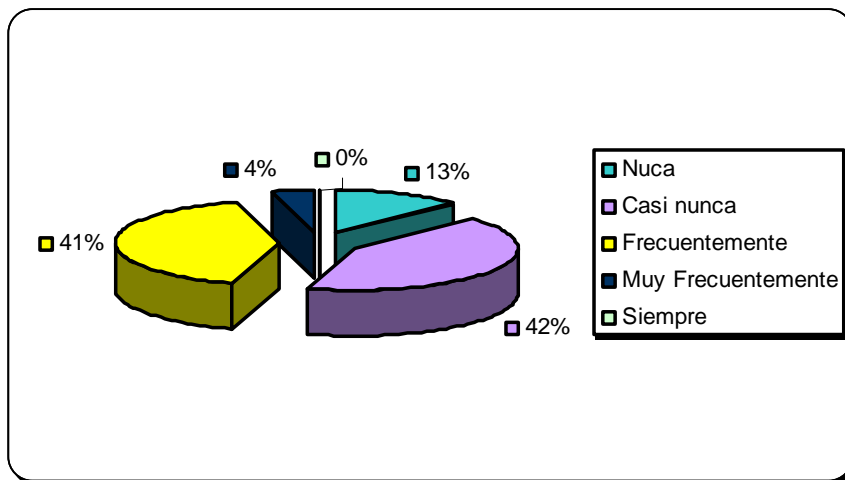


Figura 3.9: Resultado pregunta 1

- **Pregunta 2**

¿Ingresa con facilidad la llamada cuando se comunica a la ESPE - Sangolquí y a sus sedes?

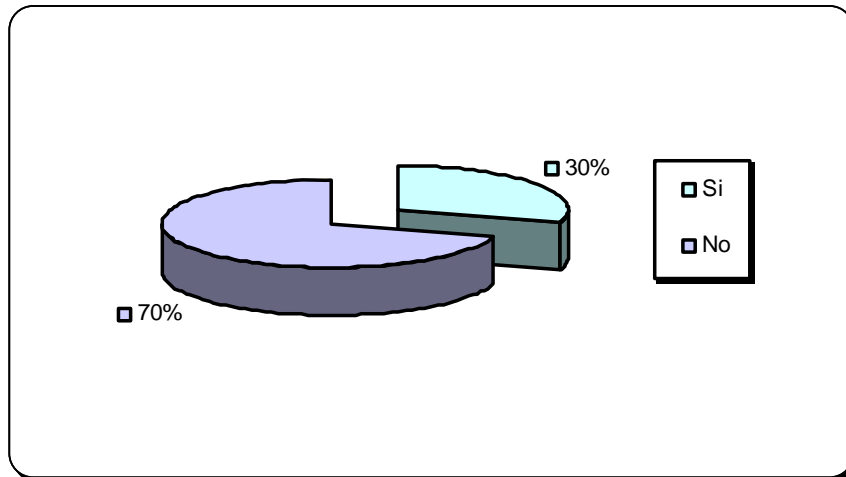


Figura 3.10: Resultado pregunta 2

- **Pregunta 3**

¿Cómo considera usted el funcionamiento de las líneas telefónicas internas y externas de la ESPE?

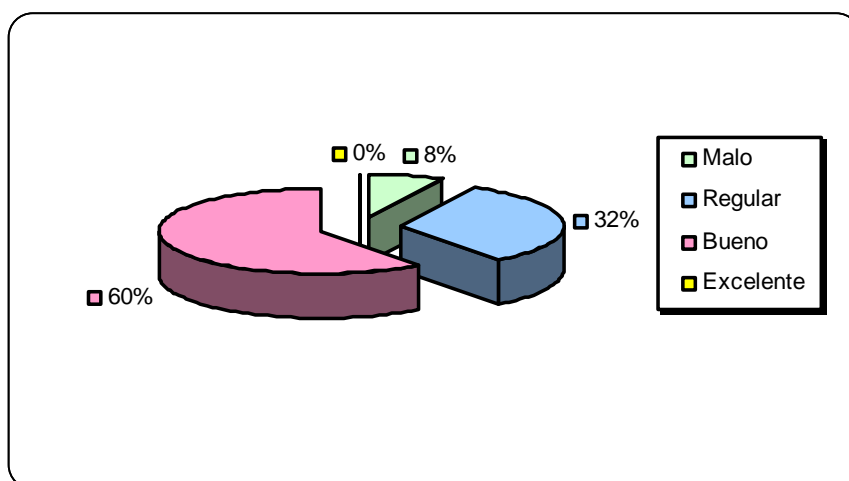


Figura 3.11: Resultado pregunta 3

- **Pregunta 4**

¿Es importante que tenga una línea telefónica individual en su estación de trabajo?

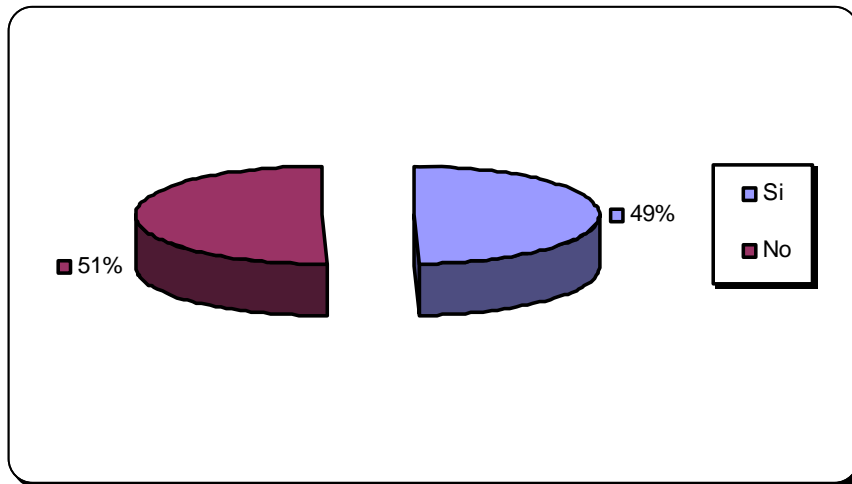


Figura 3.12: Resultado pregunta 4

- **Pregunta 5**

¿Le gustaría tener en su computadora servicios de mensajería, chat, correo de voz, buzón de mensajes?

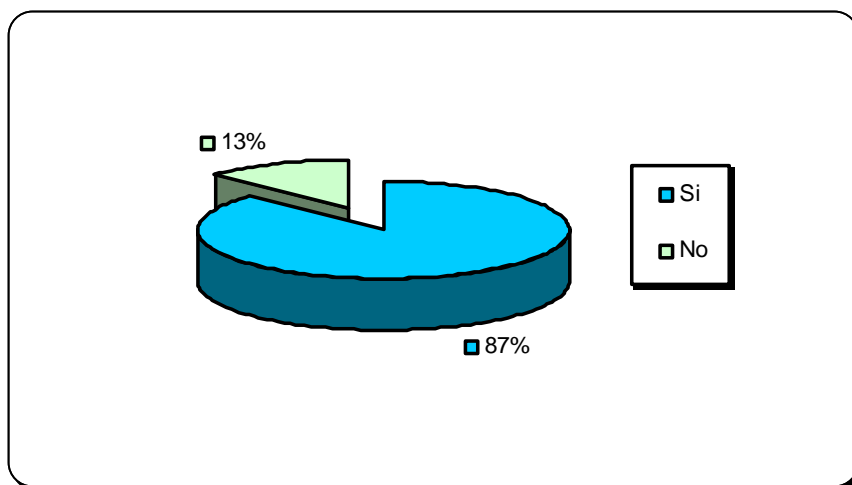


Figura 3.13: Resultado pregunta 5



- **Pregunta 6**

¿Ha escuchado sobre la tecnología de Voz sobre IP (VoIP)?

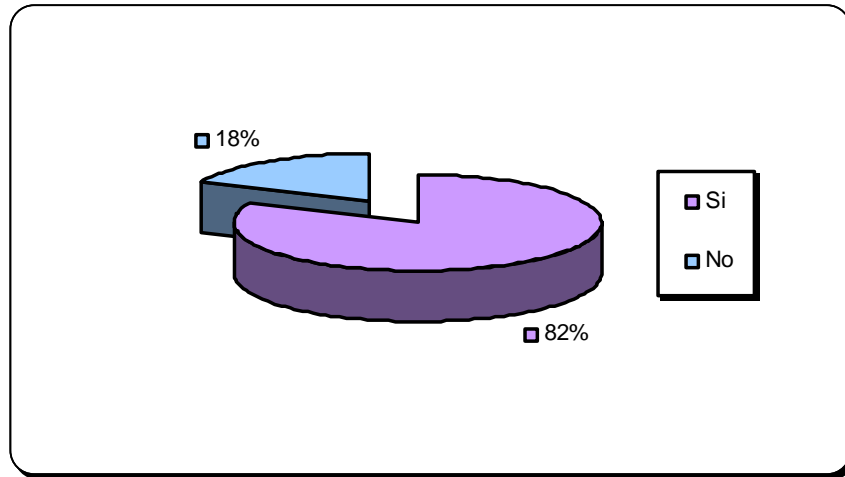


Figura 3.14: Resultado pregunta 6

- **Pregunta 7**

¿Que uso le daría a Voz sobre IP en la ESPE?

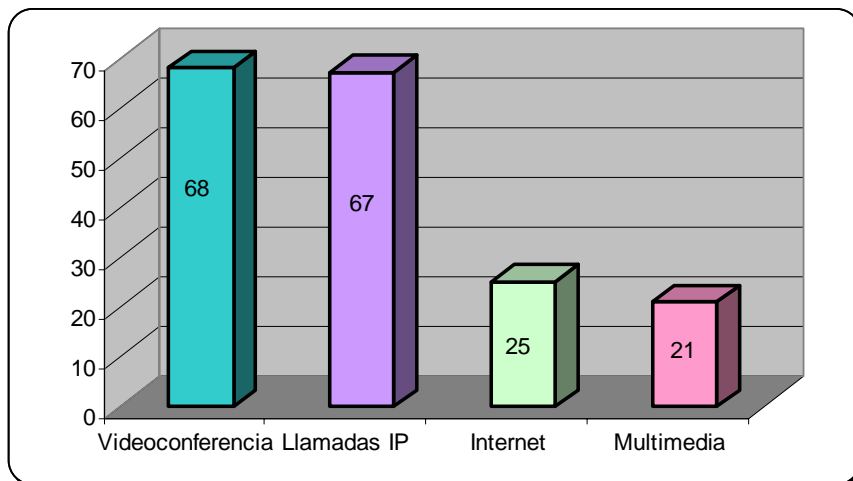


Figura 3.15: Resultado pregunta 7

### **3.3.2.5.- Conclusiones**

Con la pregunta 1 (Véase la figura 3.9) podemos observar que las personas que se comunican desde la ESPE a sus sedes y viceversa es de Casi Nunca y Frecuentemente con un porcentaje de 42% y 41% respectivamente, mostrando una leve diferencia que se encuentra sustentada por las respuestas de la pregunta 2 y 3 donde se ve claramente el estado en el que se encuentra la comunicación. En la pregunta 2 (Véase la figura 3.10) y 3 (Véase la figura 3.11) podemos notar que las llamadas no ingresan con facilidad, debido a que sólo recepta 1 de las 36 líneas con las que cuenta la universidad y esto ocasiona que el resto de las llamadas se pierdan y mantenga un estado de congestión en horas pico, pero cabe recalcar que internamente la comunicación es aceptable. Por otro lado, es inaceptable que en una universidad de prestigio como la ESPE el rango de “excelente y siempre”, respectivamente, tenga un porcentaje de 0% para categorizar al funcionamiento de las líneas.

Las preguntas 4 (Véase la figura 3.12) y 5 (Véase la figura 3.13) muestran que los usuarios no necesitan una línea telefónica ya que la mayoría del personal no trabajan en un horario de tiempo completo; pero la otra fracción de usuarios si desearían tener una línea personal para mejorar su trabajo, facilitar los papeles en la función administrativa y para comunicarse más rápido, haciendo uso de servicios como mensajería, chat y correo de voz.

Las preguntas 6 (Véase la figura 3.14) y 7 (Véase la figura 3.15) son orientadas a la optimización de la red de la ESPE y podemos ver que el grado de conocimiento de los usuarios acerca de la tecnología de Voz sobre IP es alto con un porcentaje del 82%. La ESPE debe procurar alcanzar un alto nivel de excelencia en cuanto al servicio que brinda a sus usuarios, adoptando así una tecnología capaz de soportar servicios como videoconferencia, llamadas IP, multimedia, etc. lo mismo que con el ancho de banda que actualmente la ESPE maneja entre sedes es posible brindar, por esto, se encuentra justificado la implementación de Voz sobre IP.

### **3.4.- Análisis y Diseño de la Red VoIP utilizando el protocolo SIP**

#### **3.4.1.-Resolución de las necesidades de la ESPE**

Después de haber analizado la encuesta, se ha llegado a la conclusión de que la ESPE debe mejorar su servicio de telefonía, por lo que, se ha adquirido una central de Voz sobre IP que se encuentra implementada desde Abril del 2006, la misma que abastece sólo a un 40% de usuarios; por lo cual con el protocolo SIP se podría proporcionar una aplicación paralela que permita la realización de llamadas telefónicas internas y hacia las sedes sobre redes de paquetes utilizando softphone o teléfonos estándares dando mayor flexibilidad, escalabilidad, bajos costos y beneficios a un mayor número de usuarios, tomando en cuenta que la infraestructura que actualmente posee la ESPE y sus sedes es apta para implementar estas aplicaciones.

En conclusión podemos decir que las necesidades de la ESPE son:

- Realizar una distribución coherente y organizada de las líneas telefónicas.
- Reducción de costos de líneas telefónicas mediante la implementación de VoIP.
- Mejorar los servicios a los usuarios a través de la implementación de VoIP.
- Optimizar el ancho de banda de la ESPE para mejorar el tráfico que circula por el mismo.

La solución mediante la tecnología de VoIP con el protocolo SIP es la más óptima para mejorar los servicios requeridos por la ESPE. Los requerimientos técnicos y las especificaciones para la tecnología de VoIP y SIP se explican en el Capítulo II; los parámetros que básicamente se toman en cuenta para VoIP son calidad de servicio, retardo o latencia y el codec que se va a utilizar y para SIP es un protocolo que pertenece al Nivel de Aplicación, que se utiliza para iniciar sesiones interactivas multimedia entre usuarios de redes IP.

#### **3.4.2.-Solución propuesta para la ESPE y sus Sedes**

La presente solución propuesta para la ESPE maneja equipos convencionales, que utiliza la infraestructura de las redes de datos. Este es un sistema completamente convergente, es decir, que pueden trabajar con teléfonos y computadoras utilizando el

mismo medio de transmisión, sin que se afecten ni interfieran las señales de voz y las señales de datos.

### 3.4.2.1.- Diseño

La solución tecnológica se basa en el esquema de Convergencia de Redes como muestra la figura 3.16, esta propuesta incluye voz y datos en una sola infraestructura. Dicha integración implica para los usuarios de la ESPE que se debe gastar el mínimo valor a cambio de una solución óptima, alta integración, sofisticación de aplicaciones, flexibilidad, facilidad de gestión y conexión con sitios remotos.

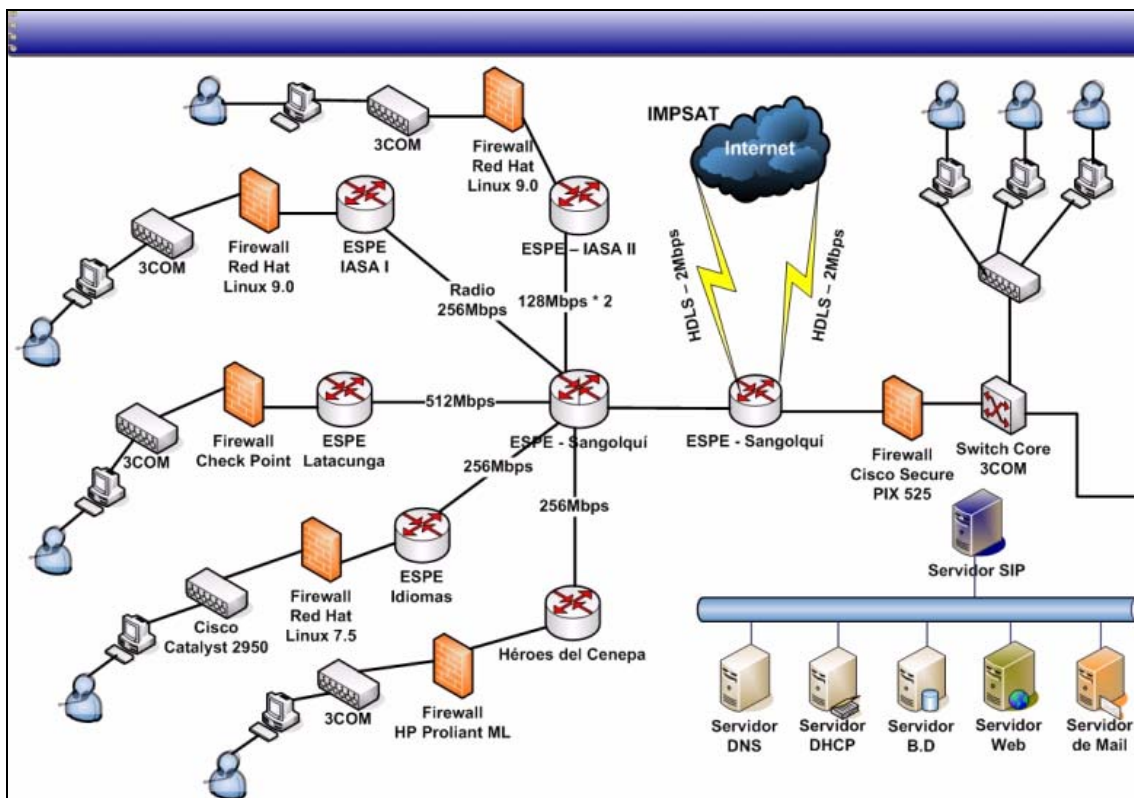


Figura 3.16: Diseño de la WAN con SIP

### 3.4.2.2.- Características del Diseño

El servidor de aplicaciones SIP deberá ser incorporado físicamente en la red interna de la ESPE – Sangolquí, donde se encuentran los otros servidores de Web,

Correo electrónico, etc. ya que es la matriz en donde se administra y distribuye los canales para la comunicación con las demás sedes.

Para el funcionamiento de la aplicación se debe hacer lo siguiente:

1. Crear y configurar una VLAN tanto en el switch de core del campus Sangolquí como en el switch de cada una de las sedes, donde se debe ingresar la dirección del servidor en su respectivo puerto.
2. Habilitar los puertos bidireccionalmente, es decir, tanto en el firewall del campus Sangolquí como en el firewall de cada una de las sedes que va a utilizar el protocolo SIP:
  - Puertos que usa SIP: 5060 y/o 5061
  - El rango del 16384 al 16842 UDP (no se debe habilitar todos estos puertos por seguridad, se debe ir probando por que canal se escucha).
3. Asignar un rango de DHCP al servidor SIP.
4. En el fichero "sip.conf" además se debe configurar los siguientes parámetros:
  - externip: dirección IP que se va a poner en los mensajes de SIP si se encuentra detrás de un NAT.
  - localnet: dirección IP de la red local y la máscara de subred.
  - nat: habilita la traducción de la dirección de red para dar salida a redes públicas que se encuentran con direccionamiento privado.
  - fromdomain: dominio en mensajes SIP cuando se activa como un agente de usuario (cliente).
5. Instalar y configurar el softphone (SJphone) en cada una de las computadoras que se va a utilizar en la ESPE y sus sedes.

#### **3.4.2.3.- Ventajas**

- La ventaja de este diseño es el costo, ya que la ESPE cuenta con todos los equipos necesarios para la implementación de esta aplicación, sólo es

necesario adquirir un servidor, Linux Red Hat Enterprise, Headsets (audífonos) e instaladores del softphone (SJphone).

- Los usuarios de la ESPE – Sangolquí y sus sedes pueden encontrar y comunicarse con quien necesiten, independientemente de dónde y cómo estén localizados.
- El cliente indica por si mismo sus preferencias, teniendo la posibilidad de integrar soluciones de comunicación con aplicaciones comerciales, gracias a que SIP proporciona un paquete de herramientas que permite ampliar el alcance de sus ofertas.
- SIP permite mayor escalabilidad y flexibilidad para soportar una alta cantidad de usuarios, ya que tiene una gran habilidad para manejar un considerable número de llamadas gracias a la arquitectura cliente/servidor que esta posee.

#### **3.4.2.4.- Desventajas**

- Se debe resaltar que así como PSTN, VoIP no puede prestar servicio a todos sus clientes (por ejemplo, una llamada GSM no puede manejar más de algunos cientos o un par de miles de clientes).
- La utilización del codec G.711 permite tener a un número limitado de usuarios de la ESPE debido a que ocupa una cantidad elevada (64 Kbps) de ancho de banda.
- La calidad y servicio dentro de las transmisiones IP no está garantizado el éxito. Se debe priorizar la transmisión de paquetes de voz sobre los paquetes de datos, además la transmisión no debe pasar de los 150 ms.

#### **3.4.2.5.- Costo**

El análisis de costos se basó en los requerimientos y el consumo de ancho de banda, para dar servicio a los usuarios más importantes de la ESPE y sus sedes; tomando en cuenta que esto sólo es un prototipo.

El costo aproximado de esta propuesta, se muestra en la tabla 3.12:

Tabla 3.12: Costo estimado

Descripción	Cantidad	Precio Unitario	Precio Total
Servidor SIP	1	\$2000	\$2000
Instaladores Red Hat Linux Enterprise ES	1	\$799	\$799
Auriculares Plantronics	15	\$40	\$600
<b>TOTAL</b>			<b>\$3399</b>

### 3.4.2.6.- Equipos

- **Servidor SIP**



Figura 3.17: Servidor SIP

El servidor SIP cuenta con las siguientes características estándar (Véase la tabla 3.17), con las cuales tiene un óptimo desempeño; pero si se desea puede ampliar los requerimientos de hardware.

Tabla 3.13: Características del Servidor.

Características	Descripción
Monitor	Samsung SyncMaster 793s (17 pulgadas)
Procesador	Intel Pentium IV 2.6 Ghz, socket 478
Memoria	512 Mb PC- 266 Kingston
Disco Duro	40 Giga Bytes 7200RMP
Tarjeta Madre	Intel 845EPI socket 478
Tarjeta de Red	RED 10/100 Mbps, LG
Tarjeta de Red	RED 10/100 Mbps, SMC
Audio	VT8233 AC'97 Audio Controller, Integrada
CD - ROM	Samsung 52X Max
Teclado	Genius PS/2 (101/102 teclas)
Mouse	Genius Opticos PS/2 (3 botones)

- **Audífonos Plantronics DSP 400**

**Plantronics DSP 400** digital – enhanced es un receptor estéreo de cabeza plegable con sonido estereofónico. El diseño plegable permite una fácil manipulación del mismo. Su micrófono con cancelación de ruido realiza con exactitud las palabras. El centro de control de audio PerSono™ permite que los usuarios ajusten el micrófono y las características de audio como volumen, bajo y triple.

Sus características principales son:

- Full stereo 16 bits, 48 Khz output to headphone.
- 24 bits, 10 dB signal to noise codec.
- 32 bits digital audio processing.
- 20 Hz – 20Khz speaker frequency response.
- 2 canales de 48 Khz.





Figura 3.18: Auriculares Plantronics DSP 400

### 3.4.2.7.- Software

- **SJphone**

**SJphone** un programa de telefonía a través del protocolo VoIP que permite utilizar un innovador sistema de comunicación telefónica vía Internet desde un PC. Para ello, se debe tener conectado un dispositivo a través de un modem o de la red local a Internet.

Las opciones y capacidades del software facilitarán todo un entorno sumamente sencillo con el cual se podrá establecer todo tipo de llamadas a cualquier otro usuario de SJphone mediante la introducción de su dirección IP.

Este sistema ofrece una gran cantidad de servicios y ventajas, entre las cuales podemos mencionar:

- Correo de voz
- Conferencias
- Transferencia de llamadas
- Llamada en espera

- **Red Hat Linux Enterprise**

**Red Hat Linux Enterprise** es la plataforma informática principal para código abierto. Es vendida por suscripción, entrega valor continuo y es certificada por los vendedores superiores de hardware y software de la empresa. Desde el escritorio al centro de datos, Linux Enterprise junta la innovación de la tecnología de código abierto y de la estabilidad de una plataforma verdadera de la empresa-clase.

Las soluciones de Red Hat Linux Enterprise están disponibles sobre una base anual por sistema. Hay tres ediciones para la suscripción: Básico, estándar, y premio; cada uno con los niveles de ayuda y varias opciones de entrega.

