Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE SERVICIOS DE VOZ SOBRE IP BASÁNDOSE EN PROTOCOLO SESSION INITIATION PROTOCOL (SIP) UTILIZANDO CONVERGENCIA DE REDES

Luis Armando Gálvez Catalán
Asesorado por el Ing. Enrique Edmundo Ruiz Carballo

Guatemala, octubre de 2007

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE SERVICIOS DE VOZ SOBRE IP BASÁNDOSE EN PROTOCOLO SESSION INITIATION PROTOCOL (SIP) UTILIZANDO CONVERGENCIA DE REDES

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR:

LUIS ARMANDO GÁLVEZ CATALÁN
ASESORADO POR EL ING. ENRIQUE EDMUNDO RUIZ CARBALLO

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO ELECTRÓNICO

GUATEMALA, OCTUBRE DE 2007

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Angel Dávila Calderón
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Guillermo Antonio Puente Romero
EXAMINADOR	Ing. Jose Anibal Silva de los Angeles
EXAMINADORA	Ing. Julio Rolando Barrios Archila
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE SERVICIOS DE VOZ SOBRE IP BASÁNDOSE EN PROTOCOLO SESSION INITIATION PROTOCOL (SIP) UTILIZANDO CONVERGENCIA DE REDES,

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, el 12 de julio de 2007.

Luis Armando Gálvez Catalán

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

Guatemala, 18 de Septiembre de 2007

Ingeniero
Julio Cesar Solares Peñate
Coordinador de Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería,
Universidad de San Carlos de Guatemala
Presente.

Estimado Ingeniero Solares:

Por este medio me dirijo a usted para informarle que habiendo asesorado al estudiante **Luis Armando Gálvez Catalán** con carné No. **2000-10491**, en el trabajo de graduación **"Estudio de factibilidad para la implementación de servicios de voz sobre Ip basándose en protocolo Session Initiation Protocol (SIP) utilizando convergencia de redes"** y llenando éste los objetivos trazados, extiendo la aprobación del mismo.

Por lo tanto, el autor de éste trabajo y yo como asesor, nos hacemos responsables del contenido y conclusiones del mismo.

Sin otro particular, me suscribo tentamente.

Ingeniero Enrique Edmundo Ruiz Carballo
Asesor

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

Guatemala, 2 de OCTUBRE 2007.

Señor Director
Ing. Mario Renato Escobedo Martìnez
Escuela de Ingenierìa Mecànica Elèctrica
Facultad de Ingenierìa, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: **Estudio de factibilidad para la implementaciòn de servicios de voz sobre Ip basàndose en protocolo Session Initiation Protocol (SIP utilizando convergencia de redes, desarrollado** por el estudiante; Luis Armando Gàlvez Catalàn, por considerar que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Julio Cèsar Solares Peñate
Coordinador Area de Electrònica

JCSP/sro

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

El Director de la Escuela de Ingenierìa Mecànica Elèctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Area, al trabajo de Graduación del estudiante; Luis Armando Gàlvez Catalàn, titulado: **Estudio de factibilidad para la impiementaciòn de servicios de voz sobre Ip basàndose en protocolo Session Initiation Protocol (SIP) utilizando convergencia de redes,** procede a la autorización del mismo.

Ing. Mario Renato Escobedo Martìnez
DIRECTOR

UNIVERSIDAD DE SAN CARLOS
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA
MECANICA ELECTRICA
GUATEMALA

GUATEMALA, 3 DE OCTUBRE 2,007.

A mi madre y a mi padre, quienes me han enseñado con sus ejemplos las lecciones más importantes de la vida.

AGRADECIMIENTOS A:

Dios Por haberme dado el don del entendimiento

Mis padres y hermano Por apoyarme incondicionalmente en todo momento de mi carrera y de mi vida. En especial a mi madre, por tantas noches de desvelo y tantos consejos que me han traído hasta aquí.

Familia A mi abuelo Antonio Gálvez Ortiz, que fue un ejemplo desde los primeros días de mi vida. A mi bisabuela Maria Luisa Ortiz, que me dio su cariño y amor desde siempre. A mi abuelita Esperanza de Jesús Castillo, quien me dio grandes lecciones de vida. Que en paz descansen.

A mi tío Jorge, por todo su apoyo y por haber depositado en mí siempre tanta confianza. A mi padrino Ing. Carlos Hermosilla gracias por sus consejos y por apoyarme siempre. A mi novia por haberme motivado a terminar este trabajo de graduación.

Amigos A todos mis amigos de la universidad, con quienes aprendí el significado real de la palabra amistad, juntos compartimos además de las aulas, las alegrías y los sufrimientos. En especial a Henry

Cifuentes, Leonel Torres, y Rodolfo Ixtamalic, en paz descansen mis colegas.

Compañeros de trabajo A todos mis compañeros y ex-compañeros de trabajo, en especial a Telma Herrera y Carlos de León, por su amable colaboración en este trabajo de graduación. A mis compañeros del NOC Regional, Pedro Mérida, Carlos, Laura, Julio, Juan Pablo, Harim, Selvin, Kelvin, Rafael y Luis Carlos, con quienes aprendí lo que es trabajar como un verdadero profesional.

Catedráticos Por compartir sus conocimientos y experiencias para formar nuevos profesionales. En especial a los ingenieros Enrique Ruiz y Guillermo Puente.

Universidad A la Universidad de San Carlos, por haber sido un segundo hogar para hacer de mí un buen profesional, pero sobre todo, por hacer de mí una mejor persona.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Ancho de Banda Capacidad de transmisión en unidades de datos por segundo de un canal físico de comunicaciones.

ASN.1 (*Abstract Syntax Notation One*) Es un tipo de notación abstracta utilizada para representar estructuras de datos.

Broadcast Modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultanea.

Canal de comunicación Medio de transmisión por el que viajan las señales portadoras de la información que se intercambia entre un emisor y un receptor.

Clase de servicio Es un método para administrar el tráfico en una red que agrupa tipos similares de tráfico y los trata como una clase de tráfico.

Codec Abreviatura del término codificador-decodificador, describe una especificación desarrollada en software o hardware con capacidad para transformar un flujo de datos.

Dial plan Establece el patrón de números necesarios que se anteponen a un número telefónico para realizar una llamada.

Escalabilidad Propiedad de la red para poder evolucionar a nuevas tecnologías sin modificar su topología.

Ethernet Tecnología de redes de computadoras de área local (LANs) basada en tramas de datos que define las características de cableado y señalización de nivel físico, y los formatos de trama del nivel de enlace de datos del modelo OSI.

Firewall Elemento de una red utilizado para controlar el acceso a servicios o dispositivos utilizando políticas de red.

Handshaking Sistema de negociación automatizado utilizado por dispositivos electrónicos para establecer comunicaciones entre ellos.

Host Es un servicio brindado para almacenar paginas *web* en un servidor, también se conoce con este nombre a la dirección en donde se almacena la página web.

HTTP (*HyperText Transfer Protocol*) Protocolo utilizado para la navegar en Internet.

ISDN (*Integrated Services Digital Networ*) Es una evolución de la red de telefonía que permite la integración de servicios con un único acceso.

MIME (*Multipurpose Internet Mail Extensions*) Una serie de convenciones destinadas a facilitar el intercambio de todo tipo de archivos a través de Internet y de forma transparente para el usuario.

MPEG (*Moving Picture Experts Group*) Nombre por el cual se conoce al grupo de estándares que se utiliza para codificar información audiovisual en un formato digital.

NAT (*Network Address Translation*) Mecanismo utilizado por routers IP que convierte, en tiempo real, las direcciones incompatibles utilizadas en los paquetes transportados en direcciones compatibles.

NSP (*Network Service Provider*) Es una empresa que vende ancho de banda o acceso a una red, generalmente incluye acceso a Internet.

PBX	(*Private Branch Exchange*) Es un servicio ofrecido por una empresa de telecomunicaciones, por el cual cierta cantidad de líneas o números son agrupadas en un único número que se publica.
Proxy	Hace referencia a un programa o dispositivo que hace una acción en representación de otro, se utiliza mayormente para conexiones a Internet.
QoS	(*Quality of Service*) Tecnología que garantiza que se transmitirá cierta cantidad de datos en un tiempo dado.
Router	Dispositivo de *hardware* utilizado para la interconexión de redes, también conocido como enrutador.
SMTP	(*Simple Mail Transfer Protocol*) Protocolo de red basado en texto utilizado para el intercambio de mensajes.
VPN	(*Virtual Private Network*) Tecnología de red que permite una extensión de la red local sobre una red pública como por ejemplo Internet.
Webcam	Tipo de cámara utilizada para transmitir imágenes en tiempo real a través de Internet.

RESUMEN

Los sistemas de voz sobre IP (VoIP) transmiten la señal de voz en forma de paquetes a través de cualquier red IP convencional, a diferencia de los sistemas de telefonía convencional, esto implica que el canal de comunicación puede ser utilizado por varios usuarios simultáneamente. La idea de transmitir señales de voz y datos sobre una misma red nos lleva a pensar en un sistema en donde converjan distintas tecnologías que nos permitan reducir costos de operación y desarrollar nuevas aplicaciones como videoconferencias, llamadas telefónicas, envío de mensajes instantáneos, etc. Esto hace necesario la utilización de protocolos estandarizados que cumplan con ciertas características para facilitar la expansión de la red y la implementación de estas aplicaciones.

El protocolo SIP fue diseñado para establecer, modificar y terminar sesiones multimedios. Una de sus principales ventajas es que es bastante fácil de decodificar ya que es muy similar al protocolo HTTP, utilizado en Internet y que goza de bastante popularidad. La implementación de una red convergente basándose en SIP representa algunos retos técnicos pero también brinda una amplia gama de nuevas aplicaciones y servicios. En este trabajo de investigación se estudia a fondo la estructura y modo de funcionamiento de este protocolo. Luego de un análisis técnico y económico se concluye que es bastante recomendable tomar en cuenta el protocolo SIP cuando sea necesario desarrollar un sistema de comunicaciones, para optimizar los recursos de una red IP ya establecida.

OBJETIVOS

General

Analizar la factibilidad técnica y económica de implementar un sistema de VoIP utilizando protocolo SIP y convergencia de redes.

Específicos

1. Estudiar los conceptos relacionados con la convergencia de redes para definir sus beneficios y sus requerimientos técnicos.
2. Analizar las características de los distintos tipos de tráfico que pueden transmitirse en una red de datos.
3. Conocer a fondo las características generales y el funcionamiento del *Session Initiation Protocolo* (SIP).
4. Establecer las ventajas que representa la utilización del protocolo *Session Initiation Protocol* (SIP) para optimizar los recursos disponibles en una red de datos.
5. Realizar un análisis que establezca si es factible técnica y económicamente implementar una red convergente utilizando *Session Initiation Protocol* (SIP).

INTRODUCCIÓN

Tradicionalmente se han utilizado distintas redes para transmitir diferentes tipos de servicio, por ejemplo, la red conmutada para la transmisión de señales de voz operada por proveedores de servicios telefónicos, redes de datos en pequeñas empresas o la red de televisión por cable. Estas redes poseen características que satisfacen los requerimientos específicos del tipo de tráfico que transmiten. Es evidente que si se integran todas estas redes en una sola se pueden obtener considerables beneficios en eficiencia y ahorro de costos de operación. En los últimos días ha surgido la idea de transmitir señales multimedia sobre redes IP. Lo que ha generado el desarrollo de protocolos como el *Session Initiation Protocolo* (SIP) que facilitan la transmisión de información en tiempo real.

El fin principal de implementar un sistema de VoIP sobre una red convergente responde básicamente a la necesidad de reducir costos, en el área de las telecomunicaciones. Un sistema bien diseñado y optimizado puede brindar grandes beneficios a sus usuarios, en una empresa que cuente con una red de datos relativamente grande puede llegar a sustituir a la red de telefonía. En otros casos puede representar una manera de ahorrar dinero en llamadas a larga distancia utilizando una infraestructura compartida con otros usuarios al mismo tiempo. En Guatemala existen varios posibles escenarios en los que podría aplicarse una solución SIP VoIP para optimizar recursos y reducir costos. Los beneficios tangibles pueden apreciarse casi de inmediato y la solución presenta una relación beneficio/costo en un plazo no muy largo.

1. CONVERGENCIA DE REDES Y VOZ SOBRE IP

1.1. Diferencia entre tráfico de datos y voz

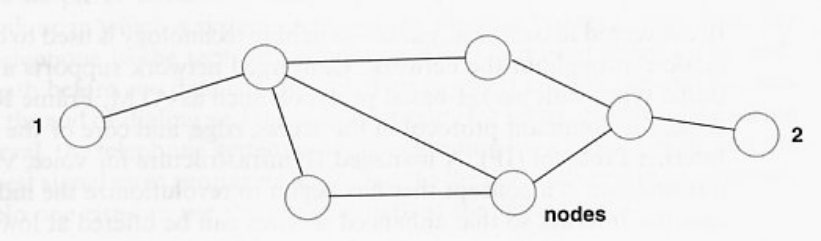
En el pasado las redes tanto de voz como de datos se habían mantenido separadas una de la otra. Esto debido a que las características del tráfico de ambas no permitían su interacción. Los avances en la tecnología de redes ha hecho posible la construcción de redes con capacidad de transmitir distintos tipos de tráfico. En la actualidad, básicamente existen dos tipos de redes: las que emplean conmutación de circuitos y las que utilizan conmutación de paquetes. Un ejemplo de una red que utiliza conmutación de circuitos es la red de telefonía. Con esta técnica el sistema "busca" un camino físico entre el aparato telefónico del receptor y el transmisor. Es necesario establecer un camino de punto a punto antes de que cualquier información sea transmitida. Por otro lado, la conmutación de paquetes transmite pequeñas cantidades de información basándose en una dirección destino contenida en cada paquete.

1.1.1. Características de tráfico de datos

Las redes de datos pueden clasificarse de acuerdo a la extensión que cubren, redes de área local (LAN), de área metropolitana (MAN) y de área ancha (WAN). En un principio todas las redes eran diseñadas basándose en conmutación de circuitos. A finales de los años sesenta se desarrolló la técnica de conmutación de paquetes para redes que cubren grandes áreas geográficas. Una red de este tipo se compone de varios nodos conectados entre sí por distintos medios de transporte. Utilizando la conmutación por paquetes la

información se divide en pequeños “paquetes” de información. Cada paquete incluye información dentro de un encabezado, entre estos: número de serie, dirección de destino, etc. Cada paquete es enviado a su destino individualmente y son re-ensamblados al llegar para formar el mensaje original. Es importante hacer notar que cada paquete puede tomar una ruta diferente a los demás. Esto supone las siguientes ventajas: la red puede soportar varias conexiones simultáneamente, la transmisión de los mensajes cortos no son afectados por los mensajes más largos y es más eficiente que la conmutación de circuitos. Finalmente, la interconexión de muchos nodos en una sola red es relativamente sencilla y económica ya que un solo canal es utilizado por varios usuarios a la vez, aunque esto último puede presentar una desventaja ya que la red podría llegar a saturarse si los usuarios son demasiados.

