



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

**Implantacion de sistemas de telefonia IP bajo
plataforma Linux utilizando Asterisk**

TESINA

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Thomas Billy Joel MORALES OLAECHEA

Carlos Enrique DURAND FLORES

ASESOR

Juan Carlos GONZÁLEZ SUAREZ

Lima, Perú

2006



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Morales, T. & Durand, C. (2006). *Implantacion de sistemas de telefonia IP bajo plataforma Linux utilizando Asterisk*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios autor/ asesor

Datos de autor	
Nombres y apellidos	Thomas Billy Joel Morales Olachea
Tipo de documento de identidad	DNI
Número de documento de identidad	40743878
URL de ORCID	-----
Datos de autor	
Nombres y apellidos	Carlos Enrique Durand Flores
Tipo de documento de identidad	DNI
Número de documento de identidad	40397296
URL de ORCID	-----
Datos de asesor	
Nombres y apellidos	Juan Carlos González Suarez
Tipo de documento de identidad	DNI
Número de documento de identidad	07566359
URL de ORCID	0000-0002-2309-9133
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Raúl Armas Calderón
Tipo de documento	DNI
Número de documento de identidad	07156168
Miembro del jurado 1	
Nombres y apellidos	Daniel Quinto Pazce
Tipo de documento	DNI

Número de documento de identidad	10372726
Datos de investigación	
Línea de investigación	C.O3.10 Redes de datos, Tecnologías de la información y comunicación.
Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento.
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Lima Latitud: -12.056445 Longitud: -77.085994
Año o rango de años en que se realizó la investigación	2004 - 2006
URL de disciplinas OCDE	https://purl.org/pe-repo/ocde/ford#2.02.04



"Año de la Innovación Institucional y del Sesquicentenario de la Fundación de la Facultad de Medicina"

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

Fundada en 1551

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Escuela Académico Profesional de Ingeniería de Sistemas

PROGRAMA DE ACTUALIZACIÓN PROFESIONAL PARA OPTAR EL TÍTULO DE
INGENIERO DE SISTEMAS

Acta de Sustentación de Tesina

Siendo las ^{horas} 21:45 del día 13 de Julio del año 2006, se reunieron los docentes designados como miembros de Jurado de la Tesina, presidido por el Ing. Raúl Armas Calderón, Lic. Daniel Quinto Pazce (Miembro) para la sustentación de la Tesina intitulada **"IMPLANTACION DE SISTEMAS DE TELEFONIA IP BAJO PLATAFORMA LINUX UTILIZANDO ASTERISK"**, por el **Sr. Br. Carlos Enrique Durand Flores**; para optar el Título Profesional de Ingeniero de Sistemas

Acto seguido de la exposición de la Tesina, el Presidente invitó al graduando a dar respuesta a las preguntas establecidas por los Miembros de Jurado.

El graduando en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros de Jurado, el graduando obtuvo la nota de ¹⁶ (En letras) ^{Dieciséis}.

A continuación el Presidente del Jurado, Ing. Raúl Armas Calderón declara al graduando **Ingeniero de Sistemas**.

Siendo las ^{22:35} horas, se levantó la sesión.


Ing. Raúl Armas Calderón
Presidente


Lic. Daniel Quinto Pazce
Miembro



"Año de la Innovación Institucional y del Sesquicentenario de la Fundación de la Facultad de Medicina"

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

Fundada en 1551

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Escuela Académico Profesional de Ingeniería de Sistemas

PROGRAMA DE ACTUALIZACIÓN PROFESIONAL PARA OPTAR EL TÍTULO DE
INGENIERO DE SISTEMAS

Acta de Sustentación de Tesina

Siendo las ^{21:45} horas del día ¹³ de Julio del año 2006, se reunieron los docentes designados como miembros de Jurado de la Tesina, presidido por el Ing. Raúl Armas Calderón, Lic. Daniel Quinto Pazce (Miembro) para la sustentación de la Tesina intitulada **"IMPLANTACION DE SISTEMAS DE TELEFONIA IP BAJO PLATAFORMA LINUX UTILIZANDO ASTERISK"**, por el **Sr. Br. Thomas Billy Joel Morales Olachea**; para optar el Título Profesional de Ingeniero de Sistemas

Acto seguido de la exposición de la Tesina, el Presidente invitó al graduando a dar respuesta a las preguntas establecidas por los Miembros de Jurado.

El graduando en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros de Jurado, el graduando obtuvo la nota de ¹⁶ (En letras) ^{Dieciséis}.

A continuación el Presidente del Jurado, Ing. Raúl Armas Calderón declara al graduando **Ingeniero de Sistemas**.

Siendo las ^{22:35} horas, se levantó la sesión.

Ing. Raúl Armas Calderón
Presidente

Lic. Daniel Quinto Pazce
Miembro



Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Escuela Profesional de Ingeniería de Sistemas

F O R M A T O N° 005

DECLARACION JURADA DE ORIGINALIDAD

TESINA

IMPLANTACIÓN DE SISTEMAS DE TELEFONÍA IP BAJO PLATAFORMA LINUX UTILIZANDO ASTERISK

Carlos Enrique Durand Flores, identificado con DNI N° 40397296, de la Facultad de Ingeniería de Sistemas e Informática - Escuela Profesional de Ingeniería de Sistemas.

DECLARO BAJO JURAMENTO

Que la **Tesina**, que presento es original e inédito, no siendo copia parcial ni total del trabajo de Investigación, desarrollado en el Perú o en el extranjero. En caso contrario, de resultar falsa la información que proporciono, me sujeto a los alcances de lo establecido en el artículo N° 411 del Código Penal concordante en el artículo N° 32 de la Ley N° 27444, la Ley del procesamiento Administrativo General y las Normas Legales de Protección a los Derechos de Autor.
En fe de lo cual firmo la presente

Lima 03 de Octubre.2025



Huella digital

Carlos Enrique Durand Flores
Firma y Nombre completo
DNI: 40397296

F O R M A T O N° 005

DECLARACION JURADA DE ORIGINALIDAD

TESINA

Implantación de Sistemas De Telefonía IP bajo Plataforma Linux utilizando Asterisk

Thomas Billy Joel Morales Olaechea, identificado con DNI N° 40743878, de la Facultad de Ingeniería de Sistemas e Informática - Escuela Profesional de Ingeniería de Sistemas.

DECLARO BAJO JURAMENTO

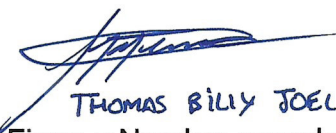
Que la Tesina, que presento es original e inédito, no siendo copia parcial ni total del trabajo de Investigación, desarrollado en el Perú o en el extranjero. En caso contrario, de resultar falsa la información que proporciono, me sujeto a los alcances de lo establecido en el artículo N° 411 del Código Penal concordante en el artículo N° 32 de la Ley N° 27444, la Ley del procesamiento Administrativo General y las Normas Legales de Protección a los Derechos de Autor.

En fe de lo cual firmo la presente

Lima 24 de junio 2025

Huella digital




THOMAS BILLY JOEL MORALES OLAECHEA
Firma y Nombre completo
DNI: 40743878

Dedicado a nuestros padres por el sacrificio de darnos una buena educación, por el apoyo y ejemplo de vida que siempre nos brindan.

RESUMEN

Implantación de Sistemas de Telefonía IP bajo Plataforma Linux utilizando Asterisk

**CARLOS DURAND FLORES
THOMAS MORALES OLAECHEA**

JUNIO – 2006

Asesor : Ing. Juan Carlos Gonzáles Suárez
Grado : Ingeniero de Sistemas e Informática

El presente proyecto constituye un marco conceptual viable para llevar acabo el desarrollo de la implantación de un sistema de telefonía de altas prestaciones de comunicación sobre Voz IP, el cual tiene por objetivo resolver el problema de reducción de costos, así como cumplir los exigentes niveles de comunicación como fidelidad de audio y tiempo de respuesta, lo cual permite construir un sistema de telefonía a una fracción del costo real del de una plataforma tradicional. Este modelo de telefonía permite cambios en el mercado de centrales telefónicas privadas (PBX)

Este sistema de telefonía sobre Voz IP consiste en una avanzada solución que permite a las compañías, la integración entre las redes de transmisión de voz y datos, esta implantación permite transmisión de señales telefónicas a través de la INTRANET y/o INTERNET obteniendo las prestaciones básicas de una central convencional como son ruteo de llamadas, reenvío, puede funcionar como un gateway de comunicaciones integradas. Por ejemplo, tiene la funcionalidad de digitalizar y enviar por email los mensajes

de voicemail, recepción y gestión de llamadas con menús interactivos, con lo cual permitiríamos grandes ahorros a las empresas con altos presupuestos en llamadas internacionales. Asimismo permite intercomunicación entre empresas multinacionales o conectando Call Centers y sucursales en un mismo país, o programarlos como IVR para realizar automáticamente miles de llamadas a sus clientes.

Palabras Clave:

VozIP.

IP.

PBX.

Internet.

Integración de redes. Transmisión
de voz y datos. Intercomunicación.

Gateway.

Voicemail.

Call Centers.

IVR.

ABSTRACT

Implantation of System Telephony IP under Platform Linux using Asterisk

**CARLOS DURAND FLORES
THOMAS MORALES OLAECHEA**

JUNE – 2006

Asesor : Juan Carlos Gonzáles Suárez
Grade : System and Informatics Engineer

The following project is a conceptual description that can guide to the development of a telephony system of high quality communication on VoIP which has as objective not only the decrease of costs, but also match the demanding characteristics of communication: audio fidelity and response time, which allows building a telephony system of high quality communication with a very low cost (compared with a traditional telephony system's cost). This model of telephony allows changes in the market of Private Branch eXchange (PBX).

The telephony on VoIP consists in an advance solution that allows companies the integration among voice transmission and data nets. This system, also, allows the transmission of telephony signals through the Intranet and/or Internet achieving the basic characteristics of a conventional telephony centre: call routing, forwarding, working as an integrated communication gateway, eg: the system can digitalize and send by e-mail the voicemail messages, reception and manage calls with interactive menus; that

way we could allow companies to save a huge amount of money spent in international calls. Furthermore the system allows communication among multinational companies or connecting Call Centers and branch offices in the same country or programming them as IVR to make thousands of calls to their clients automatically.

Keywords:

VoIP

IP

PBX

Internet

Networks Integration.

Voice and Data Transmission

Intercommunication

Gateway

Voicemail

Callcenters

IVR

INDICE

RESUMEN.....	I
ABSTRACT.....	III
INDICE	1
INTRODUCCIÓN	6
CAPITULO I.....	9
1. PLANTEAMIENTO DEL PROBLEMA	9
1.1 Antecedentes y formulación del problema	9
1.2 Justificación e Importancia.....	10
1.3 Definición del Problema.....	11
1.4 Limitaciones y Alcance	12
1.5 Variantes del Problema	13
CAPITULO II	14
2. OBJETIVOS	14
2.1 Objetivos Generales	14
2.2 Objetivos Específicos.....	14
CAPITULO III	16
3. MARCO CONCEPTUAL	16
3.1 Antecedentes de la Investigación	16
3.2 Bases aspectos técnicos y estándares de VoIP	20
3.2.1 Los estándares de compresión. Codecs de VoIP.....	20
3.2.1.1 Técnicas basadas en formas de onda	22

3.2.1.2	Técnicas basadas en vocoders	24
3.2.1.3	Técnicas mixtas	25
3.2.1.4	Comparativa resumen de codecs y aspectos técnicos de los mismos	31
3.2.2	Protocolos de red y transporte en los que se apoya VoIP	32
3.2.2.1	RTP	34
3.2.3	Calidad de servicio (QoS) en VoIP	46
3.2.3.1	Parámetros de QoS	49
3.2.3.2	Medida de Parámetros de QoS	54
3.2.3.3	Modelos de QoS	56
3.2.3.4	La medida de calidad MOS (Mean Opinion Score)	64
3.3	Normativas VoIP	70
3.3.1	H.323	70
3.3.1.1	Arquitectura H.323	77
3.3.2	SIP	80
3.3.2.1	Arquitectura SIP	82
3.3.2.2	Servicios SIP	84
3.3.3	MGCP y MEGACO	86
3.3.4	IAX	89
3.3.4.1	Propiedades Básicas	90
3.3.4.2	Objetivos de IAX	91
3.3.5	Asterisk	92
3.3.5.1	Funcionalidades generales	93
3.3.5.2	Esquema Conceptual	94
3.3.5.3	Funcionalidades tipo centralita clásica	94