Tabla 3.14: Características de Red Hat Linux Enterprise ES

Características	Basic Editions	Standard Editions	Premium Editions
Descarga de S.O: S.O, código, y documentación de imágenes.	Si	Si	Si
Actualizar el módulo de Red Hat Network. Servicio 1 año.	Si	Si	Si
Actualizaciones de Productos	Si	Si	Si
Instalación y Documentación (CDs)	Opcional	Si	Si
Soporte de Web	1 año de Instalación y configuración Básica	24x7	24x7
Soporte vía telefónica	30 días de Instalación y configuración Básica. North Am: 9-9 ET M-F Global: 9-5 GMT/CET M-F	North Am: 9-9 ET M-F Global: 9-5 GMT/CET M-F	24x7 (severity 1)
Alcance de Cobertura	30 días teléfono / 1 año web Instalación y configuración Básica	1 año: cobertura estándar	1 año: Cobertura Premium

## Capítulo IV: Pruebas de Funcionamiento

### 4.1.- Antecedentes

En esta práctica se detallará la configuración de una aplicación que permita realizar la implementación de un Servidor SIP, el cual será la PBX Asterisk y al mismo tiempo tendrá las funciones de servidor: Proxy, DNS y DHCP; haciendo uso de los equipos y la red de datos de la ESPE.

### 4.2.- Objetivo General

Configurar e implementar una aplicación de un Servidor SIP en el Sistema Operativo Red Hat Linux 9, para la ESPE.

### 4.3.- Objetivos Específicos

- Instalar Red Hat Linux 9 con los siguientes servicios:
  - Servicio DHCP
  - Servicio DNS
  - Servicio httpd
  - Servicio proxy (SQUID)
- Permitir el acceso a Internet.
- Conocer los principales comandos y archivos de configuración utilizados para la configuración de Asterisk.
- Definir los diferentes servicios a utilizarse con el softphone:
  - Buzón de voz.
  - Conferencia.
  - Música en espera.
  - Transferencia de llamadas.

- Realizar prácticas que permitan comprobar el correcto funcionamiento de la aplicación con los softphone tanto en la intranet como en la wan.

#### 4.4.- Equipos y Materiales

- CD's de Instalación de Red HatLinux 9
- Un PC (Servidor) Linux.

Las características técnicas y principales del servidor, en el cual se implementa VoIP con SIP se muestran en la tabla 4.1; con las cuales se obtiene un óptimo desempeño; pero si se desea puede ampliar los requerimientos de hardware.

Tabla 4.1: Características básicas del Servidor SIP.

Características	Descripción
Procesador	Intel Pentium IV 2.6 Ghz
Memoria	512 Mb
Disco Duro	40 Giga Bytes 7200RMP
Tarjeta Madre	Intel 845EPI
Tarjeta de Red	RED 10/100 Mbps, LG
Tarjeta de Red	RED 10/100 Mbps, SMC
Audio	VT8233 AC'97 Audio Controller, Integrada

- PC's (Cliente). Lo mínimo que necesita es un procesador Intel Celeron 300 con 32MB para Windows 98SE, 128MB para Windows 2000 y 256 para Windows XP. Se debe tener instalado la versión más reciente de DirectX (7.0 - 9.0), es lo más recomendado.
- Patch Cords Punto a punto.
- Switch
- Headsets: Plantronics, Suoya, Sonic.
- Instaladores del SjPhone.
- Parlantes y micrófono.

## 4.5.- Diagrama de la Red

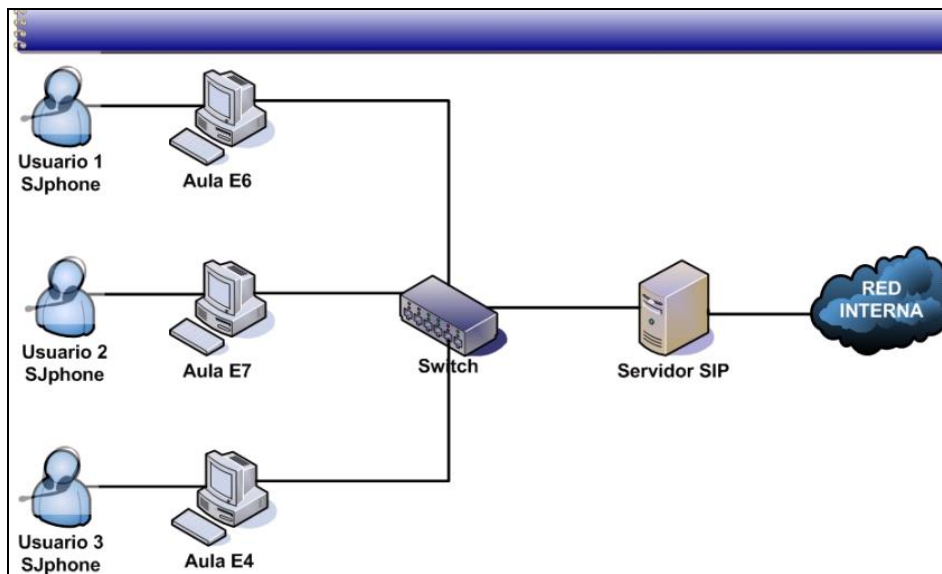


Figura 4.1: Diagrama de la Red.

## 4.6.- Desarrollo

Los pasos que se deben seguir para la configuración del Proxy SIP Server son los siguientes:

- Instalación de Linux
- Configuración de Apache (httpd)
- Configuración DHCP
- Configuración DNS
- Configuración Squid
- Configuración de Asterisk
- Configuración de SJphone

A continuación, se detalla cada uno de los pasos mencionados.

### 4.6.1.-Instalación de Linux

En primer lugar se procedió a instalar Red Hat Linux 9 en la computadora que funcionará como servidor SIP, mientras que los clientes podrán tener cualquier versión de Windows, para nuestro caso, es Windows XP.

A continuación se mencionará los aspectos principales que se requieren para la instalación:

- El tipo de instalación escogido es: Custom (personalizado) -> Next.

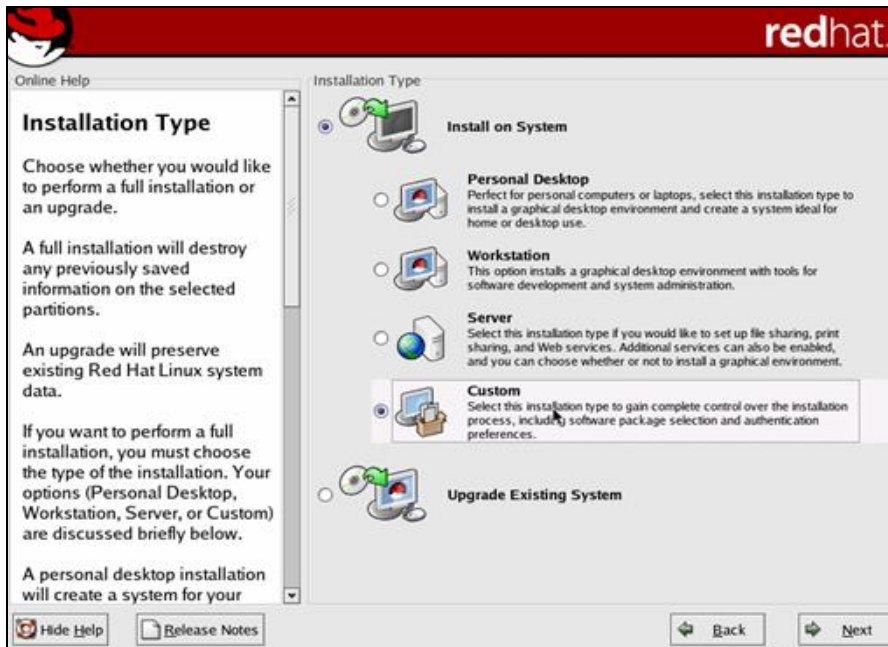


Figura 4.2: Selección del tipo de instalación.

- En la configuración de red se muestra las tarjetas de red que detecta el sistema y le damos un nombre al equipo, en nuestro caso [www.voipsip.com](http://www.voipsip.com) -> Next

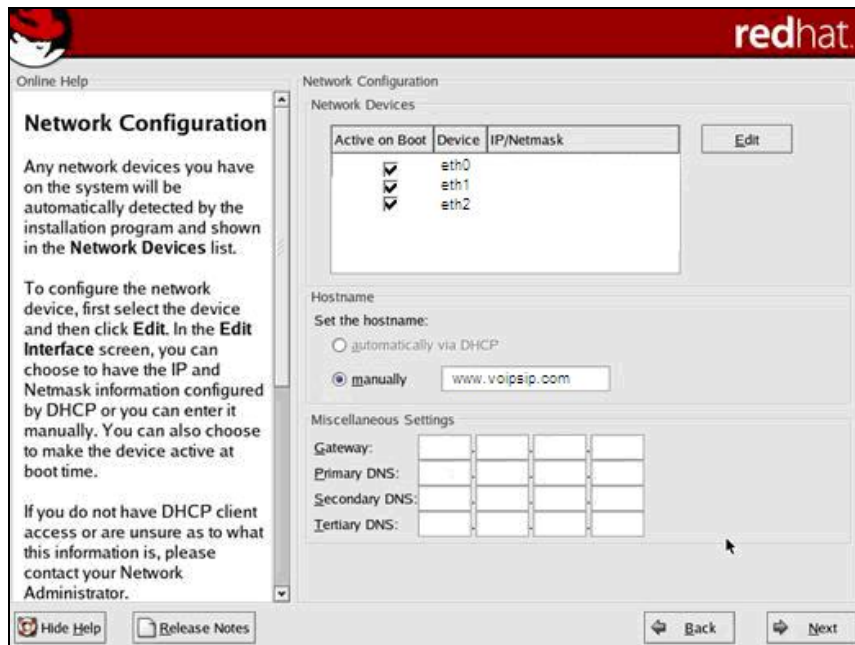


Figura 4.3: Configuración de Red.

- Escogemos la opción de No firewall para no tener problemas posteriores con la administración de la red -> Next

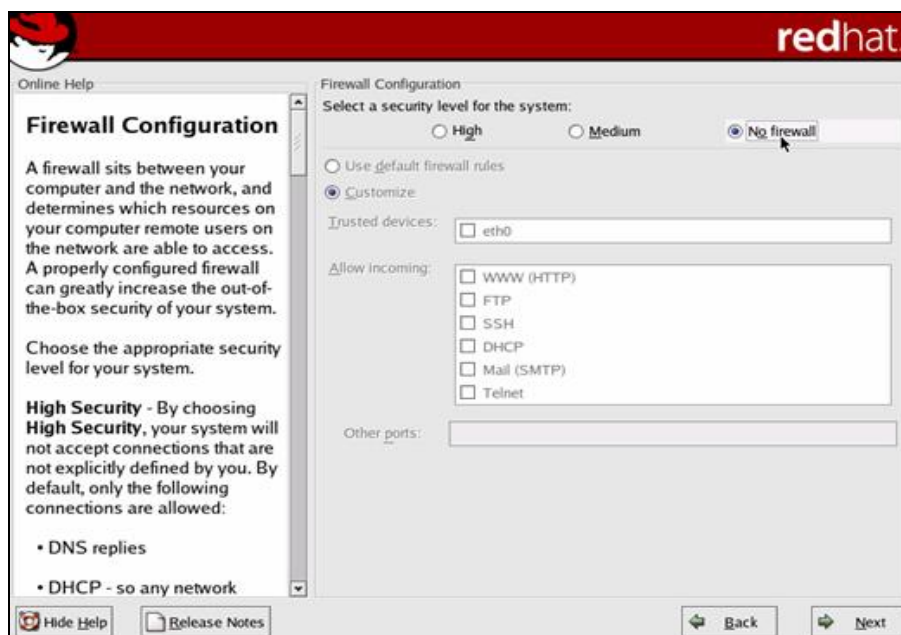


Figura 4.4: Configuración de Firewall

- Para la instalación de los paquetes del sistema, se lo realizó de forma personalizada de acuerdo a los requerimientos del servidor, entre los cuales están:
  - Editores
  - Server Configuration Tools
  - Web Server
  - Mail Server
  - Windows File Server
  - DNS Name Server
  - Network Servers
  - Desarrollo del Kernel

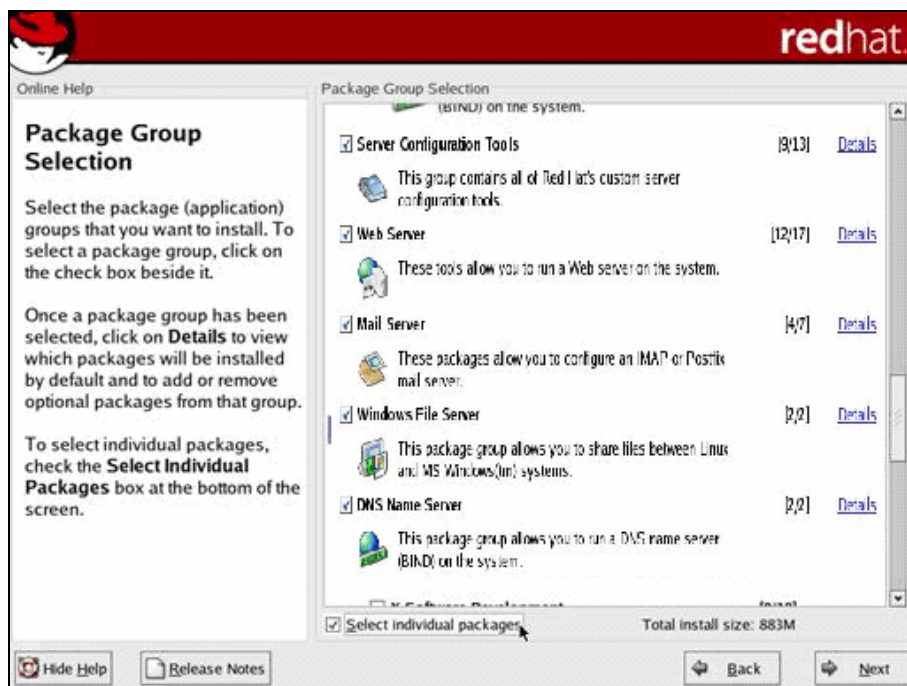


Figura 4.5: Selección del grupo de paquetes.

- A continuación, se espera unos minutos para que termine la instalación.

#### 4.6.2.- Configuración de Apache (httpd)

La configuración de apache se realiza a través de varios archivos localizados en /etc/apache/ siendo el principal /etc/apache/httpd.conf donde se configura los



posibles servidores virtuales (apache puede responder a distintos nombres y proporcionar webs diferentes a cada uno de ellos), y todo lo relacionado con su funcionamiento. El servicio se levanta en una ventana de consola con el siguiente comando:

```
# service httpd start
```

### **4.6.3.-Configuración DHCP**

Se puede configurar un servidor DHCP mediante el archivo de configuración `/etc/dhcpd.conf`.

El primer paso al configurar un servidor DHCP es crear el archivo de configuración que almacena la información de red de los clientes. Se pueden declarar opciones globales para todos los clientes, o bien opciones para cada sistema cliente.

Algunos parámetros deben empezar con la palabra clave option, otros definen valores no opcionales o que controlan el comportamiento del servidor DHCP.

Se debe tomar en cuenta los siguientes puntos para la configuración:

- Option routers [ip del servidor]
- Option subset-mask [máscara de red]
- Option domain-name “nombre del dominio”
- Option domain-name-servers [ip del servidor]
- Range dynamic-bootp [ip inicio] [ip fin]

### **4.6.4.-Configuración DNS**

DNS es el sistema que convierte las direcciones IP en nombre de dominio, más fáciles de recordar.

Para realizar la configuración de DNS se utilizó la herramienta Webmin, que es una de las mejores maneras de administrar un sistema tanto remota como localmente y se ejecuta en un servidor Web.

El archivo de configuración se encuentra ubicado en el directorio `/etc/named.conf`. Este archivo utiliza una sintaxis simple, este formato posibilita una fácil configuración de las zonas seleccionadas (zona maestra y reversa) de las direcciones ip (ip del servidor e ip salida al internet), con características tales como listas de control de acceso y registro por categorías.

El nombre de dominio en nuestro caso es `www.voipsip.com`

#### **4.6.5.-Configuración Squid**

Squid es un Proxy a nivel de aplicación para HTTP, HTTPS y FTP. También puede ejecutar peticiones DNS más rápido de lo que puede hacerlo la mayoría del software cliente. SQUID es ideal para acelerar el acceso a `www`, y para controlar el acceso a sitios web (utilizando paquetes como `squidGuard`).

Squid por defecto utiliza el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto o bien que lo haga en varios puertos a la vez.

```
http_port 3128
```

Para levantar un servidor Proxy utilizamos el SQUID, y para su configuración modificamos los siguientes parámetros del archivo: `/etc/squid/squid.conf`

Algunos de los parámetros que se deben modificar:

- Parámetro `http_port`: 3128
- Parámetro `mem_cache`: 8Mb
- Controles de acceso: `acl localhost src [ip-servidor /mask-address]`
- Parámetro `cache_mgr`: `cache_mgr root@voipsip.com`

## **4.6.6.- Asterisk**

### **4.6.6.1.- Introducción**

La plataforma software de Incom está basada en el software Asterisk. Asterisk es un proyecto de software libre que ha desarrollado un PBX (Sistema de Telefonía Privado) basado en software. Este software es extremadamente flexible y perfecto para desempeñarse en ambientes de producción de cualquier escala. Es muy versátil, permite la conexión a diferentes tipos de redes, maneja distintos protocolos de comunicaciones, procesa gran cantidad de algoritmos de codificación, puede manejar varias clases de terminales de voz y dispone de un gran abanico de funcionalidades y aplicaciones. El nombre de asterisk se describe claramente el objetivo del proyecto: proviene del símbolo "\*", utilizado en DOS y UNIX como carácter comodín.

Asterisk puede funcionar sobre varios sistemas operativos como FreeBSD, Mac OS X, NetBSD, OpenBSD o Solaris. Sin embargo, Linux es la principal plataforma de desarrollo y que soporta el hardware de la empresa Digium, diseñado específicamente para Asterisk.

### **4.6.6.2.- Arquitectura**

Asterisk actúa como un middleware conectando las tecnologías de telefonía de bajo nivel con aplicaciones de alto nivel. Las tecnologías telefónicas que soporta incluyen las IP como SIP, H.323, IAX, MGCP y SCCP y las tradicionales TDM.

Asterisk está diseñado para conseguir la máxima flexibilidad. Cuando Asterisk arranca el "Cargador Dinámico de Módulos" que carga e inicializa los drivers que proveen los canales, formatos de archivo, backend de grabación del detalle de llamadas, codecs y aplicaciones enlazándolos con las apropiadas APIs (Programación de Interfaces de Aplicación) internas. A partir de entonces la PBX acepta llamadas desde interfaces direccionándolas según el plan de numeración (dialplan), usando el "lanzador de aplicaciones" para llamar a los terminales, conectar al buzón de voz, llamar a través de los enlaces externos, etc. El "traductor de codecs" permite a canales comprimidos con diferentes codecs hablar entre ellos.

Hay 4 APIs definidos en módulos cargables facilitando la abstracción de hardware y protocolos. Usando este sistema de módulos cargables la base de Asterisk no se debe preocupar de cómo se conecta el llamante, que codecs están en uso, etc.

- **API de canal:** el canal API maneja el tipo de conexión que se esta recibiendo de una llamada, sea una conexión VoIP, ISDN, PRI o otra tecnología. Los módulos dinámicos se cargan para manejar los detalles de más bajo nivel de estas conexiones.
- **API de aplicaciones:** permite ejecutar varios módulos de tareas. Comunicación, paginación, buzón de voz, la transmisión de datos en línea y cualquier otra tarea que un sistema del PBX pudiera realizar ahora o en el futuro son manejados por estos módulos separados.
- **API de traducción de codecs:** carga los módulos de codec para soportar varios formatos de codificación de audio como GSM, Mu-Law, A-law, e incluso MP3.
- **API de formato de archivo:** maneja la lectura y la escritura de los diferentes formatos de archivo para el almacenamiento de datos en el sistema de archivos.

La estructura modular es lo que permite que asterisk integre el hardware de conmutación y las tecnologías de VoIP; además, cargar todas las aplicaciones como módulos permite un sistema flexible, facilitando que el administrador diseñe el mejor camino para las llamadas al sistema PBX y modifique los mismos para satisfacer las cambiantes necesidades de comunicación.

#### 4.6.6.3.- Instalación

Para configurar un sistema Asterisk debe tener instalados los siguientes paquetes:

- ncurses y ncurses-devel
- openssl y openssl-devel
- zlib y zlib-devel
- bison y bison-devel
- fuentes del kernel 2.4 o 2.6

Luego se procede a descargarse de la página <http://www.asterisk.org/download> los instaladores de cada componente de asterisk:

- Zaptel
- Libpri
- Asterisk
- Sounds

Adicionalmente se debe descargar los ficheros de música Mpg123 de la página [página http://www.mpg123.de](http://www.mpg123.de)

#### **4.6.6.3.1.- Mpg123**

- Una vez descargado el paquete de instalación, se lo debe copiar en el directorio `/usr/src` y descomprimirlo.

- `# cd /usr/src`
  - `# tar -zxvf mpg123-0.59r.tar.gz`

- Compilarlo:

- `# cd mpg123-0.59r`
  - `# make clean`
  - `# make`
  - `# make linux-help`
  - `# make linux` (este comando se escoge de acuerdo a la versión del kernel).
  - `# make install`

#### **4.6.6.3.2.- Zaptel**

- Una vez descargado el paquete de instalación, se lo debe copiar en el directorio `/usr/src` y descomprimirlo.

- `# cd /usr/src`

```
o # tar -zxvf zaptel-1.2.4.tar.gz
```

- Se debe situar en el directorio # cd zaptel-1.2.4
- Para instalar ztdummy, necesario para music-on-hold y meetme sin ninguna tarjeta de Digium hay que editar el archivo Makefile sustituyendo:

```
MODULES=zaptel tor2 torisa wusb wfxo wfxs \  
ztdynamic ztd-eth wctlxxp wct4xxp wctellxp # ztdummy
```

por:

```
MODULES=zaptel tor2 torisa wusb wfxo wfxs \  
ztdynamic ztd-eth wctlxxp wct4xxp wctellxp ztdummy
```

- Compilarlo:

```
o # make clean  
o # make install
```

#### **4.6.6.3.3.- Libpri**

- Una vez descargado el paquete de instalación, se lo debe copiar en el directorio /usr/src y descomprimirlo.

```
o # cd /usr/src  
o # tar -zxvf libpri-1.2.2.tar.gz
```

- Compilarlo:

```
o # make clean  
o # make install
```

#### **4.6.6.3.4.- Asterisk**

- Una vez descargado el paquete de instalación, se lo debe copiar en el directorio /usr/src y descomprimirlo.

- o # cd /usr/src
- o # tar -zxvf asterisk-1.2.4.tar.gz

- Compilarlo:

- o # make clean
- o # make install
- o # make samples

- Para ejecutar Asterisk en la consola se ejecuta:

- o asterisk -vvvc

#### 4.6.6.3.5.- Sonidos

- Una vez descargado el paquete de instalación, se lo debe copiar en el directorio /usr/src y descomprimirlo.

- o # cd /usr/src
- o # tar -zxvf asterisk-sounds-1.2.1.tar.gz

- Compilarlo:

- o # make install

Por defecto los prompts de Asterisk están en ingles, pero la aplicación tiene soporte multiidioma. Primero se deben añadir los prompts en castellano al sistema. Para ello hay que añadir los siguientes directorios en /var/lib/asterisk:

- Sounds/es
- Sounds/digits/es
- Sounds/letters/es
- Sounds/phonetic/es

Los prompts en castellano deben grabar en ficheros wav. En el enlace [http://www.telecomabmx.com/asterisksounds/AsteriskSounds\\_ES.tar.gz](http://www.telecomabmx.com/asterisksounds/AsteriskSounds_ES.tar.gz) se pueden

encontrar todos los prompts ya grabados, pero con acento mexicano. Se deben grabar en los directorios anteriores. Desde el archivo de configuración del plan de numeración (extensions.conf) se puede indicar en que momento utilizar cada idioma.

#### **4.6.6.4.- Configuración de Asterisk**

Para la configuración de la PBX se va a utilizar el protocolo SIP, que es muy parecido a HTTP o a SMTP. El mensaje consiste en una cabecera (header) y un cuerpo. Es un protocolo que usa la codificación UTF- 8 y el puerto 5060 para conexiones tcp y udp, y ofrece todas las gamas de posibilidades de la telefonía moderna. Dado que es un protocolo muy flexible es posible agregar funciones y aumentar la operabilidad.

##### **4.6.6.4.1.- Archivos de Configuración**

Todos los archivos de configuración se encuentran en /etc/asterisk, para este caso solo utilizaremos algunos:

- sip.conf
- extensions.conf
- voicemail.conf
- meetme.conf
- phone.conf
- enum.conf
- musiconhold.conf

#### **4.6.7.- SJphone**

SJphone un programa de telefonía a través del protocolo VoIP que permite utilizar un innovador sistema de comunicación telefónica vía Internet desde un PC. Para ello, se debe tener conectado un dispositivo a través de un modem o de la red local a Internet.



Las opciones y capacidades del software facilitarán todo un entorno sumamente sencillo con el cual se podrá establecer todo tipo de llamadas a cualquier otro usuario de SJphone mediante la introducción de su dirección IP.