Figura 1. **Nodos en una red conmutada por paquetes**



Fuente: Ellis, Juanita y otros, **Voice Video, and Data Network Convergence**

Una red de datos interconecta nodos a los cuales se conectan terminales que utilizan el enlace de diferentes formas, conexiones punto a punto y *broadcast* por ejemplo. Todos los nodos en una red *broadcast* comparten el mismo canal de comunicación, el protocolo de red controla el acceso y maneja las colisiones que ocurren cuando más de un nodo intenta utilizar el canal al mismo tiempo.

La transmisión de datos implica la transferencia de información entre programas de computadora. Así como los humanos manejan un lenguaje común, los programas manejan protocolos en común para establecer comunicación entre otros programas. Un protocolo define el formato y significado de los datos que se están intercambiando. En un principio se utilizaban programas monolíticos que se caracterizaban por proveer varios servicios, pero eran extremadamente difíciles de modificar. Para solucionar este problema se introdujo el concepto de “capas”. Una capa es simplemente un programa o grupo de programas que provee servicios a la capa superior y utiliza servicios de una capa inferior. Cuando se realiza un cambio en alguna capa, únicamente se ve afectada la capa superior a esta. Los programas ubicados en las capas mas bajas proveen servicios manejando la información de manera concreta. Los programas ubicados en capas superiores manejan la información de manera abstracta: estructuras de datos para programas de aplicación, gráficos, etc. Y los programas en las capas medias se encargan de transformar la información concreta en abstracta. Asimismo el concepto de capas se aplica también a los protocolos, los programas en cada capa que utilizan el mismo protocolo para comunicarse se les denominan *peers*, que traducido al español significa “igual” o que pertenece al mismo grupo.

1.1.2. Características de tráfico de voz

Tradicionalmente las redes de telefonía han utilizado conmutación de circuitos, cuando se realiza una llamada básicamente se está estableciendo un circuito entre las dos terminales, de aquí viene el término conmutación de circuitos. Una red de telefonía tradicional utiliza una interfase de dos cables para conectarse a la red y requiere el respaldo de un circuito hibrido para transmitir y recibir señales. El rango audible de frecuencias varia de 20 a 20000 Hz, la mayor parte de la energía utilizada al hablar se concentra en el rango de 600 a 3400 Hz.

Se requieren de tres tipos de señales en una red de telefonía tradicional: de supervisión, de alerta y de direccionamiento. Las de supervisión monitorean el estado de los aparatos, verifican si algún aparato esta descolgado o cuando se finaliza una llamada. Las señales de alerta involucran el mantener al tanto al usuario de el estado de las llamadas, por ejemplo la alerta cuando alguien está llamando (ring) o los tonos sobre la línea (ocupado, llamando, etc). Finalmente las señales de direccionamiento permiten al usuario marcar extensiones específicas. Debido a que la telefonía tradicional opera en un modelo maestro/esclavo, el equipo debe emular dos tipos de interfases, el lado del usuario y el de la red. El lado del usuario esperaría recibir una señal del lado de la red. Para esto se utilizan los puerto FXS (*Foreing Exchange Service)* y FXO *(Foreing Exchange Operator)*. Un puerto FXS provee 48V DC y acepta dígitos marcados, su opuesto es un puerto FXO que se utiliza para conectarse a una red conmutada proveyendo servicios y supervisión. Las redes primitivas de telefonía realizaban la conmutación por medio de operadores humanos que conectaban los circuitos físicos.

1.1.3. Tecnología de Convergencia

La tecnología de convergencia propone un cambio drástico en la manera en que las empresas de telecomunicaciones manejan el tráfico de voz y datos. En una red de convergencia se utiliza tecnología de conmutación de paquetes para transmitir información. El tráfico tanto de voz como de video y datos tiene características que difieren grandemente entre ellos, esto dificulta la transmisión sobre una misma red. El tráfico de datos tiende a ser continuo y consume un gran ancho de banda por momentos cortos, mientras que el tráfico de voz es predecible y requiere una ruta estable y con poco retardo entre punto y punto. Finalmente el tráfico de video es una mezcla de estos dos últimos. De cualquier manera, la convergencia de redes representa un reto para poder mezclar distintas tecnologías y equipos.

1.2. Elementos de una red convergente

Uno de los aspectos más importantes de las modernas redes convergentes es que su arquitectura permite que sus funciones puedan dividirse en componentes lógicos. Permitiendo así brindar soluciones con un elevado nivel de escalabilidad e interoperabilidad. Podemos distinguir entonces los siguientes elementos que forman una red convergente: Estructura IP, puertas de acceso, controladores, procesadores adjuntos y terminales.

1.2.1. Estructura IP

Es la base para una red convergente, ésta provee la infraestructura física para transportar voz, datos y videos utilizando protocolo IP. Debe utilizar herramientas especializadas para manejar y asegurar QoS (calidad de servicio).

1.2.2. Puertas de acceso (*Gateways)*

Las puertas de acceso o *gateways* son equipos que se utilizan para acceder redes de distintos tipos. Básicamente se encargan de "traducir" protocolos, existen dos tipos: *Media Gateways* y *Signaling Gateways*.

Media gateways: típicamente se conforma de múltiples interfases físicas que pueden incluír: Ip, generalmente *Ethernet* para acceder a la red IP; FXS, para conectarse directamente a teléfonos análogos; FXO, para conectarse a líneas troncales; y otras más para interconectar aplicaciones más especializadas, líneas digitales y redes inalámbricas por ejemplo. Además de la conexión física de los medios, un media gateway también se encarga de la traducción entre protocolos y de la conversión de medios analógicos a digitales. Esta última la realiza por medio de codificadores/decodificadores o codecs.

Signaling gateways: las puertas de acceso de señalización son tipos especializados de gateways que se encargan de traducir la señalización y transporte de una red conmutada por circuitos a una estructura IP y viceversa.

1.2.3. Controladores

Controladores de medios: el MC (*media controler)* es el elemento principal que realiza el proceso de llamada en una estructura IP. Se le conoce también como *media gateway controler*, *gatekeeper* o incluso servidor de telefonía. Se encarga de realizar las funciones de control y administración necesarias para mantener la integridad de la red en los distintos ambientes. Provee las funciones de: autenticación, autorización, control y ruteo de llamadas, funciones de telefonía como PBX, políticas de seguridad, etc.

Unidad de control multipunto: MCU por sus siglas en inglés, son utilizados en un ambiente IP para conectar varios usuarios a una misma conexión. Se utilizan generalmente para brindar servicios de conferencia de audio o video.

1.2.4. Procesadores adjuntos y terminales

Procesadores adjuntos: es un dispositivo que provee servicios periféricos a una red convergente, podemos mencionar servidores de aplicaciones avanzadas y servidores de administración de red.

Terminales: en este contexto se refiere a puntos finales basados en IP, dispositivos como teléfonos IP, unidades de video o *soft-phones*, software emulador de teléfonos. Se conectan directamente entre ellos o bien a algún *gatekeeper/softswitch* para realizar conexiones en entornos IP o bien a un media *gateway* para interactuar con estaciones no IP.

1.3. Voz sobre IP

1.3.1. Requerimientos de VoIP sobre una red IP

El objetivo de un sistema de VoIP siempre será alcanzar la mejor calidad de voz transmitida. Existe un balance entre las limitantes de los medios físicos y una calidad aceptable de transmisión de voz. Se requiere básicamente que la red IP tenga bajos tiempos de retardo (*delay)*, poca pérdida de paquetes y un bajo nivel de *jitter*. El termino *jitter* se refiere a la variación del tiempo que tarda un paquete en llegar a su destino y el tiempo en el que s e esperaba que llegara. Teniendo un bajo nivel de *jitter* se evita el recibir paquetes

desordenadamente, esto afecta una transmisión de voz, en la cual los paquetes deben seguir un estricto orden, ya que se trata de una transmisión en tiempo real y no hay mucho tiempo para ordenarlos. También se debe considerar la utilización uniforme de protocolos a través de la red y evitar conversiones digitales/analogas en la medida de lo posible ya que de lo contrario paulatimanete se degrada la calidad de la voz. Si se piensa utilizar una PC como terminal o *softphone*, se debe prestar atención a la calidad de los transductores, tarjetas de audio e incluso componentes internos de la PC a utilizar ya que incluso un disco duro de poca velocidad puede afectar la señal.

Otro tema de vital importancia es el ancho de banda disponible en la red, las redes en las que propiamente es posible modificar el ancho de banda son ideales para la transmisión de voz. Redes como Internet ofrecen muy pocas posibilidades, ya que el ancho de banda requerido por una llamada varia dependiendo que tipo de codec se utilice, ver tabla I. Algunos expertos afirman que el ancho de banda mínimo requerido no debe ser menor al 75% del total de ancho de banda disponible en el enlace. Y este ancho de banda disponible debe calcularse sumando los requerimientos del tráfico de VoIP, de video y datos que se esté considerando manejar para una aplicación específica.

Tabla I. **Codecs comúnmente utilizados**

Standard	Coding Type	Bit Rate (Kbps)	MOS
G.711	PCM	64	4.3
G.729	CS-ACELP	8	4.0
G.723.1	ACELP	6.3	3.8
	MP-MLQ	5.3	

Fuente: Ellis, Juanita y otros, **Voice Video, and Data Network Convergence**

1.3.2. Protocolos y otros elementos que afectan VoIP

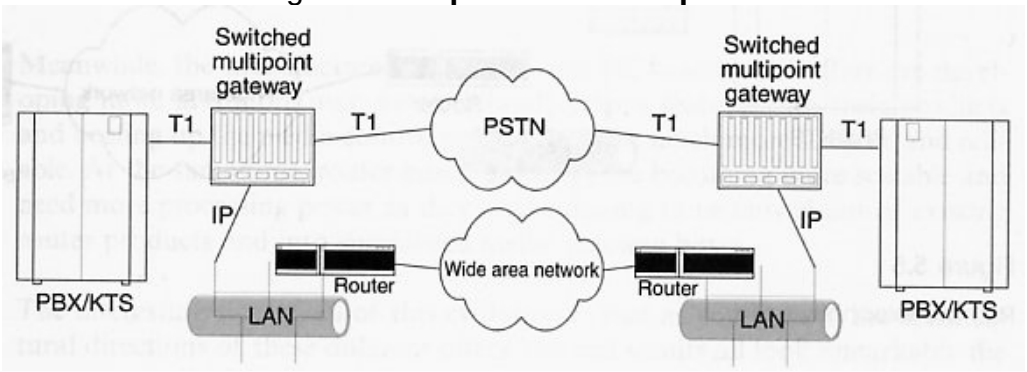
La calidad de la voz en la red va a ser tan buena como lo sea en sus partes más susceptibles. Esto obliga a prestar atención a la calidad de servicio (QoS) en toda la red por medio de la utilización de mecanismos y herramientas especializadas. La red debe ser capaz de darle prioridad a paquetes de voz por sobre paquetes de datos ordinarios, utilizando distintos métodos para manejo de colas (*queuing)*. El manejo de colas por prioridad (*priority queuing*) transmite los paquetes en un estricto orden de prioridad, beneficiando a los paquetes de voz pero eventualmente puede llegar a crear grandes retardos en tráfico de otro tipo. Otra opción es el manejo de colas por pesos justos (*weighted fair queuing*) que asigna "pesos" según la prioridad deseada para cada paquete tomando en cuenta el tiempo para procesarlo, una vez se le asigna un peso a todos los paquetes estos son transmitidos en estricto orden según su peso. La principal desventaja de este último es que requiere un mecanismo complejo por lo que debe ser implementado en *software* y esto puede agregar retardos no deseados. Quizá el método basado en clases (*class-based queuing*) sea el más práctico ya que este asigna cierto porcentaje de ancho de banda en el tiempo según la prioridad de cada una de las clases de paquetes que se deseen manejar.

Una red de convergencia debe ser diseñada tomando en cuenta los siguientes factores: confiabilidad y redundancia, escalabilidad, facilidad de administración y disponibilidad de ancho de banda. Existen ciertas limitantes en el momento de implementar mecanismos propios de una red de datos, por ejemplo la encripción utilizada en una VPN puede aumentar significativamente la latencia afectando la calidad de la voz.

1.3.3. Arquitectura básicas

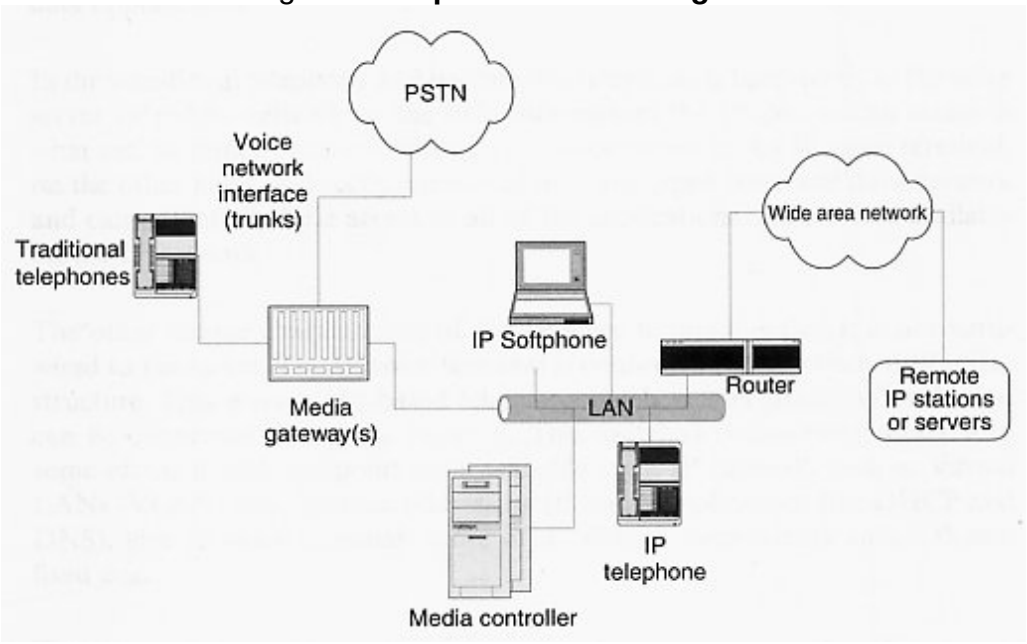
Existen varias arquitecturas para implementar VoIP que pueden ser funcionales para una gran variedad de aplicaciones. Algunos ven VoIP como una tecnología de comunicación de voz que requiere herramientas y habilidades especialmente desarrolladas. Otros lo ven como una aplicación más que se adhiere a la estructura IP ya implementada. Existen varias combinaciones de elementos que dan origen a una gran cantidad de soluciones para el mismo problema. Hay redes basadas en PBX que se forman básicamente integrando una interfase NIC a una planta convencional y permiten de esta manera la utilización de recursos basados en IP. La principal ventaja radica en la popularidad y utilización de las plantas PBX y su amplio desarrollo de más de cuarenta años, sin embargo su desventaja es que sus servicios no fueron diseñados para una red IP y no pueden traducirse fácilmente. También hay arquitecturas basadas en *routers*, en PCs y en puertas de enlace especializadas. La evolución hacia las redes convergentes reúne características de cada una de estas arquitecturas y el resultado es marcadamente similar. La diferencia entre cada una radica en que tipo de puerta de enlace se utiliza, puede ser una PBX, un router, PC o bien un equipo especializado. En las figuras 2 y 3 se muestran dos tipos diferentes de topologías.