3.3.5.4	Funcionalidades tipo centralita avanzada	95
3.3.5.5	Funcionalidades Voz IP.....	95
3.3.5.6	Problemas nativos de la Voz IP.....	96
3.3.5.7	Problemas de configuración (Complejidad)	97
3.3.5.8	Integración de Asterisk.....	97
3.3.5.9	Asterisk y la Telefonía Tradicional	98
CAPITULO IV		103
4. MARCO METODOLOGICO		103
4.1	Tipo de Investigación	103
4.2	UNIVERSO O POBLACIÓN.....	104
4.2.1	Determinación del Universo	104
4.2.2	Determinación de la Muestra.....	105
CAPITULO V		106
5. IMPLANTACION METODOLOGICA Y TECNOLOGICA.....		106
5.1	Descripción de la situación actual de la empresa	106
5.2	Modelo de Implantación de la Solución	109
5.2.1	Los medios físicos, características y equipamiento necesarios para la implantación	110
5.2.1.1	Terminales IP	111
5.2.1.2	Red LAN	113
5.2.1.3	Red WAN.....	113
5.2.1.4	Servidor Linux con Asterisk.....	115
5.2.2	Configuración del Servidor Asterisk	118
5.2.2.1	IP PBX	119
5.2.2.2	Configuración de Terminales IP	128

5.3	Ventajas obtenidas al implantar Asterisk como PBX.....	131
5.3.1	Ahorro de costos.....	131
5.3.2	Productividad.....	134
5.3.3	Optimización de Recursos.....	134
5.3.4	Compatibilidad con el Tele trabajo	135
5.3.5	Calidad de Servicio a los clientes	136
5.4	Costos de Implantación y beneficios	136
5.4.1	Beneficios de Asterisk frente a lo tradicional	136
5.4.2	Económico.....	137
5.4.3	Robusto	138
5.4.4	Potente.....	138
5.4.5	Flexible.....	139
5.4.6	Protege la inversión	140
5.5	Especificaciones de Seguridad	141
5.5.1	Amenazas	142
5.5.2	Recomendaciones de Seguridad	144
5.5.2.1	Encriptación	145
5.5.2.2	Configuración Adecuada de los componentes	146
5.5.2.3	Disponibilidad de la Red	147
5.5.2.4	Utilización de un Firewall y un IDS	147
5.6	Posibles escenarios de Instalación con Asterisk	149
5.6.1	Centralita Nueva con conexiones y extensiones de varios tipos	150
5.6.2	Pasarela para dotar a una centralita tradicional de servicios nuevos	150
5.6.3	Pasarela para dotar a una centralita tradicional de nuevas extensiones	

5.6.4	Varias Oficinas con un Asterisk Centralizado	152
5.6.5	Varias Oficinas con Sistemas Asterisk interconectados	152
CAPITULO VI.....		154
6.	CONCLUSIONES	154
GLOSARIO DE TERMINOS		156
REFERENCIAS BIBLIOGRÁFICAS		163
ANEXOS		168
ANEXO N° 1		168
	RSVP/IntServ	168
ANEXO N° 2.....		175
	MPLS	175
INDICE DE TABLAS.....		178
INDICE DE FIGURAS		179

INTRODUCCIÓN

El crecimiento y fuerte implantación de las redes IP, tanto en local como en remoto, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP lo que no significará en modo alguno la desaparición de las redes telefónicas conmutadas, sino que habrá, al menos temporalmente, una fase de coexistencia entre ambas, y por supuesto la necesaria interconexión mediante pasarelas (gateways), denominadas genéricamente pasarelas VoIP. Este aspecto ha sido abordado tanto por ITU (International Telecommunication Union) como por el IETF (Internet Engineering Task Force).

Si a todo lo anterior, se le suma el fenómeno Internet, junto con el potencial ahorro económico que este tipo de tecnologías puede llevar acarreado, la conclusión es clara: El VoIP (Protocolo de Voz Sobre Internet -

Voice Over Internet Protocol) es un tema "caliente" y estratégico para las empresas.

La telefonía IP es un modelo que comprende toda la funcionalidad que ofrece la telefonía tradicional, pero bajo un nuevo esquema de transporte bajo el protocolo IP y una estructura de redes.

Si bien es cierta la idea de una red única que permita la integración entre las redes de voz y datos no es nueva. La progresiva modernización y mejora de los sistemas de transmisión de datos, han hecho posible que estándares definidos hace ya algún tiempo, estén empezando a dar sus primeros pasos y esto permite que surja una nueva alternativa de implementación de una central telefónica.

En una central telefónica existen al menos 700 funciones, y que las mismas deben estar disponibles en las soluciones que se ofrezcan. Las amplias opciones del mercado abierto, han sido quienes han hecho que protocolo IP ganara sobre otras tecnologías similares que existen desde los '90, donde se hablaba de voz sobre ATM, Frame Relay VOFR y otras.

Otro de los mayores beneficios de la telefonía IP es el valor agregado de las aplicaciones con una gran reducción de costos. Existen excelentes aplicaciones de VOIP como Asterisk que han permitido una plataforma tecnológica profesional que permite realizar Call Centers, IVR, Casilleros de

Voz, Servicios de Menús de Voz, Fax y muchas otras opciones que costarían muchos miles de dólares implementar utilizando otras tecnologías.

El propósito de este proyecto es brindar una alternativa de solución al problema de comunicaciones dentro de una organización proponiéndoles un sistema de telefonía basado en Voz sobre IP lo cual les permitirá reducir costos en comunicación y brindarles muchas mas funcionalidades de las que una central tradicional les ofrece como lo son: transferencia ciega, pick up de llamadas, buzón de voz, caller id en espera, llamada en espera, colas de llamadas, conferencias, colas con prioridad, funcionalidades avanzadas como IVR (Interactive Voice Response), funcionalidades digitales como Buzón de Voz (Buzón de voz enviados por email), configuración en Base de datos, extensiones, usuarios, los cuales pueden ser almacenados en BD (MySQL, MSSQL, ODBC * ...). Con esto no solo daríamos solución al costoso problema de comunicaciones sino que a su vez estaríamos ofreciendo la posibilidad de ampliar sus medios de comunicación utilizando la infraestructura actual. También se proporciona una implementación de la arquitectura, para probar que esta tecnología permite grandes beneficios a un costo realmente mínimo y a su vez es de fácil administración e implantación.

CAPITULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1 Antecedentes y formulación del problema.

Desde hace tiempo, los responsables de comunicaciones de las empresas tienen en mente la posibilidad de utilizar su infraestructura de datos, para el transporte del tráfico de voz interno de la empresa. No obstante, es la aparición de nuevos estándares, así como la mejora y abaratamiento de las tecnologías de compresión de voz, lo que está provocando finalmente su implantación.

Después de haber constatado que desde un PC con elementos multimedia, es posible realizar llamadas telefónicas a través de Internet, podemos pensar que la telefonía en IP es de baja calidad, pues la calidad de voz que obtenemos a través de Internet es muy pobre. No obstante, si en nuestra empresa disponemos de una red de datos que tenga un ancho de banda importante, también podemos pensar en la utilización de esta red para el tráfico de voz entre las distintas delegaciones de la empresa. Las ventajas que obtendríamos

al utilizar nuestra red para transmitir tanto la voz como los datos son evidentes.

Actualmente las empresas gastan en la implementación y mantenimiento de centrales telefónicas tradicionales que le brindan un servicio de comunicación de telefonía conmutada la cual viene asociada a una o quizás mas de una línea telefónica que genera un tráfico de llamadas facturada, esto genera un gasto mensual a la empresa.

Ante esto, utilizando la infraestructura actual de la empresa y a través del uso de la tecnología que planteamos, es que pensamos dar una solución integral y así reducir los costos de comunicación ofreciendo el mismo servicio, con calidad, con mayores beneficios a nivel tecnológico, y a un costo mínimo.

1.2 Justificación e Importancia.

A través del presente proyecto, queremos brindar una solución a las organizaciones en la cual podrán implementar un sistema totalmente transparente y atractivo para los usuarios con reducido gasto de operador telefónico ofreciendo los servicios tradicionales de voz e introduciendo además servicios innovadores. Al integrar la telefonía con los PCs y la red de datos disponiendo así de una

plataforma para desarrollar cualquier idea y proyecto que se plantee. Con lo cual la organización podrá obtener mayores canales de comunicación y a su vez un mayor uso de sus recursos.

Viendo el tema económico, cabe pensar que la empresa se puede beneficiar de esta tecnología implementándola por su propia cuenta, total o parcialmente, haciendo uso incluso (dependiendo de la empresa) del ancho de banda no utilizado en determinados momentos de la red de datos de la compañía, teniendo por lo tanto coste mensual nulo o pequeño (si hay que redimensionar la red de datos), de una manera similar a como se realizan las llamadas entre extensiones de una misma centralita.

1.3 Definición del Problema.

Actualmente las empresas cuentan con sistemas de comunicación basadas en centrales telefónicas tradicionales que en su mayoría son costosas en implementación y mantenimiento lo cual hace elevado su costo.

Es por ello que se hace viable la idea de integrar el tráfico de voz y datos en la empresa mediante su red de datos, obteniendo así telefonía IP, su coste de implementación será muy inferior al coste de implementación de una central telefónica tradicional, las llamadas

realizadas a través del operador de telecomunicaciones o telefonía tradicional siempre será mayor al tráfico de llamadas realizadas mediante telefonía IP.

1.4 Limitaciones y Alcance.

Las limitaciones y alcances de cómo llevar a cabo la implantación en una empresa analizando las diferentes alternativas tratará este proyecto, para lo cual, primero se estudiarán las tecnologías y protocolos involucrados, las posibilidades, limitaciones y características de los mismos y se presentarán unos ejemplos teórico-prácticos de implantación de Telefonía IP a empresas hipotéticas en 2 partes diferenciadas: Telefonía IP para la comunicación entre distintas delegaciones (a través de la WAN, o trunking IP) y Telefonía IP para la comunicación en el interior de una oficina a través de la LAN (haciendo las funciones tradicionales de una PBX mediante uno o varios modestos servidores.

El inconveniente principal que se presenta en implementar un sistema de Telefonía IP en este escenario es la inversión inicial requerida en los equipos necesarios para hacer funcionar esta tecnología, inversión que se verá amortizada en un plazo relativamente corto. Además hubo que satisfacer el resto de

condicionantes necesarios para conseguir que la calidad percibida en el audio sea comparable a una llamada tradicional.

1.5 Variantes del Problema.

Las variantes son generadas por aquellos problemas o circunstancias que se dan en el ambiente a la hora la implantación.

- El espacio libre del ancho de banda utilizado por la empresa dependerá del uso del mismo por los empleados.
- El trafico de llamadas de salida diarias implicara en un pequeño porcentaje la distribución del ancho de banda
- Si se implementara la cantidad de estaciones esto implicaría que se tendría que ampliar el numero de extensiones o anexos en la empresa.

CAPITULO II

2. OBJETIVOS

2.1 Objetivos Generales.

Proporcionar e Implantar una solución que permita utilizar una misma infraestructura de redes para transmitir voz y datos con mayores funcionalidades y menores costes de comunicación utilizando los recursos actuales.

2.2 Objetivos Específicos

- Analizar y evaluar el estado actual de la infraestructura de redes.
- Converger las redes de datos y voz a una sola red.
- Ahorrar en infraestructuras: equipamiento de datos más barato que el de voz.
- Disminuir costes de gestión y mantenimiento: sólo habría una red
- Reducir inversiones en equipos.

- Brindar un servicio adecuado a las necesidades de la organización en cuanto a comunicación.
- Implementar un servicio de calidad y más atractivo promoviendo la madurez de las tecnologías Voz IP.

CAPITULO III

3. MARCO CONCEPTUAL

3.1 Antecedentes de la Investigación

A mediados de los 70, la agencia de proyectos avanzados de defensa de los EEUU (DARPA) se interesó en una red de conmutación de paquetes que permitiera la interconexión de distintos centros de investigación asociados a ésta a lo largo de los Estados Unidos.