Este sistema ofrece una gran cantidad de servicios y ventajas, entre las cuales podemos mencionar:

- Correo de voz
- Conferencias
- Transferencia de llamadas
- Llamada en espera

#### 4.6.7.1.- Instalación

Para configurar SJphone se debe descargar los instaladores de la página <http://www.sjlabs.com/sjp.html>.

- Ejecutamos el instalador, y enseguida nos muestra una pantalla de bienvenida para la instalación wizard del SJphone.



Figura 4.6: Pantalla de bienvenida

- Leemos y aceptamos el acuerdo de licencia. -> Next.

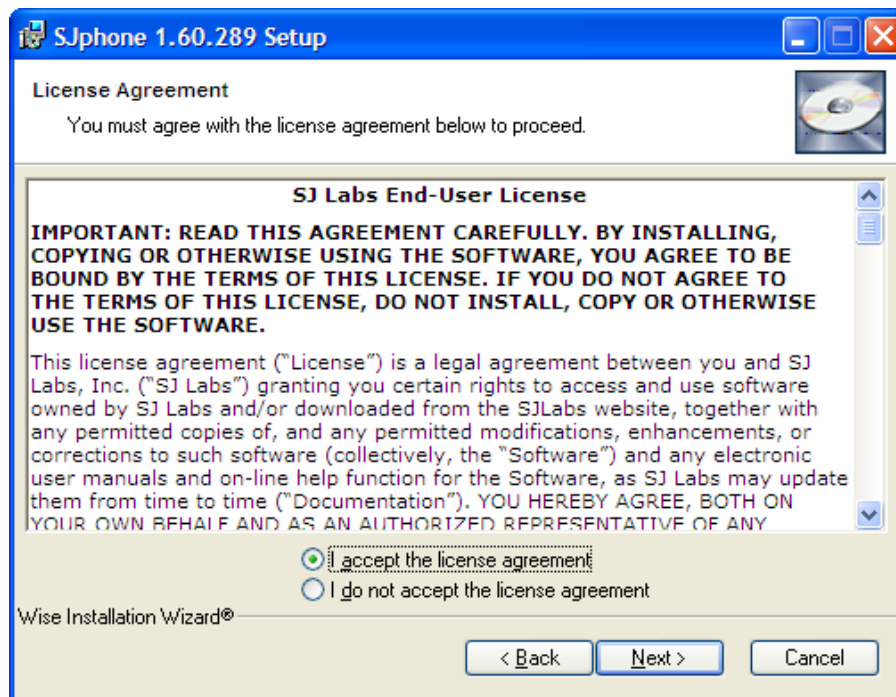


Figura 4.7: Licencia

- La instalación ha terminado correctamente. -> Finish.

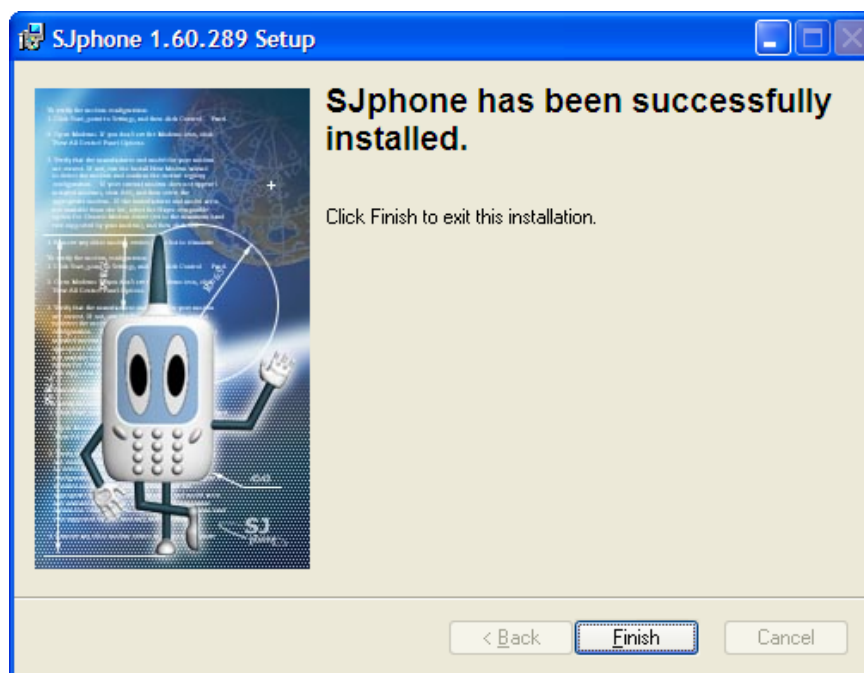


Figura 4.8: Pantalla final de instalación.

- Seguidamente se nos abrirá la pantalla del teléfono y podemos empezar con la configuración del mismo.



Figura 4.9: Pantalla de inicio del SJphone.

Para conocer más detalles acerca de la instalación y el funcionamiento del Siphone vea el Anexo B.

## 4.7.- Práctica de Laboratorio

### 4.7.1.-Configuración de la Red

Se utilizó dos tarjetas de red (Vea la figura 4.10), la primera para la administrar red interna (Vea la figura 4.11) y la segunda para tener salida al Internet (Vea la figura 4.10).

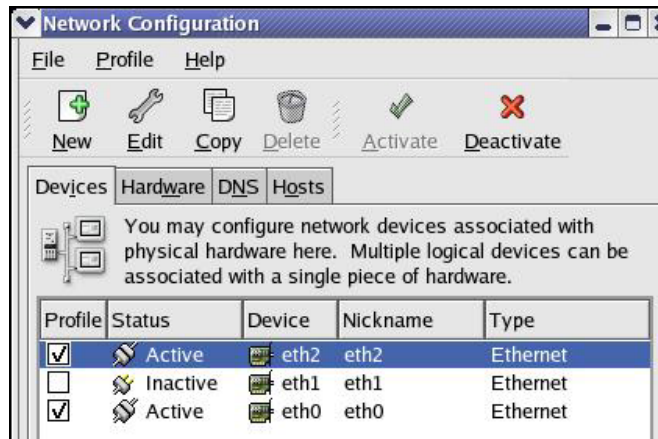


Figura 4.10: Configuración de la Red

- eth0



Figura 4.11: Configuración eth0

- eth2



Figura 4.12: Configuración eth2

- Configuración del nombre del sistema, dominio y nombre del servidor

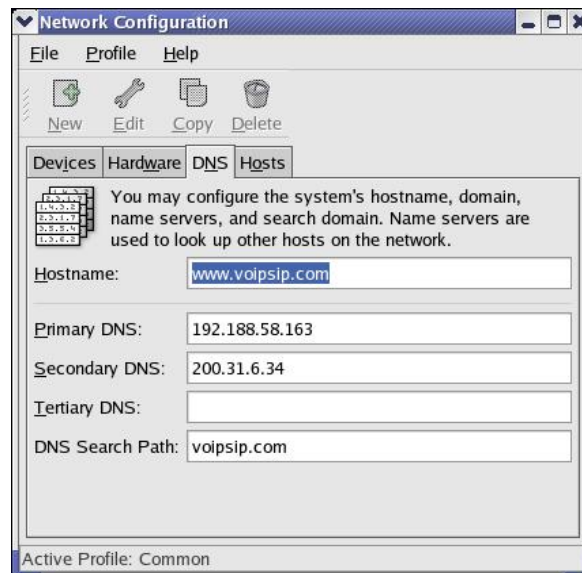


Figura 4.13: Configuración del DNS

## 4.7.2.-Configuración del DNS

Para la configuración del DNS ingresamos al browser de Webmin y damos clic en las siguientes opciones:

- Servers -> BIND DNS Server -> Create master zone.
- Create -> Return to zone list -> Apply changes



Figura 4.14: Crear la zona maestra

- Creamos el registro de direcciones.
- Address -> Create -> Return to zone list -> Apply changes.

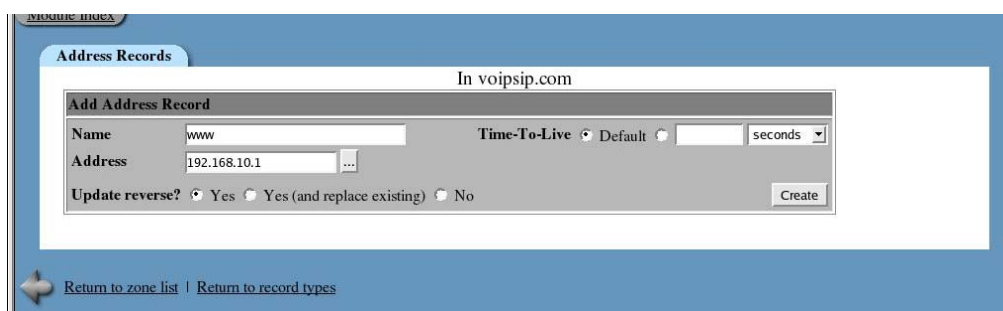


Figura 4.15: Registro de direcciones

- Creamos la zona reversa
- Create new zone -> Reverse (Addresses to Name)
- Create -> Return zone list -> Apply changes.

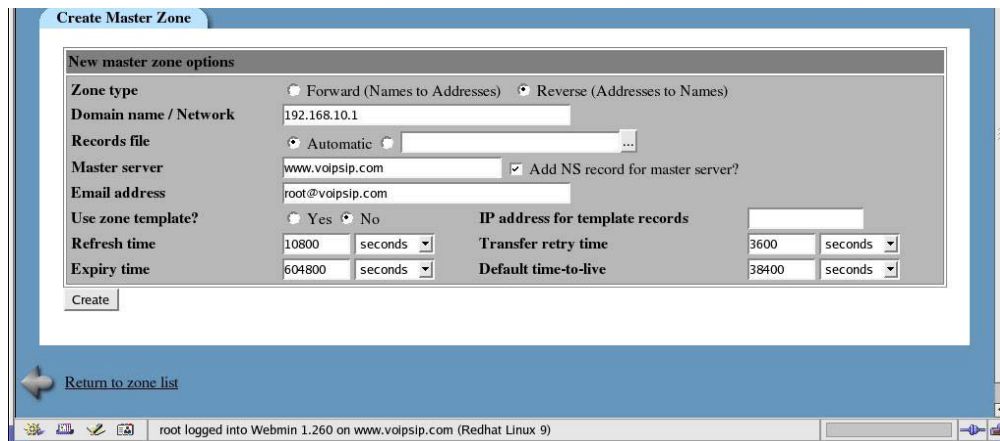


Figura 4.16: Zona reversa

- Creamos el registro de direcciones de reversa.
- Reverse Address -> Create -> Return to zone list -> Apply changes.

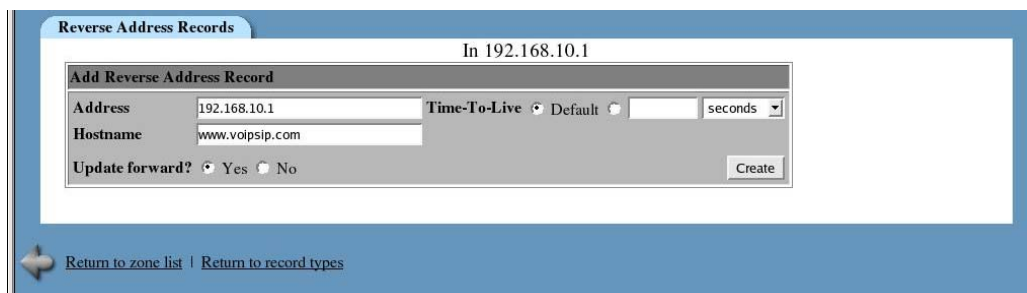


Figura 4.17: Registro de direcciones de reversa

- Creamos la zona reversa de la dirección que va a salir a Internet.
- Create new zone -> Reverse (Addresses to Name)
- Create -> Return zone list -> Apply changes.
- Reverse Address -> Create -> Return to zone list -> Apply changes.
- En la zona voip.com creamos el registro de direcciones de la dirección IP de salida al Internet.
- De la misma forma en la zona de dirección IP del servidor se crea el registro de direcciones de salida al Internet.

### 4.7.3.-Configuración de DHCP

Para la configuración de DHCP sólo se debe modificar los siguientes parámetros:

- Option routers: 192.168.10.1
- Option subnet-mask: 255.255.255.0
- Option domain-name: "www.voipsip.com"
- Option domain-name-servers: 192.168.10.1
- Range dynamic-bootp: 192.168.10.5 192.168.10.20

### 4.7.4.-Configuración de Asterisk

La programación de los ficheros se encuentra en /etc/asterisk.

- **phone.conf**

echocancel = high (para cancelar el eco)

#### 4.7.4.1.- Configuración del servidor SIP

Para configurar el servidor SIP se debe modificar lo siguiente:

- **sip.conf**

Cuadro 4.1: Fichero sip.conf

```
[general]

context = default
realm = 192.168.10.1
port = 5060
bindport=5060
bindaddr=0.0.0.0
dtmfmode = rfc2833
disallow = all
allow = ulaw
allow = ilbc
allow = gsm
```



- 1) *context*: Define el contexto por defecto para todos los clientes definidos y será el valor a utilizar a menos que se defina un contexto diferente dentro de la configuración propia del cliente SIP.
- 2) *realm*: El dominio de autenticación de SIP, 192.168.10.1.
- 3) *port*: El puerto en el que se escuchan las conexiones SIP entrantes. El valor por defecto es 5060.
- 4) *bindport*: Puerto por donde escuchará asterisk, 5060.
- 5) *bindaddr*: La dirección IP en la que se escuchan las conexiones SIP entrantes. Si la máquina tiene múltiples direcciones IP esta opción permite seleccionar una de estas como dirección de conexión, de otra manera el sistema escuchará en todas las direcciones IP disponibles.
- 6) *Dtmfmode*: Define el modo en que el cliente maneja la señalización DTMF, también es usado para determinar como se debe escuchar los tonos, como cuando alguien marca una extensión (RFC 2833<sup>55</sup>).
- 7) *disallow*: <codec>/all. Desactiva todos los codecs.
- 8) *allow*: <codec>. Permite el uso de codecs en orden de preferencia. Se debe utilizar disallow = all antes de poder asignar codecs con este parámetro.

#### **4.7.4.2.- Definición de canales**

Para esto se tiene que editar nuevamente el archivo sip.conf. Los clientes deben ser declarados en este archivo antes de poder recibir o hacer llamadas.

Por lo tanto para que se puedan usar los canales SIP, los usuarios SIP (Véase los cuadros 4.2, 4.3 y 4.4) deben tener permiso para registrarse en asterisk vía SIP.

---

<sup>55</sup> Véase en glosario de términos

Cuadro 4.2: Usuario 1

```
[jessy]

type=friend
secret=password
username=jessy
host=dynamic
nat=no
callerid="Jessyka" <215>
qualify=1000
mailbox=215
context=med
transfer=yes
disallow=all
allow=gsm
allow=ulaw
allow=ilbc
```

Cuadro 4.3: Usuario 2

```
[ale]

type=friend
secret=password
username=ale
host=dynamic
nat=no
callerid="Alexandra" <216>
mailbox=216
context=med
transfer=yes
qualify=1000
disallow=all
allow=gsm
allow=ulaw
allow=ilbc
```

Cuadro 4.4: Usuario 3

```
[jose]

type=friend
secret=password
username=jose
host=dynamic
nat=no
qualify=1000
transfer=yes
callerid="Jose" <217>
mailbox=217
context=med
disallow=all
allow=gsm
allow=ulaw
allow=ilbc
```

- 1) *type*: Define la clase de conexión que tendrá el cliente. Las opciones disponibles son:
  - *peer*: Dispositivo que recibe llamadas desde un servidor PBX.
  - *user*: Dispositivo que hace llamadas a través de un servidor PBX.
  - *friend*: Dispositivo que puede hacer y recibir llamadas a través de un servidor PBX.
- 2) *secret*: Define la contraseña del cliente. Recibe un valor alfanumérico.
- 3) *username*: Define el nombre de usuario o el número de la extensión definida en el plan de numeración del servidor DreamPBX. Por lo general este valor debe ser el mismo que utiliza el cliente para registrarse.
- 4) *host*: Define la dirección IP o el nombre del dispositivo (que se pueda resolver a través de un DNS). También puede tomar el valor de "dynamic", en este caso se espera una conexión desde cualquier dirección IP. Esta opción es de utilidad en redes que utilizan asignaciones dinámicas de IP con DHCP.
- 5) *nat*:( yes o no) Define si el servidor está detrás de NAT o no.
- 6) *qualify*: Verifica si el cliente es alcanzable.
- 7) *transfer*: Para transferir llamadas.
- 8) *callerid*: Para identificar a un usuario cuando realice una llamada.

- 9) Mailbox: Número del Buzón de voz que posee cada usuario.

#### 4.7.4.3.- Configuración del Plan de Marcación

El fichero `extensions.conf` es el corazón del funcionamiento de Asterisk, aquí se define como se deben manejar las llamadas. Consiste en una lista de instrucciones que Asterisk debe seguir, que son iniciados por dígitos recibidos por un canal o alguna aplicación.

El plan de marcación está formado por cuatro partes principales: `contexts`, `extensions`, `priorities` y `applications`.

- 1) *context*: son nombres de grupos de extensiones, estos contienen partes diferentes del plan de marcación e interactúan entre ellos. Una extensión es definida en un contexto.
- 2) *extensions*: dentro de cada contexto se puede definir una o más extensiones. Una extensión es una instrucción que asterisk ejecutará, activado por una llamada entrante o por dígitos marcados en un canal. Las extensiones especifican que sucede con las llamadas, como hacer sus vías a través del plan de marcado. Una extensión completa consta de tres componentes:
  - El nombre o número de la extensión.
  - La prioridad, cada extensión puede incluir múltiples pasos; el número de paso es llamado la "prioridad".
  - La aplicación o comando que ejecuta algunas acciones en la llamada.
- 3) *priorities*: cada extensión puede tener múltiples pasos, llamadas prioridades. Cada prioridad es numerada secuencialmente, empezando con 1. Cada prioridad ejecuta una aplicación específica.
- 4) *applications*: son el trabajo pesado del plan de marcado. Cada aplicación realiza una acción específica en el canal actual, como el modo de tocar un sonido, aceptando el tono de entrada o al colgar la llamada.

- **extensions.conf**

Cuadro 4.5: Fichero extensión.conf

```
[med]

exten => 215,1,Answer
exten => 215,2,Dial(SIP/jessy,10)
exten => 215,3,Voicemail(215@context)
exten => 215,4,Hangup

exten => 216,1,Answer
exten => 216,2,Dial(SIP/ale,10)
exten => 216,3,Voicemail(216@context)
exten => 216,4,Hangup

exten => 217,1,Answer
exten => 217,2,Dial(SIP/jose,10)
exten => 217,3,Voicemail(217@context)
exten => 217,4,Hangup

exten => 501,1,Meetme(700|M)

exten=> 500,1,VoiceMailMain (mailbox@context)

exten => 9000,1,WaitMusicOnHold(20)
```

A continuación se detalla la definición de una extensión:

1. *exten*: permite declarar una extensión.
2. *215*: es el número de extensión que se marca.
3. *1, 2, 3 y 4*: representa la prioridad, la cual determina el orden en el que se ejecutarán las aplicaciones.
4. *dial()*: pasa la llamada por el canal SIP que pertenece al usuario (en este caso *jessy*) y el teléfono de esta extensión (*215*) sonará durante 10 segundos, en caso de que la llamada no sea contestada, se enviará al buzón de voz.
5. *voicemail()*: conectara a la casilla del buzón de voz, con la finalidad de dejar el mensaje de voz, en este caso el número de la casilla del usuario *ale* es 500.

#### 4.7.4.4.- Aplicaciones del Servidor

Los ficheros que se utilizan para las aplicaciones de buzón de voz, conferencia, llamada en espera y transferencia de llamadas, deben estar ligados con otros ficheros para que puedan culminar su ejecución.

##### 4.7.4.4.1.- voicemail.conf

La casilla de voz o voicemail, es el encargado de configurar los parámetros para el sistema de buzón de voz.

El archivo esta dividido en dos secciones, la sección general, que contiene distintos parámetros, en este caso solo utilizaremos el que indica en que formato se guardan los mensajes recibidos y el idioma en el que se escuchará la grabación de la casilla. La segunda sección indica la configuración individual de cada casilla.

El formato para declarar una casilla de voz es la siguiente:

*password, nombre, dirección de mail para los mensajes de voz*

Cuadro 4.6: Fichero voicemail.conf

```
[general]

format=wav
language=SetLanguage(es)
sendvoicemail=yes

[other]

215 => 1234,jessy,jessy@voipsip.com
216 => 4567,ale,ale@voipsip.com
217 => 7890,jose,jose@voipsip.com
```

- 1) *format*: Define el formato en cual será grabado el mensaje de voz.
- 2) *language*: Especifica el idioma que será utilizado para los mensajes.

- 3) *sendvoicemail*: contexto para enviar desde el voicemail, si no escucha, envía un mensaje desde el voicemail que no será permitido.

#### 4.7.4.4.2.- **meetme.conf**

Para habilitar una sala de conferencia tenemos que editar `meetme.conf`, en `extensions.conf` definiendo el número (en este caso 501) y este llama a la sala 700, así que solo hay que definir una sala 700 en `meetme.conf`.

No se necesita password, ni siquiera algún tipo de identificación, ya que el que llame, será agregado a la conferencia.

Cuadro 4.7: Fichero `meetme.conf`

```
[rooms]
conf => 700
```

#### 4.7.4.4.3.- **musichold.conf**

Para una llamada en espera se debe definir en el fichero `extensión.conf` el número 9000 para escuchar la música que reproduce Asterisk para este servicio.

Para habilitarlo hay que descomentar lo siguiente en el fichero `zapata.conf`.

```
musiconhold=default
```

Cuadro 4.8: Fichero musichold.conf

```
[moh_files]

default => /var/lib/asterisk/moh-native,r
acc_1 => mp3:/var/lib/asterisk/mohmp3/acc_1
acc_2 => mp3:/var/lib/asterisk/mohmp3/acc_2
acc_3 => mp3:/var/lib/asterisk/mohmp3/acc_3
acc_4 => mp3:/var/lib/asterisk/mohmp3/acc_4
acc_5 => mp3:/var/lib/asterisk/mohmp3/acc_5
acc_6 => mp3:/var/lib/asterisk/mohmp3/acc_6
acc_7 => mp3:/var/lib/asterisk/mohmp3/acc_7
acc_8 => mp3:/var/lib/asterisk/mohmp3/acc_8
acc_9 => mp3:/var/lib/asterisk/mohmp3/acc_9
acc_10 => mp3:/var/lib/asterisk/mohmp3/acc_10
```

#### 4.7.5.-Configuración de Usuario del Softphone

Por cada PC se debe registrar el usuario que corresponde, para lo cual se debe seguir los siguientes pasos:



Figura 4.18: Usuario no registrado



- Clic en el botón Options, el cual mostrará el panel principal de opciones del Siphone. Elija la pestaña User Information y se llena los campos con los datos del usuario.

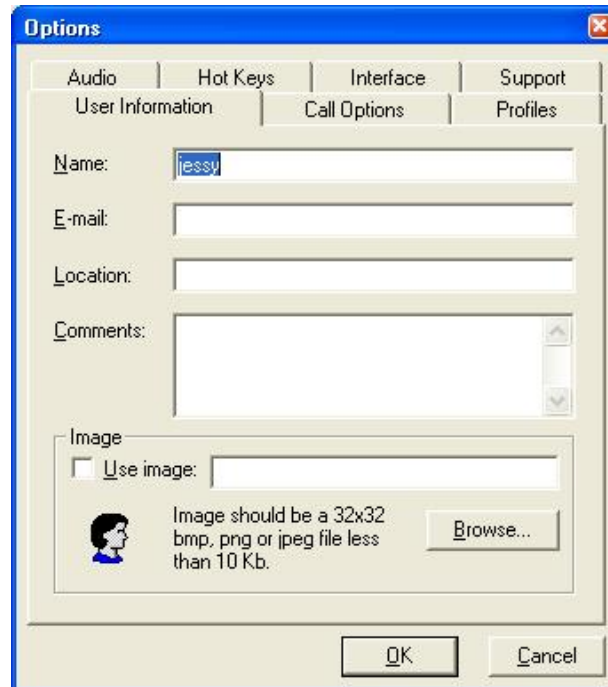


Figura 4.19: Pestaña User Information

- Luego se selecciona la pestaña Profiles -> New -> Ok.

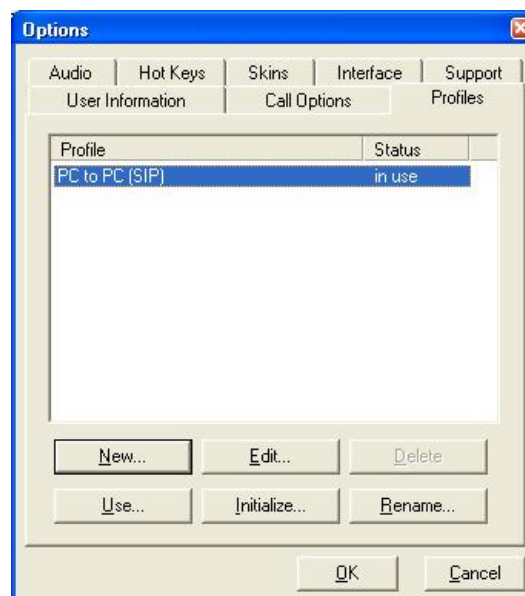


Figura 4.20: Pestaña Profiles

- Se ingresa un nombre para el perfil de tipo Calls through SIP Proxy y se presiona el botón OK.