Figura 2. **Arquitectura multipunto**



Fuente: Ellis, Juanita y otros, **Voice Video, and Data Network Convergence**

Figura 3. **Arquitectura convergente**



Fuente: Ellis, Juanita y otros, **Voice Video, and Data Network Convergence**

1.4. Video sobre la red convergente

1.4.1. Características del tráfico de video

La codificación digital permite que señales de alrededor de 300Kbps puedan transmitir señales de video adecuadas para algunas aplicaciones. Una de las aplicaciones más importantes es la videoconferencia, para un sistema de estos no es necesario tener una señal de muy alta calidad. A diferencia que una señal de televisión, cuyo estándar es de 30 cuadros por segundo, una señal de videoconferencia requiere unos 10 ó 15 cuadros por segundo. Esto es debido a que se supone que en una transmisión de videoconferencia no se espera presenciar mucho movimiento, a excepción de gente hablando, moviendo los labios o haciendo ademanes a baja velocidad. El grupo de ingeniería de imágenes en movimiento o MPEG (*Moving Picture Experts Group)* ha desarrollado estándares de compresión de video conocidos como: MPEG1, MPEG2 y MPEG4. La diferencia entre ellos radica básicamente en la capacidad de cada uno para comprimir imágenes de buena calidad, esto implica que la calidad de la imagen es proporcional a los recursos de procesamiento necesarios. MPEG4 incluye un codificador de video muy avanzado que requiere demasiados recursos de procesamiento por lo que no es muy factible su utilización en transmisiones de tiempo real, a diferencia de MPEG1 y MPEG2 que no requieren mayores recursos. MPEG1 fue desarrollado para comprimir video en discos compactos, mientras que MPEG2 es más complejo y cubre aplicaciones como DVD y televisión de alta definición. En la tabla II se muestran los requerimientos de ancho de banda según el código de compresión.

Tabla II. **Códigos de compresión y su ancho de banda**

	Typical Image Size	Typical Bandwidth	Max Bandwidth
MPEG1	352 × 240 (std profile)	1.5 Mb/s	2.5 Mb/s
MPEG2	720 × 480 (main profile@main level)	5 Mb/s	15 Mb/s
MPEG4	720 × 480 (main profile, L2)	2 Mb/s	4 Mb/s

Fuente: Ellis, Juanita y otros, **Voice Video, and Data Network Convergente**

1.4.2. Soporte de video en la red convergente

Existen varios componentes de red necesarios para soportar la transmisión de señales de video sobre la red: terminales, guardianes de puerta *(gatekeepers)*, *gateways* y MCUs. Estos componentes cumplen una función muy similar a los descritos anteriormente para VoIP. Las terminales y los MCUs son los dispositivos que se encuentran en un punto final de la red y ofrecen la interfaz entre los usuarios y la red. El *Gatekeeper* esta relacionado al protocolo H.323, a este se le asigna el control de varios recursos de video conferencia como terminales, *gateways* y MCUs. Su papel es brindar servicios para asegurar la transmisión de tráfico de video. Finalmente los *gateways* cumplen la función de traducción de protocolos, direcciones y de códigos de compresión.

Un requerimiento fundamental para la transmisión de video sobre una red conmutada por paquetes es que haya suficiente ancho de banda para que los paquetes de video sean transmitidos sin problemas. Para una videoconferencia basada en ISDN se requieren de 128-384Kbps, una basada en protocolo H.323 requiere alrededor de 384-768Kbps y así hasta una transmisión de televisión de alta definición que requiere más de 20Mbps. Debe procurarse la menor taza de

pérdida de paquetes, ya que un uno por ciento de pérdidas puede provocar pérdida de audio y la aparición de cuadros en la imagen y un dos por ciento de pérdidas puede hacer que la señal de video sea inutilizable mientras que el audio se distinga perfectamente. También es vital mantener bajos el nivel de *jitter*, tanto como la latencia, ya que esto evitará efectos no deseados en la señal. Y es recomendable evitar políticas de mecanismos como *firewalls* o NAT ya que algunos protocolos asignan puertos dinámicamente y estos mecanismos pueden llegar a bloquearlos, impidiendo así la transmisión correcta de la señal.

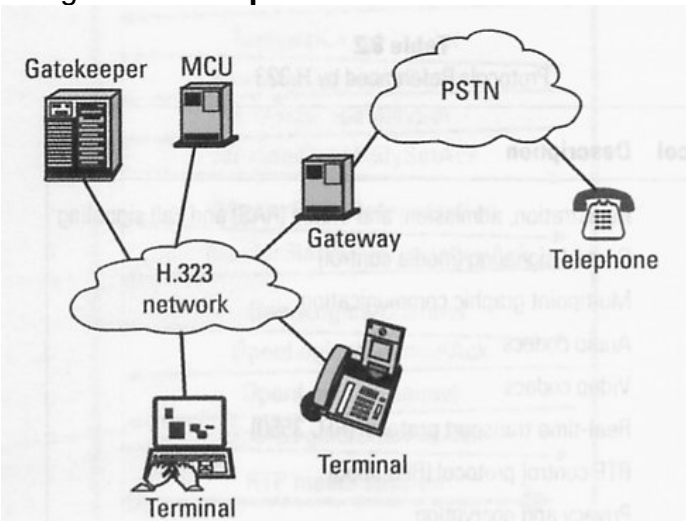
1.5. Protocolos y estándares utilizados en redes convergentes

1.5.1. H.323

H.323 es el estándar de la "Unión Internacional de Telecomunicaciones" ITU-T, por sus siglas en inglés, por medio del cual se debiera transmitir VoIP. Originalmente fue desarrollado para transmisión de videoconferencias en segmentos de LAN, provee los requerimientos técnicos para transmitir voz sobre redes en donde no existe ningún medio para asegurar la calidad del servicio o ancho de banda. Define cuatro componentes principales: *Gatekeepers*, Terminales, *Gateways* y MCUs. Los últimos tres son dispositivos de punto final que generan y terminan un flujo de paquetes multimedia que puede incluir voz, video o datos. El *gatekeeper* hace las funciones de un administrador y actúa como un punto central para el tráfico en una "zona". Se conoce como zona a un *gatekeeper* y todos los dispositivos que se registran en él. Brinda los servicios de: traducción de direcciones, control de admisión, autorización de llamadas, control de ancho de banda y control de llamadas. La estructura del protocolo permite que los paquetes de audio, video y de registro

utilicen el protocolo UDP, mientras los datos y las señales de control utilizan TCP por ser más confiable. Todos los dispositivos de punto final deben soportar como mínimo *codecs* G.711, el soporte de video y datos es opcional. Siempre que haya presente un *gatekeeper* todos los dispositivos de punto final deben registrarse en él y solicitar autorizaciones para aceptar o generar una llamada. El *gatekeeper* no es un elemento indispensable para el funcionamiento de una red H.323 pero su ausencia limita considerablemente el rendimiento de los dispositivos de punto final. En la figura 4 se pueden observar la distribución de los distintos componentes de una red H.323.

Figura 4. **Componentes de una red H.323**



Fuente: Johnston, Allan B. **SIP, Understanding the Session Initiation Protocol**

1.5.2. SIP

El protocolo de iniciación de sesión SIP, por sus siglas en inglés S*ession Initiation Protocol*, es un protocolo de control que funciona en la capa de aplicación. Su función es la de establecer, modificar y terminar sesiones multimedia o llamadas. Estas sesiones multimedia pueden incluir video conferencias, telefonía a través de Internet, etc. El protocolo SIP puede invitar tanto a usuarios humanos como a "máquinas", como por ejemplo un dispositivo de almacenamiento masivo. Los invitados pueden ser agregados a sesiones ya establecidas y que han sido anunciadas por un tercero. También es capaz de brindar movilidad al usuario, este término en telecomunicaciones se define como la habilidad de los usuarios finales para originar y recibir llamadas desde cualquier elemento terminal en cualquier parte de la red. La manera de direccional del protocolo SIP funciona de la forma sip:password@host. Una dirección se puede designar a usuarios individuales tanto como a grupos. Las principales funciones de señalización del protocolo son las siguientes:

- Localización de puntos terminales
- Contactar un punto terminal para determinar si está dispuesto a establecer una sesión.
- Intercambio de información para permitir el establecimiento de una sesión.
- Modificación de sesiones ya establecidas.
- Finalizar sesiones existentes.
- Proveer información presencial.
- Solicitar información presencial
- Notificación de eventos.

2. PROTOCOLO SIP *SESSION INITIATION PROTOCOL*

2.1. Introducción a SIP

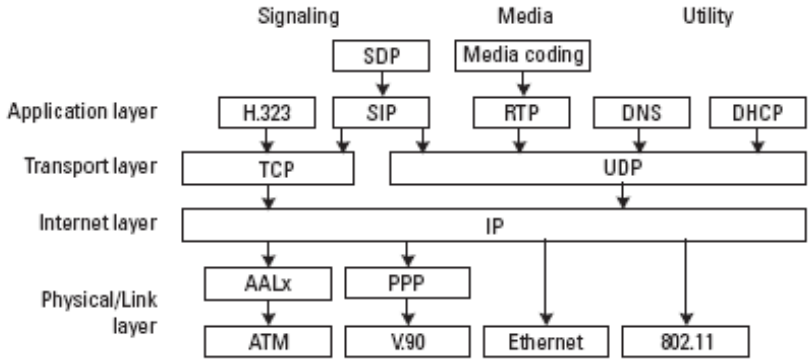
2.1.1. Historia

El protocolo SIP fue desarrollado por la IETF (*Internet Engineering Task Force)*, esta es una organización formada por un grupo de personas que hacen contribuciones de carácter técnico y de otros tipos que dirigen la evolución de Internet y sus tecnologías. No existe ninguna membresía formal, por lo que cualquiera puede participar. Existen dos tipos de documentos: *Internet-Drafts* (IDs) y *Request for Comments* (RFCs). Los primeros son los documentos que están en proceso de desarrollo dentro del grupo mientras que los segundos son los estándares numerados de Internet. Un estándar inicia su vida como un ID y luego evoluciona en un RFC cuando existe un consenso y existe alguna implementación funcional del protocolo. SIP fue sometido como un ID en 1997 por grupo IETF *Multi-Party Multimedia Session Control Working Group* MMUSIC, luego de hacer cambios significativos se creó una segunda versión en 1998. El protocolo alcanzó el nivel de estándar en marzo de 1999 y fue publicado bajo el número RFC 2543 en abril de ese mismo año. En septiembre de 1999 se formó el grupo de trabajo SIP quienes desarrollaron otro ID que evolucionó en el RFC 3261 haciendo obsoleto al anterior y adicionalmente han publicado varios RFCs de extensiones de este protocolo.

2.1.2. Relación de SIP con Internet

El protocolo SIP incorpora elementos de dos protocolos de Internet ampliamente utilizados: HTTP y SMTP. De HTTP toma su diseño cliente-servidor y la utilización de URLs y URIs; de SMTP toma el esquema de texto codificado y estilo del encabezado. Según la figura 5 podemos observar que el protocolo Internet se divide en cuatro capas principales, empezando por la capa física o de enlace de datos (*physical/link layer)* que se encarga de establecer las especificaciones del tipo de interfase a utilizar que puede ser una red LAN, línea telefónica, etc. La capa de Internet es la que se encarga de enrutar los paquetes a través de la red utilizando direcciones IP. Estos paquetes pueden perderse, retrasados o bien recibirse fuera de secuencia ya que IP trabaja en un esquema de *best-effort* o mejor esfuerzo. La capa de transporte utiliza un número de puerto de la capa de aplicación para entregar el datagrama o segmento a la aplicación correcta en el la dirección IP correspondiente. Algunos números predefinidos están asignados a protocolos específicos, a estos se les conoce como números de puertos “conocidos”. SIP utiliza el puerto conocido 5060 o 5061. Existen varios protocolos para transporte de los cuales podemos mencionar TCP, UDP y TLS entre otros. La capa más alta es la capa de aplicación, esta incluye protocolos de señalización y protocolos de transporte de medios. En esta capa se encuentran los protocolos SIP, RTP y H.323 por mencionar algunos. En la figura 5 se observa el modelo de capas de Internet.

Figura 5. **Estructura de capas de Internet**



Fuente: Johnston, Allan B. **SIP, Understanding the Session Initiation Protocol**

Uno de los más grandes fuertes de Internet es el poder utilizar nombres en vez de direcciones numéricas. Esto lo logra a través del servicio DNS (*Domain name service)* o servicio de nombre de dominio, por sus siglas en ingles, es utilizado por Internet para mapear un nombre simbólico hacia una dirección IP. También es utilizado para obtener información necesaria para rutear mensajes de correo electrónico y mensajes SIP. Existen ciertos tipos de registros DNS utilizados para distintas funciones: un registro que relaciona un nombre con una dirección es llamado registro de dirección o registro A; uno que almacena información para intercambio de correos es llamado MX; uno utilizado por SIP u otros protocolos se llama registro de servicio o SRV. La mayoría de protocolos utilizan direcciones URL (*Uniform Resource Locators)*, estos son nombres utilizados para representar direcciones o "lugares" en Internet. Los URLs están diseñados para soportar distintos tipos de protocolos y recursos, sigue un formato básico esquema:direccion:parámetros_adidionales, podemos mencionar como ejemplos los siguientes: http://www.google.com/search/index.html; telnet://host.company.com:24, en este ultimo se indica que el protocolo telnet debe acceder al *host* "host.company.com" a través del puerto 24. SIP utiliza principalmente referencias URI (*Uniform Resource Indicador)* indicador uniforme

de recurso según sus siglas en inglés, son muy similares a las URLs y en algunos casos so idénticas. Se diferencian en que una URI puede contener solo algunos componentes de una URL y no necesariamente tiene que estar asociada con un dispositivo físico si no a una entidad lógica que puede cambiar de posición en la red. Esto debido a los requerimientos de movilidad del protocolo SIP, podemos decir que una URI funciona como un número telefónico para el usuario. Ejemplo: sip:usuario@phonesystem.com.

2.2. Características del protocolo SIP

2.2.1. Movilidad

La utilización del formato URI con dominios propios para direcciones SIP permite a los usuarios elegir a su proveedor de servicios. Esto es, el usuario puede usar siempre su nombre y dominio para acceder a la red SIP y será redireccionado de manera transparente en la red para contactar a otro usuario. Esto le abre las puertas para tecnologías como las de telecomunicaciones inalámbricas de tercera generación.

2.2.2. Confiabilidad

SIP posee mecanismos definidos que aseguran su confiabilidad y permiten la utilización de protocolos de transporte poco confiables, como UDP. Cuando se utilizan otros protocolos de transporte, como TCP y TLS, estos mecanismos no se utilizan ya que se asume que TCP se encargará de la corrección de errores. Estos mecanismos incluyen: temporizadores de retransmisión, números de CSeq que aumentan y manejo de mensajes de recepción.