La DARPA pronto comprendió el potencial de este tipo de redes, que permitían interconectar entre sí equipos de tecnologías y fabricantes diferentes. Con la tarea en mente de desarrollar esta conectividad heterogénea, la DARPA financió la investigación de la Universidad de Stanford y Bolt, Baranek & Newmam (BBN) para crear una serie de protocolos. El resultado de dicha investigación fue el conjunto de protocolos terminados a finales de los 70 y denominados “protocolos IP”. Los más conocidos son:

- IP (Internet Protocol)

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)ç+

Los protocolos IP pueden usarse para comunicarse a través de un conjunto cualquiera de redes interconectadas, funcionando tanto sobre redes locales como sobre redes de área extensa.

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

En telefonía pública se pueden observar diferencias entre un operador local y otro de larga distancia. Cuando nos referimos a Telefonía-IP, nos ocupamos de la aplicación pública local. Existen varias características que hacen de la Telefonía-IP un problema de complejidad elevada respecto de la VoIP. Algunos de ellos son las siguientes:

- Interoperatividad. Una diferencia inicial entre VoIP y Telefonía-IP es la interoperatividad con las redes telefónicas actuales.
- Calidad de Servicio Garantizada. Mientras VoIP se piensa en el ámbito de interconexión mediante Internet (sin calidad de servicio asegurada); en Telefonía-IP se piensa en una Backbone de alta velocidad no- bloqueante para garantizar la calidad de servicio mediante herramientas de QoS. En Telefonía-IP se aplica el concepto de carrier-grade. Este concepto puede incluir varios aspectos:
 1. redundancia de equipamiento para lograr disponibilidad elevada (por ejemplo, 99,99%).
 2. calidad vocal garantizada (bajos indicadores de errores, de retardo, de jitter y de eco, etc).
 3. Servicios de Valor Agregado. Se requiere la disponibilidad de servicios de valor agregado, similar a los ofrecidos en la red PSTN mediante la señalización SS7, conocida como red inteligente IN (Intelligent Network).

En la tecnología VoIP las llamadas se dividen en tramas de datos que se transmiten a través de una red IP. Todas las tramas

deben reconstruirse en el orden correcto, y prácticamente de forma instantánea, a diferencia de lo que ocurre con otras transmisiones sobre IP. Por ejemplo, no es necesario que los mensajes de correo electrónico lleguen inmediatamente, y además se pueden ir reconstruyendo a medida que estos llegan a su destino. La voz, sin embargo, es muy sensible a las latencias (retardos) de la red, por lo que es necesario controlarla muy de cerca. Dicho de otro modo, el control de la calidad de servicio (QoS) debe ser impecable.

El deseo de ofrecer herramientas que mejoren la productividad para aprovechar las infraestructuras de comunicaciones y la necesidad de lograr más por menos, han hecho que la telefonía IP sea necesaria para que las empresas puedan mantener su competitividad.

Las redes actuales utilizan tecnologías como MPLS para priorizar el tráfico por la red. Permiten proporcionar la QoS en prácticamente todas las conexiones nacionales/internacionales, incluidas las conexiones DSL de banda ancha. Internamente, las redes de área local Ethernet están sobradamente capacitadas para admitir la tecnología VoIP.

Por lo cual implementar un sistema de Telefonía IP mediante un equipo que enruta las llamadas de voz dentro de un edificio de oficinas es posible, Las llamadas telefónicas se transmiten en forma

de datos y se dirigen desde la LAN hasta los teléfonos IP de la empresa.

El principal analista de Gartner, Steve Koppman, afirma que este tipo de servicio “[...] promete recortar diversos costes de la empresa, porque puede combinar datos y voz en las mismas líneas, lo que reduce los costes permanentes de gestionar diversas redes. Permite externalizar la gestión de las telecomunicaciones.”

3.2 Bases aspectos técnicos y estándares de VoIP

3.2.1 Los estándares de compresión. Codecs de VoIP

El ancho de banda que históricamente se ha estimado necesario (a través de estudios de potencia de ondas sonoras para las distintas frecuencias y encuestas de legibilidad) para transportar la voz con suficiente calidad y legibilidad son entre los 3100 Hz y los 3400 Hz.

Debido a que los filtros (analógicos) con caídas muy abruptas son muy difíciles de construir (o muy caros para implementarlos en todos los equipos terminales) también históricamente se han utilizado 4 KHz en banda base para recoger esa señal de voz.

Por el teorema de Nyquist (o teorema de muestreo), al menos el doble de ese ancho de banda es necesario al digitalizar esa señal banda base, por lo que necesitamos 8 khz u 8000 muestras/seg de esa voz.

En el mundo digital se ha estimado que 8 bits suponen una resolución y calidad suficiente (ruido granular bajo en términos relativos a la hora de seguir el nivel de la onda) por lo que $8000 \text{ muestras/seg} * 8 \text{ bits} = 64 \text{ kbps}$, que es lo que se describe bajo el estándar PCM (Pulse Code Modulation, Modulación por impulsos codificados) y recogido en las normas G.711/G.713 (abarcen la cuantificación y codificación).

Adicionalmente para permitir mayores tolerancias en los niveles de la voz y para no perder legibilidad se utiliza una conversión logarítmica (llamada compansión) sobre la señal digital (leyes A en Europa o μ en USA y Japón).

Este conjunto de reglas estandarizadas que definen el proceso de digitalizar (y en otras situaciones comprimir) la voz es lo que denominamos codec. Por dar una definición más formal, podríamos decir que un codec, codificador-decodificador, es un algoritmo (implementado en software o en hardware) que sirve para digitalizar y comprimir

(que correspondería a la codificación) señales de audio y de vídeo (y también para el proceso inverso, la decodificación).

En el momento en que realizamos este proceso, cometemos un error, puesto que no vamos a poder volver a reproducir exactamente la señal original (aunque, al filtrar sólo los 4khz banda base ya estábamos eliminando buena parte de la señal, ahora perderemos un poco más todavía). Veremos que habrá varios niveles de calidad según el codec utilizado, y también de ancho de banda necesario, incluso algunos consiguen gran calidad y poco ancho de banda necesaria, pero a costa, normalmente, de una mayor complejidad y un mayor retardo.

Así pues, vamos a ver una lista no exhaustiva de *códecs* de audio existentes, agrupados según las técnicas usadas para analizar la voz.

3.2.1.1 Técnicas basadas en formas de onda

Empezamos con maneras de comprimir esta voz digitalizada en formato PCM. Las más sencillas son ADPCM (Adaptative Differential PCM, PCM adaptativo diferencial) y CVSD (Continuously Variable Slope Delta, codificación a incrementos de una envolvente

continuamente variable), ambas basadas en la “compresión” de la forma de onda.

3.2.1.1.1 PCM (G.711/G.713)

Abarcan la cuantificación y codificación, explicado en el apartado 3.2.1.

3.2.1.1.2 ADPCM

ADPCM (G.726/G.727) transmite una muestra (valor absoluto, al estilo/igual que PCM) y sus diferencias (posteriormente diversas modificaciones del estándar permitían transmitir alguna muestra patrón periódicamente, para solucionar problemas de pérdida de datos). Por lo tanto su algoritmo es muy sencillo, su retardo muy bajo (<1 ms) y su calidad muy buena (a 32 kbps, para la que fue diseñada inicialmente ADPCM, G.721), basada en el hecho, de que normalmente cuando una persona habla mantiene más o menos un nivel de voz.

Cambios lentos en el nivel son recogidas rápida y perfectamente por el algoritmo. Con un cambio muy brusco se hace un cambio de escala (equivalente a transmitir una muestra completa) y posteriormente se vuelven a transmitir las

diferencias. El intervalo de adaptación es tan pequeño que es imperceptible para un oído humano convencional.

3.2.1.1.3 Técnicas CVSD

Las técnicas CVSD básicamente son parecidas a ADPCM de 1 bit, pero elevando la tasa de muestreo para recorrer mejor la forma de onda original. No tiene ninguna ventaja actualmente. La calidad es únicamente media para 32 kbps, por lo que ADPCM le sustituyó. Por debajo de 16 kbps prácticamente no se podía usar porque la calidad era muy mala. Sin embargo las técnicas CVSD (ya que realmente no era un estándar, sino que cada fabricante lo implementaba de una manera particular) fueron bastante populares en el pasado en multiplexores de voz, ya que CVSD es una técnica muy sencilla que no precisaba de conversión $A \rightarrow D$, siendo por lo tanto mezcla entre analógico y digital.

3.2.1.2 Técnicas basadas en vocoders

Son las que menor ancho de banda utilizan (por debajo de 2.4 kbps, incluso se pretende llegar hasta 1

kbps), sin embargo la calidad de voz es baja, su retardo alto, igual que su carga de proceso. Utilizan complejos modelos matemáticos de la voz humana, a través de los cuales obtienen ciertos parámetros particulares de la conversación en curso y son transmitidos. Se consigue entender la conversación, pero no se reconoce a la persona con la que se habla.

Generalmente no se usa comercialmente, y sí militarmente, donde un bajo régimen binario facilita una compleja encriptación (por motivos de seguridad) a mucho menor coste.

3.2.1.3 Técnicas mixtas

Las técnicas más ampliamente utilizadas son las mixtas, que utilizan libros de códigos más sencillos (que los vocoders) y que añaden más información sobre la onda (que los vocoders).

Las tres más utilizadas son las CELP (y sus variantes), las RPE-LTP (única posibilidad en teléfonos GSM antiguos y muy usada en VoIP en Internet) y las VSELP (teléfonos móviles americanos).

3.2.1.3.1 RPE-LTP (Regular Pulse Excitation – Long Term Prediction) (G.723)

Sencillo (poca potencia necesaria, basta con 4 MIPS) y bastante popular.

Se utiliza en Internet para audio-conferencias (popularmente llamados chats de voz), telefonía y en los teléfonos móviles GSM (es el modo FR – Full Rate) a 13 kbps y su calidad es buena, similar a la línea analógica tradicional, para ese régimen binario. Su retardo de generación de trama habitual es de 20 ms.

Una posterior incorporación al estándar, la G.723.1 únicamente utiliza 5,33 kbps ó 6,40 kbps (G.723.1) (técnicamente se convierte en Multi-Pulse ACELP, MP-ACELP). Se mantiene prácticamente la calidad en el caso de 5,33 kbps e incluso con 6,4 kbps aumenta un poquito respecto a la especificación inicial, a costa de aumentar por 4 la potencia de proceso necesaria y de triplicar su retardo (de hecho, al igual que veremos con G.729,

el análisis correlativo de la voz añade otros 8ms de retardo/latencia).

Por sus características, calidad y reducido ancho de banda requerido, esta G.723.1, en sus 2 variantes de 5,33 y 6,40kbps, es uno de los codecs más usados para VoIP.

3.2.1.3.2 CELP (Code book Excited Linear Prediction):

Variantes:

- LD-CELP (Low Delay CELP) (G.728): 16 kbps. 5 ms generación de trama.
- ACELP (Algebraic CELP).
- CS-ACELP (Conjugated Structure ACELP) (G.729, G.729a): Usado hoy en GSM a 12,2 kbps, aunque el estándar ITU-T G.729 define como régimen binario únicamente 8 kbps. 25 ms de generación de trama.
- CELP FS-1016 (estándar de comunicaciones seguras en EEUU): 4.8 kbps.

Características comunes:

- Alta calidad con alta compresión.

- Alta capacidad de proceso necesaria y gran retardo.
- Problemas con modem/fax, e incluso con los tonos DTMF (acceso a facilidades de operadora).

Estos problemas con modem/fax de estos codecs no son triviales. Veremos como las PBX/gateways han de anticiparse detectando los tonos correspondientes mucho antes de proceder a su compresión y encaminando esa llamada de datos o transmitiendo esos tonos por una ruta no comprimida. En el caso del fax (definido en el T.30), existen dos protocolos:

- T.37, *Fax Store&Forward*, que convierte un fax en un adjunto de un *e-mail*.
- T.38, también conocido como FoIP, *Fax over IP* o *Real Time Fax*, que convierte la llamada de fax en datos que transmite directamente por la red y en destino invierte el proceso.

3.2.1.3.3 LD-CELP (G.728)

Por su bajo retardo (5 ms) y relativamente alto régimen binario (16 kbps), precisa de unos 40 MIPS en el DSP, potencia muy elevada comparada con el resto de técnicas, y aunque utilice un libro de códigos menor, las operaciones de análisis de la voz con las restricciones de bajo retardo/tiempo real características de LD-CELP, suponen una carga de proceso importante.

Además tiene el inconveniente de que no utiliza técnicas de correlación (análisis de la señal), por lo que la interpolación de tramas perdidas no funciona como en los CS-ACELP o MP-ACELP.