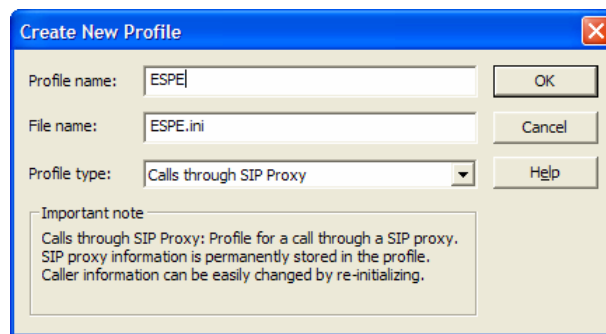


Figura 4.21: Crear Nuevo perfil

- A continuación se borra el anterior perfil, quedando así el perfil anteriormente creado. Seleccione el perfil ESPE -> Edit -> Ok.

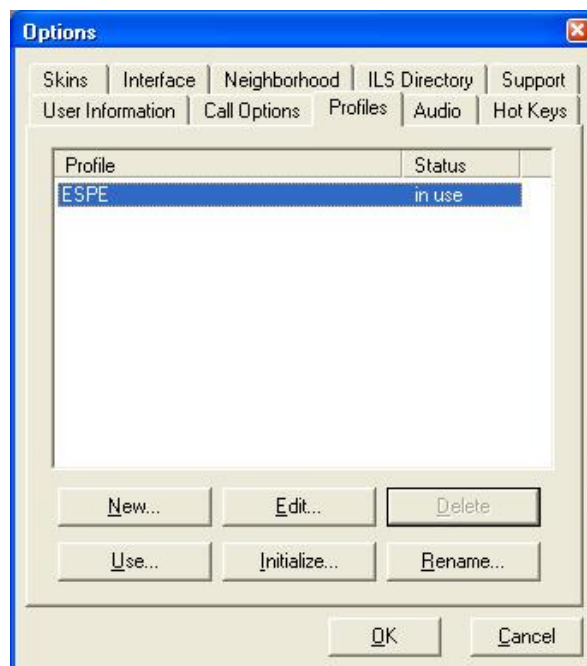


Figura 4.22: Perfil Creado

- En la ventana Opciones del Perfil, seleccione la pestaña SIP Proxy e ingrese la dirección IP del Proxy, el puerto del Proxy y Nat y -> Ok.

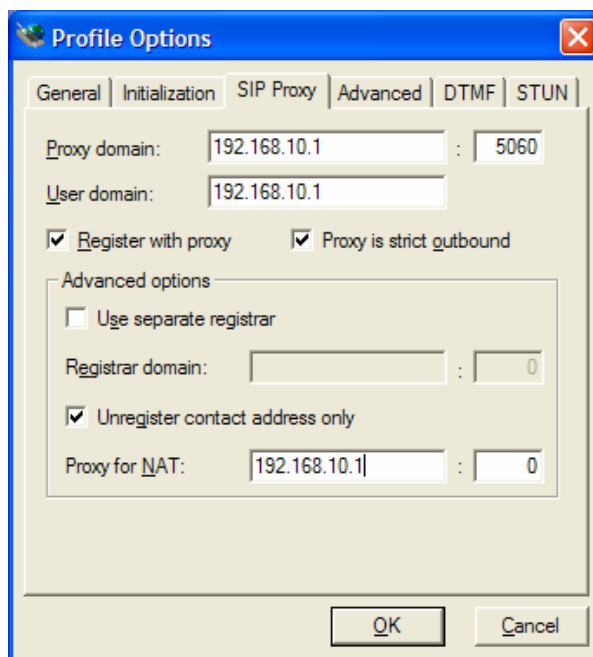


Figura 4.23: Opciones del Perfil

- o Además, en la pestaña Advanced es necesario seleccionar el uso del estado de mensajes estándar e ingresar el número de la casilla de voz asignado, el mismo que se encuentra creado en el fichero extensions.conf y el número de buzón de voz en el fichero voicemail.conf del servidor.

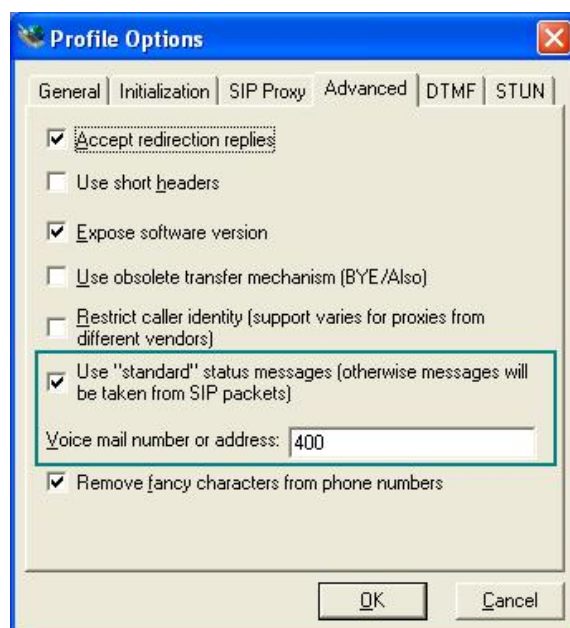


Figura 4.24: Opciones del Perfil Avanzadas

- En esta pantalla ingresamos el nombre de usuario y contraseña para autenticar que sea el mismo que se encuentra previamente creado en el archivo sip.conf.

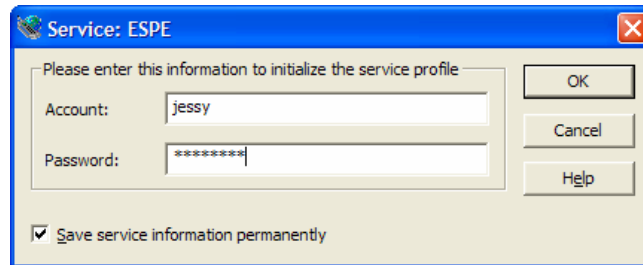


Figura 4.25: Información del usuario

- De esta manera queda configurado el usuario, como se indica en la siguiente imagen:



Figura 4.26: Usuario Registrado

#### 4.7.6.-Llamadas entre Usuarios

Para dar comienzo al Sjphone, diríjase a Inicio -> Todos los programas -> Sjphone -> SJphone. O puede hacerlo a través del acceso directo que se encuentra en el escritorio.



Figura 4.27: Acceso Directo a Sjphone

Luego nos muestra la pantalla inicial del softphone.



Figura 4.28: Pantalla Inicial del Sjphone

Cuando recibimos una llamada inmediatamente aparecerá una pantalla con un mensaje de llamada entrante:



Figura 4.29: Mensaje de llamada entrante

Para contestar la llamada, hacemos clic en el botón Accept o para rechazar la llamada hacemos clic en el botón Ignore.

Una vez que aceptamos la llamada, esta se muestra en la pantalla del S/Jphone de color verde (Véase la figura 4.30), con el nombre de usuario, el tiempo de duración de la llamada y el codec que está en uso.

Para realizar una llamada se debe marcar el número de la extensión o escribir el nombre con que se encuentra registrado y presionar Enter o dar clic en el botón Dial o a su vez, se puede dar doble clic en el nombre con el que se encuentra registrado en el libro de direcciones.

Si la línea se encuentra ocupada o no contesta, el teléfono sonará durante 10 segundos, para luego escuchar una operadora donde se puede dejar un mensaje en el buzón de voz.

Finalmente, para terminar una llamada se debe dar clic en el botón Hang up.



Figura 4.30: Pantalla Inicial del Siphone

La operación básica de una llamada SIP es la siguiente:

- a) Un cliente SIP primero obtiene una dirección donde pueda ser contactado, de la forma "jessy@192.168.10.1". Luego el cliente intenta traducir este dominio a una dirección IP para encontrar un servidor. Esta traducción se hace buscando secuencialmente en registros del servicio DNS, MX (intercambio de correo), CNAME (Canonical Name) y finalmente en los registros de direcciones.
- b) Una vez que la dirección IP del servidor fue hallada, el usuario jessy (192.168.10.16) envía el método INVITE usando ya sea UDP o TCP al servidor SIP (192.168.10.1), para llamar al usuario jose ([217@192.168.10.1](mailto:217@192.168.10.1)).
- c) En seguida el Servidor SIP, intenta localizar la llamada emitiendo una respuesta que se requiere una autenticación Proxy (407) desde el usuario jessy hacia el usuario jose.
- d) El usuario jessy confirma (ACK) que el usuario 217@192.168.10.1 ha recibido una respuesta final al método (INVITE).
- e) El servidor envía un mensaje provisional (100 -Trying), el cual le indica que está timbrando.

- f) Cuando se a realizado la llamada satisfactoriamente el servidor entrega una respuesta de éxito (200 - Ok) al método INVITE.
- g) Por su parte, el usuario jose responde el request INVITE informando al que llama que puede aceptar o rechazar la llamada.
- h) Cuando el usuario finalizó la llamada se envía el método Bye anunciando que la llamada ha terminado, el mismo que se confirma con una respuesta de éxito (200 - Ok) desde el servidor.



Figura 4.31: Llamada de usuario jessy a usuario jose.

Seguidamente, para comprender de mejor manera la operación de llamada que realiza SIP se utiliza el SJphone Log del softphone (clic derecho en la pantalla del softphone -> show log), en donde se podrá observar en tiempo real la llamada realizada del usuario jessy hacia el usuario jose, como se muestra a continuación:



#### Cuadro 4.9: SJphone Log 1

```
12:43:03 DEBUG
2006-04-24 17:43:03.433 UDP LOCAL->192.168.10.1:5060
REGISTER sip:192.168.10.1 SIP/2.0
Via: SIP/2.0/UDP
192.168.10.16;rport;branch=z9hG4bKc0a80a1000000010444d0e270000609c00000004
Content-Length: 0
Contact: <sip:jessy@192.168.10.16:5060>
Call-ID: C64661F4-EB3A-47AC-8A31-DOCEBFF2CEC5@192.168.10.16
CSeq: 2 REGISTER
From: <sip:jessy@192.168.10.1>;tag=84870238236
Max-Forwards: 70
To: <sip:jessy@192.168.10.1>
User-Agent: SJphone/1.60.289a (SJ Labs)
Authorization: Digest
username="jessy",realm="192.168.10.1",nonce="394255e4",uri="sip:192.168.10.1",response="78d662b50abdd8598257250362740664"

12:43:03 DEBUG
2006-04-24 17:43:03.433 UDP 192.168.10.1:5060->LOCAL
SIP/2.0 100 Trying
Via: SIP/2.0/UDP
192.168.10.16;rport;branch=z9hG4bKc0a80a1000000010444d0e270000609c00000004;r
eceived=192.168.10.16
From: <sip:jessy@192.168.10.1>;tag=84870238236
To: <sip:jessy@192.168.10.1>
Call-ID: C64661F4-EB3A-47AC-8A31-DOCEBFF2CEC5@192.168.10.16
CSeq: 2 REGISTER
User-Agent: www.voipsip.com
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Contact: <sip:jessy@192.168.10.1>
Content-Length: 0
```

Cuadro 4.10: SJphone Log 2

```
12:43:11 DEBUG
2006-04-24 17:43:11.385 UDP 192.168.10.1:5060->LOCAL
NOTIFY sip:jessy@192.168.10.16:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.1:5060;branch=z9hG4bK7aa935bf;rport
From: "asterisk" <sip:asterisk@192.168.10.1>;tag=as75a02a4e
To: <sip:jessy@192.168.10.16:5060>
Contact: <sip:asterisk@192.168.10.1>
Call-ID: 55db48b873fcc1493c07f8531bb8a1f7@192.168.10.1
CSeq: 102 NOTIFY
User-Agent: www.voipsip.com
Max-Forwards: 70
Event: message-summary
Content-Type: application/simple-message-summary
Content-Length: 92

Messages-Waiting: no
Message-Account: sip:asterisk@192.168.10.1
Voice-Message: 0/0 (0/0)

12:43:11 DEBUG
2006-04-24 17:43:11.385 UDP LOCAL->192.168.10.1:5060
SIP/2.0 200 OK
Via: SIP/2.0/UDP
192.168.10.1:5060;rport=5060;received=192.168.10.1;branch=z9hG4bK7aa935bf
Content-Length: 0
Call-ID: 55db48b873fcc1493c07f8531bb8a1f7@192.168.10.1
CSeq: 102 NOTIFY
From: "asterisk"<sip:asterisk@192.168.10.1>;tag=as75a02a4e
Server: SJphone/1.60.289a (SJ Labs)
To: "jessy"<sip:jessy@192.168.10.16:5060>

12:43:14 DEBUG
2006-04-24 17:43:14.529 UDP 192.168.10.1:5060->LOCAL
ACK sip:jessy@192.168.10.16:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.1:5060;branch=z9hG4bK4ca2dd86;rport
From: <sip:217@192.168.10.1>;tag=as29ffb3c
To: "jessy"<sip:jessy@192.168.10.1>;tag=849356323999
Contact: <sip:217@192.168.10.1>
Call-ID: CF67BDCF-A599-4B03-8E0F-6C8E152466D4@192.168.10.16
CSeq: 102 ACK
User-Agent: www.voipsip.com
Max-Forwards: 70
Content-Length: 0
```

### Cuadro 4.11: SJphone Log 3

```
12:43:10 DEBUG
2006-04-24 17:43:10.013 UDP 192.168.10.1:5060->LOCAL
SIP/2.0 200 OK
Via: SIP/2.0/UDP
192.168.10.16;rport;branch=z9hG4bKc0a80a100000001a444d0e2e000077ba00000009;received
=192.168.10.16
From: "jessy"<sip:jessy@192.168.10.1>;tag=849356323999
To: <sip:217@192.168.10.1>;tag=as29ffbe3c
Call-ID: CF67BDCF-A599-4B03-8E0F-6C8E152466D4@192.168.10.16
CSeq: 2 INVITE
User-Agent: www.voipsip.com
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Contact: <sip:217@192.168.10.1>
Content-Type: application/sdp
Content-Length: 214

12:43:10 INFO      Media stream information:
Multimedia Engine dump:

Drivers:
  Driver Audio Output: started
  Driver Audio Input:  started

Session: ID( 26 )

Channels:
  Channel Audio Input:  started
    Capability: undefined
    Local  RTP  = 0.0.0.0 : 49152
    Local  RTCP = 0.0.0.0 : 49153
    Remote RTP  = 192.168.10.1 : 18072
    Remote RTCP = 192.168.10.1 : 18073
    RFC2833 Enabled ( Payload Type = 101 )

  Channel Audio Output: started
    Capability: Microsoft CCITT G.711 u-Law CODEC
    Local  RTP  = 0.0.0.0 : 49152
    Local  RTCP = 0.0.0.0 : 49153
    Remote RTP  = 192.168.10.1 : 18072
    Remote RTCP = 192.168.10.1 : 18073
```

#### Cuadro 4.12: SJphone Log 4

```
12:43:10 DEBUG
2006-04-24 17:43:10.013 UDP LOCAL->192.168.10.1:5060
INVITE sip:217@192.168.10.1 SIP/2.0
Via: SIP/2.0/UDP
192.168.10.16;rport;branch=z9hG4bKc0a80a100000001a444d0e2e000077ba00000009
Content-Length: 221
Contact: <sip:jessy@192.168.10.16:5060>
Call-ID: CF67BDCF-A599-4B03-8E0F-6C8E152466D4@192.168.10.16
Content-Type: application/sdp
CSeq: 2 INVITE
From: "jessy"<sip:jessy@192.168.10.1>;tag=849356323999
Max-Forwards: 70
To: <sip:217@192.168.10.1>
User-Agent: SJphone/1.60.289a (SJ Labs)
Proxy-Authorization: Digest
username="jessy", realm="192.168.10.1", nonce="7e75ead6", uri="sip:217@192.168.
10.1", response="f6c5906db43c3841709d23eb794a672c"

12:43:10 DEBUG
2006-04-24 17:43:10.013 UDP 192.168.10.1:5060->LOCAL
SIP/2.0 100 Trying
Via: SIP/2.0/UDP
192.168.10.16;rport;branch=z9hG4bKc0a80a100000001a444d0e2e000077ba00000009;r
eceived=192.168.10.16
From: "jessy"<sip:jessy@192.168.10.1>;tag=849356323999
To: <sip:217@192.168.10.1>
Call-ID: CF67BDCF-A599-4B03-8E0F-6C8E152466D4@192.168.10.16
CSeq: 2 INVITE
User-Agent: www.voipsip.com
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Contact: <sip:217@192.168.10.1>
Content-Length: 0
```

Cuadro 4.13: SJphone Log 5

```
12:43:10 DEBUG
2006-04-24 17:43:10.003 UDP 192.168.10.1:5060->LOCAL
SIP/2.0 407 Proxy Authentication Required
Via: SIP/2.0/UDP
192.168.10.16;rport;branch=z9hG4bKc0a80a100000001a444d0e2d00005adc00000008;r
eceived=192.168.10.16
From: "jessy"<sip:jessy@192.168.10.1>;tag=849356323999
To: <sip:217@192.168.10.1>;tag=as5d871aeb
Call-ID: CF67BDCF-A599-4B03-8E0F-6C8E152466D4@192.168.10.16
CSeq: 1 INVITE
User-Agent: www.voipsip.com
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Contact: <sip:217@192.168.10.1>
Proxy-Authenticate: Digest realm="192.168.10.1", nonce="7e75ead6"
Content-Length: 0

12:43:10 DEBUG
2006-04-24 17:43:10.003 UDP LOCAL->192.168.10.1:5060
ACK sip:217@192.168.10.1 SIP/2.0
Via: SIP/2.0/UDP
192.168.10.16;rport;branch=z9hG4bKc0a80a100000001a444d0e2d00005adc00000008
Content-Length: 0
Call-ID: CF67BDCF-A599-4B03-8E0F-6C8E152466D4@192.168.10.16
CSeq: 1 ACK
From: "jessy"<sip:jessy@192.168.10.1>;tag=849356323999
Max-Forwards: 70
To: <sip:217@192.168.10.1>;tag=as5d871aeb
User-Agent: SJphone/1.60.289a (SJ Labs)
```

#### Cuadro 4.14: SJphone Log 6

```
12:43:03 DEBUG
2006-04-24 17:43:03.463 UDP 192.168.10.1:5060->LOCAL
SIP/2.0 200 OK
Via: SIP/2.0/UDP
192.168.10.16;rport;branch=z9hG4bKc0a80a1000000010444d0e270000609c00000004;received=192.168.
10.16
From: <sip:jessy@192.168.10.1>;tag=84870238236
To: <sip:jessy@192.168.10.1>;tag=as3d4ddb8
Call-ID: C64661F4-EB3A-47AC-8A31-DOCEBFF2CEC5@192.168.10.16
CSeq: 2 REGISTER
User-Agent: www.voipsip.com
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Expires: 120
Contact: <sip:jessy@192.168.10.16:5060>;expires=120
Date: Mon, 24 Apr 2006 17:49:01 GMT
Content-Length: 0

12:43:03 INFO      Registration of sip:jessy@192.168.10.1 succeeded.
12:43:03 INFO      Network interfaces state monitoring started
12:43:03 INFO      Discovery procedure for local network interface 192.168.10.16 : 0
initiated
12:43:03 INFO      Importing components...
12:43:03 INFO      Import complete
12:43:09 INFO      Initiating SIP call to sip:217@192.168.10.1

12:43:10 DEBUG
2006-04-24 17:43:10.003 UDP LOCAL->192.168.10.1:5060
INVITE sip:217@192.168.10.1 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.16;rport;branch=z9hG4bKc0a80a100000001a444d0e2d00005adc00000008
Content-Length: 221
Contact: <sip:jessy@192.168.10.16:5060>
Call-ID: CF67BDCF-A599-4B03-8E0F-6C8E152466D4@192.168.10.16
Content-Type: application/sdp
CSeq: 1 INVITE
From: "jessy"<sip:jessy@192.168.10.1>;tag=849356323999
Max-Forwards: 70
To: <sip:217@192.168.10.1>
User-Agent: SJphone/1.60.289a (SJ Labs)
```

Cuadro 4.15: SJphone Log 7

```
12:44:40 INFO          HangUp

12:44:40 DEBUG
2006-04-24 17:44:40.691 UDP LOCAL->192.168.10.1:5060
BYE sip:217@192.168.10.1 SIP/2.0
Via: SIP/2.0/UDP
192.168.10.16;rport;branch=z9hG4bKc0a80a10000000eb444d1dc40000038300000331
Content-Length: 0
Call-ID: 8C53FDE2-5C32-47FC-980D-46A0183762FC@192.168.10.16
CSeq: 3 BYE
From: "jessy"<sip:jessy@192.168.10.1>;tag=123513202155
Max-Forwards: 70
To: <sip:217@192.168.10.1>;tag=as05f10a4a
User-Agent: SJphone/1.60.289a (SJ Labs)
Proxy-Authorization: Digest
username="jessy",realm="192.168.10.1",nonce="66a2aa23",uri="sip:217@192.168.10.1",response="6ec89c2a04fce172eb8c1eaa87a95843"

12:44:40 DEBUG
2006-04-24 17:44:40.691 UDP 192.168.10.1:5060->LOCAL
SIP/2.0 200 OK
Via: SIP/2.0/UDP
192.168.10.16;branch=z9hG4bKc0a80a10000000eb444d1dc40000038300000331;received=192.168.10.16;rport=5060
From: "jessy"<sip:jessy@192.168.10.1>;tag=123513202155
To: <sip:217@192.168.10.1>;tag=as05f10a4a
Call-ID: 8C53FDE2-5C32-47FC-980D-46A0183762FC@192.168.10.16
CSeq: 3 BYE
User-Agent: www.voipsip.com
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Contact: <sip:217@192.168.10.1>
Content-Length: 0
X-Asterisk-HangupCause: Normal Clearing

12:49:40 INFO          Call 235 ended: Hangup acknowledged
12:49:40 INFO          SIP: Session terminated.
```

El encabezado Via hace un trazado del progreso de la invitación de cliente a servidor, permitiendo que las respuestas encuentren el camino de regreso y ayuda a los servidores a encontrar loops.

Después que se recibe e interpreta el mensaje de solicitud SIP, el receptor del mismo responde con un mensaje o varios de respuesta (código de estado). La respuesta tiene un código y un mensaje. Los códigos se dividen en clases, al modo de HTTP, del 100 al 600, por ejemplo 100 es Trying.

#### 4.7.6.1.- Informaciones Adicionales

En la tabla 4.2 encontraremos los nombres de usuario, número de extensión, número de buzón de voz y la contraseña asignada a cada usuario:

Tabla 4.2: Usuarios de la red.

Usuarios	Contraseña	Extensión	Número de Casilla de Voz	Contraseña Buzón de Voz
jessy	password	215	400	1234
ale	password	216	500	4567
jose	password	217	600	7890

- Para realizar una conferencia se debe dar doble clic en el botón de conferencia “Conf” en el panel principal del SJphone o también, haciendo doble clic en el nombre de usuario en libro de direcciones.
- Para transferir una llamada se debe marcar la extensión o buscar en el libro de direcciones el nombre de la persona a la cual se requiere pasar la llamada.
- Para poner música en espera a una llamada se debe dar clic en el botón hold o a su vez dar doble clic en la llamada.

##### 4.7.6.1.1.- Buzón de Correo

1. Si se desea escuchar los mensajes de voz puede marcar el número de buzón de voz asignado para cada usuario respectivamente o presionar el botón de buzón de voz en el Sjphone, que permite acceder a este servicio, por ejemplo uno de los números es: 400.
2. En seguida se escuchará a la operadora, la cual pedirá el password de la casilla de voz.
3. Para el usuario jessy el password de buzón de voz es el 1234.
4. Se debe tener en cuenta que los mensajes de voz están en el siguiente path en el servidor SIP:



/var/spool/asterisk/voicemail/<context>/<mailbox>/INBOX

#### 4.7.6.1.2.- Codecs

Durante la práctica se realizó varias pruebas utilizando los diferentes codecs que soporta el Siphone. Para escoger el codec que nos permita obtener una llamada con calidad se debe tomar en cuenta varios factores como: eco, retardo, interferencias, etc.

Tabla 4.3: Codecs del Siphone.

Codec	G.711 (u-law)	ILBC (30ms)	GSM	ILBC (20ms)
Eco y Volumen	Poco	Corto y Alto	Largo y Mediano	Incapacidad de comunicación entre los medios
Desempeño al hacer multitareas	Bueno	Bueno	Bueno	
Retardo	Poco	Poco	Poco	
Interferencias			Distorsión en la voz (Poco)	
Soporta	Si	Si	Si	

De acuerdo a la tabla 4.3, el codec que mejor desempeño y funcionalidad tuvo durante la llamada fue G.711, debido a que presenta poco retardo y eco en la voz, causando menor dificultad en la interacción entre usuarios. Además es un codec de libre distribución.