2.2.3. Autenticación

En SIP la autenticación toma dos formas generales, una es la autenticación de un agente por cualquier tipo de servidor y la otra es la autenticación de un agente por otro agente. La autenticación mutua entre servidores Proxy también es posible utilizando certificados. Pueden utilizarse métodos de autenticación tanto simples como robustos, en el primer caso se basan en el esquema sencillo de *HTTP Digest* que utiliza mecanismos simples de traducción y comparte una clave secreta entre dos servidores, los métodos más robustos utilizan esquemas que envuelven medios encripción bastante complejos para verificar certificados.

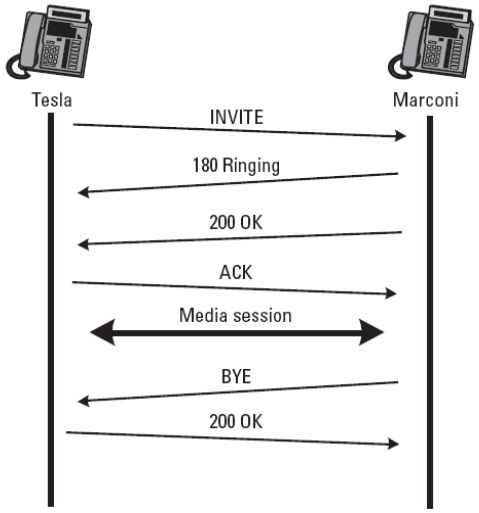
2.2.4. Interoperabilidad y Escalabilidad

SIP ha sido ampliamente aceptado, ya que permite brindar servicios sobre redes basadas en tecnología de próxima generación. También es capaz de interactuar con otros protocolos como H.323 y ISUP (parte del usuario de ISDN) permitiendo a los proveedores de servicio pensar en aplicaciones más allá de VoIP. SIP es extensible y escalable debido a la sencillez de sus mensajes y a su naturaleza tipo cliente-servidor.

2.3. Manejo de una sesión SIP

2.3.1. Estableciendo una sesión simple

Figura 6. **Secuencia de mensajes para establecer una sesión SIP**



Fuente: Johnston, Allan B. **SIP, Understanding the Session Initiation Protocol**

La figura 6 muestra como se realiza el intercambio de mensajes entre dos dispositivos SIP que pueden ser teléfonos SIP, computadoras de mano (*palmtops)* o incluso teléfonos celulares. Se asume que ambos dispositivos están conectados a una red IP como Internet por ejemplo. La parte que llama inicia el intercambio enviando el mensaje INVITE, este contiene los detalles del tipo de sesión que se desea establecer. SIP es un protocolo codificado en texto, los campos listados en este mensaje son llamados campos de encabezado. Las primeras líneas del mensaje son llamadas líneas de inicio y mencionan el método a utilizar, la URI del destinatario y la versión SIP utilizada, todos separados por espacios. Cada dispositivo que inicia o re envía un mensaje SIP escribe su dirección en un campo de encabezado.

Existe un campo llamado Call-ID que se utiliza como identificador de una sesión en particular, el usuario que origina la llamada genera una cadena de caracteres única y luego agrega el carácter "@" y el nombre del *host* para volverla una dirección global única. Una combinación de etiquetas y el Call-ID son utilizadas para identificar la sesión establecida ya que pueden existir varias sesiones entre los mismos usuarios. Los campos básicos necesarios para establecer una sesión SIP son: Via, Max-Forwards, To, From, Call-ID, CSeq.

Existen otros cinco métodos o tipos de mensajes SIP definidos en la especificación RFC 3261 y otros en extensiones RFC. El siguiente mensaje "180 Ringing" es un ejemplo de mensaje de respuesta, estos son de tipo numérico y se clasifican según el primer dígito del número. Pueden ser acompañadas de una cadena de texto que brinde más información. El mensaje se crea copiando varios de los campos del mensaje INVITE anterior e indica que el usuario ha recibido el mensaje de invitación y hay una alerta que le advierte de esto, puede ser un sonido en el teléfono, un mensaje en la pantalla de una PC o cualquier otro método que llame su atención. Cuando el usuario decide aceptar la llamada envía un mensaje "200 OK", que es un ejemplo de mensaje de clase exitosa. Y el paso final es confirmar la sesión multimedia con una solicitud de *acknowledgment*, esto es una confirmación de que el usuario respondió correctamente. Es en este punto en donde la sesión empieza a utilizar la información de medios incluida en los mensajes SIP. Al terminar la sesión se envía un mensaje "BYE" y se espera una respuesta "200 OK" para darla por terminada definitivamente.

Este intercambio de mensajes demuestra que el protocolo SIP es un protocolo de señalización punto a punto y que no se necesita de una red SIP o de un servidor SIP presente para iniciar una sesión. También demuestra la naturaleza cliente-servidor del protocolo, aunque un poco diferente de otras encontradas en protocolos de Internet como http, FTP, etc. Ya que cada sesión establecida requiere que ambos usuarios funcionen por momentos como clientes, cuando envían mensajes, y en otros como servidores, cuando contestan estos mensajes.

2.3.2. Mensajería presencial y protocolos de transporte

La información presencial se puede considerar como el estado de un dispositivo en un instante particular, puede indicar si algún usuario está conectado, si está ocupado o incluso puede transmitir información de su posición geográfica por medio de coordenadas. Se requiere de un protocolo presencial cuando se piensa mantener una suscripción a largo plazo entre dispositivos que pueden o no estar disponibles en distintos momentos. Como se mencionó anteriormente, se utilizan distintos protocolos para el transporte de mensajes.

UDP: (*User Datagram Protocol*) Este protocolo de transporte proporciona un medio de transporte poco confiable pero de alta velocidad a través de Internet. El mensaje es transmitido sobre un datagrama UDP simple o paquete. Para los mensajes más largos existe una forma compacta de SIP que economiza espacio al representar algunos campos con un solo caracter. El puerto utilizado para la transmisión es escogido de un grupo de puertos sobre el 49172 o bien se utiliza el 5060.

La falta de *handshaking* en el transporte UDP implica que algunos paquetes puedan perderse, sin embargo el *cheksum* le permite descartar datagramas con errores y solicitar su reenvío.

TCP: (*Transmission Control Protocol*) Provee transporte confiable sobre IP, utiliza una secuencia de números y mensajes de recibido para asegurar que cada bloque de datos (segmento) ha sido recibido. Los segmentos perdidos son re-transmitidos hasta que son recibidos correctamente. TCP representa un transporte confiable con un costo de complejidad y de retraso en la red. Se utiliza para mensajes con una extensión mayor a 1000 octetos.

TLS: (*Transmission Layer Security*) Es basado en el protocolo SSL (*Secure Socket Laye*) utilizado principalmente en navegadores de Internet y utiliza TCP para transporte. Se compone de dos partes: transporte y *handshake*. El primero provee un medio de transporte confiable y privado ya que sus paquetes son encriptados. El segundo se utiliza para establecer la conexión, negociar las claves de encripción y proveer autenticación. SIP aprovecha ambas ventajas de TLS sin embargo la encripción y autenticación solo funcionan para conexiones de un salto.

2.4. Clientes y Servidores SIP

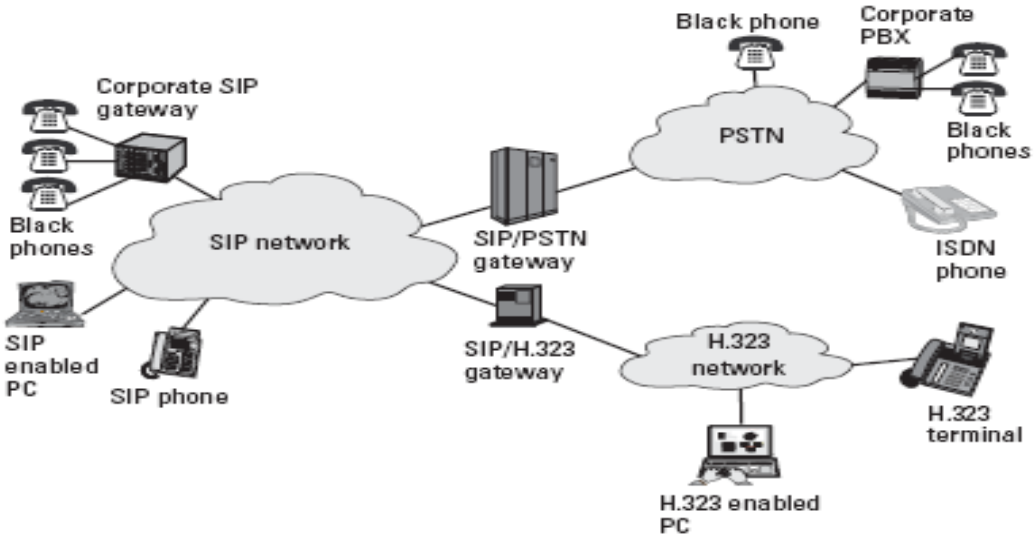
2.4.1. Agentes

Agente usuario: UA, es un dispositivo que toma información de un usuario y actúa como un agente para establecer y cancelar sesiones con otros agentes. Un UA debe mantener el estado durante las llamadas que origina o participa, debe soportar UDP y también TCP si se transmiten mensajes grandes. Debe contener aplicaciones cliente y servidor, también debe soportar SDP para la descripción de medios y debe anunciar sus habilidades y características en cada una de las peticiones que envía.

Agente presencial: PA, este dispositivo es capaz de recibir solicitudes de suscripción y generar notificaciones de estado definidas por SIP. Un PA recolecta información presencial de un cierto número de dispositivos que puede provenir de un servidor de registro, un dispositivo SIP o de cualquier otra fuente que no soporte SIP. Lo primero que realiza un PA es autenticar al suscriptor, luego establece un dialogo y envía notificaciones a través de este.

Agentes usuario espalda-espalda: B2BUA (*Back-to-Back User Agent)* es un tipo de dispositivo que reformula una solicitud y la reenvía como una nueva solicitud. Las respuestas a estas solicitudes también son reformuladas y enviadas en sentido contrario. Se puede utiliza para ocultar la identidad de dos dispositivos que se deseen comunicar, al modificar los mensajes evita que un usuario conozca los parámetros fundamentales del otro. Este tipo de dispositivos contrasta con la naturaleza punto a punto del protocolo SIP y la información puede sufrir aumentos en latencia y pérdida de paquetes.

Figura 7. **Red SIP con distintos *gateways***



Fuente: Johnston, Allan B. **SIP, Understanding the Session Initiation Protocol**

2.4.2. Puertas de Enlace

También conocidos como *gateways*, son aplicaciones que funcionan como interfases entre una red SIP y otras redes con diferentes tipos de señalización. Son básicamente un tipo de UA en el cual el usuario es otro protocolo y no un humano. En un *gateway* SIP – H.323 se finaliza la ruta de señalización convirtiéndola en H.323, sin embargo el UA SIP y la terminal H.323 pueden intercambiar información de medios RTP directamente el uno con el otro sin tener que pasar por el *gateway*. En el caso de un *gateway* SIP – PSTN se finalizan ambas rutas ya que este también convierte la información RTP que viene de la red IP a un formato de línea. Esta conversión permite realizar llamadas desde y hacia la PSTN utilizando SIP. La principal diferencia entre un *gateway* y un UA es el número de usuarios que soporta, un *gateway* puede soportar cientos y hasta miles de usuarios, un UA solo uno.

2.4.3. Servidores

Los servidores SIP son elementos de red que pueden ser programados para cumplir distintas funciones, el protocolo define tres tipos de servidores. Estos servidores pueden ser integrados lógicamente en un solo equipo o pueden funcionar como equipos separados, incluso algunos agentes pueden tener funciones de redireccionamiento integrados. Esto está especificado en el RFC 3261.

Servidores Proxy: Éste dispositivo recibe una solicitud SIP de un UA u otro servidor Proxy y actúa en nombre del UA re transmitiendo o respondiendo a la solicitud. A este no se le permite modificar las solicitudes ni las respuestas siguiendo reglas estrictas diseñadas para mantener la transparencia de la naturaleza punto a punto del protocolo SIP pero que le permiten al servidor realizar valiosas funciones para los UA. Estos servidores tienen acceso a bases de datos o servicios de localización para poder determinar hacia donde realizar el próximo salto. Estas bases de datos pueden contener información presencial, de registro SIP o de cualquier otro tipo que ayude a localizar a un usuario. El servidor no necesita entender una solicitud SIP para reenviarla, este solo debe responder a solicitudes enviadas por algún UA, no debe tener habilidades multimedia y solo se basa en la información de los campos en los encabezados. La única limitante al número de servidores que pueden retransmitir un mensaje se encuentra en el valor del campo Max-Forwards que se decrementa con cada salto y se descarta el mensaje cuando este llega a cero.

Servidores de redireccionamiento: Éste únicamente responde a solicitudes pero no las retransmite, también utiliza bases de datos para buscar usuarios. Esta información es enviada de regreso a quien realizó la solicitud en un formato de clase de respuesta (3xx) que concluye la transmisión.

Servidores de registro: Éste tipo de dispositivo acepta solicitudes de registro, transmitiendo la información del contacto a otros servidores disponibles. Generalmente se requiere que el UA sea autenticado para evitar el acceso a usuarios son autorizados. Una solicitud de registro puede ser utilizada para obtener listas de usuarios registrados, eliminar registros de usuarios o agregar direcciones URI al registro.

2.5. Comparación SIP versus H.323

Ambos protocolos fueron diseñados por distintas entidades para propósitos completamente diferentes. H.323 fue desarrollado por la ITU, su diseño e implementación reflejan sus bases y herencia de PSTN ya que utiliza codificación binaria y reutiliza partes del protocolo de señalización ISDN. SIP fue desarrollado por la IETF con perspectiva orientada hacia su escalabilidad y el aprovechamiento de los recursos de Internet. Mientras que H.323 fue desarrollado en la época de los inicios de VoIP y videoconferencias sobre IP, SIP y su arquitectura apegada a Internet sigue ganando auge y se está convirtiendo en el protocolo estándar para señalización en redes IP de telecomunicaciones o telefonía IP como también se le conoce.

2.5.1. Diferencias fundamentales

La primera diferencia radica en sus esquemas de codificación utilizados por cada protocolo, mientras que SIP es un protocolo basado en texto como HTTP y SMTP, H.323 utiliza mensajes con codificación binaria ASN.1. Esto resulta en una desventaja para H.323 ya que, aunque resulta en un mensaje compacto, agrega complejidad a la implementación. Un protocolo codificado en texto no requiere de herramientas especiales para monitorear e interpretar mensajes permitiendo el diseño de aplicaciones simples. Otra diferencia radica en que H.323 es un protocolo exclusivamente de señalización, cuando SIP provee además de la señalización información presencial y mensajería instantánea. Esta combinación más la utilización de direccionamiento siguiendo el esquema URI brinda la movilidad mencionada anteriormente. También el es importante notar que SIP ha sido adoptado por varios vendedores clave en el campo de las PCs y de las telecomunicaciones, aunque puede que no reemplace al H.323 en un corto plazo. Ambos han coexistido desde hace un tiempo y poco a poco se han vuelto similares de cierta manera. Por ejemplo, ambos protocolos nacieron en lados opuestos del espectro y poco a poco se han ido acercando el uno al otro, SIP se diseño para emplear UDP exclusivamente pero el soporte de TCP se ha vuelto cada vez más importante, por otro lado H.323 en un inicio no podía utilizar UDP exclusivamente.