Como ventaja decir que con LD-CELP aún se pueden transmitir datos a 2.4 kbps.

3.2.1.3.4 CS-ACELP (G.729 y G.729a)

Con la revisión a del estándar de la ITU-T se mejoró ligeramente la calidad del sonido y se redujo a la mitad la potencia necesaria para su implementación (de 20 a 10 MIPS para 8 kbps). El

retardo de generación de trama típico se sitúa en unos aceptables 25 ms.

Bajo la capacidad de un teléfono móvil GSM de hoy día de utilizar EFR (Enhanced Full Rate) está usándose por debajo una codificación CS-ACELP a 12.2 kbps.

Con 12.2 kbps se puede dar la impresión de estar ante una calidad de audio superior a la línea telefónica analógica tradicional, pero inferior a una digital de RDSI (G.722, se utilizan 7 KHz. en 64 kbps, lo cual se acerca a calidad musical de radio FM), con lo cual nos podemos hacer una idea de lo popular que es hoy en día (sin embargo, conviene recordar que en G.729 el régimen binario se limita a 8kbps).

Un aspecto muy importante de CS-ACELP es que sigue funcionando correctamente cuando se pierden paquetes debido a que utiliza interpolación para dichos paquetes (interpolación que funciona dignamente debido a los análisis correlativos a los que la voz es sometida en este protocolo, y que imponen 5ms adicionales de latencia/retardo). Con pérdidas de hasta el 5 %, la calidad de voz sigue

siendo muy buena, con 5 – 10 % la calidad es correcta y con hasta el 20 % de pérdida y según los casos (la estadística de esas pérdidas), se puede llegar todavía a tener una conversación inteligible.

3.2.1.4 Comparativa resumen de codecs y aspectos técnicos de los mismos

Se muestra a continuación en la Tabla 1, casos típicos de paquetización de los distintos codecs, el grado de compresión, el ancho de banda consumido a nivel IP con y sin compresión de cabeceras y con el uso de PPP tal y como se utilizará.

Codec	Grado de compresión	BW neto de la voz (kbps)	Tiempo de generación de trama (ms)	Longitud de trama (bytes)	Tamaño paquete IP (bytes)	BW IP (Kbps)	BW IP con cRTP (Kbps)	BW nivel de enlace: cRTP+PPP (kbps)
G.711	1:1	64	20	160	200	80	65,6	67,2
G.726	2:1	32	10	40	80	64	34,4	39,2
G.726	2.5:1	24	10	30	70	56	26,4	31,2
G.728	4:1	16	10	20	60	48	18,4	23,2
G.729A	8:1	8	20	20	60	24	9,6	11,2
G.729A	8:1	8	60	60	100	13,3	---	---
G.723.1	10:1	6,4	60	48	88	11,7	6,8	7,6
G.723.1	12:1	5,33	60	40	80	10,7	5,7	6,5

Tabla 1 Efectos del tipo de *códec*, tamaño de la muestra, uso de cRTP en el ancho de banda.

No obstante, existen cierta libertad a la hora de paquetizar los distintos *codecs*, tal y como muestra la Tabla 2.

Codec	Rango de tamaño en bytes de la trama	Tamaño por defecto de la trama (en bytes)	Régimen binario de la voz
G.711	40-240	160	64kbps
G.723.1 a 5.3kbps	20-240	40	5.3kbps
G.723.1 a 6.4kbps	24-240	48	6.3kbps
G.726 a 32kbps	20-240	40	32kbps
G.726 a 24kbps	15-240	30	24kbps
G.726 a 16kbps	10-240	20	16kbps
G.728	10-240	10	16kbps
G.729a	10-240	20	8kbps

Tabla 2. Rangos de los tamaños de paquete posibles para los distintos codecs

3.2.2 Protocolos de red y transporte en los que se apoya VoIP

Veremos en este apartado los protocolos de red y transporte específicos de los que se vale la VoIP para tratar de cumplir sus objetivos lo más eficientemente posible. No es el objetivo de este apartado mostrar UDP, TCP o IP, por tanto se tratarán principalmente RTP y RTCP.

RTP provee servicios de envío y recepción de información con características de tiempo real. Estos servicios incluyen la caracterización de la carga útil de los paquetes, asignación del número de secuencia, establecimiento de sellos temporales y monitorización del envío. Las aplicaciones, habitualmente ejecutan estas conferencias sobre el protocolo

de transporte UDP y hacen uso de los servicios que ofrecen los niveles inferiores.

A continuación, se va a desarrollar detenidamente esto, viendo la relación entre VoIP y RTP, y de cómo se apoyan en UDP e IP; así como las principales características del RTCP.

Es conocido que la arquitectura de protocolos TCP/IP, a nivel de transporte, tiene 2 posibilidades, dos tipos de tráfico: UDP (User Datagram Protocol, protocolo de datagramas de usuario) no orientado a conexión y TCP (Transmisión Control Protocol, protocolo de control de transmisión), orientado a conexión y fiable, por lo que no es adecuado para la transmisión de datos en tiempo real, ya que da prioridad a la fiabilidad y no a la entrega inmediata de la información.

La transmisión fiable proporcionada por la retransmisión típica de TCP es indeseable, pues en caso de retransmisión, los paquetes retransmitidos aumentarían el retardo, lo cual en el escenario que estamos, es hasta más nocivo que la pérdida del paquete (pues si llega tarde, ya será inútil, y además la retransmisión provoca una mayor saturación de la red). Además, como vimos en el apartado 3.2.1, algunos codecs permiten que algunos paquetes puedan perderse y la calidad de la voz seguir siendo suficiente.

Por ello, debido a la naturaleza sensible al tiempo del tráfico de voz, UDP/IP fue la elección lógica para transportar la voz. Sin embargo, se necesitaba más información en una base paquete a paquete de la que ofrecía UDP. Por tanto, para el tráfico en tiempo real o sensible al retraso, el Internet Engineering Task Force (IETF) adoptó el RTP. VoIP circula en la parte superior del RTP, que transita a su vez en la parte superior del UDP. Así, VoIP es transportado con una cabecera de paquetes RTP/UDP/IP.

3.2.2.1 RTP

Como su nombre indica, el protocolo RTP (*Real-time Transport Protocol*), proporciona servicios de audio y vídeo en tiempo real extremo a extremo sobre una red de paquetes; dando a las estaciones receptoras información que no está en las corrientes UDP/IP sin conexión.

El proceso de transporte implica dividir en paquetes el flujo de bits que proporciona el codec, enviar dichos paquetes por la red y reensamblar el flujo de bits original en el destino. Este proceso resulta bastante complejo debido a que existen pérdidas de paquetes, retrasos diferentes en su viaje por la red e incluso una alteración en el orden en que llegan al

receptor. Por tanto, el protocolo de transporte debe permitir al otro extremo detectar todas estas pérdidas. Además, también debe proveer de información temporal para que el receptor pueda compensar el jitter (variabilidad del retardo). Para cumplir todos estos requerimientos, el RTP define:

- Formato de los paquetes, que se divide en dos partes: la cabecera y la carga útil. La primera proporciona al receptor la información necesaria para reconstruir el flujo de *bits*, mientras que la segunda constituye el propio flujo de bits.
- Mecanismo empleado para fragmentar el flujo de información de paquetes.

Como se dijo en la introducción de este apartado, RTP no proporciona mecanismos fiables de entrega de datos, sino que dicha responsabilidad recae en los niveles inferiores. Tampoco garantiza una entrega correcta de la información, ni el orden de llegada de los paquetes y, por tanto, los usuarios deben asumir que la infraestructura de red es lo suficientemente fiable para desarrollar estas funciones con la calidad requerida.

El propósito inicial del protocolo RTP era soportar multicast, esto es, aplicaciones de conferencia y entornos broadcast en los que se utiliza la difusión para distribuir información. Es importante señalar que RTP no realiza ninguna reserva de recursos a fin de evitar la pérdida de paquetes y el jitter, sino que permite al receptor recobrar la información en presencia de éstos. De esta forma, se puede utilizar RTP para servicios interactivos como la telefonía por Internet.

Aunque RTP fue creado para satisfacer las necesidades de los participantes en conferencias multimedia, no se limita a esta función y desarrolla un gran número de tareas de control. A continuación, se pasan a describir todas las funciones que realiza el protocolo:

- **Fragmentación:** cada paquete RTP contiene un número de secuencia empleado para la detección de pérdidas durante el reensamblado del mensaje en recepción.
- **Sincronización intramedia:** los paquetes del mismo flujo pueden sufrir retardos diferentes,

dando lugar a la aparición del jitter. Para compensarlo, las aplicaciones emplean buffers que utilizan las marcas temporales proporcionadas por RTP para medir este jitter.

- **Identificación del tipo de carga:** en una red de paquetes, tanto las condiciones de la red como la pérdida de paquetes y el retardo de los mismos varían incluso en el transcurso de una misma llamada. Los codecs se diferencian en su capacidad para trabajar adecuadamente bajo distintas condiciones de pérdidas (tal y como se ha visto a lo largo del capítulo 3.2.1). Por tanto, es deseable ser capaz de cambiar dinámicamente la codificación de la información (es decir, de la carga útil) en la misma medida en que varían las condiciones de la red. Para ello, RTP contiene un identificador del tipo de carga en cada paquete, el cual describe el tipo de codificación que se ha empleado en su generación.
- **Indicación de trama:** las señales de audio y vídeo se envían en unidades lógicas

denominadas tramas. Es necesario indicar al receptor el principio y el fin de cada una de las tramas, a fin de que pueda sincronizarse con niveles superiores, para lo que se emplea un *bit* de marca.

- **Identificación de fuente:** en una sesión *multicast* existen varios usuarios participantes y debe haber algún modo de poder identificar al usuario que generó un determinado paquete. Ésta es la misión del campo SSRC (*Synchronization Source*).

Las funciones anteriores se soportan gracias a la cabecera de RTP que se puede ver en la parte superior de la Figura 1 donde se observan los siguientes campos:

- **Versión (2 *bits*):** identifica la versión del protocolo.
- **Identificador de Relleno o Padeo (1 *bit*):** determina que el paquete contiene octetos de relleno, en caso de estar activado. El último

octeto advierte del número de *bytes* que se han sido añadidos como relleno.

- **Extensión (1 *bit*):** describe el tipo de cabecera; y en caso de estar activo el formato de la cabecera sería extendido.
- **CSCR (*Count o Contributing Source Count*) (4 *bits*):** contiene el número de participantes que han contribuido en los datos.
- **Marcador (1 *bit*):** este valor es interpretado por los protocolos como un evento o paquete específico. Puede emplearse, por ejemplo, para describir los paquetes finales de un flujo, indicando que éste va a finalizar.
- **Tipo de carga útil (7 *bits*):** identifica el formato de la carga de RTP y, por tanto, el tipo de interpretación que debe realizar la aplicación de la misma.
- **Sello Temporal o *Timestamp* (32 *bits*):** refleja el instante de muestreo del primer octeto del paquete. Este campo permite

establecer cálculos para determinar el *jitter* en la recepción y sincronizar la comunicación. Por lo tanto, este campo será de vital importancia en lo que respecta a la medición de parámetros de QoS.

▪ **SSRC o Synchronization Source (32 bits):**

fija un identificador para los paquetes de un determinado flujo. De esta forma, se puede establecer una recuperación de sincronismo en el destino.

V=2	P	X	CC	M	PT	Número de secuencia	
Marca para la temporización							
identificador de origen de sincronización							
Puerto de origen						Puerto de destino	
Longitud						Suma de verificación	
Versión		IHL		Tipo de servicio		Longitud total	
Identificación						Indicaciones	Compensación. de fragmentos
Tiempo de existencia				Protocolo		Suma de verificación de la cabecera	
Dirección de origen							
Dirección de destino							
Opciones							Relleno

Figura 1 Cabeceras RTP, UDP e IP

Así pues, se ve que la cabecera que añade RTP a los datos generados por el nivel de aplicación, describe la información necesaria para la correcta transmisión y recepción de los paquetes, y que

consta de al menos 12 bytes, dependiendo del número de participantes en la conferencia.

RTP es, por lo tanto, imprescindible para el tráfico en tiempo real, pero existen algunos inconvenientes. Las cabeceras IP/RTP/UDP tienen 20, 12 y 8 bytes, respectivamente. Esto se agrega a una cabecera de 40 bytes que es dos veces más grande que la carga útil cuando se utiliza G.729 con dos muestras de voz (20 ms); lo que supone una excesiva sobrecarga, tal y como se vio en la Tabla 1.