Su limitante es que ocupa 64 kbps del ancho de banda, cuya desventaja se puede presentar en un momento de excesiva congestión en la red, por lo cual se recomienda pedir al proveedor más ancho de banda y poner prioridades a los paquetes de voz para evitar congestión o a su vez se puede usar un codec que consuma menos ancho de banda como por ejemplo el codec G.729, por el cual se debe pagar una licencia por cada usuario.

## Capítulo V: Conclusiones y Recomendaciones

### 5.1.- Conclusiones

- La continua evolución de las redes basadas en el Protocolo Internet (IP) permite la penetración de diversas aplicaciones tales como las llamadas telefónicas sobre infraestructura de red IP o a través de Internet, la convergencia de las redes de voz y de datos sobre un protocolo común y el desarrollo de multimedia.
- La tecnología seguirá evolucionando hacia un escenario final donde dispondremos de una red multiservicio que integre todo tipo de contenidos (voz, vídeo y datos) y que nos permita entregarlos de forma personalizada a cualquier tipo de usuario, en cualquier tipo de terminal, con la calidad requerida e independientemente de donde se encuentren ubicados.
- El despliegue de servicios de telefonía basados en VoIP y las peculiaridades de éstos en comparación con el servicio tradicional y los requisitos de interoperabilidad de todas estas tecnologías, hacen necesario disponer de una tecnología que facilite las labores de identificación de cada usuario independientemente de número y tecnología de soporte de dicho servicio (RTC, RDSI, SIP, H.323, etc.).
- En general la arquitectura de red IP básica da lugar a tiempos de transmisión variables, en particular cuando el tráfico es intenso. Por ejemplo, puesto que en Internet no hay un control total de la gestión del tráfico, la calidad de extremo a extremo no puede garantizarse y por lo general sólo se ofrece una transmisión de paquetes con arreglo a la fórmula del "mejor esfuerzo".
- VoIP utiliza el mismo medio de transmisión y la misma salida de cableado estructurado, sin que afecten ni interfieran a las señales de voz y las señales de datos. Además se reducen los costos al usar la misma infraestructura de red LAN y WAN con la que la ESPE ya dispone, para proporcionar nuevos servicios tanto en lugar como en funcionalidad.

- Los costos de administración de sistemas basados en VoIP son más económicos que los propietarios de PBX tradicionales, permitiendo incrementar la productividad de los empleados.
- Se escogió el protocolo SIP porque posee muchos puntos como: sencillez, flexibilidad y robustez, adecuado para establecer sesiones de llamadas telefónicas vía Internet. Por lo cual se perfila como la apuesta clara de futuro, con servicios de multiconferencia y multimedia en tiempo real. Además en un mundo IP, con la Web como canal de comunicación por defecto, ofrece cada vez mayor de tecnologías de acceso y soluciones de movilidad, tiene sentido optar decididamente por SIP.
- La potencialidad del protocolo SIP viene dada por los contenidos de los mensajes, ya que permite descomponer las aplicaciones para admitir servicios más complejos, además trata a la voz como una aplicación más de la red y una única infraestructura, SIP puede soportar muchos servicios diferentes, lo que lo hacen un protocolo prometedor.
- Asterisk es un IP-PBX completo con software libre que permite agregarle funcionalidad SIP a un bajo costo; también permite al usuario la opción de control y decisión para contratar el servicio o proveerlo internamente. Además puede trabajar desde un simple servidor de VoIP hasta una compleja PBX conectada a la PSTN a través de una tarjeta Wildcard TDM400P, con esto se puede amoldar a cualquier situación real dentro de una empresa o institución, como es el caso de la ESPE.
- El sistema diseñado para la ESPE permite que cualquier usuario con una conexión a Internet, pueda realizar una llamada telefónica a otro usuario que se encuentre registrado, mediante el uso de su dirección IP o una extensión asignada como único identificador.
- Después de haber realizado varias llamadas utilizando los diferentes codecs disponibles en el SJphone, el que brindó una mejor calidad en la llamada fue el codec G.711 debido alto nivel en la escala del MOS (Mean Opinion Score), ya que presento un mínimo retardo, ninguna distorsión, poco eco en la voz y es de libre distribución, permitiendo así una buena interacción entre el emisor y el

receptor pero cuyo único inconveniente son los 64Kbps que ocupa de ancho de banda.

## **5.2.- Recomendaciones**

- Es importante seleccionar un codec adecuado para el teléfono SIP, para tener un buen audio y poder establecer una cantidad de ancho de banda considerable, ya que si la red se encuentra saturada se debe priorizar los paquetes de voz, para mantener una buena calidad y servicio.
- Las pruebas fueron sobre una red pública, Internet, en la cual se recomienda tomar en cuenta el factor QoS, ya que al no contar con este el costo a asumir es muy elevado en cuanto a pérdidas de paquetes e inteligibilidad de las conversaciones.
- Conocer que codecs puede soportar el softphone, además saber bien las especificaciones como si es de libre distribución o se debe pagar por la licencia, el ancho de banda que ocupan y la calidad de audio de acuerdo al MOS.
- Se debe tener un sistema de Cableado estándar para tener una red de voz eficiente, ya que el eco que se puede producir en el softphone depende de la distancia que existe entre el emisor y el receptor.
- El cableado de las dependencias de la ESPE y sus sedes, deben estar estructurados (voz y datos), todos estos componentes deben cumplir los estándares establecidos para Cableado Estructurado en Edificios Comerciales.
- Se debería implementar este sistema que trabajará de forma paralela a la central, ya que VoIP con SIP es más flexible y escalable lo cual permitirá a futuro integrar mayores aplicaciones; considerando el tipo de codec a utilizar y el ancho de banda disponible.
- Se recomienda como una continuación del protocolo SIP realizar una aplicación de video conferencia compatible con IPv6 y disponible en varias plataformas.

## BIBLIOGRAFÍA

- Internet Communications Using SIP. Sinnreich, Henry.
- IP Telephony - The Integration of Robust VoIP Services. Douskalis, Bill.
- O'Reilly Media, Inc., Agosto 2005. Asterisk The Future of Telephony. Jim Van Meggelen, Jared Smith, and Leif Madsen.

## BIBLIOGRAFIA WEB

- VoIP en la red del operador  
<http://www.aslan.es/boletin/boletin30/acterna.shtml>
- Manual sobre redes basadas en el Protocolo Internet (IP)  
<http://www.itu.int/ITU-D/e-strategy/publications-articles/pdf/IP%20Policy%20Handbook-S.pdf>.
- Tecnología de VoIP  
<http://html.rincondelvago.com/tecnologia-de-voz-sobre-ip.html>
- Telefonía IP  
<http://www.monografias.com/trabajos16/telefonía-senalizacion/telefonía-senalizacion.shtml>
- Protocolos para VoIP  
[http://www.cudi.edu.mx/primavera\\_2005/presentaciones/rodolfo\\_castaneda.pdf](http://www.cudi.edu.mx/primavera_2005/presentaciones/rodolfo_castaneda.pdf).
- Seguridad en el Protocolo VoIP  
<http://www.laflecha.net/articulos/seguridad/voip/>
- Voz IP y Aplicaciones de Comunicación Inteligente  
[http://www.clipmedia.net/galera/PTV/nl\\_3/VozIP.pdf](http://www.clipmedia.net/galera/PTV/nl_3/VozIP.pdf).
- La Capa de Control  
[http://www.telefonica.es/sociedaddelainformacion/pdf/publicaciones/telecomunicacionesng/capitulos/07\\_la\\_capa\\_de\\_control.pdf](http://www.telefonica.es/sociedaddelainformacion/pdf/publicaciones/telecomunicacionesng/capitulos/07_la_capa_de_control.pdf)

- Protocolo MGCP  
[http://telematica.cicese.mx/revistatel/archivos/Telem@tica\\_Anoll\\_No27.pdf](http://telematica.cicese.mx/revistatel/archivos/Telem@tica_Anoll_No27.pdf)
- SIP Center - What is SIP  
<http://www.sipcenter.com/>
- THIS IS THE WAY - Session Initiation Protocol  
[http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/SIP/Session%20Initiation%20Protocol%20\(SIP\)%20Tutorial%20-%20Slides.pdf](http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/SIP/Session%20Initiation%20Protocol%20(SIP)%20Tutorial%20-%20Slides.pdf).
- SIP: Session Initiation Protocol
  - <http://greco.dit.upm.es/~david/TAR/trabajos2002/01-SIP-%20Diego-Acosta.pdf>.
  - [http://www.videnet.gatech.edu/cookbook.es/list\\_page.php?topic=3&url=sip.htm&level=1&sequence=7&name=Session%20Initiation%20Protocol%20\(SIP\)](http://www.videnet.gatech.edu/cookbook.es/list_page.php?topic=3&url=sip.htm&level=1&sequence=7&name=Session%20Initiation%20Protocol%20(SIP))
  - <http://www.ahciet.net/comun/portales/1000/10002/10007/10302/docs/009.pdf>.
  - <http://www.rediris.es/app/ptyoc/store/dl10/memoria.pdf>.
- SIP: Session Initiation Protocol, IRIS-MMEDIA  
[http://www.rediris.es/mmedia/gt/gt2003\\_1/sip-gt2003.pdf](http://www.rediris.es/mmedia/gt/gt2003_1/sip-gt2003.pdf)
- Arquitectura de los sistemas multimedia de Internet ENFOQUES  
<http://www.rediris.es/rediris/boletin/65/enfoque1.pdf>.
- H.323
  - <http://www.comunicaciones.unitronics.es/tecnologia/H.323.html>
  - <http://www.rediris.es/mmedia/salas/>
  - [http://www.videnet.gatech.edu/cookbook.es/list\\_page.php?topic=3&url=H323\\_hardware.htm&level=1&sequence=1&name=H.323](http://www.videnet.gatech.edu/cookbook.es/list_page.php?topic=3&url=H323_hardware.htm&level=1&sequence=1&name=H.323)
  - [http://www.btwsa.com.ar/siteDocs/\\_h323.asp](http://www.btwsa.com.ar/siteDocs/_h323.asp)
- Instalación Asterisk
  - <http://www.asterisk-online.com.ar/wiki/tiki-pagehistory.php?page=Instalaci%C3%B3n+Asterisk&diff=2>

- <http://www.asterisk-online.com.ar/wiki/tiki-index.php?page=Configuraci%C3%B3n+SIP>
- <http://www.asteriskguru.com/tutorials/>
- [http://www.gecko-soft.com/asterisk\\_instalar.html](http://www.gecko-soft.com/asterisk_instalar.html)
- <http://www.linuxmall.cl/ta.html>
  
- Asterisk Software  
<http://www.asterisk.org/download>
  
- SJphones for Asterisk  
<http://www.sjlabs.com/sjp.html>
  
- Glosario
  - <http://www.tugurium.com/gti/index.asp>
  - <http://www.redaccionvirtual.com/redaccion/glosario/default.asp>

## Glosario de Términos

### ACF

Mensaje de confirmación de Admisión

### ARJ

Mensaje de Rechazo de Admisión

### ARQ

Automatic Repeat Request. En comunicaciones, petición del receptor al emisor para que vuelva a transmitir una trama al detectar errores en la recepción.

### ATM

Protocolo orientado a conexiones de alta velocidad para el transporte de varios tipos de tráfico a través de una red. ATM empaqueta los datos en una celda de 53 bytes de longitud fija que se puede intercambiar rápidamente entre conexiones lógicas de una red. El modo de transferencia asincrónica hace referencia a una serie de tecnologías relacionadas de software, hardware y medios de conexión, llamada también ATM.

ATM permite a las redes utilizar los recursos de banda ancha con máxima eficacia, mientras se mantiene la calidad del servicio (QoS) para los usuarios y programas que tengan requisitos estrictos de funcionamiento.

### BCF

BandwidthConfirm

### BRJ

BandwidthReject



## **BRQ**

BandwidthRequest

## **Codec**

Es una abreviatura de Compresor-Decompresor. Describe una especificación implementada en software, hardware o una combinación de ambos, capaz de transformar un archivo con un flujo de datos (stream) o una señal. Los codecs pueden codificar el flujo o la señal (a menudo para la transmisión, el almacenamiento o el cifrado) y recuperarlo o descifrarlo del mismo modo para la reproducción o la manipulación en un formato más apropiado para estas operaciones. Los codecs son usados a menudo en videoconferencias y emisiones de medios de comunicación.

## **DSP**

Digital Signal Processor (Procesador Digital de Señal).

## **EIGRP**

Extended Internal Gateway Routing Protocol. Protocolo implementado en los routers Cisco system que mejora el protocolo IGRP de gateway fronterizo interno.

## **Enrutamiento**

Proceso de descubrimiento de una ruta hacia el host destino. El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

## **Frame Relay**

Sistema de transmisión basado en la conmutación de paquetes, que permite la entrega confiable de paquetes sobre circuitos virtuales (VC), mediante una forma de encapsulamiento HDLC entre dispositivos conectados. Mucha de la funcionalidad de la capa de red se manipula en la capa de Enlace. Algunos de los conceptos usados en Frame Relay han sido incorporados en ATM.

## **FTP**

File Transfer Protocol. Protocolo que define como debe ser la transferencia de ficheros entre computadoras. También se designa por FTP al programa encargado de la transferencia de ficheros utilizando dicho protocolo.

## **Gateway**

Dispositivo que conecta dos redes con diferentes arquitecturas de red, permitiendo la transferencia de datos entre ellas. La pasarela o Gateway ejecuta una conversión de protocolos para poder interconectar las dos redes. Puede implementar diversos niveles de seguridad, como VPN o firewall.

## **HDSL**

High Digital Subscriber Line (Línea Digital de Subscriptor de Alta Velocidad). Tecnología simétrica, que proporciona la misma velocidad de transmisión en ambas direcciones. HDSL es el DSL más avanzado. Se ha utilizado para proporcionar transmisiones T1 sobre el par trenzado existente sin las necesidades adicionales requeridas para los circuitos del T1 como es la instalación de repetidores. HDSL precisa de dos pares de cables y admite distancias de hasta 3.5 Km, mientras que HDSL-2 precisa solamente de un par de cables y distancias de hasta 5.5 Km. HDSL no permite compartir la línea con los teléfonos analógicos.

## **HTTP**

HyperText Transfer Protocol, es el protocolo de alto nivel del World-Wide-Web que rige el intercambio de mensajes entre clientes y servidores del Web. Su característica principal es la de no mantener la conexión entre transacciones. Diseñado para atender a sistemas hipermedia.

## **ICQ**

Sistema de búsqueda de usuarios asociados a un grupo conectados a Internet. Desarrollado por Mirabilis en 1995, se ha convertido en uno de los programas de mensajería instantánea más extendidos. Por medio de este programa se puede hablar, enviar mensajes y archivos, jugar o usarlo como una herramienta de trabajo, todo ello

en tiempo real. Permite seleccionar la forma de comunicación que se desee, texto, voz, conferencias en grupo, transferencia de archivos.

## **IDS**

Intrusion Detection System. Sistema para monitorizar los eventos de un sistema o red en busca de signos que indiquen problemas de seguridad. Está compuesto por tres elementos fundamentales: fuentes de información, motor de análisis y mecanismos de respuesta.

## **IETF**

Internet Engineering Task Force (Grupo de Trabajo en Ingeniería de Internet). Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad. Fue creada en EE.UU. en 1986.

## **IP**

Internet Protocol (Protocolo de Internet). Protocolo de red de nivel 3 (según el modelo OSI) que proporciona las funciones de encaminamiento de datagramas a través de una interconexión de redes. Las direcciones de los ordenadores base emplean un campo de 32 bits, que se divide en uno, dos o tres octetos de número de red. El resto se emplea para el direccionamiento dentro de las redes. Se empleó inicialmente en la red DARPA. Este protocolo no proporciona recuperación de errores, control de flujo, ni garantiza la fiabilidad de la red física, que quedaron en el protocolo TCP.

## **IP Multicast**

Extensión de la tecnología del multicasting de la red de área local a una red del TCP/IP. Los ordenadores principales envían y reciben los datagramas del multicast, los campos de destinación de los cuales especifican direccionamientos del grupo del ordenador principal del IP más bien que direccionamientos individuales del IP. Un ordenador principal indica que es un miembro de un grupo por medio del protocolo de la gerencia del grupo del Internet.

## **IPS**

Intrusion Prevention System (Sistema de prevención de intrusiones). Sistema que combina las capacidades de bloqueo de un cortafuegos y las de análisis de un IDS. Está diseñado para detener ataques antes de que tengan éxito.

## **LAN**

Local Area Network (Red de Área Local). Red de ordenadores de reducidas dimensiones. Por ejemplo una red distribuida en una planta de un edificio.

## **LDAP**

Lightweight Directory Access Protocol, es un protocolo de red que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP puede considerarse una base de datos (aunque su sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas.

## **MPEG**

Moving Picture Experts Group. Es un estándar de compresión de audio, video y datos establecido por la Unión Internacional de Telecomunicaciones.

Originariamente había 4 tipos diferentes MPEG-1, 2 ,3 y 4 que se diferencian en la calidad y ancho de banda usado. Ofrece tres ventajas: compatibilidad mundial, gran compresión y poca degradación de la imagen. Una cadena MPEG se compone de tres capas: audio, video y una capa a nivel de sistema. Esta última incluye información sobre sincronización, tiempo, calidad, etc.

## **OSI**

Open System Interconnection. Conjunto de normas, definidas por la ISO, para la comunicación de los sistemas abiertos y las reglas para llevar a cabo su implantación. Define una estructura de protocolos en siete niveles o capas. En una estación de trabajo el control se transfiere de un nivel al siguiente hasta llegar al más

bajo, que comunica por un canal físico con otra estación, donde sube de nuevo por la jerarquía de protocolos.

## **OSPF**

Primero la ruta libre más corta. Protocolo de enrutamiento por estado de enlace jerárquico, que se ha propuesto como sucesor de RIP en la comunidad de Internet. Entre las características de OSPF se incluyen el enrutamiento de menor costo, el enrutamiento de múltiples rutas, y el balanceo de carga.

## **PBX**

Private Branch Exchange (Central Telefónica Privada). Conmutador de un teléfono analógico o digital ubicado en las instalaciones del suscriptor y que se usa para conectar redes telefónicas privadas y públicas.

## **PCM**

Pulse Code Modulation. Sistema de modulación en el que los pulsos que constituyen una portadora de impulsos se dividen en grupos, modulándose cada grupo para representar los valores cuantificados de la señal analógica a transmitir. Esta técnica se emplea en los codificadores-decodificadores para convertir una señal analógica en digital. Se muestrean las señales 8000 veces por segundo; cada uno de estos muestreos se representa por 8 bits para un total de 64 Kbps. Se hace un uso extensivo de esta técnica en los sistemas digitales de transporte de voz.

## **Peer to Peer**

Comunicación entre niveles iguales en el estándar ISO. En su extensión más amplia es una red sin un servidor central, en la que todos los ordenadores pueden ser tanto servidores como clientes según se requiera.

## **PPP**

Point to Point Protocol. Protocolo que permite a una computadora usar los protocolos TCP/IP (Internet) con una línea estándar de teléfono y un modem de alta velocidad, pudiendo de esta forma conseguir el acceso a la Red Internet.

## **PSTN**

La red telefónica conmutada (abreviada RTC; en inglés Public Switched Telephony Network o PSTN) es una red de teléfono diseñada primordialmente para la transmisión de voz, aunque pueda también transportar datos, por ejemplo, en el caso del fax o de la conexión a Internet a través de un módem acústico.

## **RDSI**

Red Digital de Servicios Integrados, es una red que procede por evolución de la red telefónica existente, que al ofrecer conexiones digitales de extremo a extremo permite la integración de multitud de servicios en un único acceso, independientemente de la naturaleza de la información a transmitir y del equipo terminal que la genere.

## **RFC 2833**

RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

## **RFC 2543**

Protocolo de señalización para conferencias, telefonía, notificación de eventos y mensajería instantánea por Internet.

## **RFC 2705**

La sección del interfaz presenta una descripción conceptual del protocolo MGCP, presentando las convenciones de nombramiento, el uso de la descripción de la sesión del protocolo SDP y los procedimientos que componen MGCP.

## **RFC 822**

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.

## **RIP**

Protocolo de información de enrutamiento. Protocolo suministrado con los sistemas BSD de UNIX. El Protocolo de Gateway Interior (IGP) más común de la Internet. RIP utiliza el número de saltos como métrica de enrutamiento.

## **Router**

Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa. Denominado a veces gateway (aunque esta definición de gateway se está volviendo obsoleta).

## **RSVP**

Protocolo de Reserva de Recursos, es un protocolo de nivel de red en la estructura de capas de Internet y OSI, que permite reservar los canales o rutas en redes Internet para la transmisión por unidifusión y multidifusión.

Provee un mecanismo para negociar con la red una calidad de servicio requerida a una conexión específica. Se utiliza cuando es conocido el ancho de banda requerido, el retardo y la probabilidad de pérdida soportable.

Se utiliza en protocolos de VoIP, emisión de programas de televisión y diversas aplicaciones sensibles a variaciones en el flujo.

## **SCCP**

Signaling Connection Control Part, es un componente del protocolo suite SS7 que proporciona funciones adicionales a las partes de transferencia de mensaje (MTP). SCCP proporciona ambos servicios de red: sin conexión y conexión orientada, para transferir información de señalización a través de redes de telecomunicación, tales como GSM.

## **SIGTRAN**

El Protocolo SIGTRAN es definido como un grupo de protocolos y capas de adaptación para transportar la información de señalización sobre las redes IP. SigTran es usado como protocolo entre el Gateway Controller y el Signaling Controller entonces MTP1, MTP2 y SigTran residen en el Signaling Gateway. En este caso MTP3 y los protocolos de alto nivel residen en el Gateway Controller.

## **SMTP**

Simple Mail Transfer Protocol (Protocolo de Transferencia Simple de Correo). Es el protocolo usado para transportar el correo a través de Internet.

## **SNMP**

Simple Network Management Protocol. Permite a un servidor TCP/IP que ejecuta una aplicación SNMP, interrogar a otros nodos para estadísticas y condiciones de error de la red. Los otros servidores, que proporcionan agentes SNMP responden a estas preguntas y le permiten a un solo servidor recoger estadísticas de muchos nodos de la red.

## **SOAP**

Simple Object Access Protocol. Protocolo basado en XML/HTTP para el acceso a servicios, objetos y servidores remotos independiente de la plataforma. Es un modo abierto y extensible para que las aplicaciones se comuniquen a través de la Web utilizando mensajes basados en XML, con independencia de los sistemas operativos, modelos de objetos o lenguajes de programación que cada aplicación utilice.

## **SRTP**

Secure Realtime Protocol (Protocolo de Tiempo Real Seguro). Es el mismo protocolo RTP pero con funciones de Seguridad; tales como: confidencialidad y verificación de la información. Este protocolo es de gran utilidad para VoIP ya que no interfiere en la calidad de la conversación.



## **T.120**

T.120 es un estándar de la ITU-T (International Telecommunications Union), para la comunicación de los datos y control de la conferencia, para la comunicación interactiva multimedia: de múltiples puntos y de punto a punto.

## **TCP**

Transmission Control Protocol (Protocolo de Control de Transmisión). Protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de dúplex completo. Es parte de la pila de protocolo TCP/IP.

Desarrollado por el DARPA en 1973 para la interconexión de redes. Por otra parte, establece una línea de diálogo entre el emisor y el receptor antes de que se transfieran los datos. Trata cada paquete de forma independiente e incluye en la cabecera información adicional para así controlar la información.

## **TLS**

Transport Layer Security. Protocolo del tipo EAP que garantiza la privacidad y la seguridad de datos entre aplicaciones cliente/servidor que se comunican vía Internet. Trabaja en dos niveles: El protocolo de registro TLS, situado en el nivel superior de un protocolo de transporte seguro como TCP, asegura que la conexión es privada empleado encriptación simétrica de datos y asegura que la conexión es fiable. También se utiliza para la encapsulación de protocolos de nivel superior, tales como el TLS handshake Protocol. Permite la autenticación entre el servidor y el cliente y la negociación de un algoritmo de encriptación y claves criptográficas antes de que el protocolo de la aplicación transmita o reciba cualquier dato. TLS es un protocolo independiente que permite que protocolos de niveles superiores se sitúen por encima de él de manera transparente.

## **Token Ring**

Arquitectura de red con topología de anillo, que pasa una señal o testigo entre las estaciones conectadas. Un dispositivo toma la señal, transmite sus datos, y libera la señal después de que los datos han completado el circuito del anillo eléctrico. La

velocidad de transmisión es de 4 ó 16 Mbps. La especificación de este protocolo se recoge en la norma IEEE 802.5 y la ISO 8802.5.

## **UDP**

User Datagram Protocol, es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene asentimiento, ni control de flujo, por lo que los paquetes pueden pisarse unos a otros; y tampoco sabemos si ha llegado correctamente, ya que no hay asentimiento. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

## **UIT o ITU**

Unión Internacional de Telecomunicaciones (ITU, International Telecommunication Union). Es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas Administraciones y Empresas Operadoras.

## **VoIP**

La Voz sobre 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 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.

## **VPN**

Virtual Private Network (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.

## **WAN**

Una Red de Área Amplia (WAN), es una red que ofrece servicios de transporte de información entre zonas geográficamente distantes. Es el método más efectivo de transmisión de información entre edificios o departamentos distantes entre sí. Esta forma de comunicación aporta, como nota diferencial respecto a las Redes de Área Local (LAN) o las Redes de Área Metropolitana (MAN), que el ámbito geográfico que puede cubrir es considerablemente más amplio.