2.5.2. Ventajas de cada protocolo

H.323 es ampliamente utilizado en pequeñas redes destinadas a reemplazar a la PSTN en algunas redes para manejar llamadas telefónicas simples y predomina en el mercado de las videoconferencias sobre IP. Sin embargo SIP esta posicionado correctamente para manejar videoconferencias sencillas utilizando *web-cams*, al parecer esta será tendencia en un futuro para las videoconferencias en general. La principal ventaja de SIP es simplemente que está basado en la arquitectura de Internet.

2.5.3. Conclusión

Aunque ambos protocolos poseen ciertas similitudes y a pesar que H.323 domina ciertos nichos en el mercado actualmente, SIP, con su codificación basada en texto, mensajería presencial e instantánea y arquitectura basada en Internet, está destinado a ser el protocolo de señalización a elegir en el futuro de las telecomunicaciones basadas en IP.

3. OPERACIÓN DE SIP

3.1. Mensajes de solicitud

3.1.1. Métodos

Las solicitudes SIP se conocen como métodos, funcionan como verbos en el protocolo, ya que siempre solicitan una acción en especial. Existen seis métodos, especificados en el documento RFC3261 (INVITE, REGISTER, BYE, ACK, CANCEL y OPTIONS) y siete más especificados en RFCs separados (REFER, SUBSCRIBE, NOTIFY, MESSAGE, UPDATE, INFO y PRACK).

INVITE se utiliza para establecer sesiones entre agentes. El cuerpo de mensaje incluye información del dispositivo que lo envía. REGISTER es utilizado por un UA para comunicarle la dirección URI de un contacto a una red SIP, este método es necesario cuando un UA va a recibir llamadas de un servidor Proxy. El método BYE se utiliza para terminar una sesión ya establecida, este solo es utilizado por agentes que participen de una sesión y sus respuestas también son generadas por otros agentes. ACK es la respuesta de confirmación que se envía al final de una solicitud INVITE, para los otros mensajes no es necesario tener una respuesta de confirmación solo se utilizan mensajes de respuesta. CANCEL finaliza búsquedas o intentos de llamadas pendientes, puede ser generado por agentes o por servidores y es utilizado únicamente tiene efecto sobre un INVITE ya que ningún otro método puede tomar tanto tiempo en resolver. OPTIONS es utilizado para interrogar a un agente o servidor sobre sus capacidades y disponibilidad, su respuesta a este debe ser una lista.

El método REFER es utilizado por un agente para solicitar a otro agente el acceso a una fuente URI o URL, este puede ser enviado desde dentro o afuera de un dialogo existente. SUBSCRIBE es utilizado por un agente para establecer una suscripción con el propósito de recibir notificaciones de un evento en particular, establece un dialogo entre un agente presencial y un agente de usuario. NOTIFY es el mensaje utilizado por un agente de usuario para proveer información de algún evento en particular, es la respuesta al método descrito anteriormente. MESSAGE se utiliza para transportar mensajes instantáneos (IM) utilizando SIP, generalmente consiste de un mensaje corto intercambiado en tiempo real por dos participantes de una conversación. Estos pueden ser enviados dentro o fuera de un dialogo, pero estos no pueden formar un dialogo por sí mismos. INFO envía información de señalización de una llamada hacia otro agente de usuario con el que se desee establecer una sesión, no envía características de los medios utilizados para realizar la llamada. PRACK, este método es utilizado para enviar un mensaje de recepción satisfactoria provisional. Finalmente el método se utiliza para modificar el estado de una sesión sin cambiar el estado del dialogo, puede utilizarse para silenciar una llamada (*mute*), colocar la llamada en espera (*hold*) o para modificar atributos antes de establecer la sesión.

3.1.2. Esquemas URI y URL utilizados por SIP

El protocolo SIP puede utilizar cierto número de direcciones utilizando esquemas URI y URL. Estas direcciones se utilizan en distintos lugares dentro de los encabezados de mensajes para indicar un destino en particular. Un ejemplo de SIP URI utiliza el esquema anteriormente descrito SIP ":", seguido de un nombre de usuario y un *host* o bien una dirección IP seguido por otro ":" y el número de puerto e incluso por un ";" y una serie de parámetros extra.

SIP:armando.galvez@ingenieriausac.edu:5060;transport=udp;user=ip

Tabla III. **Esquemas URI utilizados por SIP**

Esquema	Significado	Utilización
`sip`	SIP URI	Utilizada en encabezados de mensajes
`sips`	SIP URI segura	Igual que una SIP URI, provee encripción utilizando TLS
`tel`	URI de telefonía	Representa un número telefónico
`pres`	URI presencial	Utilizada para representar el URI de un agente presencial
`im`	URI mensaje instantáneo	Cliente de mensajería instantánea
`mailto`	URL de correo	Puede incluirse en respuestas de registro o redireccionamiento
`http`	URL de web	Puede utilizarse en encabezados para enviar mensajes de alerta o error.

En el ejemplo anterior se utiliza el puerto 5060 que es el asignado al protocolo SIP, para una dirección SIPS URI el puerto seria el 5061. El parámetro transport indica el protocolo de transporte a utilizar, UDP generalmente. Existen otros parámetros que indican el método, tiempo de vida del mensaje (ttl), direcciones multicast (maddr), etc. Una SIPS URI tiene la misma estructura, pero inicia con el nombre sips, e implica que utilizará transporte TLS y sus mecanismos de seguridad. Cuando aparece el parámetro user=phone se asume que el parámetro usuario corresponde a un número telefónico y permite la utilización de parámetros adicionales en la URI. El esquema URI de telefonía puede ser utilizado para identificar un recurso por medio de un número telefónico. Existen dos tipos de números, locales y globales. Como su nombre lo indica, los locales se pueden utilizar solo en ciertas áreas y los globales en cualquier parte.

3.1.3. Cuerpo del mensaje

El cuerpo de un mensaje SIP contiene distintos tipos de información y a veces tiene cuerpo de mensaje, esto lo especifica un campo de encabezado llamado Content-Disposition. Existen campos que especifícan el formato del cuerpo del mensaje, su codificación y el número de octetos en un mensaje. Esto último es bastante útil para saber donde finalizan los mensajes ya que varios de estos pueden ser transmitidos en un paquete TCP. Los cuerpos de mensaje SIP no debe exceder el tamaño del MTU UDP de la red ya que los servidores Proxy pueden rechazar los mensajes si son demasiado largos. Los mensajes transportan la información del cuerpo de mensaje de la misma manera que lo hace un correo electrónico con archivos adjuntos.

3.2. Mensajes de respuesta

Un mensaje de respuesta es generado por un agente o servidor SIP que ha recibido una solicitud, estos mensajes pueden contener campos de información adicionales o bien pueden ser simples confirmaciones de recibido. Estos se componen de un código y una frase descriptiva, en sí SIP podría funcionar únicamente con el código. Existen seis tipos de respuesta posibles para los mensajes SIP, cinco fueron tomados prestados de HTTP y el sexto fue creado para SIP exclusivamente.

3.2.1. Tipo informacional 1xx

Los mensajes tipo informacional son utilizados para indicar el progreso de una llamada, pueden contener cuerpo de mensaje y utilizan el codigos 1xx. Podemos mencionar entre algunos de estos mensajes: 180 Ringing, descrito anteriormente; 100 Trying, indica que alguna acción se esta realizando; 181 Call Is Being Forwarded, que indica que la llamada esta siendo transferida hacia otro punto y se utiliza cuando el proceso puede tomar mucho tiempo para brindarle información del status al usuario; 182 Call Queued, utilizado para indicar que el mensaje INVITE ha sido recibido y que se procesará en una cola; 183 Session Progress, contiene información sobre el progreso de una sesión, generalmente se utiliza para brindar tonos de ocupado, de ring o anuncios pregrabados cuando se realizan conexiones hacia la PSTN. Este último mensaje permite establecer una sesión antes de que la llamada sea respondida.

3.2.2. Tipo exitosos 2xx

Indican que la solicitud se ha realizado exitosamente o que ha sido aceptada. La respuesta 200 OK tiene dos usos en SIP, en el caso en que se utiliza para aceptar una invitación a una sesión, este incluye un cuerpo de mensaje que contiene la información requerida de los medios utilizados. Cuando se utiliza como respuesta a otras solicitudes indica la recepción exitosa de la solicitud y detiene las posibles retransmisiones. 202 Accepted, indica que la solicitud ha sido entendida y aceptada por el servidor aunque no implica que se este procesando.

3.2.3. Tipo redireccionamiento 3xx

Este tipo de respuestas generalmente son enviadas por un servidor SIP que actúa como un servidor de redireccionamiento en respuesta a una invitación, también se utilizan para implementar servicios de redireccionamiento de llamadas. Entre estos tenemos: 300 Multiple Choices, que contiene varios camos Contact indicando que el servicio de localización ha indicado múltiples posibles localizaciones para la SIP URI; 301 Moved Permanently, indica en el campo Contact su nueva dirección URI permanente que puede ser almacenada; 302 Moved Temporarily, contiene una URI que es válida pero no permanente; 305 Use Proxy, contiene una URI que corresponde a un servidor Proxy que brinda información autoritativa acerca del usuario que se desea contactar; 380 Alternative Service, esta responde una URI que indica el tipo de servicio que el usuario llamado desearía, puede ser un redireccionamiento a un servidor de mensajes de voz.

3.2.4. Tipo error del cliente 4xx

Este tipo de respuesta es utilizado por servidores o agentes para indicar que la solicitud no pudo llevarse a cabo según lo solicitado. La respuesta específica del cliente debe incluir en los campos de información la razón del error y como puede reformularse la solicitud, esto para que la solicitud no vuelva a enviarse sin ser modificada. Entre estas respuestas podemos mencionar las que indican que receptor no ha entendido la solicitud, 400 Bad Request. Las que indican que el receptor necesita de parámetros adicionales para poder procesar la solicitud: 406 Not Acceptable, 407 Proxy Authentication Required, 411 Length Required, 421 Extension Required, 429 Provide Referror Identity. Algunas simplemente indican que se necesitan permisos especiales para acceso o utilización de recursos: 402 Payment Required, 403 Forbidden, 428 Use Authentication Token. Otras envían mensajes de error debido a falta de información o información errónea en los campos: 409 Conflict, 413 Request Entity Too Large, 414 Request-URI Too Long, 416 Unsupported URI Scheme, 420 Bad Extensión, 484 Address Incomplete, 485 Ambiguous, 493 Requiest Undecipherable. También están las que indican el estado temporal o permanente de la localización del usuario: 404 Not Found, 410 Gone, 480 Temporarily Unavailable, 486 Busy Here, 491 Request Pending.

3.2.5. Tipo error de servidor 5xx

Este tipo de respuestas indican que el mensaje no pudo ser procesado debido a algún problema con el servidor, pueden contener en el campo Retry-After un período de tiempo de espera para poder reenviar la solicitud. 500 Server Internal Error, indica que el servidor tiene algún problema que le impide procesar la solicitud. 501 Not Implemented, cuando el servidor no tiene la capacidad de procesar la solicitud requerida. 502 Bad Gateway y 504 Gateway Time Out, es enviada por un servidor Proxy cuando actúa como puerta de enlace y existe algún problema en la otra red que impide la realización de la solicitud. 503 Service Unavailable, indica que el servicio solicitado no esta disponible temporalmente. 505 Version Not Supported, indica que la solicitud es rechazada debido a que la versión del protocolo no es compatible.

3.2.6. Tipo error global 6xx

Estas respuestas indican que el servidor sabe que la solicitud no podrá llevarse a cabo en ningún momento y no debe ser reenviada a otros servidores. Entre estas tenemos: 600 Busy Everywhere, que es una versión global del mensaje 486 Busy Here; 603 Decline, al igual que la anterior indica que el receptor está ocupado o no desea contestar la llamada; 604 Does Not Exist Anywhere, es una especie de 404 Not Found con aplicación global; 606 Not Aceptable, se utiliza para implementar negociación de sesiones e indica que algunos aspectos de la sesión no son aceptables pero que otros sí.

3.3. Campos de encabezado

Generalmente estos siguen las reglas de HTTP e incluyen toda la información necesaria para el establecimiento de sesiones y el manejo de mensajes en SIP.

3.3.1. Campos comunes en mensajes de solicitud y respuesta

Existen dieciséis campos de encabezado comúnmente utilizados tanto en mensajes de solicitud como en mensajes de respuesta. Alert-Info es un campo que puede usarse para indicar la URI de cierto tipo de tono en especial. Allow-Events es utilizado para indicar que tipo de eventos son soportados. Call-ID es un campo obligatorio en todas las solicitudes y respuestas SIP, es la parte que identifica cada una de las llamadas entre agentes. El campo Contact se utiliza para presentar la URI de un recurso solicitado. CSeq almacena un número decimal que contabiliza una secuencia de comandos realizados. Date indica la fecha en la que se envío el mensaje en un formato similar a HTTP. El campo From es obligatorio que indica quien es el generador de la solicitud por medio de SIP URI. Organization es utilizado para indicar la organización a la cual pertenece el generador del mensaje. Record-Route se utiliza para crear una ruta a través de un Proxy para que las solicitudes subsecuentes en una sesión puedan realizarse directamente entre dos agentes. Retry-After indica el tiempo en el que un recurso o servicio estará disponible nuevamente. Subject se utiliza para indicar el tema de la sesión, puede ser utilizado como mensaje de llamada para que el usuario receptor decida si contesta o no la llamada. Supported este campo se utiliza para hacer una lista de las opciones implementadas por un agente o servidor. El campo Timestamp se utiliza para marcar el tiempo exacto

en el que una solicitud fue generada, utiliza algún formato numérico. To es un campo obligatorio que indica quien va a recibir el mensaje por medio de un SIP URI. User-Agent nos brinda información acerca del agente que genera la solicitud. Via es un campo utilizado para grabar la ruta tomada por una solicitud y se utiliza para enviar de regreso la respuesta a dicha solicitud.

3.3.2. Campos exclusivos para mensajes de solicitud

El campo Accept esta definido en HTTP y se utiliza para indicar que tipos de medios de Internet son soportados en el cuerpo de mensaje. Accept-Contact especifica hacia que URIs puede ser enviada la solicitud en un Proxy, además puede contener otros parámetros para darle control al usuario sobre la manera en que se maneja el mensaje en el Proxy. Accept-Encoding y Accept-Language, también están definidos en HTTP y se utiliza para especificar el esquema de codificación y el lenguaje utilizado en el cuerpo de mensaje. Authorization es un campo que se usa para enviar las credenciales de un usuario o agente. Call-Info provee una URI con información relativa a la configuración de la sesión. Event se utiliza para indicar que paquete de evento está siendo utilizado por el método. In-Reply-To se utiliza para indicar como referencia el Call-ID en caso de que no se haya podido establecer una sesión o llamada. Join se utiliza para almacenar la información requerida para unificar dos diálogos o sesiones. Priority y Privacy es utilizado por un agente para establecer la urgencia y el nivel de privacidad de una solicitud respectivamente. Proxy-Authorization y Proxy-Require contienen información relativa a servidores Proxy, el primero porta las credenciales de un agente según solicitud de un servidor y el segundo una lista de las capacidades y extensiones que un agente requiere de un Proxy.