Se puede comprimir esta gran cabecera a de 2 a 5 bytes utilizando cRTP (cRTP, Compressed RTP, también llamado genéricamente Header Compression, Compresión de cabeceras).

3.2.2.1.1 cRTP

El proceso se lleva a cabo por el router que da salida a la WAN. PPP, FRL, HDLC y RDSI son los protocolos de nivel 2 que permiten esta característica.

Se muestra en la Figura 2 cómo efectúa el proceso un router de Cisco.

Básicamente, cRTP funciona porque aunque cada paquete puede tener una gran variedad de valores a lo largo de los 40bytes de cabeceras involucradas, las diferencias de paquete a paquete (entre paquetes seguidos, relacionados) son pequeñas, que son las que se codifican. En destino, se reconstruyen con menor esfuerzo. En principio, cRTP está más indicado para enlaces de baja velocidad, donde la complejidad del proceso produce más ganancia e incluso disminuye el retardo. Sin embargo, en enlaces más rápidos y/o gran cantidad de paquetes a comprimir con cRTP, la compresión puede aumentar significativamente el retardo. Para ello, algunos routers implementan técnicas compatibles con el estándar para minimizar este retardo, por Ej., en Cisco, “Express cRTP” (en Cisco 2600 en adelante) o más aún dcRTF (Distributed cRTF) (en Cisco 7500 y superiores, ya orientados a Operadores de Telecomunicaciones).

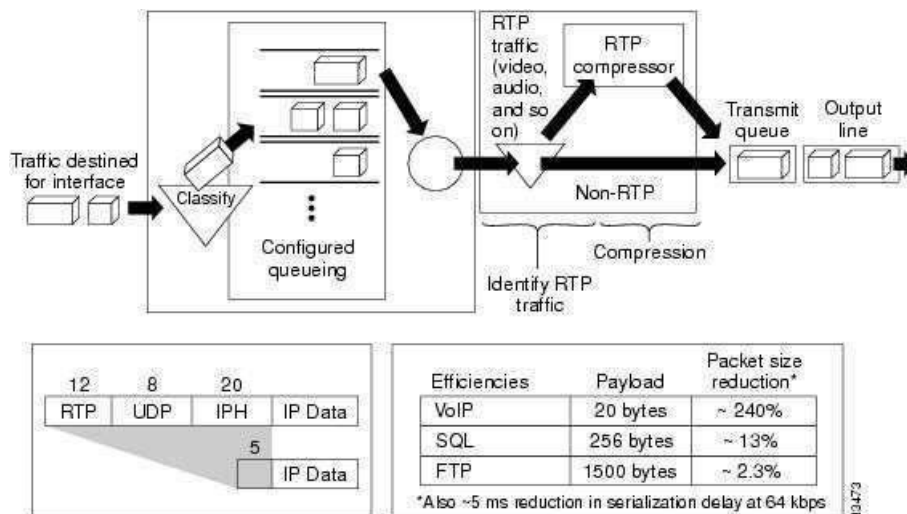


Figura 2 Funcionamiento de cRTP

3.2.2.1.2 sRTP

Otra variante sobre RTP es sRTP (secure RTP). sRTP (definido en la RFC3711, en estado de propuesta de estándar) es ideal para proteger tráfico de VoIP porque puede ser usado junto con cRTP y no tiene apenas efectos en la QoS (es otro elemento que potencialmente añade retardo, pero mucho menos que cRTP), por lo que nos interesa especialmente. Estos hechos proporcionan enormes ventajas, especialmente en *códecs* de baja tasa binaria, como por Ej. G.729 y G.723.1.

sRTP pues, cubre el hueco de aportar seguridad sobre IP en comunicaciones en tiempo

real, en las que, por ineficiencia, no era de aplicación IPsec.

3.2.2.2 RTCP

El protocolo RTCP se basa en la transmisión periódica de paquetes de control entre los participantes de la sesión RTP. De hecho, emplea los mismos mecanismos que RTP y deberían ser los niveles subyacentes los que provean servicios de multiplexación y control de los paquetes.

RTCP desarrolla cuatro funciones primordiales:

- **Evaluación de la Calidad:** La primera de las tareas desarrolladas por RTCP sirve como elemento de control para la distribución de los paquetes. De esta forma, las entidades tendrán información sobre el estado del resto de participantes, permitiendo, de este modo, la resolución y prevención de problemas.
- **Identificación de la Fuente RTP:** El protocolo RTCP transporta un identificador a nivel de transporte del origen de datos RTP. Este

identificador recibe el nombre de CNAME (*Canonical Name*) y permite establecer mecanismos de sincronización entre las distintas sesiones RTP, por Ej. entre la señal de audio y vídeo.

- **Caracterización de la Tasa de transferencia:** La tercera función del protocolo RTCP permite adaptar la tasa binaria de las distintas entidades en función del número de participantes involucrados.
- **Identificación de Usuarios:** Finalmente, este protocolo puede servir como referencia para presentar en los interfaces de usuario los identificadores del resto de participantes en la conferencia. De esta forma, se añade un nuevo servicio a la mera monitorización de la conferencia.

El protocolo RTCP permite mecanismos de envío de información sobre el estado de la comunicación realizada sobre RTP, tanto al receptor como al transmisor. Para ello, envía mensajes de información de tipo SR (*Sender Report*) si han sido enviados por la

entidad que inició la conferencia, o bien, RR (*Receiver Report*) si han sido enviados por el destinatario.

En ocasiones, el protocolo RTCP puede enviar mensajes a los participantes de la conferencia en los que se describen las operaciones realizadas y la gestión de los servicios propuestos por RTP. De esta forma, se añaden los mensajes SDES (*Source Description*) que determina la entidad que origina los datos y en los que se incluye el CNAME, APP (*Application Defined*) que define el acceso a los servicios de aplicación y BYE, que da por finalizada la sesión de RTP.

Diferentes mensajes pueden ser encapsulados dentro del mismo paquete RTCP. De esta forma, se debe señalar en el inicio del mensaje el tamaño del mismo e identificar los siguientes mensajes incorporados en el paquete.

3.2.3 Calidad de servicio (QoS) en VoIP

La calidad de servicio (QoS, *Quality of Service*) tiene una gran variedad de significados. Normalmente, QoS hace referencia tanto a la clase de servicios (CoS, *Class of Service*) como al tipo de servicio (ToS, *Type of Service*). El objetivo

básico de éstos es conseguir el ancho de banda, retardo y variación del mismo necesarios para una aplicación determinada.

Una CoS permite al administrador de la red agrupar diferentes flujos de paquetes, teniendo cada uno requisitos de latencia y ancho de banda diferentes. Un ToS es un campo (actualmente de tres *bits*, lo que permite agrupar ocho flujos de paquetes o CoS) en una cabecera de Protocolo Internet (IP) que permite que tenga lugar una clase de servicio.

Así, los nuevos servicios basados en IP generan nuevos tipos de tráfico que varían tremendamente en sus requerimientos. Generalmente, estos nuevos tipos de aplicaciones incorporan gráficos de alta resolución, vídeo, audio..., lo que conlleva una mayor demanda de ancho de banda. Por otra parte, puede tratarse de flujos de datos multimedia (con transmisión simultánea de múltiples tipos de información relacionada con la misma fuente, una complementando a la otra) en tiempo real con estrictos requerimientos de temporización, fiabilidad o funcionalidades *multicast*.

Asimismo, todos estos factores requieren una óptima asignación de recursos con objeto de ofrecer el servicio

solicitado sin penalizar por ello, a otro tipo de aplicaciones a usuarios. Hasta ahora, IP ha proporcionado un servicio *best-effort*, donde los paquetes se almacenan y envían sin garantía de servicio y los recursos de red se comparten equitativamente, por lo que para poder responder a estas nuevas funcionalidades es necesario añadir un cierto grado de QoS a la red. De esta forma, se ve que los servicios tradicionales de la red Internet disponen de una calidad denominada "*best effort*"; es decir, que la red ofrece el mejor esfuerzo posible para satisfacer los retardos mínimos; lo cual puede no ser óptimo, pero sí suficiente para servicios que no requieren tiempo-real como el *web*. En cambio, para servicios en tiempo real, como la VoIP, se busca un retardo mínimo y una variación de este también mínima.

Finalmente, a partir de los requerimientos de los usuarios, se pueden deducir un conjunto de requerimientos funcionales que se deberán traducir en una serie de requerimientos técnicos por parte de la red.

Así, el objetivo fundamental que debe perseguirse es encontrar una forma de relacionar la calidad de servicio que la red puede aportar con la calidad de servicio percibida por el usuario final (*mapping* QoS), ya que éste es quien finalmente va a determinar que un servicio tenga o no tenga éxito.

Además, hay que apuntar que se puede disponer de varias herramientas para conseguir la necesaria QoS para un usuario o aplicación. Pero, es importante anotar que las herramientas utilizadas para implementar estos servicios no son tan importantes como el resultado final conseguido así pues para cada situación y parámetros de red hay que determinar qué herramientas utilizar para optimizar los resultados.

3.2.3.1 Parámetros de QoS

Se puede concluir que se entiende por calidad de servicio la posibilidad de asegurar una tasa de datos en la red (ancho de banda), un retardo y una variación de retardo (*jitter*) acotados a valores contratados con el cliente. En las redes Frame Relay o ATM la calidad de servicio se garantiza mediante un contrato de **CIR** (*Committed Information Rate*) con el usuario. Para disponer de una calidad de servicio aceptable en redes soportadas en protocolo IP, se han diseñado protocolos como RTP (visto en el apartado 3.2.2.1) y RSVP (analizado en detalle en el Apéndice A.2). Por otro lado, un problema evidente es que cuando se soporta un servicio de voz sobre IP (VoIP), por ejemplo, los paquetes son cortos y el encabezado es largo

comparativamente. En este caso, se requiere un encabezado reducido y un proceso de fragmentación e intercalado LFI (Link Fragmentation & Interleaving). Mediante **QoS** (*Quality of Service*) se tiende a preservar los datos con estas características.

Ahora se van a analizar los parámetros que interesa destacar y que más adelante, en el desarrollo de las pruebas, se necesitarán conocer con mayor detalle: retraso o latencia, *jitter* y ancho de banda.

3.2.3.1.1 Retardo/Latencia

El retardo o latencia en VoIP se caracteriza por el tiempo que tarda la voz en salir de la boca del que está hablando y en llegar al oído del que está escuchando.

Existen tres tipos de retardo que son inherentes a las redes de telefonía actuales: de **propagación**, de **serialización** y de **manejo**. El retardo de propagación es causado por la velocidad de la luz en la fibra óptica o en las redes basadas en cobre. El retardo de manejo, también llamado retardo de procesamiento, define muchas causas diferentes

de retraso (empaquetado, compresión y *switching* de paquetes), y está causado por dispositivos que transmiten la trama a través de la red.

El retardo de serialización es la cantidad de tiempo que se tarda en colocar un *bit* o *byte* en una interfaz (su influencia es relativamente pequeña normalmente).

3.2.3.1.2 Variación del retardo (*jitter*)

La variación del retardo (*jitter*) es un problema que existe sólo en las redes basadas en paquetes. Cuando está en un entorno de voz por paquetes, el remitente espera transmitir de forma fiable paquetes de voz en un intervalo regular (por ejemplo, enviar una trama cada 20 *ms*). Esos paquetes de voz se pueden retrasar por toda la red de paquetes y no llegar con el mismo intervalo de tiempo regular a la estación receptora (por ejemplo, puede que no sean recibidos cada 20 *ms*). La diferencia entre cuándo se esperaba recibir el paquete y cuándo se recibe en realidad es lo que se llama *jitter*. Es por ello, que es necesario un *buffer de jitter* (según interpretaciones

también es llamado buffer de *de-jitter*) que oculte esta variación retraso.

Cuanta más *jitter* haya, más necesitará ser compensado el *buffer* de *jitter* por la impredecible naturaleza de la red de paquetes.

Si la red de datos está bien construida y se toman las precauciones apropiadas, la variabilidad del retardo es normalmente un problema menor y el *buffer* de *jitter* no contribuye significativamente al retraso total de extremo a extremo.

Es aquí, donde las *timestamps* de RTP juegan un papel importante, al ayudar a determinar qué el *jitter*, si lo hubiera, existe dentro de la red.