# Anexos

**Anexo A: Formato de la encuesta realizada a los usuarios de la red de la ESPE**

**FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA**

**ENCUESTA PARA EVALUAR EL CONOCIMIENTO Y LAS NECESIDADES DE LOS USUARIOS ACERCA DE LOS SERVICIOS QUE BRINDA LA RED DE LA ESPE**

**OBJETIVO:** Determinar los requerimientos de los usuarios para mejorar los servicios de la red.

**INSTRUCCIONES:** Lea detenidamente las preguntas y conteste con total sinceridad marcando con una **x** las opciones de su gusto.

<b>Facultad:</b>	<b>Cargo:</b>	<b>Sexo:</b> <input type="radio"/> Femenino <input type="radio"/> Masculino
1.- Con que frecuencia se comunica desde la ESPE - Sangolquí a las Sedes y viceversa?	<input type="radio"/> Nunca <input type="radio"/> Frecuentemente <input type="radio"/> Siempre <input type="radio"/> Casi Nunca <input type="radio"/> Muy Frecuentemente	
2.- Ingresar con facilidad la llamada cuando se comunica a la ESPE - Sangolquí y a sus Sedes?	<input type="radio"/> Si <input type="radio"/> No Porqué?	
3.- Cómo considera usted el funcionamiento de las líneas telefónicas internas y externas de la ESPE?	<input type="radio"/> Malo <input type="radio"/> Bueno <input type="radio"/> Regular <input type="radio"/> Excelente	
4.- Es importante que tenga una línea telefónica individual en su estación de trabajo?	<input type="radio"/> Si <input type="radio"/> No Porqué?	
5.- Le gustaría tener en su computadora servicios de mensajería, chat, correo de voz ?	<input type="radio"/> Si <input type="radio"/> No Porqué?	
6.- Ha escuchado sobre la tecnología de Voz sobre IP (VoIP)?	<input type="radio"/> Si <input type="radio"/> No	
7.- Qué uso le daría a Voz sobre IP en la ESPE?	<input type="checkbox"/> Videoconferencia <input type="checkbox"/> Internet <input type="checkbox"/> Llamadas IP <input type="checkbox"/> Multimedia	

## **Anexo B: Manual de Uso e Instalación del SJphone™**

SJphone™ es un softphone que permite hablar en Internet en cualquier PC de escritorio, notebooks, PDAs, Teléfonos-IP de ordenadores independientes e incluso con líneas convencionales y teléfonos móviles. Soporta ambos estándares de industria SIP y H.323, y es completamente ínter operable con la mayoría de Proveedores de Servicios de Telefonía de Internet (ITSP) y software y hardware de VoIP.

Para realizar llamadas en el mundo, se necesita abrir una cuenta con un servicio de Telefonía IP y obtener su perfil, o hacer su propio perfil en su SJphone™.

Los usuarios avanzados pueden hacer su propia red de VoIP usando también: H.323 Gatekeeper, SIP proxy, IPPBX, ILS Directory server, y otros componentes. Además se puede conectar a teléfonos convencionales usando Gateways H.323/SIP.

### **Características del SJphone**

La compatibilidad de SIP permite hablar en Internet:

- Directamente con la mayoría de softphones SIP y Teléfonos-IP de ordenadores independientes (como Cisco 7940).
- Con otras personas de su compañía a través de su sistema IP-PBX SIP o Proxies (como Asterisk, Broadsoft y otros).
- Con todas las personas alrededor del mundo usando cuentas SIP ITSP como FWD ([www.fwd.pulver.com](http://www.fwd.pulver.com)).
- Con un teléfono regular usando Gateways SIP.

La compatibilidad de H.323 permite hablar en Internet:

- Directamente con otros softphones H.323 y Teléfonos-H.323 de ordenadores independientes.
- Con otras personas de su compañía a través de su sistema IP-PBX H.323 como Cisco Call Manager.
- Con todas las personas alrededor del mundo usando cuentas H.323 ITSP
- Con computadoras o teléfonos en redes privadas a través de Gatekeeper.
- Con un teléfono regular usando Gateways H.323.

## **Características que hacen al SJphone™ más fácil de usar**

- Los Skins (máscaras) permiten cambiar la apariencia del panel principal del SJphone™.
- Llamar a cualquier host por su nombre o dirección IP.
- Inter operabilidad con más proveedores de servicios IT.
- Servicio rápido de conmutación entre: ITSP, IP-PBX, Gatekeeper, Gateway, o en un ambiente SIP Proxy y GUI.
- Contactos, call logs (anotación de las actividades que se producen en un ordenador) y tiempo de marcado.
- Llamar a un computador o a un teléfono de red privada a través de un Gatekeeper.
- Call transfer (transferencia de llamadas), hold (música en espera), y silencio.
- Puede aceptar llamadas automáticamente o rechazarlas de inmediato (el modo "Do Not Disturb") o después de un tiempo específico.
- Detecta automáticamente los SJphones™ vecinos.
- Conserva y administra una lista de las múltiples llamadas.
- Indicación de entrada y salida del nivel de sonido y control.
- Ajusta automáticamente el volumen del micrófono.
- Ajusta automáticamente el nivel de detección de silencio.
- Soporta la mayoría de teléfonos USB.
- Soporta la mayoría de codecs: G711, GSM, iLBC, (G729 disponible solo en versiones comerciales).
- Detección automática de NAT.
- Llamadas desde/hacia un proveedor de red IP usando la tecnología transversal.

## **Características de Usuarios Avanzados**

- Llamadas multisesión
- 3-vías de conferencia usando diferentes protocolos VoIP.
- Selección manual del codec.
- Soporte de DNS en la pila de SIP.
- Directorio ILS (Internet user Location Service).
- Soporta sintaxis avanzadas para un URL SIP.
- Selecciona tablas del protocolo de transporte SIP (TCP/UDP).

- Ventana de anotación de actividades (Log) para operaciones de monitoreo.

## **Requerimientos del Sistema**

Corre en PCs con Windows 98SE/ME/2000sp4/XPSP2/2003 Server (los usuarios de Windows 2000 necesitan instalar Microsoft Installer 2.0 antes de la instalación del SJphone™).

### **Requerimientos de Hardware:**

Lo mínimo que se necesita en un procesador Intel Celeron 300 con 32MB para Windows 98SE, 128MB para Windows 2000 y 256 para Windows XP.

Una tarjeta de sonido full-duplex con un micrófono y parlantes o cualquier teléfono USB. Tener instalado la versión más reciente de DirectX (7.0 - 9.0), es lo más recomendado. Se recomienda tener los drivers para la tarjeta de sonido y teléfonos USB.

Cualquier tipo de conexión broadband TCP/IP como wireless (802.11x, 802.16x), Ethernet o conexiones de área extendida (WAN) como: DSL, E1/T1, etc.; son recomendadas. Puede obtener una mejor calidad de sonido con una conexión de banda ancha pero con un modem analógico v.90 es suficiente si se usa una compresión de voz con un codec apropiado.

Si necesita llamar desde/hacia una PSTN, debe tener una cuenta ITSP o un acceso a H.323 o un Gateway SIP como CISCO 26xx/36xx/3700/53xx, etc.

### **Instalación del SJphone™**

Para instalar SJphone™:

- Bajarse y ejecutar el archivo de instalación.
- Seguir las instrucciones de las pantallas.

Una vez descargado el instalador lo ejecutamos.





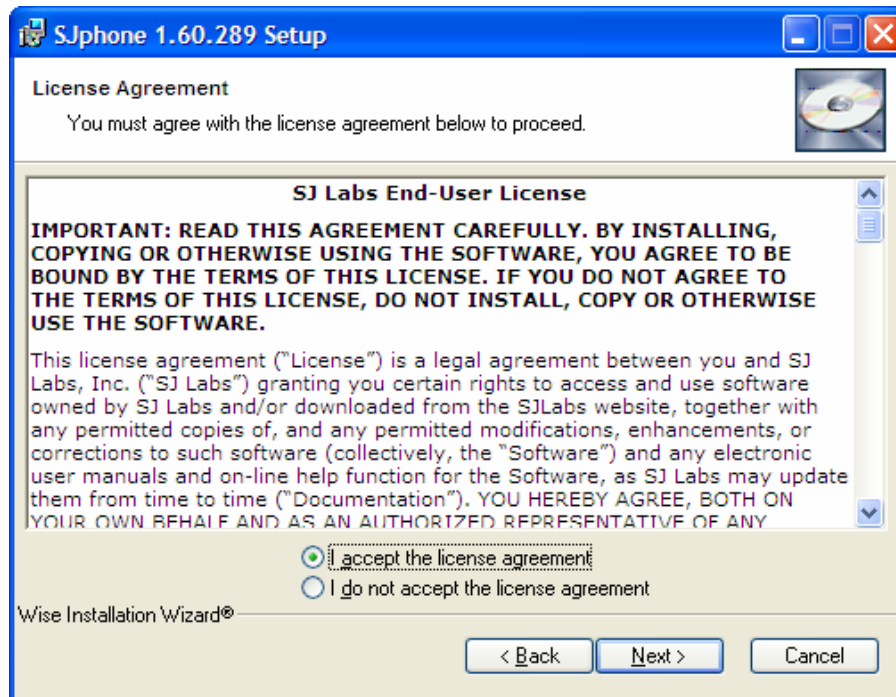
Extrayendo archivos para instalación

Enseguida nos muestra una pantalla de bienvenida -> Next.



Ventana de bienvenida al Wizard de Instalación del Siphone

Leemos y aceptamos el acuerdo de licencia -> Next.



Licencia del SJphone

La instalación ha terminado correctamente -> Finish.



Ventana Final de Instalación

Aparece una ayuda wizard para realizar ajustes de audio para el SJphone. Para comenzar: Cierre todos los otros los programas que utilizan o registran el sonido y cerciórese de que los altavoces y el micrófono estén conectados y encendidos -> Next.



Audio Wizard: Paso 1

Verificamos que este activada la casilla del DirectX; esto es, para que tenga un mejor funcionamiento -> Next.



Audio Wizard: Paso 2

Seleccionamos el dispositivo de audio para la lectura y grabación de voz ->  
Next.



Audio Wizard: Paso 3

Compruebe que los altavoces o el auricular estén enchufados y girados, para ajustar el volumen del aparato de lectura, haga clic en el botón Test para oír una muestra del sonido -> Next.



Audio Wizard: Paso 4

Para probar el micrófono y para ajustar el nivel de grabación, lea el texto siguiente en el micrófono. "Estoy utilizando la configuración wizard de audio. Ahora está comprobando si mi micrófono es conectado y trabajando correctamente. El slider ajustará automáticamente el nivel de la grabación. Usted puede supervisar el nivel del micrófono en el indicador y ajustarlo manualmente en el nivelador de slider -> Next.



Audio Wizard: Paso 5

Verificar que la configuración de audio este ajustada correctamente: Haga clic en el botón Record y diga algo en el micrófono por 10 seg. Haga clic en el botón Play para escuchar la grabación -> Next.



Audio Wizard: Paso 6

Si desea cambiar las configuraciones de audio para SPhone, corra este wizard otra vez: Cuando usted tiene problemas con el audio, cuando usted ha cambiado el dispositivo de audio de lectura o de la grabación del teléfono o cuando usted ha instalado un dispositivo nuevo de audio, por ejemplo, un nuevo microteléfono USB -> Finish.



Audio Wizard: Paso 7

Si desea desinstalar SJphone™, debe ir a Panel de Control -> Add/Remove Programs -> SJphone -> Install/Uninstall.

Finalmente muestra la pantalla de inicio del SJphone™.

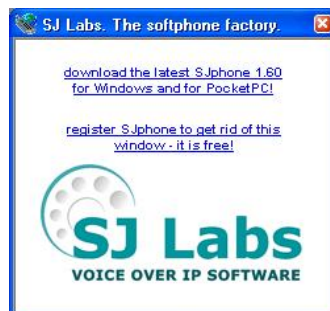


Pantalla de Inicio del SJphone

### Registrando SJphone™

La registraci3n es gratuita; si desea puede recibir informaci3n a cerca de nuevas publicaciones de SJphone™.

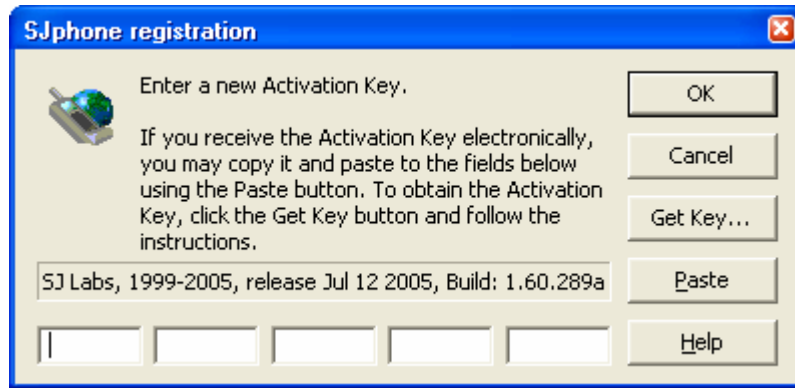
Al terminar la instalaci3n, aparece autom3ticamente una ventana para registrarse y damos clic en el v3nculo: [register Siphone to get rid of this window – it is free.](#)



Ventana de Registraci3n

O también puede:

- Clic en el botón de Opciones en el panel principal de SJphone™.
- Seleccione la pestaña Support -> botón Register.
- Para obtener la clave de un clic en el botón Get Key.



### Activación de Clave

La página de registración pide que ingrese los siguientes datos:

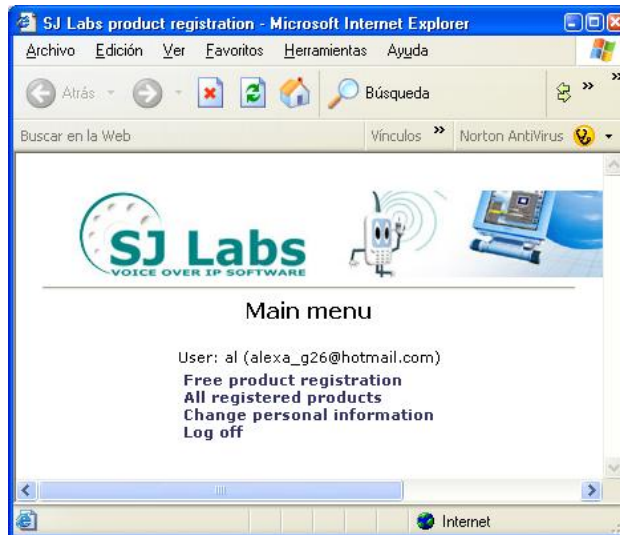
- Haga clic en el botón de Register.

### Información personal



Envía un correo a su e-mail, en el cual se encuentra un link para finalizar la registración.

A continuación, muestra la siguiente pantalla donde se debe seleccionar la opción Free Product Registration:



Menu Principal de Registración

Escogemos en que sistema operativo se va a trabajar, en nuestro caso Windows XP -> Clic en Register.



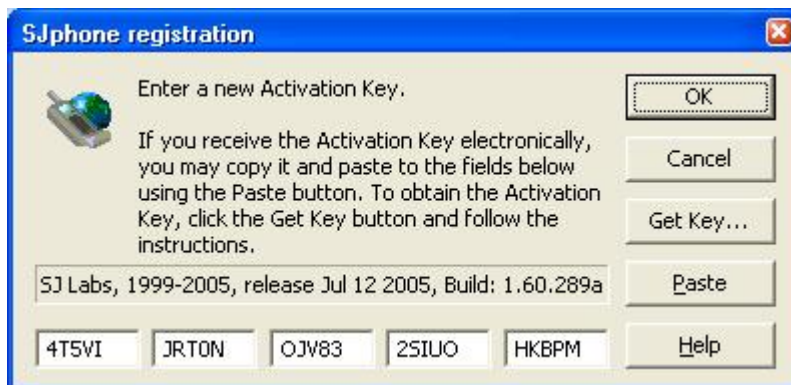
Elección del Sistema Operativo

Muestra la pantalla de registraci3n completa.



### Registraci3n Completada

Copiamos y pegamos el c3digo de activaci3n en el mensaje de registraci3n del SJphone y damos clic en el bot3n OK.



### Ingresando el C3digo de Activaci3n

### Controles del Panel Principal

Para dar comienzo al SJphone™, dirijase a Inicio -> Todos los programas -> Sjphone -> SJphone.

La pantalla principal del softphone muestra las siguientes opciones:



Controles del Panel Principal

- **Call to:** Tipo de dirección IP, host mane, nickname o el número de teléfono al que quiere llamar.
- **Status:** Muestra el status de la llamada.
- **Mic:** Indica el nivel de entrada del sonido para la sesión actual.
- **Speaker:** Indica el nivel de salida del sonido para la sesión actual.

### Botones

- **Dial:** Clic en este botón para marcar el tipo de dirección en la llamada al campo. Shortcut key: Alt + d -> Enter.
- **Hangup:** Clic en este botón para terminar la llamada. Shortcut key: Alt + h -> Enter.
- **Conference:** Clic en este botón para unir usuarios a la conversación.
- **Hold:** Clic en este botón para poner a una llamada en espera.

- **Transfer:** Clic en este botón para transferir la llamada a otra dirección específica.
- **Contacts:** Clic en este botón para activar los contactos SJphone™.
- **Voice Mail:** Clic en este botón para recibir los mensajes de voz.
- **Options:** Clic en este botón para activar el panel de Opciones del SJphone™ y configurarlas. Shortcut key: Alt + o
- **Mute:** Clic en este botón para silenciar la voz.
- **Speak:** Clic en el botón Speak para reactivar la conversación. Shortcut key: Alt + m and Alt + s.

### Sliders

- **Mic:** Use el slider para ajustar el volumen del micrófono.
- **Speaker:** Use el slider para ajustar la salida de volumen del sonido.

Puede mirar las propiedades demandadas haciendo clic derecho y seleccionando el item Propiedades en el menú pop-up. Las propiedades de los mensajes de sesión pueden aparecer:



Propiedades de Sesión

### Contactos

Permite almacenar información de los usuarios que regularmente llama. También tiene un directorio ILS, Neighbor logs y anotador de llamadas marcadas, recibidas y perdidas (Call logs: Dialed, Missed, and Received).



Llamadas realizadas, recibidas y perdidas

- **Call:** Clic en este botón para llamar a la persona seleccionada.
- **Clear Log:** Clic en este botón para quitar todos los registros en este anotador de actividades.
- **Properties:** Clic en este botón para ver la información acerca del contacto seleccionado.
- **Remove:** Clic en este botón para quitar el archivo seleccionado desde el log.
- **to Phonebook:** Clic en este botón para añadir y seleccionar contactos.
- **Clear All Logs:** Clic en este botón para limpiar todos los logs.
- **Help:** Clic en este botón para activar ayuda del SJphone™.



## Opciones de Llamadas

### Phonebook

Se puede utilizar el panel de Phonebook en contactos para almacenar la información sobre los contactos que usted desea llamar más adelante. Además, puede almacenar un número de teléfono o una secuencia avanzada de marcado.

- **Call:** Clic en este botón para llamar al contacto seleccionado.
- **Add:** Clic en este botón para agregar un nuevo contacto o expediente.
- **Delete:** Clic en este botón para quitar el contacto o expediente seleccionado del Phonebook.
- **Edit:** Clic en este botón para modificar el contacto o expediente seleccionado.
- **Help:** Clic en este botón para activar la ayuda de SJphone™.



### Directorio Telefónico

- **Full Name:** Campo para el nombre completo del usuario.
- **Nick:** Campo para el nick del usuario.
- **E-mail:** Campo para el e-mail del usuario.
- **Phone:** Campo para el número de teléfono del usuario.
- **Edit Dialstring:** Seleccione esta casilla si se desea utilizar una secuencia avanzada de marcado. Va a la sección Place a call para los detalles.
- **Dialstring:** Campo avanzado para dialstring del usuario.
- **Comments:** Campo para los comentarios.

### Neighbors

Se puede ver a otras personas que estén utilizando SJphone™ en la red local, puede llamarlos o agregar a los contactos.

**Nota:** Esta característica trabaja solamente en redes de área local. Si utiliza un firewall personal en su computadora, cerciórese de que no bloquee el puerto 5003 del UDP.

- **Call:** Clic en este botón para llamar a un vecino seleccionado.
- **Refresh:** Clic en este botón para restaurar la lista de vecinos.

- **to Phonebook:** Clic en este botón para agregar a un contacto desde la lista de vecinos al Phonebook.
- **Propierties:** Clic en este botón para ver la información sobre un vecino seleccionado.
- **Help:** Clic en este botón para activar la ayuda de SJphone™.



Vecinos de la Red

 A screenshot of a dialog box titled 'Respondent'. It contains the following fields:
 

- Name: Sra. Eliana
- Nick: Ely
- E-mail: eli@voipsip.com
- Phone: (empty field)
- Edit dialstring
- Dialstring: sip:eliana@192.168.10.1
- Comments: (empty text area)

 At the bottom, there are three buttons: 'OK', 'Cancel', and 'Help'.

Datos del Usuario

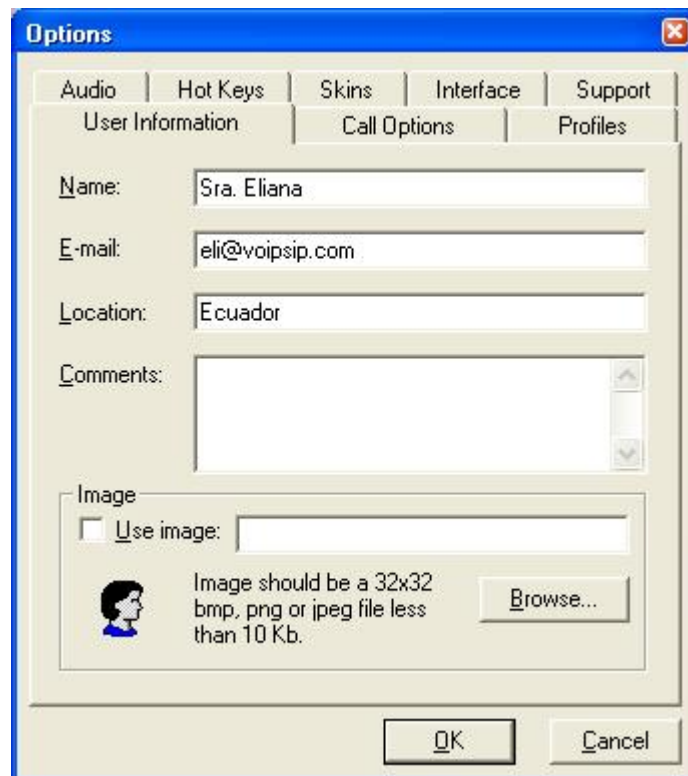


## Configurando SJphone

### User Information

Para personalizar la información del usuario, se puede cambiar esta información en cualquier momento.

- **Name:** Campo para ingresar su nombre.
- **E-mail:** Campo para ingresar su e-mail
- **Location:** Campo para ingresar localización
- **Comments:** Campo para comentarios.
- **Image:** Si desea puede agregar una foto a su información personal. El resto de los usuarios de SJphone™ lo verán en su panel principal.
- **Use Image:** Seleccione esta casilla si quisiera que otros usuarios de SJphone™ visión su foto.
- **Browse:** Clic en este botón para buscar la foto.



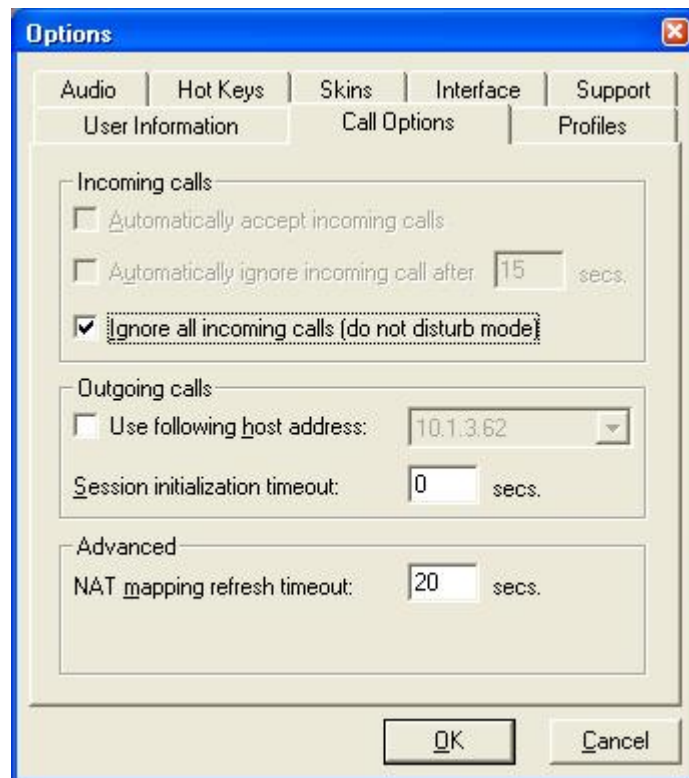
Información del Usuario

Durante la configuración, SJphone™ escribe el nombre de la conexión de Windows en el campo conocido. Si estos campos se dejan en blanco, SJphone™ utiliza el "usuario de SJ Labs(R) SJphone(TM)" como el username para llamadas H.323, su dirección IP y el puerto 5060 para llamadas SIP.