P-Asserted-Identity y P-Preferred-Identity, el primero se utiliza entre dos intermediarios seguros para identificar un agente autorizado y el segundo es utilizado por un agente para indicarle a un intermediario seguro que identidad prefiere. Max-Forwards indica el máximo número de saltos permitidos para un mensaje. Reason puede utilizarse para indicar la razón del porque un intento esta siendo cancelado. Refer-To y Reply-To contiene una URI o URL a la cual se está haciendo referencia y a quien se debe responder, respectivamente. Referred-By provee al receptor información sobre quien refiere. Replaces se utiliza para el control de llamadas. Reject-Contact almacena una URI de la cual no se puede enviar mensajes. Request-Disposition puede utilizarse para solicitar a los servidores un redireccionamiento o búsqueda paralela. Require se utiliza para hacer una lista de los recursos que un agente requiere para procesar una solicitud. Route provee la información correspondiente a la ruta. RAck se utiliza para confirmar de recibido a una respuesta provisional. Session-Expires especifica el tiempo en el que una sesión expirará. Subscription-State indica el estado actual de una suscripción.

3.3.3. Campos exclusivos para mensajes de respuesta

Authentication-Info puede ser incluido en respuestas cuando se utiliza autenticación mutua. Error-Info se utiliza para enviar información adicional respecto a alguna falla que haya ocasionado un error. Min-Expires se utiliza en el mensaje 423 Interval Too Brief enviado por un servidor de registro que rechaza una solicitud debido a que los contactos tienen un tiempo muy corto de vida. Min-SE se incluye en la respuesta 422 Session Timer Interval Too Small indicando un número de segundos que es el mínimo tiempo permitido para la sesión. Proxy-Authenticate y WWW-Authenticate, la primera es una petición que se hace a un

Proxy para que este provea las credenciales necesarias, incluye la naturaleza de la petición y la segunda se hace a un agente. Server es utilizado para proveer información correspondiente al agente que genera la respuesta. Unsupported indica las aplicaciones que no son soportadas por el servidor. Warning se utiliza en las respuestas para proveer información más específica acerca de algún problema. RSeq es utilizado en respuestas provisionales de tipo 1xx para solicitar transporte confiable.

3.3.4. Campos en el cuerpo de mensaje

Recordemos que el cuerpo de mensaje es como un archivo que se adjunta al mensaje, estos campos contienen información acerca del cuerpo de mensaje. Allow se utiliza para indicar los métodos que pueden ser utilizados por el usuario que responde. Content-Encoding, Content-Disposition, Content-Language, Content-Length y Content-Type indican: el esquema de codificación, la función, el lenguaje, el número de octetos y el tipo de medio utilizados por el cuerpo de mensaje respectivamente. Expires se utiliza para indicar el intervalo de tiempo en el que es válido el contenido de un mensaje. MIME-Version se utiliza para indicar la versión del protocolo MIME que se utilizó para crear el cuerpo de mensaje.

3.4. Flujo de llamada

A continuación se presentan tres posibles casos en los que se puede establecer una sesión SIP.

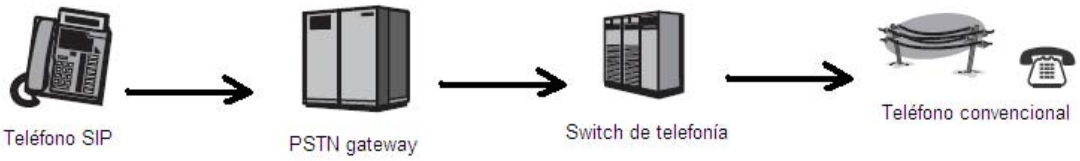
3.4.1. De SIP hacia PSTN utilizando puerta de enlace

Este caso representa una llamada telefónica realizada desde un dispositivo SIP hacia un teléfono de la red de telefonía. Se utiliza una SIP *gateway* para conectarse a la PSTN, el proceso puede describirse en algunos pasos. El teléfono SIP recolecta los dígitos a marcar y los coloca en una SIP URI utilizada en los encabezados correspondientes. El usuario puede marcar el número completo, incluyendo códigos de área y de país, pero también se puede configurar el dispositivo SIP para que este los agregue a una URI global. Se debe configurar el teléfono SIP con una IP del *gateway* PSTN para que este pueda enviar una invitación directamente al dominio de este. El *gateway* inicia la llamada hacia la PSTN seleccionando una troncal hacia el siguiente *switch* de la red. Los dígitos marcados del mensaje SIP (INVITE) ahora son decodificados y codificados nuevamente a lenguaje de PSTN, luego el *switch* envía un mensaje indicando que la troncal ha sido tomada y se utilizará para establecer el canal de comunicación en dos direcciones. Cuando se generan los tonos de llamada, el *gateway* envía la respuesta 183 Session Progress indicando que este iniciará la transmisión de audio por RTP para ser escuchada por el usuario que llama indicándole que la llamada está en progreso. La llamada se completa cuando es contestado el teléfono en el otro extremo, lo que hace que el *gateway* envíe una respuesta 200 OK al dispositivo SIP y este la confirma. Como ya existía una transmisión de audio RTP esta se mantiene y se inicia el

intercambio de mensajes de voz. Para finalizar la llamada, el usuario que llama envía un BYE hacia el *gateway* y este lo envía hacia la PSTN y contesta un 200 OK de regreso. La PSTN utiliza su señalización interna para terminar la sesión de su lado. Este último intercambio de mensajes para finalizar llamadas no depende de la respuesta de uno del otro.

En un caso inverso, una llamada iniciada por la PSTN hacia un teléfono SIP, el *gateway* recibe la solicitud y genera una invitación al usuario a través de un servidor Proxy. Este busca en una base de datos el número en la invitación y este está relacionado a una URI que le da la ubicación del teléfono SIP. Al ser contactado el teléfono SIP envía una señal de que esta procesando la llamada e inicia la transmisión de voz cuando el usuario contesta el teléfono de ese lado.

Figura 8. **Elementos involucrados en una llamada de SIP a PSTN**



3.4.2. Búsqueda Paralela

En este caso el dispositivo que inicia la llamada recibe distintas ubicaciones posibles para el usuario al que se desea llamar. En vez de intentar con las posibilidades una a la vez, el agente de usuario utiliza búsqueda paralela enviando invitaciones a las distintas posibles ubicaciones. Al no encontrarse en una ubicación, esta devolverá un mensaje 404 Not Found; o bien

un 180 Ringing que indica que lo esta buscando. Pero el usuario que responda a la ubicación correcta enviará un 180 Ringing seguido de un 200 OK. Automáticamente se cancelan todas las demás solicitudes en proceso ya que el usuario ha sido encontrado y puede iniciarse la sesión.

3.4.3. H.323 hacia SIP

Otra posibilidad que se debe tomar en cuenta y que prueba la interoperabilidad del protocolo SIP con otro protocolo de VoIP es una llamada entre una terminal H.323 y una SIP a través de un *gateway* H.323/SIP. Suponiendo que la terminal H.323 es la que inicia la llamada, el *gatekeeper* es el encargado de convertir el alias H.323 en una dirección servida por el *gateway*. La parte H.323 abre los canales TCP de su lado, el *gateway* responde de la misma manera abriendo el canal TCP y envía un mensaje INVITE hacia un Proxy y este lo envía hacia el receptor de la llamada. En este caso, los mensajes utilizados por H.323 no tienen ninguna información sobre los medios utilizados, por lo que el INVITE tampoco. El receptor envía un mensaje 180 y luego un 200 para indicar que ha contestado la llamada, la información de los medios que está en el cuerpo de mensaje SDP se almacena en el *gateway* y este se encarga de la traducción entre H.323 y SIP. Una vez la parte H.323 termina de hacer el intercambio correspondiente a sus códigos, se establece la sesión multimedia confirmando con un mensaje ACK.

Figura 9. **Elementos involucrados en una llamada H.323 hacia SIP**

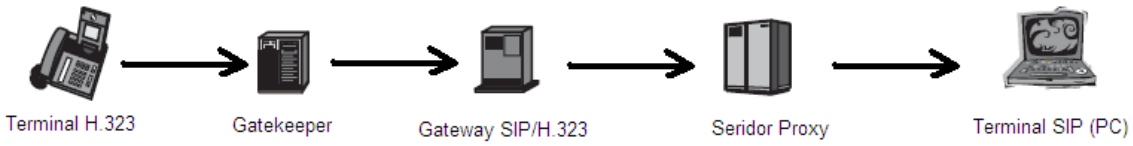


Fig no. 9 Elementos involucrados en llamadas H.323 hacia SIP

4. ANÁLISIS TÉCNICO Y ECONÓMICO

4.1. Convergencia sobre redes ya establecidas

Es obvio que cualquier nueva solución tecnológica que implique convergencia de redes debe acoplarse a algún estándar ya establecido para que sea rentable. Y la opción más viable es la de adaptarse a la estructura IP debido a su amplio desarrollo y al auge que ha tomado el Internet. Es por eso que es indispensable realizar un análisis a fondo de la factibilidad de implementar el protocolo SIP para el manejo de sesiones multimedios sobre una red IP, en donde generalmente se maneja exclusivamente tráfico de datos. En base a lo expuesto en los capítulos anteriores con respecto a los conceptos y funcionamiento del protocolo SIP, a continuación se proponen algunas consideraciones importantes y un análisis de factibilidad económica para la implementación de una solución de este tipo.

4.2. Consideraciones Importantes

4.2.1. Criterio de selección de productos y proveedores

Uno de los primeros pasos para implementar una red convergente con servicios de VoIP utilizando el protocolo SIP es seleccionar adecuadamente los equipos a utilizar y el proveedor de estos. Se debe iniciar haciendo una evaluación de las necesidades que haya que cubrir; pueden tomarse en cuenta parámetros como: tamaño de la red, requerimientos del usuario sobre señal de voz, aplicaciones especializadas, mensajería, etc.

También se debe prestar atención a los conocimientos que estos equipos requieren de parte de los usuarios o administradores de la red, ya que de nada serviría tener los mejores equipos si nadie va a poder utilizarlos. Las características del equipo seleccionado deben ser las que más se adecuen a las necesidades anteriormente mencionadas. Otros factores a considerar incluyen la experiencia del proveedor en el campo de VoIP e incluso la solvencia económica del fabricante. Esto debido a que se requerirá el respaldo del proveedor para mantener la red en óptimo funcionamiento. Finalmente no podemos descartar el factor precio, aunque no sea el más decisivo.

4.2.1.1. Requerimientos de hardware

El hardware utilizado debe poseer algunas características importantes. Si se van a utilizar soluciones basadas en PC es importante que sean escalables y confiables, por lo tanto es vital que los equipos (*gateways*, servidores y otros) puedan fácilmente aumentar la capacidad de tráfico que manejan. Uno de las consideraciones importantes al hablar de escalabilidad en la topología de la red se refiera al número de enlaces que se van a conectar eventualmente a un nodo de VoIP. Así como también se debe tomar en cuenta el número de nodos adicionales que eventualmente podrían ser agregados cuando sea necesario escalar a un nivel más alto y poder mantener la misma topología. La interoperabilidad del *hardware* es obligatoria ya que se va a trabajar con distintas tecnologías, incluso es recomendable que el fabricante de los productos participe del desarrollo de estándares a nivel mundial para garantizar su compromiso con la solución que ofrece.

4.2.1.2. Requerimientos de software

Se debe asegurar que el fabricante tenga completo soporte sobre el protocolo SIP ya que es indispensable estar al día a los cambios realizados conforme el estándar vaya evolucionando. Esto no solo es crítico para la correcta operación del sistema, sino que también asegura la inversión en el tiempo. También se requiere interoperabilidad con aplicaciones de terceros para facilitar una rápida expansión e implementación de nuevos servicios. Se siguiere una plataforma de *software* integrada ya que evita tener sistemas de administración duplicados y facilita el desarrollo de nuevos servicios. En el mejor de los casos el proveedor debe tener buena relación con otros proveedores que pueden ayudar a implementar aplicaciones de valor agregado como servicios de fax, mensajería, VPNs, etc.

4.2.2. Esquema de Implementación

Una vez se haya seleccionado el producto y el proveedor se debe proceder a la planificación de la implementación de la solución. Se identificarán cinco pasos fundamentales para la correcta planeación e implementación.

Paso 1. Establecer las prioridades de la aplicación: Las prioridades se establecen basándose en las necesidades de los futuros usuarios y en base a estas se debe planificar la implementación.

Paso 2. Auditoría de la red: A continuación se procede a diseñar la red convergente tomando en cuenta las redes ya implementadas. Es recomendable realizar un estudio del tráfico de la red de datos para determinar que protocolos utilizan la red y evaluar los requerimientos de ancho de banda

de cada uno. Se deben establecer políticas para establecer prioridades a ciertas aplicaciones que son indispensables y aislar el tipo de tráfico o protocolos que utilizan.

Paso 3. Objetivos de la red: El próximo paso es establecer que tipos de tráfico debe soportar la red, es decir, establecer las aplicaciones que utilizarán los usuarios e incluso el nivel de calidad de servicio que están de acuerdo a aceptar. Esto ayuda a definir y priorizar los objetivos de la red convergente, ya que esta puede ser orientada en distintas direcciones. Dependiendo de los objetivos, se podría crear una red una red dedicada al desarrollo de nuevas aplicaciones que ayudarían a fortalecer la eficiencia y la productividad, también puede que se diseñe una que sirva para ahorrar costos de operación al optimizar los recursos disponibles sacrificando un poco la calidad de los servicios.

Paso 4. Diseño técnico y planeamiento de la capacidad: En esta etapa se debe determinar el criterio de diseño a utilizar para adaptar la red IP para que soporte SIP VoIP. Existen algunos parámetros clave que se deben tomar en cuenta como: tipo de codificación y compresión, estos son determinados por las aplicaciones a utilizar y el ancho de banda disponible; Técnicas de QoS, en esta etapa es recomendable que las políticas específicas para cada tipo de tráfico hayan sido definidas; Planificación de capacidad de ancho de banda, esta debe tomar en cuenta los encabezados, el tipo de compresión, la utilización y dependerá también del tipo de transporte utilizado por SIP para el envío de mensajes. También se debe definir el plan de marcación o *dial plan* que se utiliza para que el *gateway* “entienda” los dígitos marcados por el usuario y pueda realizar una llamada.