3.2.3.1.3 Ancho de banda

Por último, el ancho de banda es uno de los parámetros más importantes a la hora de diseñar una red VoIP. Dependiendo de qué *códec* se esté utilizando y de cuántas muestras de voz se quiera por paquete, la cantidad de ancho de banda por llamada puede incrementarse drásticamente.

La tabla 1 muestra varios de anchos de banda que puede consumir un codec en función de varios parámetros como la “altura” de la torre de protocolo en la que lo midamos, el número de muestras en cada trama, de si se usa o no compresión de cabeceras, etc.

Como ejemplo recojamos el llamativo caso de G.729. Si G.729 utiliza dos muestras de *10 ms*, consume *20 bytes* por trama, lo que supone *8 kbps*. Las cabeceras del paquete, que incluyen IP, RTP y el UDP, añaden *40 bytes* a cada trama. Como vemos, la cabecera de los protocolos involucrados (llamado normalmente *overhead* de protocolo) es el doble de la cantidad de la carga útil/neta (*payload*).

De la misma manera, hay que tener en cuenta que el ancho de banda que suponen las cabeceras de la capa 2 (PPP, *Frame Relay*...). Por tanto, la misma llamada G.729 puede consumir diferentes cantidades de ancho de banda, dependiendo de qué capa de enlace de datos se utiliza (*Ethernet*, *Frame Relay*, PPP, etc.).

3.2.3.2 Medida de Parámetros de QoS

La medida de los parámetros QoS del nivel de red deben traducirse en parámetros QoS a nivel de usuario; ya que el aspecto esencial de la evaluación de un servicio es la opinión que los usuarios de dicho servicio tienen de él, dado que éste expresa su grado de satisfacción y es lo que determina finalmente que una aplicación o servicio sea o no un éxito. Por lo tanto, para que se cumpla el objetivo final de la red, que no es otro que dar servicio a los usuarios finales, son necesarios tanto los parámetros de red como los de usuario, y, por lo tanto, también la definición de una relación cuantitativa entre ellos.

Se debe tener especial cuidado en separar las funciones que tienen lugar en los límites de la red de aquellas que ocurren en el corazón o *backbone* de la misma. Es importante separar ambas funciones para conseguir la mejor calidad de servicio (QoS) posible.

3.2.3.2.1 Variantes de los Parámetros QoS

Básicamente, la QoS tiene cuatro variantes: la QoS que el usuario desea, la que el proveedor

ofrece, la que el proveedor consigue realmente y la que el usuario percibe finalmente. En cualquiera de ellas existen algunos parámetros muy condicionados por las características técnicas de la red.

La identificación de un conjunto de parámetros de red es algo necesario para realizar una buena gestión de ella. La clasificación de los parámetros se realiza atendiendo a dos categorías:

- **Métricas:** miden los atributos QoS cuantificables y se dividen a su vez en métricas de rendimiento, niveles de seguridad e importancia relativa.
- **Políticas:** miden principalmente políticas de gestión y los niveles de servicio, describen las especificaciones del comportamiento del sistema.

Las métricas de rendimiento de nivel de red se dirigen a dos principales aspectos: la disponibilidad y la sensibilidad. La disponibilidad de red puede caracterizarse por métricas tales como conectividad, tasa de errores, probabilidad de pérdidas de

paquetes; mientras que las métricas comunes de sensibilidad de red son retardo unidireccional, latencia ida y vuelta, jitter y ancho de banda disponible.

Es muy importante determinar las características de cada aplicación (flujos de tráfico, longitudes de los paquetes...), los parámetros que determinan su funcionamiento y de los que se debe llevar a cabo un mayor control, para poder satisfacer adecuadamente los requerimientos demandados por los usuarios finales.

El diseño de cualquier red se verá beneficiado por un conocimiento detallado de las aplicaciones y servicios que deberá soportar; ya que en caso contrario, no se podrán determinar cuáles deben ser las prestaciones de la red.

3.2.3.3 Modelos de QoS

Los servicios de datos y multimedia tienen distintos requerimientos de calidad principalmente en lo que se refiere a la latencia/retardo y *jitter*. Para satisfacer los requerimientos de calidad se acude al

manejo de las colas de paquetes, la reserva de ancho de banda y la gestión del tráfico. Para obtener estos objetivos en diversos ámbitos se han usado distintos modelos de QoS.

3.2.3.3.1 Tipos de modelos de QoS

Se detallan aquí los distintos modelos de QoS: clase de servicio en redes LAN, tipo de servicio sobre protocolo IP y calidad de servicio sobre redes IP. Por otro lado, se han definido las características de la calidad de servicio que también serán descritas: servicio garantizado (mediante reserva de ancho de banda), diferenciado (mediante prioridad de tráfico) y el "mejor esfuerzo".

- **CoS (*Class of Service*):** CoS se logra mediante 3 bits que se ingresan en un campo adicional de 4 *bytes* (etiqueta denominada *Tag* o *Label*) dentro del protocolo MAC. Estos 3 *bits* permiten definir prioridades desde 0 (máxima) a 7 (mínima) y ajustar un umbral en el buffer de entrada y salida del *switch* LAN para la descarga de paquetes. Para más detalles, ver el servicio VLAN que es

soportado por esta versión de funcionamiento para servicios de capa 2. Se ocupa la IEEE 802.x en los siguientes estándares:

- **.IEEE 802.1p.** Determina el uso de un *Tag* en el encabezado de MAC con 3 bits de precedencia. Se define el protocolo para registro de CoS **GARP** (*Generic Attribute Registration Protocol*). Las aplicaciones específicas del GARP son el registro de direcciones *multicast* **GMRP** (*Multicast GARP*) y de usuarios VLAN con protocolo **GVRP** (*LAN GARP*).
- **.IEEE 802.1Q.** Servicio VLAN para realizar enlaces troncales punto a punto en una red de *switch*.
- **.IEEE 802.3x.** Este *standard* examina el control de flujo en enlaces *Ethernet* del tipo *full-duplex*. Se aplica en enlaces punto-a-punto (*Fast y Gigabit Ethernet*). Si existe congestión, se emite hacia atrás un paquete llamado "*pause*"

frame" que detiene la emisión por un período de tiempo determinado. Una trama denominada "*time-to-wait zero*" permite reiniciar la emisión de paquetes.

- **.IEEE 802.1D.** Define el protocolo **STP** (*Spanning-Tree Protocol*). Se diseñó para permitir que en una red de *bridge* y *switch* de muchos componentes se formen enlaces cerrados para protección de caminos. Se intercambia información de la topología de la red que permite construir el árbol. De esta forma, se crean puertas redundantes en el cableado, el protocolo STP deshabilita automáticamente una de ellas y la habilita en caso de falla de la otra. Cada puerto tiene una ponderación en costo (el administrador de la red puede modificar el costo para dar preferencia a cierta puerta).
- **ToS (*Type of Service*):** es sinónimo de CoS en la capa 3. Sobre el protocolo IP se define el

ToS con 3 *bits* (del segundo *byte* del encabezado IP) para asignar prioridades. Se denomina señal de precedencia.

- QoS (*Quality of Service*): en redes IP se define la tasa de acceso contratada **CAR** (*Committed Access Rate*) en forma similar al CIR de *Frame Relay* y ATM. La calidad QoS se ve garantizada mediante protocolos de reserva **RSVP** (descrito en el Apéndice A.2) y de tiempo real **RTP** (descrito en el apartado 3.2.2).

3.2.3.3.2 Clasificación de la QoS

- **Guaranteed/Integrated Services:** se utiliza para obtener un retardo máximo extremo a extremo. Fue introducido por el IETF en 1994 (RFC 1663). Se trata de un servicio análogo al CBR (*Constant Bit Rate*) en ATM. Se puede aplicar un concepto de reserva de tasa de *bit* (mediante el protocolo **RSVP** que se detalla en el Anexo 1) o el método *Leaky-bucket*. Al usuario, se le reserva un ancho de banda dentro de la

red para su uso exclusivo, aun en momentos de congestión. Se le conoce como *Hard QoS* (RFC 2212). En resumen, es un intento de mezclar lo mejor de dos paradigmas opuestos: redes de datagramas (maximizar la utilización de la red mediante multiplexación del tráfico, robustez, adaptación, etc.) y redes conmutadas (ofrecen garantías).

- ***Differentiated Services:*** el servicio diferenciado utiliza la capacidad de particionar el tráfico en la red con múltiples prioridades o **ToS** (*Type of Service*). Se dispone de 3 *bits* de precedencia para diferenciar las aplicaciones sensibles a la congestión (se brindan mediante el encabezado del protocolo IP). Es, por lo tanto, un *Soft QoS*. El control de aplicación es del tipo *leaky-bucket*. Se puede soportar la función **CAR** que permite un manejo del ancho de banda (política de tráfico). La primera línea de defensa frente a la congestión es el uso de *buffer* de datos; lo cual implica el armado de una cola de espera y el retardo correspondiente dependiendo de

la prioridad asignada en dicha cola. Por lo tanto, intenta resolver el problema de QoS demasiado rápido (con un poco más que *Best-effort* es suficiente). Su filosofía es simplista y opuesta al *IntServ* anterior, ya que no hay reservas sino prioridades, no hay flujos y no es de extremo a extremo. *Diffserv* es el protocolo que implementa los servicios diferenciados y se basa en información contenida en la cabecera de cada paquete, marcada con una determinada prioridad.

- **Best-effort:** éste es un servicio por defecto que no tiene en cuenta las modificaciones por la QoS. Se trata de una memoria buffer del tipo FIFO. Por ejemplo, una gran mayoría de clientes VoIP bajo normativa H.323 que trabajan sobre redes LAN y redes corporativas no tienen previsto garantizar la QoS, que se queda como opción para el instalador del servicio.

3.2.3.3.3 Soporte De QoS en IP

La QoS en IP es dada mediante el campo Tipo de Servicio (ToS) que se encuentra en el encabezado IP (RFC 1349, 1812). Los principales problemas de este campo son:

- Proporciona un modelo fijo y limitado para la diferenciación de tráfico.
- El campo de prioridades sólo permite codificar prioridades relativas.
- El campo tipo de servicio es demasiado pequeño y no es usado casi por ningún *router*.

Con el RFC 2474, el campo ToS se sustituye por el campo DS.

Por otro lado, los problemas de QoS en IP:

- **Fragmentación.** Es uno de los mayores problemas de IP que produce congestión; consumo de recursos, tanto de ancho de banda como de CPU.

- **Sobrecarga de control**, puesto que ICMP tiene demasiadas opciones.
- **Rutado ineficiente**, consecuencia de la fragmentación y del reparto ineficiente y descontrolado de las direcciones.

3.2.3.4 La medida de calidad MOS (Mean Opinion Score)

Es razonable que la calificación de un *códec* de audio como “bueno” o “malo”, aparte de basarse en un alto número de detalles técnicos y objetivos, tiene una gran parte de subjetividad. Así, hay dos formas de probar la calidad de la voz: **subjetiva y objetivamente**. Los humanos realizan pruebas de calidad de voz subjetivas, mientras que los ordenadores realizan pruebas de voz objetivas.

Los *códex* se han desarrollado y armonizado sobre la base de medidas subjetivas de calidad de voz. Las medidas estándar de calidad objetiva, como una total distorsión armónica y relaciones señal a ruido no se corresponden muy bien con una percepción de calidad de voz humana, lo que al final es la meta de la mayoría de las técnicas de compresión de voz.

Por ello, una prueba interesante que se usa para medir la calidad de los *códecs* y del sonido resultante de la compresión es lo que se conoce como la nota media de opinión (**MOS**, *Mean Opinion Score*). Las pruebas MOS se dan a un grupo de oyentes. Como la calidad de voz y sonido es subjetiva para los oyentes en general, es importante obtener una amplia gama de oyentes y material de prueba cuando se realiza una prueba de este tipo. Aquí, se tiene en cuenta la opinión totalmente personal de cada uno. Así, un amplio rango de personas juzga y califica de 1 a 5 (de malo a excelente) una grabación de voz que se corresponde con un determinado *códec*, para sacar luego una media con la que se obtiene la puntuación media de la opinión. Éste es uno de los parámetros que se tendrán en cuenta en nuestra comparativa entre los diferentes *códecs*.

La comprobación MOS se utiliza también para comparar cómo funciona un *códec* determinado bajo circunstancias distintas, incluidos diferentes niveles de ruidos de fondo, múltiples codificaciones y decodificaciones, etc. Después se utilizan estos datos para comparar con otros *códecs*.