## Call Options

Si desea configurar las opciones de llamada haga clic en la viñeta Call Options.

- **Incoming Calls:** Puede configurar su SJphone™ para aceptar o para rechazar automáticamente todas las llamadas entrantes. Solamente una de las siguientes casillas se puede seleccionar a la vez:
  - Automatically accept incoming calls: Seleccione esta casilla si desea que SJphone™ acepte todas la llamadas automáticamente.
  - Automatically ignore incoming call after... secs: Seleccione esta casilla si desea que SJphone™ ignore automáticamente una llamada entrante, si usted no la acepta dentro del tiempo especificado.
  - Ignore all incoming calls: Seleccione esta casilla si desea que SJphone™ ignore todas las llamadas entrantes.
  
- **Outgoing Calls:** Si su computadora tiene varias direcciones del IP, usted necesita seleccionar **Use following host address** y una dirección de la lista de direcciones disponibles. Si no selecciona esta opción, SJphone™ utiliza su dirección por defecto.
  - Use following host address: Seleccione esta casilla si su computadora tiene varias direcciones del IP y seleccione una de la lista de direcciones disponibles.
  - Session initialization timeout: Timeout por el cual el SJphone espera una registración con un Proxy SIP. Si no puede registrarse durante el timeout la sesión no comenzará. 0 deshabilite esta característica.



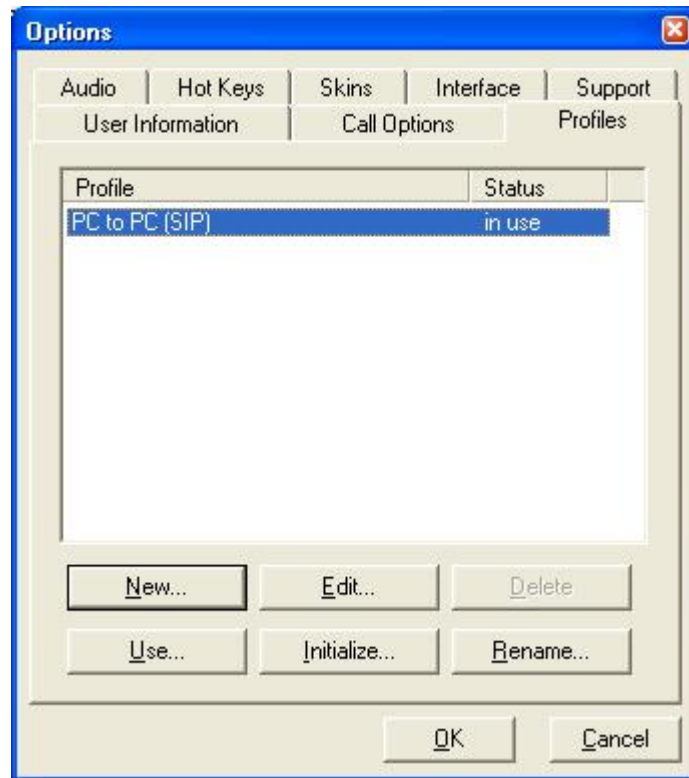
Opciones de Llamada

## Profiles

SJphone™ puede utilizar sistemas predefinidos de opciones para los tipos específicos de llamadas o para las llamadas a través de diversos abastecedores de servicio de la telefonía de Internet (ITSP) llamados service profiles.

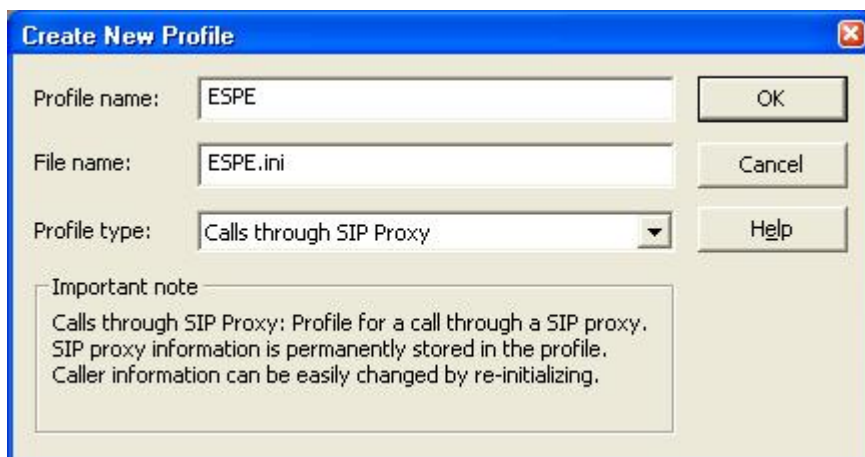
Usted puede incluso escribir su propio perfil para su IP-PBX, ITSP o parámetros de Gateway con su propio sistema de opciones, aunque eso requiere un cierto conocimiento de la tecnología de VoIP.

- **New:** Clic en este botón para crear un nuevo perfil.
- **Edit:** Clic en este botón para modificar el perfil seleccionado.
- **Delete:** Clic en este botón para borrar el perfil seleccionado.
- **Use:** Clic en este botón para poner en uso el perfil seleccionado.
- **Initialize:** Clic en este botón para inicializar el perfil seleccionado.
- **Rename:** Click en este botón para renombrar el perfil seleccionado.



### Perfiles

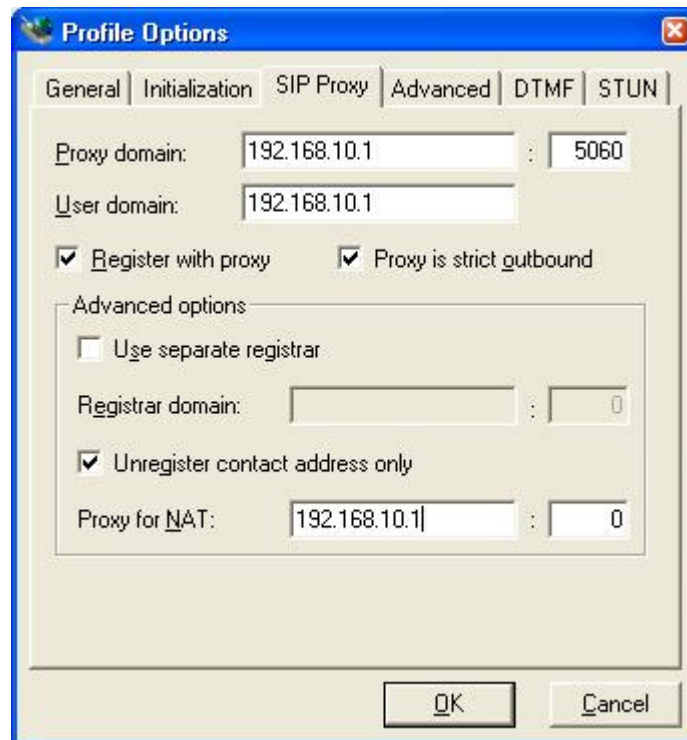
- **Para crear un Nuevo Perfil:** Seleccione el tipo de perfil en este caso “calls through SIP Proxy” y especifique el nombre del perfil -> OK. El nuevo perfil aparecerá en las lista de perfiles.



### Creando un Nuevo Perfil

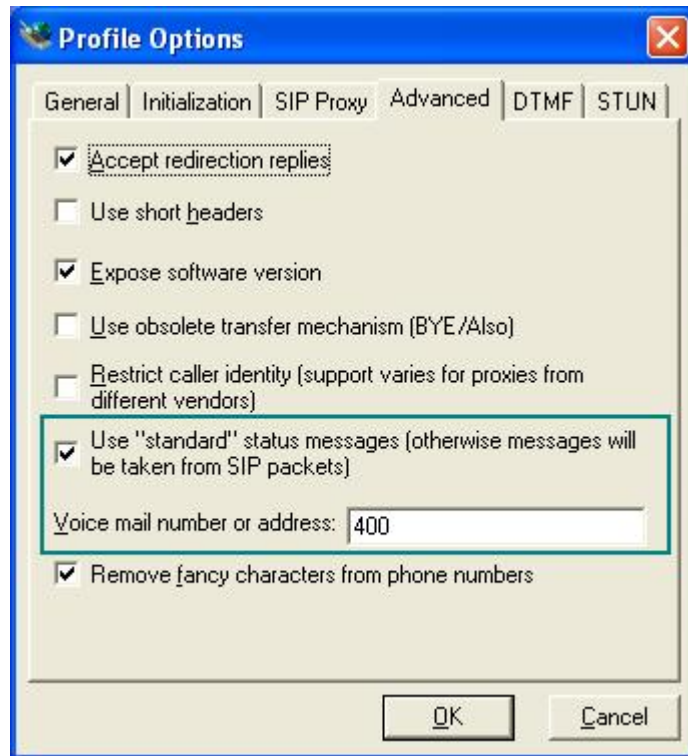
- **Para modificar un Perfil:** Seleccione el perfil -> Edit. Vaya a la pestaña SIP Proxy, aquí ingrese:

- o IP del Proxy.
- o El puerto del Proxy (5060 es el puerto que utiliza SIP).
- o Dominio del usuario.
- o IP del Proxy para NAT.



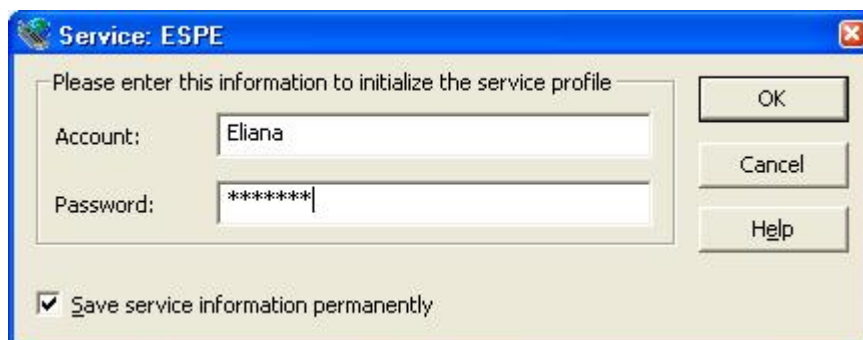
Opciones de Perfil

Además, en la pestaña Advanced es necesario seleccionar el uso del estado de mensajes estándar e ingresar el número de la casilla de voz asignado, en este caso el número que se le asigno a un usuario es 400.



Opciones del Perfil Avanzadas

Luego de esto presione el botón OK. A continuación ingrese la cuenta y el password que debe darle su proveedor de este servicio telefónico, para poder inicializar el servicio del perfil.

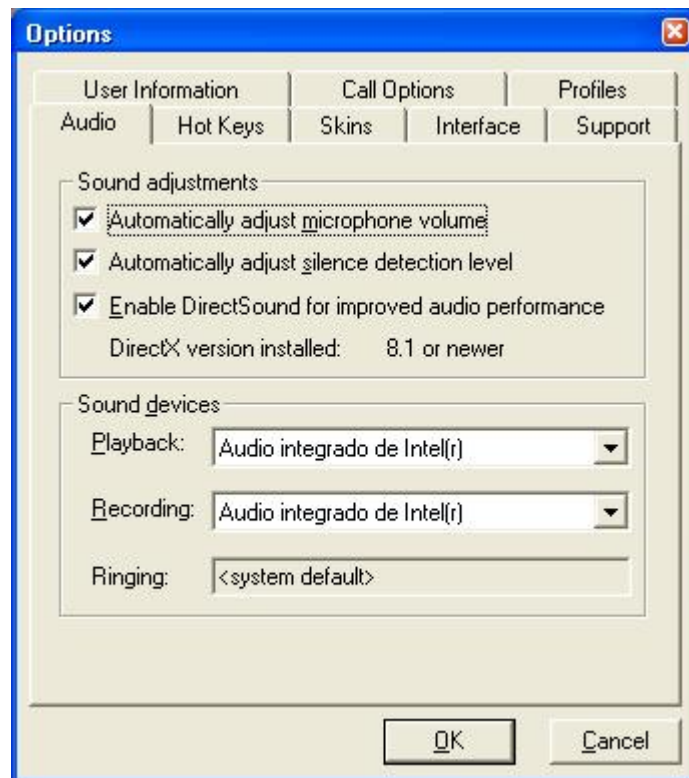


Inicialización del Perfil

## Audio

Generalmente, se puede ajustar las características de sonido del Sjphone usando los controles de audio de Windows o los controles en el panel principal.

- **Sound adjustments**
  - Automatically adjust microphone volume: Seleccione esta opción para ajustar el volumen del micrófono automáticamente.
  - Automatically adjust silence detection level: Seleccione esta opción para permitir el ajuste automático del nivel de detección del silencio.
  - Enable DirectSound for improved audio performance: Seleccione esta opción si su tarjeta de sonido soporta DirectSound.
  - DirectX version installed: Compruebe la versión de DirectX instalado en su sistema.
  
- **Sound devices**
  - Playback: Muestra que dispositivo de audio utiliza el Sjphone para el playback.
  - Recording: Muestra que dispositivo de audio utiliza el Sjphone para el registro de audio.
  
- **Compression Settings:** Clic en este botón para fijar los ajustes de compresión del Sjphone.
  
- **Advanced Settings:** Clic en este botón para configuraciones avanzadas de audio del Sjphone.

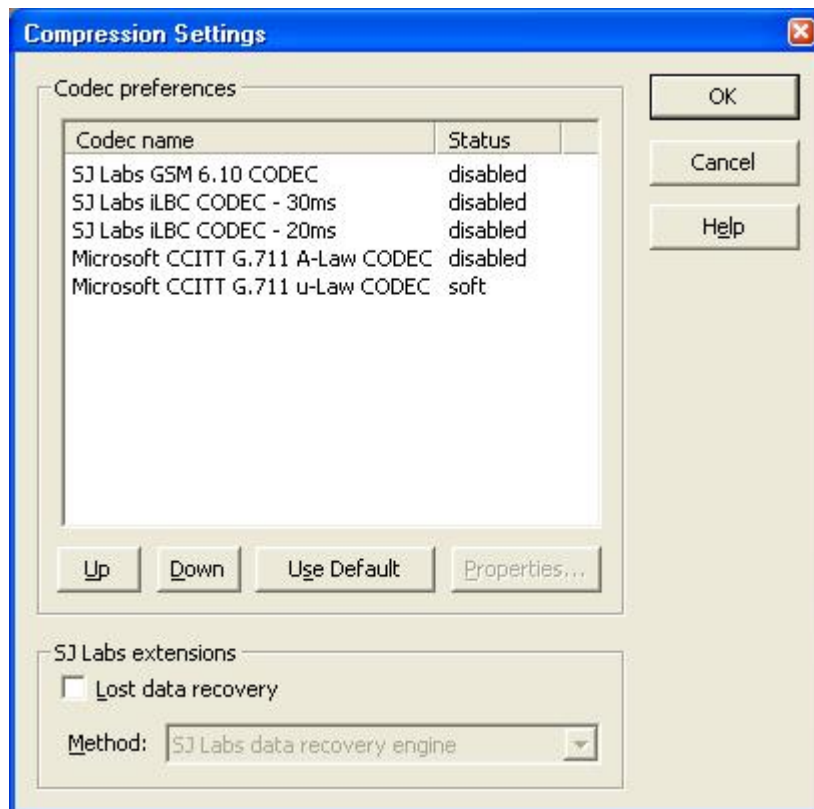


### Opciones de Audio

Cuando dos sistemas de VoIP están estableciendo una llamada, ellos negocian un codec de compresión de audio que vayan a usar. El codec para escoger depende de muchos factores: qué codecs se instalan en los sistemas, limitaciones del ancho de banda, calidad del sonido, etc. Usted puede modificar las preferencias del codec del SJphone™ en la ventana Compression Settings. Durante la negociación, SJphone™ ofrece al sistema remoto los primeros codec de la lista. Si el sistema remoto rechaza el codec, SJphone™ ofrece el siguiente hasta que acepte uno de ellos. Usted puede colocar el codecs en el orden deseado usando los botones Move Up y Move Down. El botón Use Default selecciona la preferencia del codec por defecto.

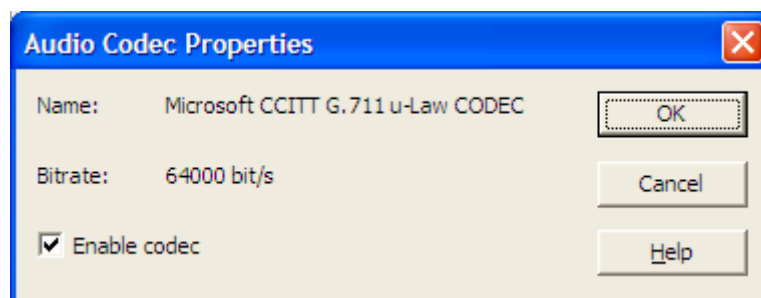
- Codec name: Muestra el nombre del codec.
- Status: Muestra el estado del codec. Podría ser:
  - Soft: el codec es implementado como un driver
  - Hard: el codec es implementado como un dispositivo de hardware.
  - Disabled: el codec es deshabilitado.





Preferencia de Codecs

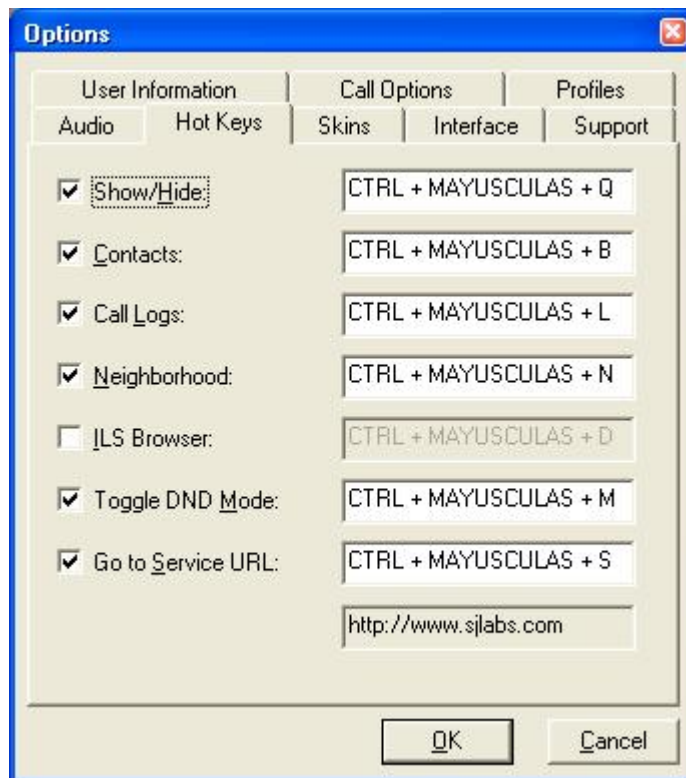
Un codec puede ser habilitado o deshabilitado en la ventana de Audio Codec Properties.



Propiedades del Codec de Audio

### Hot Keys

Se puede asignar varios accesos rápidos para realizar operaciones comunes, con la ayuda de las hot keys.

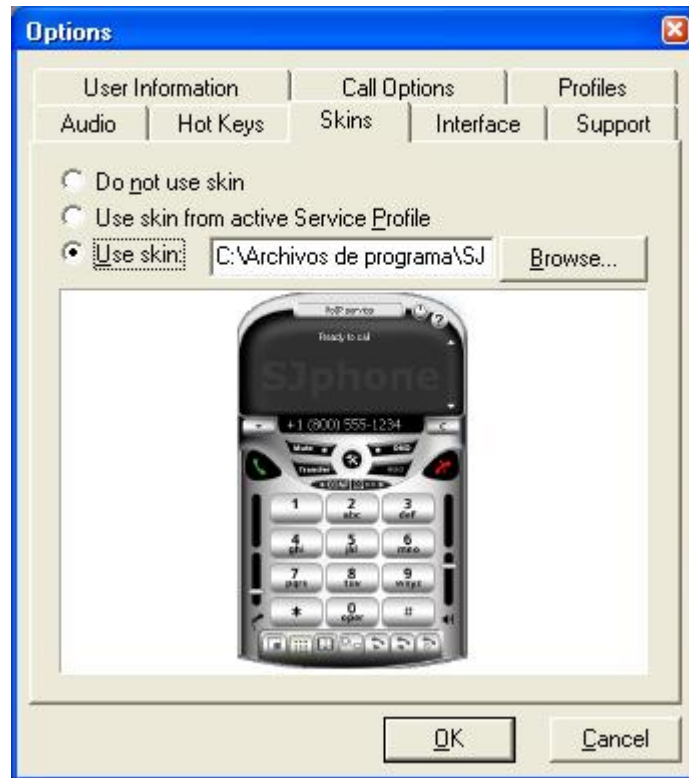


## Hot Keys

### Skins

Se puede elegir el aspecto principal del SJphone usando varios skins de acuerdo al gusto de cada usuario. Algunos skins no tienen ningún botón de opciones.

Para acceder a esta opción: clic derecho en el Sjphone -> Options, pestaña Skins.



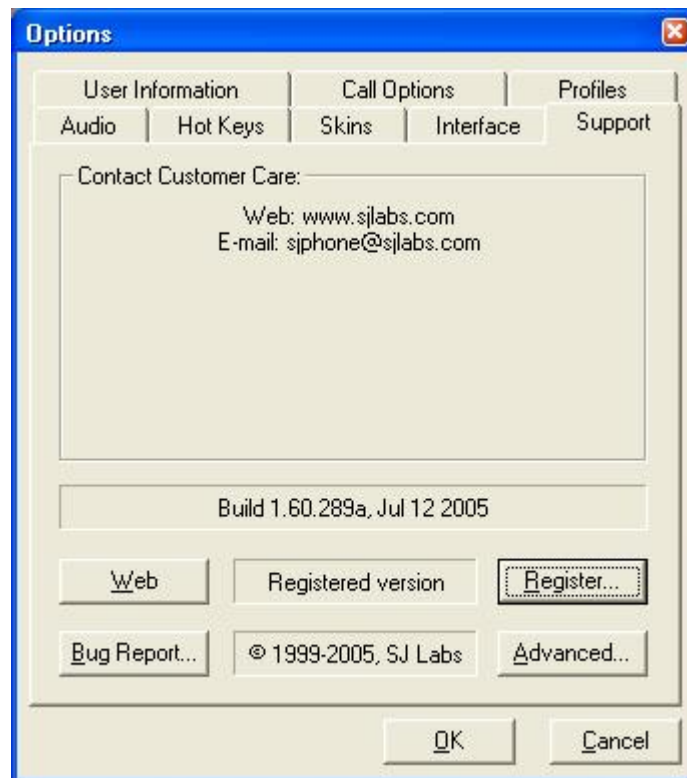
#### Opciones de Tipo de Máscara

- **Do not use skin:** Seleccione esta opción si no desea usar el skin.
- **Use skin from active Service Profile:** Seleccione esta opción si desea usar un skin específico en los servicios activos de los perfiles.
- **Use skin:** Seleccione esta opción si desea usar el skin establecido.
- **Browse:** Clic en este botón para buscar otro modelo de skin.

#### Support

La ayuda en línea alejada permite que el equipo solucione su problema remotamente. Pueden revisar opciones de la configuración y corregirlas inmediatamente en caso de necesidad. Usted necesita entrar en contacto con el equipo de la ayuda para obtener la información cómo recibir la ayuda en línea alejada.

- **Web:** Clic en este botón para visitar la página SJ Labs.
- **Bug Report:** Clic en este botón para generar un bug report e-mail.
- **Register:** Clic en este botón para registrar al SPhone™.
- **Advanced:** Clic en este botón para activar la consola remota.



### Opciones de Soporte

Se puede también registrar automáticamente la información sobre los problemas del menú de la bandeja del sistema, haciendo:

- Clic derecho en el icono system tray de SJphone, seleccione Bug Reporting y Star Recording.
- Reproduce el problema.
- Clic derecho en el icono system tray de SJphone, seleccione y seleccione Submit. Aparece la ventana de Submit Bug Report.
- Describe el problema en la ventana.
- Submit el Bug Report manualmente o automáticamente con su programa de correo del defecto. Usted puede cancelar informe seleccionando Cancel Recording.

### Como hacer una llamada

Se puede hacer una llamada a cualquier computadora que contenga H.323 o SIP compatible con el software que este en funcionamiento, un teléfono compatible de Internet de H.323 o SIP o un teléfono regular por un Gateway o un Gatekeeper.

Para hacer una llamada, se debe seleccionar un perfil y tipo apropiado para la llamada: en el campo del panel principal puede salir siguiente:

- **Una dirección IP o Nombre del Computador para una llamada directa de PC a PC:** Dependiendo del protocolo de VoIP que este usando, necesita seleccionar cualquiera, un perfil directo H.323 o SIP.

Si su computadora está en una red privada, usted necesita una llamada en H.323 a través de un Gatekeeper usando un perfil apropiado. Si no hay tales perfiles, usted necesita crear un perfil para su uso. Vaya a la página de la ayuda de los perfiles más detalles.