Paso 5. Lanzamiento de la red: Esta etapa incluye la planificación de la implementación en sí, esta se hace necesaria ya que la mayoría de aplicaciones en redes no pueden detenerse mientras se implementa la nueva red. Se recomienda realizar pruebas de laboratorio para probar la solución, como segundo paso se puede seleccionar algunos usuarios clave para realizar pruebas piloto. Para estas se puede seleccionar un número de usuarios previamente capacitados que posean alguna otra forma alternativa de realizar sus llamadas si en caso la solución no llegara a funcionar y se pueden realizar ajustes de último minuto para su funcionamiento óptimo. Cuando la fase piloto se completa satisfactoriamente se procede a implementar el plan de lanzamiento para el resto de la red.

4.2.3. Transparencia

La solución a implementar debe soportar los equipos que tradicionalmente se utilizaban con la red de voz, entre estos están maquinas de fax, teléfonos convencionales y servicios de conferencias. En cierto momento puede que una parte de los usuarios utilicen el viejo sistema y otra parte el nuevo. Por eso es indispensable que ambos sean compatibles tanto en el período de transición como para la interacción con otras redes públicas no convergentes.

4.2.4. Disponibilidad de la solución

Uno de los aspectos más difíciles de igualar respecto a la red de telefonía convencional es la robustez de esta. Los usuarios esperarán que la solución a implementar tenga el mismo nivel de confiabilidad y disponibilidad. Esto requiere que se preste atención en el momento del diseño a las posibles fuentes de error que puedan “botar” el servicio. Esto implica que la red IP debe

ser diseñada con un alto nivel de tolerancia de fallas y redundancia. Generalmente este es uno de los factores que elevan considerablemente el precio del lanzamiento de una red convergente y por ello quien diseña debe tener claras las necesidades y tolerancias de los usuarios. Incluso en una red redundante y con alta tolerancia a fallas es muy difícil alcanzar la confiabilidad deseada simplemente porque intervienen muchos más dispositivos, como conmutadores y enrutadores, entre el servidor de voz y el usuario. Generalmente se debe decidir entre ofrecer nuevas aplicaciones y tecnologías o mantener la confiabilidad del sistema tradicional. Muchas de las redes convergentes en la actualidad son una mezcla de redes tradicionales y convergentes.

4.2.5. Calidad de servicio (QoS)

Se han mencionado anteriormente la importancia de la implementación de políticas de calidad de servicio para la implementación de VoIP en una red convergente. Incluso en una red IP con buena administración de ancho de banda y latencia se hace necesario implementar políticas para garantizar que los requerimientos de ancho de banda del tráfico de voz, datos y video se cumplan. Actualmente en la industria se esta trabajando con esquemas diseñados para toda la red en general y se han desarrollado herramientas que pueden manejar estos esquemas de calidad. Se ha introducido el concepto de administración de redes basada en políticas. La mayoría de estas redes utilizan un servidor que funciona como administrador de las políticas que dictan como deben tratarse los distintos tipos de tráfico en la red. Estas políticas incluyen niveles de prioridad para paquetes de aplicaciones y protocolos en la red, manejando la prioridad de servicios de voz, correo electrónico, Internet, datos,

etc. La principal ventaja de un servidor de políticas es la posibilidad de controlar las disposiciones de QoS desde un punto central en la red, evitando la configuración de parámetros adicionales en distintos equipos de la red. Esto ahorra tiempo y elimina posibles fuentes de error mientras facilita la implementación de nuevos dispositivos en la red.

4.2.6. Seguridad

Otro tema importante es el de la seguridad. Generalmente cuando se habla de redes de voz, la seguridad se concentra en evitar fraudes de llamadas y seguridad pública. Para evitar el fraude de cobros se evita el acceso a líneas a usuarios no autorizados para que no pueda aprovecharse de estas. Se pueden habilitar sistemas de “clase de servicio” y restricciones para que los usuarios no autorizados no puedan acceder a las líneas exteriores; esto implica que el sistema debe tener mecanismos para evitar que alguien pueda cambiar estas restricciones en su propio beneficio. Esto requiere de la utilización de claves y de *firewalls* para restringir el ingreso a la red. La seguridad pública incluye el acceso a servicios como números de emergencia de tres dígitos, así como la prevención o al menos el rastreo de llamadas mal intencionadas. Las redes convergentes también son vulnerables a ataques de *hackers* y viruses que pueden corromper servidores de voz. Existen también muchas herramientas que pueden monitorear el contenido de los paquetes en una red y alguien podría decodificar llamadas y escuchar conversaciones privadas. Para esto existen otras muchas herramientas y soluciones como encripción o VPNs; también se debe limitar el acceso a las IP PBX y servidores VoIP.

4.3. Análisis económico de la solución

4.3.1. Aplicación real

Para poder realizar un estudio de los beneficios económicos que se obtienen al implementar una red convergente basada en el protocolo SIP es necesario plantear un caso concreto. Tomemos pues como referencia el caso de una empresa fabricante y distribuidora de productos de limpieza para el hogar e industria con operaciones regionales en toda Centroamérica. Las oficinas centrales y planta de producción sen encuentran en la ciudad de Guatemala. Teniendo sucursales distribuidoras en El Salvador, Honduras, Nicaragua y Costa Rica. El negocio de la empresa es vender los productos de limpieza que fabrica, cuenta con una red de vendedoras que promocionan los productos por medio de un catalogo y ellas son las únicas que tienen contacto directo con el cliente. Los reclamos, solicitudes o inquietudes son canalizados a través de las vendedoras. Existen cinco centros de distribución o tiendas en la ciudad de Guatemala donde se puede comprar el producto directamente; en el resto de países de la región existen cuatro tiendas por país. Es hacia estas tiendas donde se lleva el producto, que las vendedoras solicitan con anticipación, para que puedan recogerlo y entregarlo a sus clientes.

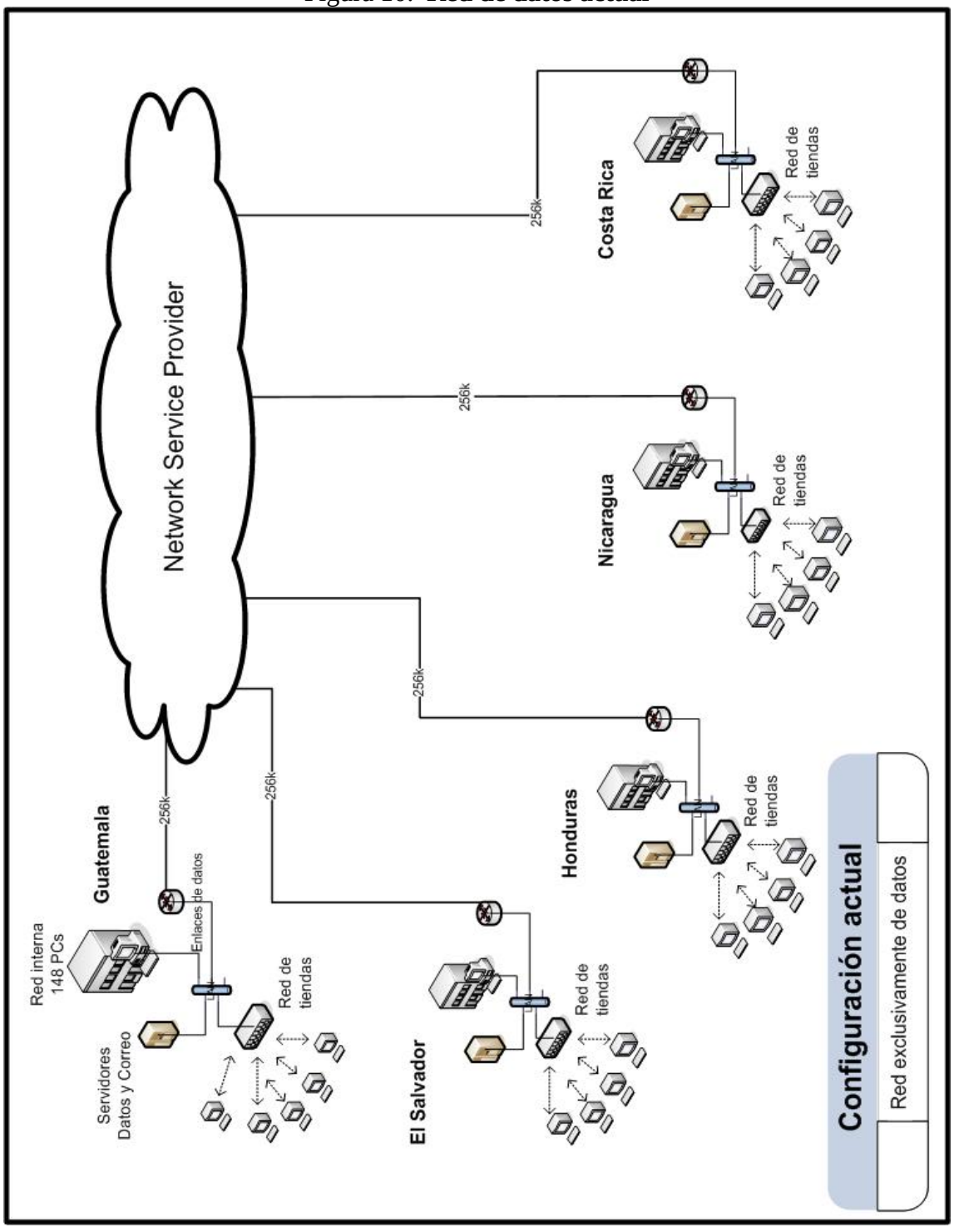
La empresa está ampliando su paleta de productos a nivel local y regional. La legislación de cada país difiere en requisitos de importación que deben cumplir los productos como registros sanitarios, tipo de empaque, precauciones, etc. Por lo que es necesario tener un canal de comunicación abierto entre las oficinas centrales, las oficinas regionales y las autoridades correspondientes en cada país.

Las oficinas centrales están dentro de las mismas instalaciones que la planta de producción, lo que facilita la comunicación dentro de la empresa. En la actualidad la empresa cuenta con una red puramente de datos por medio de la cual se gestionan los pedidos para cada país, correos electrónicos y envío de información gerencial. Esta red se compone de cinco grupos de operación, uno de ellos es su centro de operaciones en Guatemala y los otros cuatro sus centros de distribución en cada país de la región en que opera, ver figura 10.

La red del centro de operaciones en Guatemala se compone de:

- servidores de datos y correo electrónico,
- alrededor de 148 estaciones de trabajo,
- cinco sub-redes para las tiendas que se conectan por medio de enlaces de datos dedicados con 256Kbps de ancho de banda
- 4 enlaces de datos dedicados gestionados por un NSP (*Network Service Provider*) que opera a nivel regional.
- En la parte de telefonía se cuenta con una planta PBX con 160 extensiones internas disponibles y capacidad de manejar 6 líneas de la PSTN local.

Figura 10. **Red de datos actual**



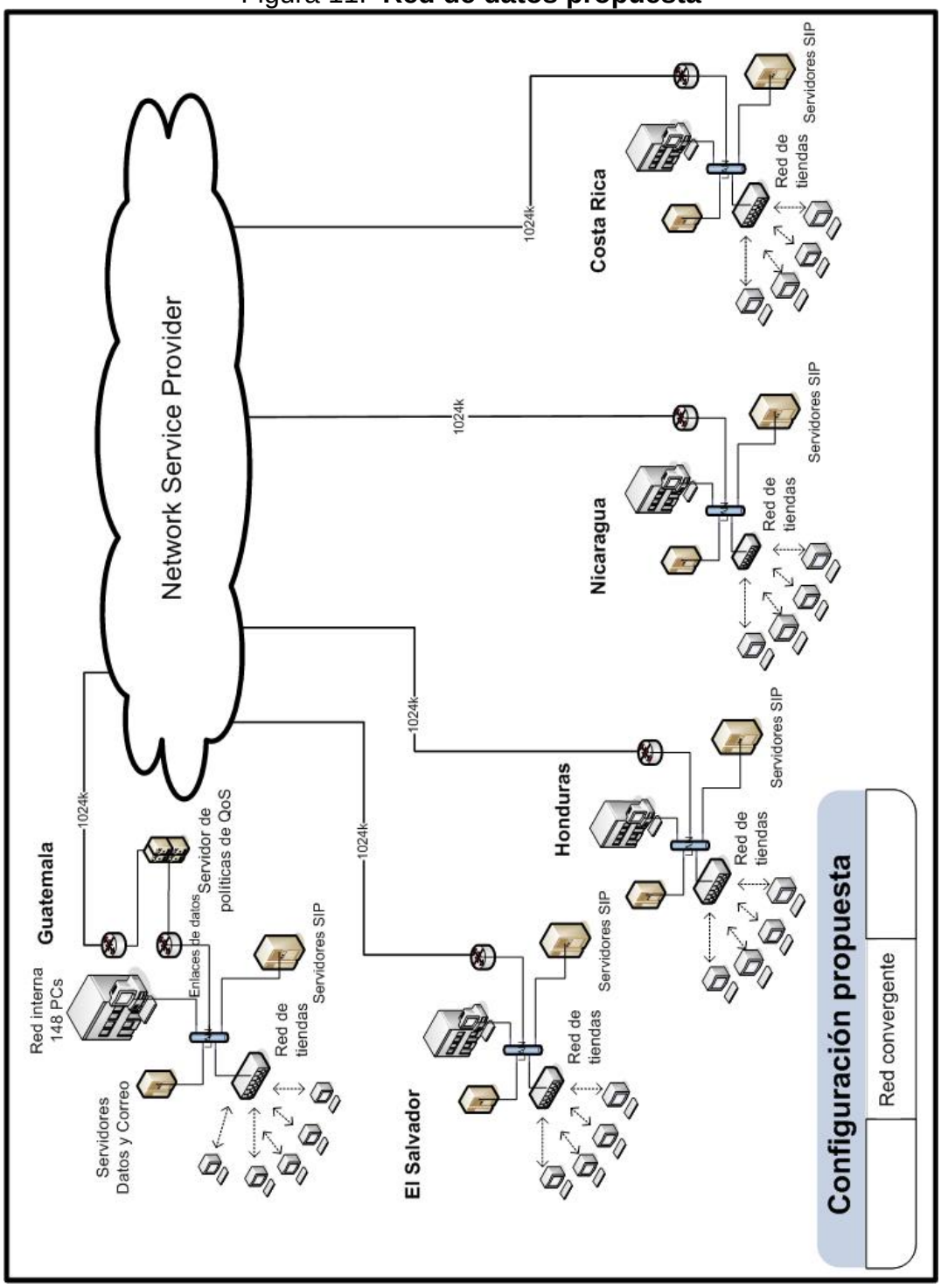
Las redes de datos en los centros de distribución tienen las siguientes características:

- Un servidor de datos y uno de correo electrónico,
- alrededor de veinticuatro estaciones de trabajo,
- cuatro sub-redes ubicadas en cada tienda (cuatro por país) hacia las cuales existe un enlace de datos dedicado con 256Kbps cada uno
- Un enlace de datos regional gestionado por un proveedor de servicio de datos (DSP) con operación en la región.
- Se utiliza un sistema de telefonía convencional gestionando un promedio de 5 líneas telefónicas por país administradas por una planta telefónica PBX con 30 extensiones internas funcionales, de las cuales 24 de ellas tienen terminales con capacidades para transferencia de llamadas entre otras.