Como se ha mencionado, aunque la puntuación MOS es un método subjetivo para determinar la calidad de la voz, no es el único para hacerlo. La ITU-T ha sacado la recomendación P.861, que cubre las maneras con las que se puede determinar objetivamente la calidad de voz utilizando la Medición de calidad de voz según la percepción (**PESQ**).

Sin embargo, **PESQ** tiene muchos inconvenientes cuando se utiliza con *códecs* de voz como los descritos en este proyecto (Apartado 3.2.1). Uno de estos inconvenientes es que lo que la “máquina” o PESQ oye no es lo que percibe el oído humano. Por lo tanto, PESQ fue desarrollado para “oír” deterioros provocados por la compresión y descompresión, pero no mide correctamente la pérdida de paquetes o el *jitter*.

Cuando se transmite en un medio en el que puede haber pérdidas de información debido a la congestión o al ruido electromagnético como una LAN, aunque éstas parezcan poco importantes en porcentaje, no hay que dejar de tenerlas en cuenta para ver cómo afectan al audio codificado. **PLC** (*Packet Loss Concealment*) “camufla” la pérdida de paquetes usando la información de otros anteriores

bien recibidos. Sólo soluciona la pérdida de paquetes aislados, no la de ráfagas de ellos perdidos. Se ha visto en el apartado de codecs (3.2.1) cuáles usan eficientemente esta técnica para mantener una calidad de audio suficiente con la pérdida esporádica de paquetes.

Hay varios sub-estándares y clasificaciones dentro de MOS, en función de si la puntuación MOS está basada en estimadores o no (MOS-E: operaciones matemáticas que relacionan las medidas subjetivas estandarizadas con las variaciones de otros parámetros métricos de sensibilidad y disponibilidad), y si se refieren a calidades conversacionales o a esfuerzos de escucha. Algunos cubren detalladamente y muestran de manera práctica las diferencias y las maneras de proceder en este aspecto, por lo que aquí nos limitaremos a una mera aproximación y a listar determinados números MOS estandarizados y estimados.

Concretamente, la escala de puntuación para la calidad de audio de un *codec* es la siguiente (MOS-LQS, MOS, *Listening Quality Scale*):

- 1 Mala
- 2 Pobre

- 3 Media
- 4 Buena
- 5 Excelente

El teléfono fijo RTB convencional se ha utilizado como referencia como MOS=4.0.

Se muestra en la tabla 3 las puntuaciones MOS de los distintos *codecs*.

<i>Técnica de compresión</i>	<i>Regimen binario</i>	<i>Calidad voz MOS</i>
G.711 (PCM)	64 kbps	4.1
G.726 (ADPCM)	32 kbps	3.9
G.727 Enhanced ADPCM	24 kbps	3.1
G.727 Enhanced ADPCM	16 kbps	2.4
G.728 (LD-CELP)	16 kbps	3.6
GSM-HR (RPE-LTP)	5,6kbps	3.0
GSM-FR (RPE-LTP)	13 kbps	3.6
GSM-EFR (ACELP)	12.2 kbps	4.2
G.729/a (CS-ACELP)	8 kbps	4.0/3.9
G.723.1 (MP-ACELP)	6.4 kbps	3.8
G.723.1 (MP-ACELP)	5.3 kbps	3.5

Tabla 3. Puntuaciones MOS de los distintos formatos de compresión.

También tenemos otra valoración MOS en función de los efectos o molestias que pueden

generar parámetros que degradan la calidad (MOSLE, MOS Listening Effort scale).

- 5 Imperceptibles.
- 4 Perceptibles, pero no molestos.
- 3 Perceptibles y ligeramente molestos.
- 2 Molestos, pero soportable.
- 1 Molestos e insoportables.

De acuerdo a la escala anterior, el retardo afecta a la calidad tal y como especifica la tabla 4.

<i>Calidad exigida</i>	<i>Conexión nacional</i>	<i>MOS</i>	<i>Conexión internacional</i>	<i>MOS</i>
Alta calidad	Hasta 150 ms	3.5 -> 4.0	Hasta 300 ms	3.0 -> 3.8
Media calidad	Hasta 200 ms	3.2 -> 3.8	Hasta 400 ms	3.0 -> 3.5

Tabla 4 Efecto MOS_{LE} sobre el retardo

Por último, otro efecto que afecta a la calidad de escucha es la pérdida de paquetes. Así pues, tenemos la siguiente lista:

Efecto MOS de la pérdida de paquetes consecutivos.

- 1 paquete: 4.2.
- 2 paquetes: 3.2.

- 3 paquetes: 2.4 (ya no es aceptable).
- 4 paquetes: 2.1 (intolerable).
- 5 paquetes: 1.7 (pérdida de comunicación).

3.3 Normativas VoIP

3.3.1 H.323

H.323 es un conjunto de protocolos, recomendación de la *ITU-T*. Es la normativa que está más instalada, simplemente por el hecho de ser la que más tiempo lleva funcionando y porque no existía ninguna otra opción anterior. H.323 fue aprobado (en 1996 en su primera versión) por una serie de gobiernos internacionales, para convertirse en la referencia mundial para la transmisión de vídeo, audio y datos, a través de un sistema de conferencia. Para establecer el marco de referencia adecuado, se definen los aspectos que han de cumplir los dispositivos que acceden a sus servicios (ordenadores, telefonía, telefonía celular, *PDA*s, sistemas de videoconferencia...).

La información transmitida se agrupa en *streams*, según sus características. De esta forma, el tráfico generado por las aplicaciones en tiempo real se puede desglosar en las siguientes clases:

- **Señales de Datos:** donde se incluye la transferencia de documentos, imágenes fijas y cualquier tipo de fichero debidamente codificado.
- **Señales de Audio:** esta clase de tráfico está compuesta por el diálogo producido entre los participantes de la conferencia, debidamente digitalizado y codificado. Opcionalmente, se emplean mecanismos de activación por la voz, que permiten cancelar la transmisión en el caso de que los terminales permanezcan en silencio, con el objeto de reducir el ancho de banda asignado a este flujo. De la misma manera, la información es codificada y comprimida adecuadamente para optimizar igualmente los recursos empleados.
- **Señales de Vídeo:** contienen la información codificada y digitalizada de las imágenes en movimiento generadas por los participantes en la videoconferencia. La tasa de transmisión de vídeo nunca superará a la seleccionada por los participantes, asegurando de esta forma los recursos para otra serie de *streams*.
- **Señales de Control:** Se usan en H.323 2 tipos de señales de control. Por un lado, se encuentran las

señales de control de comunicaciones que realizan una gestión remota de los recursos de la conferencia, posibilitando el establecimiento y deshabilitación de los canales de comunicación, a la vez que emplean otras funciones encaminadas al manejo y optimización de la conferencia. Y, por otro lado, están las llamadas de control propiamente dichas que facilitan la conexión y desconexión de los usuarios al servicio de conferencia.

Los estándares incluidos bajo H.323 definen una serie de especificaciones para el establecimiento de comunicaciones multimedia sobre las redes de paquetes, que garantiza una determinada calidad de servicio. Gracias a estos servicios, los equipos y terminales soportan el transporte en tiempo real tanto de audio, vídeo y datos, como de cualquier combinación de estos elementos. Estos servicios se basan en los protocolos RTP (Real-time Transport Protocol) y RTCP (Real-time Transport Control Protocol), así como la utilización de otros estándares existentes, como por ejemplo, el Q.931 (usado en RDSI). Hay que remarcar a su vez, que el protocolo H.323, hace mucho énfasis en la interconexión con redes tradicionales de voz.

H.323 es un conjunto de protocolos bastante complejo que no fue creado para el desarrollo simple de aplicaciones, sino para permitir que las aplicaciones multimedia se ejecutaran sobre redes de datos “no fiables”. Por lo tanto, el tráfico de voz es sólo una de las aplicaciones para el H.323. La mayoría del trabajo inicial que se realizó en esta área se centraba en las aplicaciones multimedia, donde el vídeo y los datos compartían la mayor parte del protocolo.

Los productos basados en las recomendaciones *H.323* soportan la interconexión entre diferentes participantes a través de *Internet*, con este fin, define una serie de estándares de codificación y decodificación (*códecs*) de audio y vídeo, en los que la información generada por las aplicaciones es encapsulada y transmitida a los puntos finales de la conferencia.

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

- **Direccionamiento:**

- **DNS (Domain Name Service).** Servicio de resolución de nombres en direcciones *IP* con el

mismo fin que el protocolo *RAS*, pero a través de un servidor *DNS*.

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

- **Señalización:**

- ***Q.931:*** Señalización inicial de llamada. Define el modo en que cada nivel de la arquitectura *H.323* interactúa con su entidad par correspondiente.
- ***H.225:*** Control de llamada: señalización, registro y admisión, y paquetización/sincronización del flujo de voz. Establece y desmantela conexiones entre equipos finales.
- ***H.245:*** Protocolo de control para especificar mensajes de negociación de canales. A su vez, este nivel permite seleccionar el tipo de *códecs* empleados.

- **Compresión:**
 - **Voz:**
 - Requeridos: G.711 y G.723 (vistos en el apartado 2.1)
 - Opcionales: G.728, G.729 y G.722 (vistos en el apartado 2.1)
 - **Vídeo:** H.261¹, H.263²
 - **Datos:** T.120 (opcional) que incluye:
 - T.123 como protocolo de transporte
 - T.122 y T.125 para servicios multi-conferencia/“multi-transferencia”
 - T.126 para intercambio de imágenes y notas (al estilo Netmeeting, que es un ejemplo de cliente H.323 que utiliza este protocolo).
 - T.127 para la transferencia de ficheros binarios (incluyendo multi-destino).

¹ sirve para codificar señales de vídeo con tasas de bits múltiples de 64 Kbps, (capacidad de un canal B RDSI, pues surge para RDSI). Está diseñado para trabajar en tiempo real, como precisa una videoconferencia, buscando un retardo únicamente del orden de 150 ms. Comprime imágenes en movimiento a unos 15 fps; (sin comprimir se necesitarían 18.3 Mbps). H.261 realiza tareas de predicción-entre cuadros, busca códigos de transformación y hace compensación de movimiento. También usa códigos de longitud variable para evitar el envío de información redundante. Soporta 2 resoluciones: QCIF (*Quarter Common Interchange Format*) y CIF (*Common Interchange Format*). Trata las imágenes de forma jerárquica, con cuatro capas: cuadro, grupo de bloques, macrobloque y bloque; lo que permite realizar estimaciones de movimiento en macrobloques cuando estamos codificando. Al ser estas áreas pequeñas, el estándar es útil para la videoconferencia, donde gran parte de la imagen permanece estática y es precisamente el módulo de estimación del movimiento es el que más coste computacional conlleva. Sin embargo, la decodificación, al igual que en otros estándares de compresión de audio y especialmente de vídeo, es mucho más sencilla computacionalmente hablando. Se pueden contratar la calidad con los ejemplos de [18]

² desarrollado a partir de H.261, está diseñado para aplicaciones con menor caudal de datos (<64 Kbps). Se utiliza en la transmisión de vídeo en redes telefónicas existentes y usa sobre todo el formato de imagen QCIF. Tiene el mismo esquema de bloques para el codificador y decodificador que el H.261 con la ventaja de que su sistema de corrección de errores es más eficiente, con lo que resulta más útil para medios con ruido elevado



Figura 3 Pila de protocolos en VoIP

▪ **Transmisión de voz:**

- UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos (la integridad de datos de TCP tampoco no sirve, pues un paquete que llega “tarde” es peor que uno que no llega) y al menos el aprovechamiento del ancho de banda es mayor que con TCP.
- RTP (Real-time Transport Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

▪ **Control de la transmisión:**

- RTCP (*Real-time Transport Control Protocol*). Se utiliza principalmente para detectar situaciones

de congestión de la red y tomar, en su caso, acciones correctoras.

3.3.1.1 Arquitectura H.323

Se especifican cuatro tipos de componentes, que interconectados adecuadamente proveen los servicios punto a punto a los usuarios finales. Se detalla un análisis jerárquico de estos componentes, desde aquellos que aportan funcionalidades específicas a los participantes, a los que proveen servicios de interconexión y de compatibilidad entre las arquitecturas.