Para una llamada directa SIP PC-a-PC usando una tecnología transversal NAT disponible. Vaya al NAT Transversal y a la sección de SIP para más detalles.

La mayoría de las computadoras conectadas a Internet a través de dial - up tienen asignadas direcciones IP dinámicamente, así que la única solución aquí es utilizar una cuenta Proxy o Gatekeeper.

- **Un Alias (User Name) en un Gatekeeper:** Usted necesita seleccionar un perfil para las llamadas a través de un Gatekeeper. Si no hay tales perfiles disponibles, usted necesita crear el perfil que va usar.
- **Un ID de llamada para una llamada a través de un Proxy SIP:** Usted necesita seleccionar un perfil para las llamadas a través de un Proxy SIP. Si no hay tales perfiles disponibles, usted necesita crear tal perfil que va a usar.
- **Un número de teléfono regular:** Usted necesita seleccionar un perfil para las llamadas a través de un Gateway apropiado, si desea llamar a un número de teléfono regular. Si no hay tales perfiles disponibles, usted necesita crear tal perfil que vaya a usar.

Usted también puede necesitar agregar un "prefijo" al número de teléfono para dirigir la llama a los teléfonos a través de los Gateways requeridas.

Si usted tiene Microsoft Outlook o Outlook Express instalados en su computadora, usted puede llamar los números guardados en sus contactos. Vaya a la sección de los Contactos por detalles.

Usted también puede usar un Gatekeeper para hacer una llamada a un número del teléfono regular.

- **Un Nickname en el Phonebook:** Usted necesita especificar toda la información necesaria en el Phonebook sobre el nickname que desee ingresar. Esto puede hacerse en el panel de Contactos.
  
- **Una dirección H.323:** SJphone™ soporta la sintaxis de dirección avanzada de H.323. Ningún perfil de servicio se requiere para esta llamada.
  - Un host
  - Un campo o IP H.323
  - Un número a través del Gateway H.323
  - Un usuario con el nickname registrado con el Gatekeeper H.323
  - Un número de teléfono registrado con el Gatekeeper H.323
  - Un número de teléfono externo a través del Gatekeeper H.323
  
- **Un URL SIP:** SJphone™ soporta URL con sintaxis avanzadas de SIP. Ningún perfil de servicio se requiere para esta llamada. Ningún perfil de servicio se requiere para esta llamada.
  - Un host.
  - Un usuario
  - Un número de teléfono a través de un Gateway SIP



Llamada Entrante

### Como contestar una llamada

Cuando su computadora recibe una llamada, usted oirá un ring sound. Simultáneamente, un mensaje de la Llamada Entrante aparecerá.



Mensaje de Llamada Entrante

- Para contestar la llamada, haga clic en el botón Accept o presione Alt + a o Enter.
- Para rechazar la llamada haga clic en el botón Ignore o presione Alt + i.

Usted puede configurar su SJphone™ para aceptar automáticamente o rechazar todas las llamadas entrantes.

## **Control de una llamada activa**

Usted puede poner su llamada activa en espera o puede transferirlo a otro usuario. Si SJphone™ no puede controlar la llamada, los botones de Hold y Transfer son deshabilitados.

### **Poner una llamada activa en espera**

- Doble clic a una llamada que quiera poner en espera.
- Seleccione una llamada que quiera poner en espera y haga clic en el botón Hold.
- Clic derecho a una llamada que quiera poner en espera y seleccione Hold en el menú pop – up.

### **Para continuar una llamada en espera**

- Doble clic a una llamada que desee continuar.
- Seleccione a una llamada que quiera continuar y haga clic en el botón Hold.
- Clic derecho a una llamada que quiera continuar y seleccione Resume en el menú pop – up.

### **Para transferir una llamada activa a otro usuario**

#### **Blind transfer:**

- Seleccione una llamada que quiera transferir y haga clic en el botón Transfer.
- Ingrese la dirección de usuario y
- Haga clic en el botón Transfer una vez más y presione Enter.

#### **Attended transfer:**

- Establezca una llamada a un usuario al que usted desee transferir.
- Seleccione una llamada que desee transferir y haga clic en el botón Transfer.
- Seleccione la llamada con el usuario.
- Haga clic en el botón del Transfer una vez más.



## Establecer una Conferencia

Aunque SJphone™ soporta conexiones con múltiples usuarios, usted normalmente puede hablar sólo con un usuario a la vez. Si usted quiere hablar simultáneamente con varios usuarios simultáneamente, usted necesita empezar una conferencia.

Lo puede hacer haciendo clic en el botón Conf en el panel principal del SJphone. Ahora usted puede hablar simultáneamente con varios usuarios.

También, haciendo doble clic en adds/removes los usuarios to/from la conferencia. O usted puede seleccionar varios usuarios, clic derecho, y selecciona Join to Conference/Exclude desde el item Conferencia en el menú pop - up.

Para salir del modo conferencia, haga clic en el botón Conf una vez más en el panel principal del SJphone™.



Usuarios en Conferencia

## Recibir un mensaje de voz

Para escuchar los mensajes, haga clic en el botón de Voice Mail y siga las instrucciones de la operadora.

## Para terminar una llamada

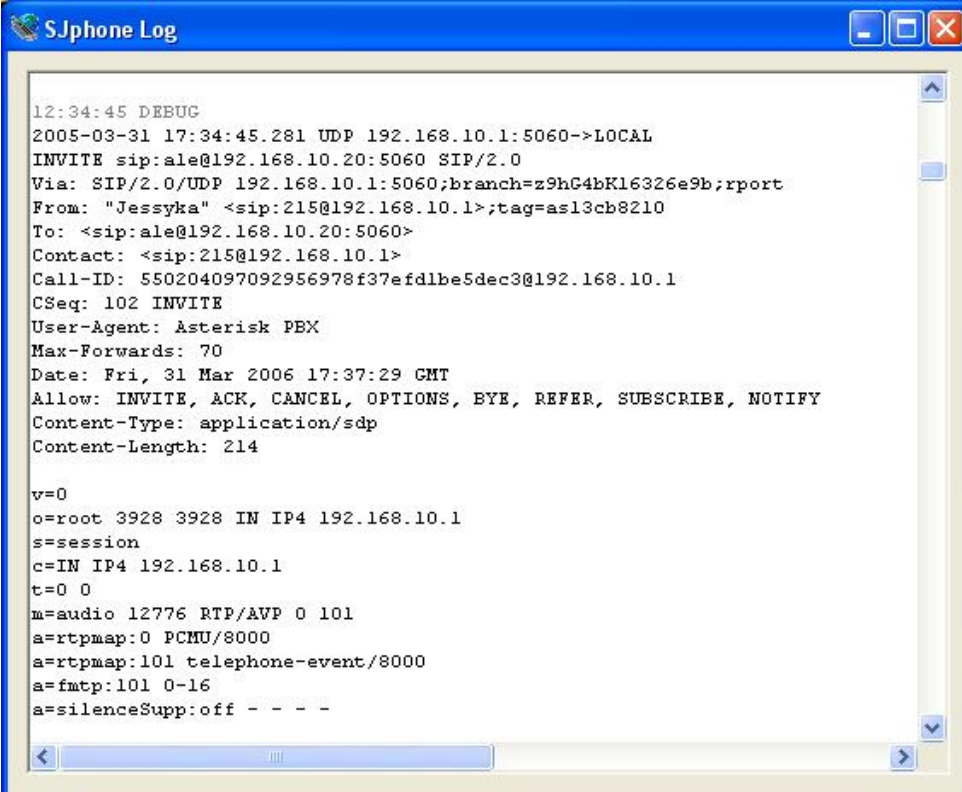
Seleccione el contacto y haga clic en el botón Hangup en el panel principal del SJphone™, o presione Alt + h o Enter.

Haga clic derecho en el contacto y seleccione el ítem Hangup en el menú pop-up. Usted puede finalizar varias llamadas simultáneamente, seleccionando el contacto, haciendo clic derecho y seleccionando Hangup en el menú pop-up.

## Log Window

La ventana Log muestra información técnica sobre el funcionamiento de SJphone™ y progreso de la llamada.

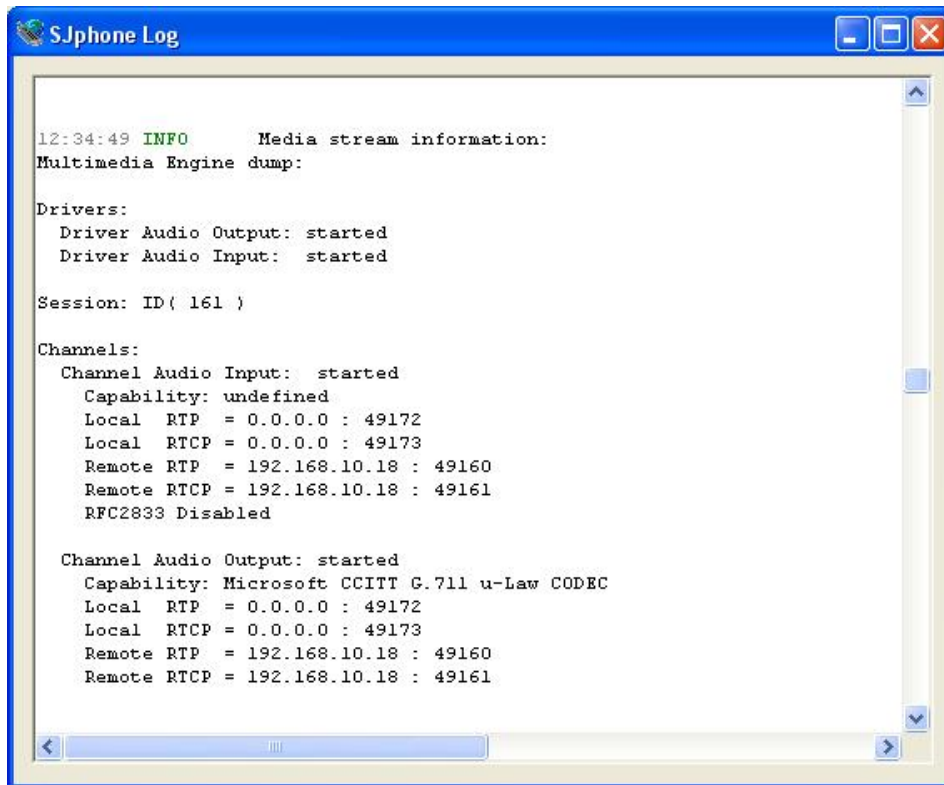
Para activar la ventana Log del SJphone™, haga clic derecho en el ícono system tray del SJphone™ y seleccione Show Log.



```
12:34:45 DEBUG
2005-03-31 17:34:45.281 UDP 192.168.10.1:5060->LOCAL
INVITE sip:ale@192.168.10.20:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.1:5060;branch=z9hG4bK16326e9b;rport
From: "Jessyka" <sip:215@192.168.10.1>;tag=as13cb8210
To: <sip:ale@192.168.10.20:5060>
Contact: <sip:215@192.168.10.1>
Call-ID: 550204097092956978f37efdlbe5dec3@192.168.10.1
CSeq: 102 INVITE
User-Agent: Asterisk PBX
Max-Forwards: 70
Date: Fri, 31 Mar 2006 17:37:29 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Content-Type: application/sdp
Content-Length: 214

v=0
o=root 3928 3928 IN IP4 192.168.10.1
s=session
c=IN IP4 192.168.10.1
t=0 0
m=audio 12776 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=silenceSupp:off - - - -
```

Sjphone Log 1



Sjphone Log 2

# ÍNDICE DE CONTENIDOS

<b>Capítulo I: Introducción .....</b>	<b>3</b>
1.1.- Planteamiento del problema .....	4
1.2.- Justificación.....	5
1.3.- Objetivos .....	6
1.3.1.- Objetivo General .....	6
1.3.2.- Objetivos Específicos.....	6
1.4.- Alcance .....	6
<b>Capítulo II: Marco Teórico.....</b>	<b>8</b>
2.1.- Voz sobre IP.....	8
2.1.1.- Introducción.....	8
2.1.2.- Generalidades.....	9
2.1.2.1.- Qué es VoIP?.....	9
2.1.2.2.- Funcionamiento.....	10
2.1.2.2.1.- Compresión de voz .....	13
2.1.2.2.2.- Estándares de Compresión.....	13
2.1.2.2.3.- Señalización.....	16
2.1.2.2.4.- Direccionamiento .....	16
2.1.2.2.5.- Enrutamiento.....	17
2.1.2.2.6.- Consumo de ancho de banda .....	18
2.1.3.- QoS (Calidad de Servicio) en las comunicaciones .....	18
2.1.3.1.- Retardo .....	20
2.1.3.2.- Jitter .....	21
2.1.3.3.- Pérdida de paquetes .....	22
2.1.4.- Seguridad.....	23
2.1.5.- Protocolos .....	26
2.1.5.1.- Pila de protocolos de VoIP.....	27
2.1.5.2.- Protocolos del Plano de datos .....	27
2.1.5.2.1.- RTP Comprimido.....	28
2.1.5.2.2.- RTCP.....	29
2.1.5.2.3.- RTCP XR.....	29
2.1.5.2.4.- CODECs.....	29
2.1.5.3.- Protocolos del Plano de Control.....	30
2.1.5.3.1.- H.323.....	31
2.1.5.3.1.1. Introducción.....	31
2.1.5.3.1.2. Protocolos incluidos en H.323.....	31
2.1.5.3.1.3. Arquitectura .....	34
2.1.5.3.1.4. Entramado (framing) y control de llamadas .....	36
2.1.5.3.1.5. Componentes H.323 .....	39
2.1.5.3.2.- SIP.....	41
2.1.5.3.2.1. Características .....	42
2.1.5.3.2.2. Arquitectura SIP .....	43
Mensajes.....	49
2.1.5.3.3.- MGCP.....	59
2.1.5.3.4.- MEGACO .....	61
2.1.5.3.5.- Comparación de Protocolos .....	64
2.1.5.3.5.1. Características .....	66
2.1.5.3.5.2. Ventajas y Desventajas.....	68
2.1.5.3.5.3. Conclusión.....	69

**Capítulo III: Análisis y Diseño de la infraestructura de la ESPE y las Sedes para comunicaciones de VoIP .....71**

3.1.-	Situación Actual .....	71
3.1.1.-	Análisis de la Red Área Local de la ESPE - Sangolquí .....	76
3.1.2.-	Análisis de la Red de Área Extendida de la ESPE y sus Sedes.....	77
3.2.-	Requerimientos del enlace de la ESPE y sus Sedes.....	79
3.2.1.-	Cálculo del consumo de ancho de banda con SIP para la ESPE y sus Sedes .....	82
3.3.-	Levantamiento de Requerimientos de la ESPE .....	83
3.3.1.-	Tamaño de la Muestra .....	83
3.3.2.-	Encuesta dirigida a los usuarios de la ESPE .....	85
3.3.2.1.-	Objetivos .....	85
3.3.2.2.-	Enfoque.....	85
3.3.2.3.-	Formato de la encuesta .....	86
3.3.2.4.-	Resultados .....	86
3.3.2.5.-	Conclusiones.....	90
3.4.-	Análisis y Diseño de la Red VoIP utilizando el protocolo SIP .....	91
3.4.1.-	Resolución de las necesidades de la ESPE .....	91
3.4.2.-	Solución propuesta para la ESPE y sus Sedes .....	91
3.4.2.1.-	Diseño .....	92
3.4.2.2.-	Características del Diseño .....	92
3.4.2.3.-	Ventajas .....	93
3.4.2.4.-	Desventajas .....	94
3.4.2.5.-	Costo.....	94
3.4.2.6.-	Equipos .....	95
3.4.2.7.-	Software .....	97

**Capítulo IV: Pruebas de Funcionamiento.....99**

4.1.-	Antecedentes .....	99
4.2.-	Objetivo General .....	99
4.3.-	Objetivos Específicos.....	99
4.4.-	Equipos y Materiales.....	100
4.5.-	Diagrama de la Red .....	101
4.6.-	Desarrollo.....	101
4.6.1.-	Instalación de Linux .....	102
4.6.2.-	Configuración de Apache (httpd) .....	104
4.6.3.-	Configuración DHCP .....	105
4.6.4.-	Configuración DNS .....	105
4.6.5.-	Configuración Squid.....	106
4.6.6.-	Asterisk .....	107
4.6.6.1.-	Introducción.....	107
4.6.6.2.-	Arquitectura.....	107
4.6.6.3.-	Instalación .....	108
4.6.6.3.1.-	Mpg123 .....	109
4.6.6.3.2.-	Zaptel .....	109
4.6.6.3.3.-	Libpri .....	110
4.6.6.3.4.-	Asterisk .....	110
4.6.6.3.5.-	Sonidos .....	111
4.6.6.4.-	Configuración de Asterisk .....	112
4.6.6.4.1.-	Archivos de Configuración .....	112
4.6.7.-	SJphone .....	112
4.6.7.1.-	Instalación .....	113
4.7.-	Práctica de Laboratorio .....	115

4.7.1.-	Configuración de la Red.....	115
4.7.2.-	Configuración del DNS.....	118
4.7.3.-	Configuración de DHCP.....	120
4.7.4.-	Configuración de Asterisk.....	120
4.7.4.1.-	Configuración del servidor SIP.....	120
4.7.4.2.-	Definición de canales.....	121
4.7.4.3.-	Configuración del Plan de Marcación.....	124
4.7.4.4.-	Aplicaciones del Servidor.....	126
4.7.4.4.1.-	voicemail.conf.....	126
4.7.4.4.2.-	meetme.conf.....	127
4.7.4.4.3.-	musichold.conf.....	127
4.7.5.-	Configuración de Usuario del Softphone.....	128
4.7.6.-	Llamadas entre Usuarios.....	133
4.7.6.1.-	Informaciones Adicionales.....	144
4.7.6.1.1.-	Buzón de Correo.....	144
4.7.6.1.2.-	Codecs.....	145
<b>Capítulo V: Conclusiones y Recomendaciones .....</b>		<b>146</b>
5.1.-	Conclusiones.....	146
5.2.-	Recomendaciones.....	148
<b>Anexos.....</b>		<b>164</b>
Anexo A: Formato de la encuesta realizada a los usuarios de la red de la ESPE .		165
Anexo B: Manual de Uso e Instalación del SJphone™ .....		166

## LISTADO DE FIGURAS

Figura 2.1: Flujo de un circuito de voz comprimido .....	10
Figura 2.2: Tipos de redes IP .....	12
Figura 2.3: Red VoIP .....	13
Figura 2.4: Codificador mpeg simplificado.....	15
Figura 2.5: Decodificador mpeg simplificado.....	15
Figura 2.6: Protocolos VoIP .....	27
Figura 2.7: Protocolo RTP .....	28
Figura 2.8: Protocolos incluidos en H.323 .....	32
Figura 2.9: Arquitectura H.323 dentro del modelo OSI.....	35
Figura 2.10: Arquitectura H.323.....	36
Figura 2.11: Componentes de la arquitectura H.323.....	39
Figura 2.12: Pila de protocolo SIP según IETF .....	42
Figura 2.13: Arquitectura SIP .....	45
Figura 2.14: Ejemplo de establecimiento de llamada mediante proxys SIP.....	47
Figura 2.15: Mensaje genérico (rfc 822).....	49
Figura 2.16: Formato general de los mensajes de solicitudes o métodos SIP.....	51
Figura 2.17: Ejemplo de un mensaje de solicitud SIP. ....	52
Figura 2.18: Formato general de los mensajes de respuesta SIP.....	53
Figura 2.19: Ejemplo de un mensaje de respuesta SIP. ....	54
Figura 2.20: Red megaco .....	62
Figura 2.21: Comparación de protocolos.....	65
Figura 3.1: ESPE – Sangolquí.....	71
Figura 3.2: Central VoIP .....	72
Figura 3.3: Ubicación de las redes en el campus ESPE – Sangolquí.....	76
Figura 3.4: Gráfico de los enlaces wan de la ESPE y sus sedes .....	78
Figura 3.5: Laboratorios especializados .....	79
Figura 3.6: Internet II proyecto cedia .....	79
Figura 3.7: Valores de MOS (Mean Opinion Score).....	81
Figura 3.8: Compresión vs. Calidad .....	82
Figura 3.9: Resultado pregunta 1 .....	86
Figura 3.10: Resultado pregunta 2 .....	87
Figura 3.11: Resultado pregunta 3 .....	87
Figura 3.12: Resultado pregunta 4 .....	88
Figura 3.13: Resultado pregunta 5 .....	88
Figura 3.14: Resultado pregunta 6 .....	89
Figura 3.15: Resultado pregunta 7 .....	89
Figura 3.16: Diseño de la wan con SIP .....	92
Figura 3.17: Servidor SIP .....	95
Figura 3.18: Auriculares plantronics DSP 400.....	97
Figura 4.1: Diagrama de la red.....	101
Figura 4.2: Selección del tipo de instalación. ....	102
Figura 4.3: Configuración de red. ....	103
Figura 4.4: Configuración de firewall .....	103
Figura 4.5: Selección del grupo de paquetes. ....	104
Figura 4.6: Pantalla de bienvenida .....	113
Figura 4.7: Licencia .....	114
Figura 4.8: Pantalla final de instalación.....	114
Figura 4.9: Pantalla de inicio del SJphone. ....	115
Figura 4.10: Configuración de la red .....	116
Figura 4.11: Configuración eth0 .....	116

Figura 4.12: Configuración eth2 .....	117
Figura 4.13: Configuración del DNS .....	117
Figura 4.14: Crear la zona maestra .....	118
Figura 4.15: Registro de direcciones .....	118
Figura 4.16: Zona reversa .....	119
Figura 4.17: Registro de direcciones de reversa .....	119
Figura 4.18: Usuario no registrado .....	128
Figura 4.19: Pestaña user information.....	129
Figura 4.20: Pestaña profiles.....	129
Figura 4.21: Crear nuevo perfil.....	130
Figura 4.22: Perfil creado .....	130
Figura 4.23: Opciones del perfil.....	131
Figura 4.24: Opciones del perfil avanzadas .....	131
Figura 4.25: Información del usuario .....	132
Figura 4.26: Usuario registrado .....	132
Figura 4.27: Acceso directo a SJphone.....	133
Figura 4.28: Pantalla inicial del SJphone.....	133
Figura 4.29: Mensaje de llamada entrante .....	134
Figura 4.30: Pantalla inicial del SJphone.....	135
Figura 4.31: Llamada de usuario jessy a usuario jose.....	136

## LISTADO DE TABLAS

Tabla 2.1: Parámetros de calidad en telefonía ip .....	19
Tabla 2.2: Tiempos de retardo de extremo a extremo (un sentido).....	21
Tabla 2.3: Requerimientos básicos de características de voz para aplicaciones de voz sobre datos. ....	23
Tabla 2.4: Tipos de codec's.....	30
Tabla 2.5: Modelo de referencia osi y estándar h.323.....	34
Tabla 2.6: Características de protocolos .....	66
Tabla 3.1: Equipos ESPE – Sangolquí .....	74
Tabla 3.2: Equipos ESPE – Latacunga .....	74
Tabla 3.3: Equipos ESPE – Idiomas.....	75
Tabla 3.4: Equipos ESPE – IASA II .....	75
Tabla 3.5: Equipos ESPE – IASA I .....	75
Tabla 3.6: Equipos ESPE – Héroes del Cenepa .....	76
Tabla 3.7: Enlace wan en el año 2001 .....	77
Tabla 3.8: Enlace wan en el año 2002 – 2003 .....	77
Tabla 3.9: Enlace wan en el año 2004 .....	77
Tabla 3.10: Enlace wan en el año 2005 .....	78
Tabla 3.11: Codec's de compresión audio que utiliza el protocolo sip.....	80
Tabla 3.12: Costo estimado.....	95
Tabla 3.13: Características del servidor.....	96
Tabla 3.14: Características de red hat linux enterprise es .....	98
Tabla 4.1: Características básicas del servidor sip.....	100
Tabla 4.2: Usuarios de la red.....	144
Tabla 4.3: Codecs del SJphone.....	145



## LISTADO DE CUADROS

Cuadro 4.1: Fichero sip.conf.....	120
Cuadro 4.2: Usuario 1.....	122
Cuadro 4.3: Usuario 2.....	122
Cuadro 4.4: Usuario 3.....	123
Cuadro 4.5: Fichero extensión.conf.....	125
Cuadro 4.6: Fichero voicemail.conf .....	126
Cuadro 4.7: Fichero meetme.conf .....	127
Cuadro 4.8: Fichero musichold.conf .....	128
Cuadro 4.9: SJphone Log 1 .....	137
Cuadro 4.10: SJphone Log 2.....	138
Cuadro 4.11: SJphone Log 3.....	139
Cuadro 4.12: SJphone Log 4.....	140
Cuadro 4.13: SJphone Log 5.....	141
Cuadro 4.14: SJphone Log 6.....	142
Cuadro 4.15: SJphone Log 7.....	143

**HOJA DE LEGALIZACION DE FIRMAS**

**ELABORADA(O) POR**

---

Jessica Chiriboga

---

Alexandra Guevara

**DECANO DE LA FACULTAD DE INGENIERIA DE SISTEMAS E  
INFORMÁTICA**

---

Tcrn. de E.M Ing. Marco Quintana

Sangolquí, 26 de Junio de 2006