Para poder reducir los costos de operación de la empresa se sugiere implementar un sistema de transmisión de voz sobre IP utilizando protocolo SIP implementando características de convergencia sobre la red de datos ya existente en la empresa. Se propone implementar un servidor por país, que estén basados en Linux y que integren las funciones correspondientes. Esto es posible debido al avanzado desarrollo de aplicaciones como *SIP Express Router* y *Asterisk* que están basadas en la plataforma Linux y pueden ser implementadas casi en cualquier distribución. También se puede hacer uso de teléfonos virtuales o *softphones* implementados en las computadoras de las estaciones de trabajo para ahorrar fondos de inversión en teléfonos SIP. Sin embargo es necesario invertir en *hardware* para implementar los servidores,

interfases para teléfonos convencionales/SIP y especialmente en equipo para asegurar QoS. Otro punto importante es el cálculo del ancho de banda adicional que será requerido al NSP para que los enlaces de datos regionales sigan funcionando correctamente. Incluimos en el análisis el costo de la capacitación al personal y la mano de obra de instalación de software y equipos. Para el correcto funcionamiento de este sistema se necesita aumentar el ancho de banda de los enlaces regionales a 1024K y los de las tiendas a 512K. En la figura 11 se muestra el diagrama de la red propuesta.

Figura 11. **Red de datos propuesta**



4.3.2. Matriz financiera

La parte fundamental en este estudio económico es la matriz financiera que incluye los gastos de inversión y los ingresos por beneficios generados por el proyecto. Esta matriz permite encontrar parámetros de decisión como el Valor Actual Neto (VAN) y la Tasa Interna de Retorno (TIR). También permite el calculo del Punto de Equilibrio que indica el período aproximado en el que se debería recuperar la inversión y facilita el calculo de la relación Beneficio / Costo. Se ha tomado en cuenta el valor del dinero en el tiempo suponiendo una tasa de ganancia durante cinco años de 7% no cumulativa como tasa interna aceptable. El proyecto será rentable si se cumple con lo siguiente:

El Valor Actual Neto (VAN) calculado debe ser mayor o igual a cero.
La Tasa Interna de Retorno (TIR) debe ser mayor a la tasa interna aceptable (establecida en un 7%).
La relación Beneficio/Costo debe ser mayor o igual a cero.

Tabla IV. **Costo actual de las llamadas realizadas en un año**

Costo de llamadas por año utilizando sistema convencional			
Minutos Promedio	**Llamadas utilizando PSTN**	**Costo minuto**	**Total**
48000	Llamadas internacionales (dentro de la sucursal)	Q1.25	Q60,000.00
48000	Llamadas internacionales (a otros operadores)	Q1.50	Q72,000.00
84000	Llamadas Nacionales (a tiendas)	Q0.50	Q42,000.00
48000	Llamadas Internacionales de otros países hacia Guatemala	Q1.50	Q72,000.00
57600	Llamadas locales en otros países (a tiendas)	Q0.50	Q28,800.00
	Gran Total		Q274,800.00
Costo de llamdas por año utilizando SIP VoIP			
Minutos Promedio	**Llamadas utilizando PSTN**	**Costo minuto**	**Total**
48000	Llamadas internacionales (dentro de la sucursal)	Q0.00	Q0.00
48000	Llamadas internacionales (a otros operadores)	Q0.50	Q24,000.00
84000	Llamadas Nacionales (a tiendas)	Q0.00	Q0.00
48000	Llamadas Internacionales de otros países hacia Guatemala	Q0.00	Q0.00
57600	Llamadas locales en otros países (a tiendas)	Q0.00	Q0.00
	Gran Total		Q24,000.00
	Ahorro anual en llamdas telefónicas		Q250,800.00

Tabla V. **Costo de los enlaces de datos**

Costo de enlace de datos por ancho de banda					
BW Actual	**BW Adicional**	**Nuevo BW**	**Enlace**	**Costo actual**	**Nuevo Costo**
256	768	1024	Datos GT-SV	Q60,060.00	Q72,996.00
256	768	1024	Datos GT-HN	Q32,340.00	Q46,200.00
256	768	1024	Datos GT-NIC	Q92,400.00	Q133,980.00
256	768	1024	Datos GT-CR	Q138,600.00	Q195,888.00
256	256	512	Datos Kioskos	Q88,704.00	Q108,662.40
			Totales	Q412,104.00	Q557,726.40
			Total de inversión en ancho de banda adicional		Q145,622.40

Tabla VI. **Matriz Financiera**

Matriz Financiera							
Costos	Descripción	Periodos					
		0	1	2	3	4	5
Costo de Equipos	Servidores Proliant Multipropósito (5)	Q46,200.00					
	Interfaces Digium	Q94,017.00					
	Servidor QoS Allot Netenforcer	Q30,030.00					
Costo de Instalación	Instalación y configuración de los equipos	Q55,000.00					
	Instalación y licencias para Zoiper Softphone	Q35,160.00					
	Capacitación de usuarios de Softphones	Q5,000.00					
	Capacitación del personal que administrará el sistema	Q23,100.00					
	Otros gastos de instalación	Q50,000.00					
	Ancho de banda adicional requerido del NSP	Q145,622.00	Q151,446.88	Q157,504.76	Q163,804.95	Q170,357.14	Q177,171.43
Costos de Operación y Mantenimiento	Mantenimiento preventivo de los equipos		Q30,000.00	Q32,100.00	Q64,347.00	Q38,851.29	Q41,570.88
	Reparación y repuestos de los equipos		Q10,000.00	Q10,500.00	Q11,025.00	Q11,576.25	Q12,155.06
	Soporte para los equipos		Q14,630.00	Q15,215.20	Q15,823.81	Q16,456.76	Q17,115.03
	Recurso humano	Q70,000.00	Q73,500.00	Q77,175.00	Q81,033.75	Q85,085.44	Q89,339.71
Total de Inversion		**Q554,129.00**	**Q279,576.88**	**Q292,494.96**	**Q336,034.50**	**Q322,326.88**	**Q337,352.11**
Beneficios							
Beneficios Tangibles	Ahorro en llamadas telefónicas		Q250,800.00	Q250,800.00	Q250,800.00	Q250,800.00	Q250,800.00
	Ahorro en mantenimiento de equipo de telefonía		Q150,000.00	Q160,500.00	Q171,735.00	Q183,756.45	Q196,619.40
Beneficios Estratégicos	Implementación de servicios de valor agregado		Q75,000.00	Q37,500.00	Q11,250.00	Q3,375.00	Q1,012.50
	Solución rápida de problemas		Q100,000.00	Q107,000.00	Q114,490.00	Q122,504.30	Q131,079.60
	Mejoramiento del sistema de comunicaciones en general		Q60,000.00	Q64,500.00	Q69,337.50	Q74,537.81	Q80,128.15
Total de Beneficios		**Q0.00**	**Q635,800.00**	**Q620,300.00**	**Q617,612.50**	**Q634,973.56**	**Q659,639.65**
Flujo Neto Efectivo		**-Q554,129.00**	**Q356,223.12**	**Q327,805.04**	**Q281,578.00**	**Q312,646.68**	**Q322,287.54**

4.3.3. Valor Actual Neto (VAN), Tasa Interna de Retorno (TIR), Punto de Equilibrio y Análisis Beneficio / Costo

Tabla VII. **Calculo de parámetros**

Valor Actual Neto	
Año	Flujo Neto
0	-Q554,129.00
1	Q356,223.12
2	Q327,805.04
3	Q281,578.00
4	Q312,646.68
5	Q322,287.54
VAN	Q209,282.28

Tasa Interna de Retorno	
TIR	37.77

Punto de Equilibrio	
PE	1.39
	1 año, 5 meses

Análisis Beneficio / Costo		
Año	Inversion	Ingresos
0	Q554,129.00	Q0.00
1	Q279,576.88	Q635,800.00
2	Q292,494.96	Q620,300.00
3	Q336,034.50	Q617,612.50
4	Q322,326.88	Q634,973.56
5	Q337,352.11	Q659,639.65
VAN	Q424,382.87	Q633,665.14
Relación Costo / Beneficio		1.49

Se calcularon los valores de los parámetros en base a la matriz financiera presentada en la tabla número seis. Se puede observar que el Valor Actual Neto (VAN) es Q209.282.28; la Tasa Interna de Retorno (TIR) es de 37.77%; el punto de equilibrio indica que la inversión se puede recuperará en un período de un año y cinco meses. Finalmente al realizar la relación Beneficio / Costo obtenemos un valor de 1.49 que siendo mayor que cero indica que los beneficios son mayores que los costos.

CONCLUSIONES

1. Únicamente las redes que integran el tráfico de voz y datos en una misma plataforma tienen una relación costo beneficio que producen ganancias a largo plazo. Esto se debe a que los equipos que soportan tanto tráfico de voz como de datos eliminan la necesidad de tener redes exclusivas para cada uno, lo que significa un ahorro de espacio, energía y se evitan los altos costos de mantenimiento y soporte que generan los equipos exclusivos para tráfico de voz.

2. Una red convergente debe cumplir con algunos requerimientos técnicos específicos para que sea factible la transmisión de los diferentes tipos de tráfico. Se debe asegurar que la estructura IP a utilizar funcione en óptimas condiciones, haciendo énfasis en el manejo de las políticas de QoS y la utilización de protocolos estandarizados.

3. Session Initiation Protocol (SIP) es un protocolo estándar basado en otros protocolos ya existentes que son bastante populares. Su estructura es relativamente pequeña y sencilla, ya que utiliza comandos en forma de líneas de texto que pueden ser fácilmente codificadas y decodificadas. Estos mensajes son intercambiados entre un cliente y un servidor lo que permite implementar aplicaciones de administración y seguridad fácilmente. La sencillez de transmisión y manejo de estos mensajes también permite que puedan interactuar con otras tecnologías y facilita la expansión.

4. Se logró constatar que técnicamente es factible implementar un sistema VoIP utilizando protocolo SIP utilizando convergencia de redes ya que existen varias opciones para cubrir los requisitos técnicos en la región. Existen varios proveedores en la región que cumplen con los requisitos mínimos para brindar un servicio de buena calidad.

5. Según los resultados del análisis económico si es factible implementar un sistema VoIP utilizando SIP y convergencia de redes ya que reduce considerablemente el costo de las llamadas telefónicas. El tiempo de recuperación de la inversión puede ser bastante corto si se utilizan los recursos ya existentes para introducir nuevos servicios.

RECOMENDACIONES

1. Antes de diseñar una red convergente se debe establecer los objetivos de dicha red, es necesario especificar los requerimientos de los usuarios para asegurar el éxito de la misma.

2. Debe consultarse los documentos de la IETF antes de iniciar el proceso para asegurarse que se esté utilizando la versión más actualizada del protocolo Standard. Esto debido a que cada vez que se publica un nuevo RFC puede que automáticamente convierta a otro en obsoleto.

3. Es aconsejable conocer a fondo la manera en que SIP funciona para poder explotar al máximo sus funciones.

4. En el momento de la selección de productos para la implementación deben tomarse en cuenta software y paquetes de licencia libre. Algunos de estos poseen un gran nivel de soporte por medio de comunidades de expertos a nivel mundial como es el caso de las plataformas basadas en Linux. Aunque su configuración represente una tarea complicada, pueden traer grandes beneficios al proveer una plataforma escalable y económica.

5. Antes de lanzar una solución SIP VoIP es recomendable realizar una serie de pruebas para asegurar un perfecto funcionamiento desde el principio y de esta manera no desanimar a los usuarios de estas nuevas tecnologías.

BIBLIOGRAFÍA

Ellis, Juanita y otros. **Voice, Video, and Data Network Convergence.** Primera edición. Academic Press, 2003.

Johnston, Allan B. **SIP, Understanding the Session Initiation Protocol.** Segunda edición. Artech House, 2004.

Madsen, Leif y otros. **Asterisk: The Future of Telephony.** Primera Edición. O'Reilly, 2005.

RADVISION Ltd. **Understanding SIP Servers.** Whitepaper, 2002.

Mehta, Princy. **Overview of Voice Over IP.** Universidad de Pennsylvania. Whitepaper, 2001.

Bhat, Vinod. **Voice Over IP – The SIP Way.** Technology Review #2001-03. Tata Consultancy Services, 2001.

Mitra, Debashish. **Network Convergence and Voice over IP.** Technology Review #2001-2. Tata Consultancy Services, 2001.

Block, Stanley y Geoffrey Hirt. **Administración Financiera.** Decimoprimera edición. McGraw Hill, 2005.

APÉNDICE

Asterisk

Asterisk es una plataforma convergente de telefonía diseñada para correr sobre Linux, una de sus principales ventajas es que funciona bajo el concepto de "*software* libre". Permite implementar aplicaciones como correo de voz, conferencias, colas de llamadas, música de espera de llamada, etc. Esta flexibilidad hace que Asterisk sea difícil de configurar ya que ofrece muchas opciones para resolver un problema. El hecho de que esté basado en Linux también significa que existe un grupo de profesionales de distintos campos de aplicación desarrollando nuevas ideas acerca de flexibilidad. Esta comunidad está dedicada a desarrollar nuevas aplicaciones y a brindar soporte a los usuarios, se puede acceder a ella a través de sitios en Internet como www.asterisk.com.

Los recursos necesarios para implementar Asterisk son similares a los requeridos por aplicaciones que funcionan en tiempo real, tiene que tener alta prioridad de acceso al microprocesador y a los buses del sistema. Es por esto que se sugiere no se corran otras aplicaciones simultáneamente en el mejor de los casos, o bien que estas tengan un nivel de prioridad bajo. Se debe prestar especial atención al momento de seleccionar el *hardware* que servirá de interfase entre Asterisk y nuestra red, se debe tomar en cuenta la aplicación principal del sistema. Es en estos puntos donde se requiere un amplio conocimiento de la plataforma para poder optimizar el recurso, ya que mientras más canales se utilicen simultáneamente se necesitará más capacidad de

procesamiento. Para montar un sistema en una mediana empresa en donde no se utilicen más de quince canales simultáneamente se puede utilizar un servidor con 1GB de memoria RAM y un microprocesador de 3GHz, los cuales están disponibles en una gran variedad en el mercado. Para sistemas en los que se necesite tener más de quince canales abiertos simultáneamente se pueden utilizar servidores con procesadores múltiples o bien varios servidores.

Es de esperarse que cualquier sistema de VoIP desarrollado en estos días necesite conectarse a otras redes como la PSTN para poder satisfacer a los usuarios. En este caso existen algunas empresas que fabrican interfases de telefonía. También existen adaptadores para conectar teléfonos convencionales al sistema, conocidos comúnmente como ATA (Adaptador de Teléfono Análogo). Sin embargo para aprovechar al máximo los recursos disponibles se pueden utilizar paquetes de *software* que emulan aparatos telefónicos conocidos como *softphones*. Estos programas de computadora abren un nuevo mundo de posibilidades en el mundo de las telecomunicaciones, algunos de estos están diseñados para “recordarnos” que estamos haciendo una llamada telefónica pero pueden crearse aplicaciones que contesten o generen llamadas por nosotros.