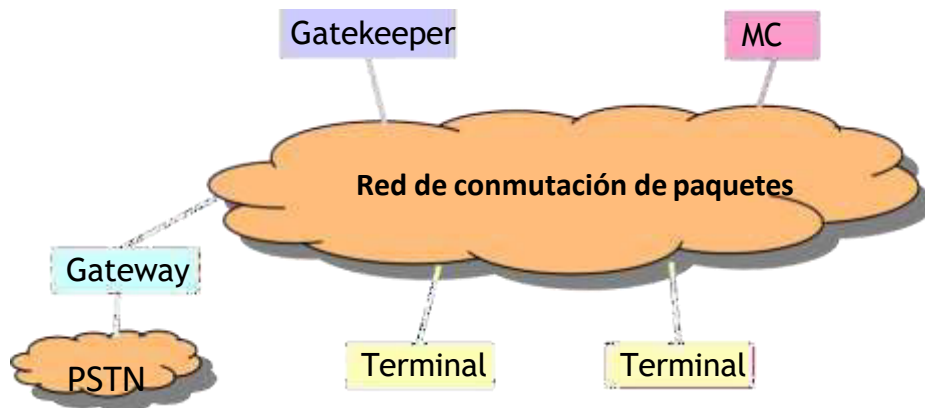


Figura 4 Descripción básica de una red basada en el estándar *H.323*. Comunicación entre los diferentes componentes: terminal, gateway, gatekeeper, MCU y router.

Estos cuatro componentes son: los terminales, gateways (permiten conexión de redes heterogéneas), gatekeepers (direcciona, autoriza, autentifica...) y MCU (soporte multiconferencia); que pueden ser observados en la Figura 4 y que a continuación se describen:

- **Gatekeeper:** se puede decir que es el elemento inteligente de la red y se encarga de servicios como la autenticación, el direccionamiento, el mantenimiento, la tarificación y la gestión del ancho de banda. Es el encargado de gestionar todos los terminales, pasarelas y *MCUs*.
- **Terminal:** son los elementos empleados en la comunicación multimedia bidireccional, y tienen que soportar la transmisión de audio y, opcionalmente, la de vídeo. Es decir, son los receptores y generadores de llamadas, como por ejemplo, un videoteléfono IP o un PC multimedia con *Netmeeting*.

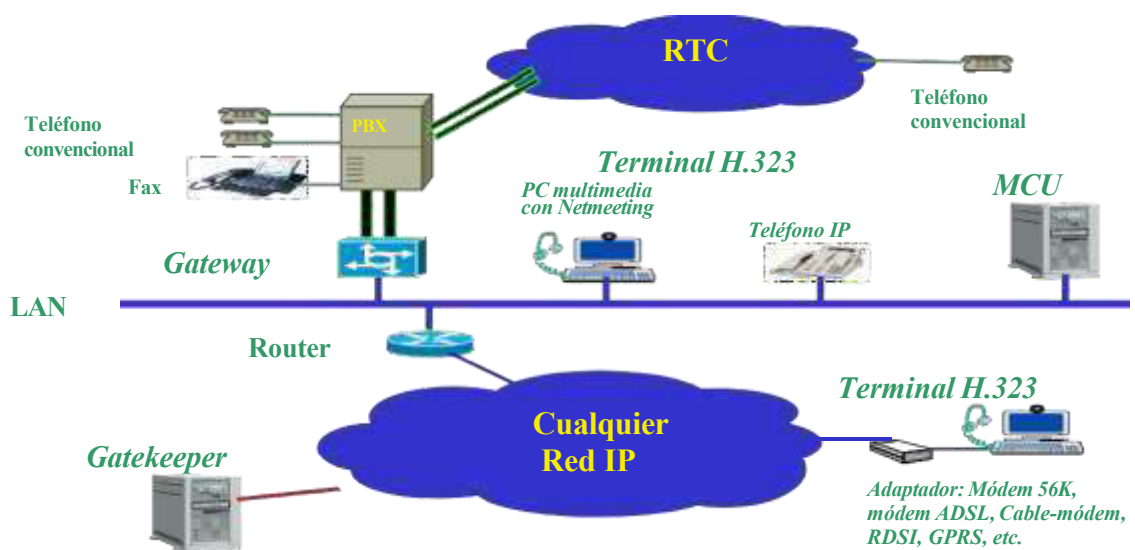


Figura 5 Esquema general de una RTC operando con cualquier Red IP con elementos H.323

- **Pasarela (*Gateway*)**: entidades o procesos que permiten la conexión de redes heterogéneas. Por ejemplo, sería el nexo entre la RTC (Red Telefónica Conmutada, o red telefónica tradicional) y la red de VoIP como se puede apreciar en la Figura 5. Realiza conversión de formatos de transmisión y procedimientos de comunicación. Su instalación es opcional.
- **MCU (*Multipoints Control Units*)**: son las entidades encargadas de gestionar una conferencia multipunto. Así, establece las negociaciones entre los terminales con el objeto de determinar los diferentes *codecs* necesarios.

Por último reseñar que tanto los gatekeepers, los gateways y los MCUs son componentes lógicos independientes, aunque pueden estar implementados en un único dispositivo físico.

En resumen, se pueden señalar las siguientes ventajas e inconvenientes de H.323.

- **Ventajas:**

- Está incluido por la mayoría de los fabricantes de *hardware* para redes IP como *Lucent*, *Cisco*, *Nortel*
- La disponibilidad de *stacks* H.323 para desarrollo de distintos fabricantes.
- La interoperabilidad con la red telefónica conmutada.

- **Desventajas:**

- La complejidad y redundancia en los protocolos definidos.
- La compleja escalabilidad.
- La dificultad para desarrollar nuevos servicios

3.3.2 SIP

El *SIP* es un protocolo de control de la capa de aplicación (señalización), independiente del protocolo de transporte, utilizado para crear, modificar y terminar sesiones con uno o más participantes, además de realizar el control de llamadas multimedia y de servicios telefónicos avanzados. Fue definido por el *IETF (Internet Engineering Task Force)* en la RFC 2543 como una alternativa a *H.323* y es una de las últimas propuestas para manejar la señalización y permitir la implementación de nuevos servicios en *VoIP*. Al estar

desarrollado por el IETF y no la ITU-T (como H.323) no sorprende el hecho de estar basado en una arquitectura cliente/servidor.

Estas sesiones multimedia incluyen audio, vídeo y datos; y pueden incluir múltiples participantes. El SIP permite que estos sean invitados a una conferencia improvisada. Esas sesiones multimedia pueden comunicarse a través de la multidifusión o unidifusión, o bien de una combinación de ambos mecanismos de entrega.

Está diseñado para ser escalable, tanto en servicios como en *hardware*, es flexible, interoperable y más sencillo. A su vez, reutiliza otros conceptos ya usados ampliamente en el mundo Internet como *URL's*, contenido *MIME*, *páginas web*, etc; siendo un protocolo basado en texto de naturaleza similar a HTTP.

Básicamente, las facetas a cubrir por el protocolo son:

- **Localización del usuario:** Determinación del sistema final de la comunicación.
- **Capacidades del usuario:** Determinación de sus capacidades para realizar la llamada, como por ejemplo, los *códecs* que soporta.

- **Disponibilidad del usuario:** Determinación de la capacidad del receptor de la llamada para establecer la comunicación.
- **Establecimiento de llamada:** Determinación de los parámetros de la llamada y establecimiento final de la comunicación.
- **Manejo de llamada:** Incluye la transferencia y la terminación de las llamadas.

3.3.2.1 Arquitectura SIP

A continuación, se describen brevemente los elementos básicos que componen una red basada en SIP:

- **Agente de usuario (UA):** son los terminales SIP que realizan el papel de un terminal o *gateway* de voz. Suelen ser aplicaciones software residentes en teléfonos *IP* o *PCs*. Pueden funcionar como:
 - *SIP User Agent Client* (UAC): funciona como cliente y envía peticiones al servidor.
 - *SIP User Agent Server* (UAS): funciona como servidor y recibe y atiende las peticiones del UAC.

Así pues, como se puede observar, existen dos tipos de mensajes SIP; los de petición (request), generados por el cliente, y los de respuesta (reply), generados por el servidor. Además, emplea el protocolo SDP (Session Description Protocol) para la descripción de la sesión a establecer entre los terminales.

- **Servidor Proxy:** se encarga básicamente de redirigir la información entre el Agente de Usuario y el resto de la red. Es decir, son los responsables primarios del encaminamiento de llamadas. Reciben las peticiones del UA, las interpretan y/o modifican y las reenvían al destino final (UA) o al servidor SIP. Tiene dos modos de funcionamiento:

- *Stateful Proxy servers:* mantienen el estado de la llamada y de la transacción (Ej.: tarificación).
 - *Stateless Proxy servers:* no mantienen información sobre el contexto de la llamada.
- **Servidores de redirección (*Redirect servers*):** acepta peticiones y devuelve direcciones destino. No genera llamadas ni respuestas y tiene una alta capacidad de procesado.

- **Servidor Registrar (*SIP Register*):** recibe los mensajes de registro de los UAs y envía su información a los *Location Servers*.

- **Servidores de localización (*location servers*):** ofrecen servicios e información para la localización de usuarios.

3.3.2.2 Servicios SIP

En la actualidad, los desarrollos de SIP se están centrando, de manera mayoritaria, en reproducir servicios de Red Inteligente, como llamada en espera, desvío de llamadas o llamada a tres(conferencia).

También están empezando a aparecer las primeras soluciones de Mensajería Unificada y de *Internet Call Waiting*.

En el futuro, se supone que la funcionalidad de SIP permitirá que tanto los proveedores como los propios usuarios den rienda suelta a su imaginación a la hora de crear nuevos servicios, gracias a lenguajes de programación como CPL (Call Processing Language o

también a iniciativas como JAIN (Java APIs for Intelligent Networks) o PARLAY/OSA.

Por seguir un desarrollo análogo a *H.323*, se enumeran a continuación las principales ventajas y desventajas de *SIP*:

▪ **Ventajas:**

- Facilita la integración de comunicaciones multimedia (mensajería unificada).
- Es escalable. Usa el modelo de Internet. En este aspecto, hay que mencionar, que los servidores mantienen el estado de una transacción SIP, no de una sesión completa.
- Es flexible y extensible, puesto que no dicta arquitecturas ni modelos de servicio y está abierto al proveedor de servicios.
- Es un sistema distribuido, también compatible con la PSTN y otros sistemas.
- Además de esto, otra de las virtudes es que puede trabajar solo o con otros protocolos como DHCP, TCP, UDP, RTP
- Permite cambiar los parámetros de una sesión en curso sin tener que desmantelarla.

- Y por supuesto, la gran movilidad que aporta; puesto que permite la localización de los usuarios en cualquier terminal y ubicación, siendo éste un aspecto clave para la integración con el escenario de la telefonía móvil.
- Como ya se ha comentado, SIP permite utilizar herramientas de fácil manejo para la creación de servicios incluso por parte del usuario final (con CPL, citado anteriormente)

▪ **Desventajas:**

- De momento, no existen muchos *stacks* SIP en el mercado aunque se están desarrollando con gran rapidez, algunos de ellos *Open Source* como VOCAL, Asterisk, etc.
- La interoperabilidad con RDSI y RTB no es tan directa, pero ya existen *gateways* de voz SIP, como por Ej. varios modelos de routers de Cisco, que ya cuentan con esta capacidad.

3.3.3 MGCP y MEGACO

Los protocolos *SGCP* y *MGCP*, estándar del IETF, fueron desarrollados para permitir que un dispositivo central,

conocido como controlador de *gateway* de medios (*MGC, Media Gateway Controller*), o *soft-switch*, pudiera controlar los puntos finales, o *gateways* de medios (*MG, Media Gateways*). Se pueden desarrollar aplicaciones mediante la utilización de API basadas en estándares que comunican con los MGC y ofrecen funcionalidad adicional (como la llamada en espera o las funciones CLASS) y aplicaciones.

Está formado por los siguientes elementos:

- **Media gateways:** elementos a controlar, que típicamente hacen de interfaz entre IP y RTC. Es decir, es donde los enlaces troncales de voz de 64 *kbps* son convertidos en paquetes y colocados en la red IP.
- **Call Agents:** elementos inteligentes que controlan de manera centralizada los *gateways*; y que también se comunican entre sí. Además, tienen una conexión a la red inteligente, para proporcionar servicios CLASS.

Tras esto, se ven a continuación las principales ventajas e inconvenientes del protocolo:

- **Ventajas:**

- Es un modelo simple, donde existen nuevos comandos en formato texto. Además, uno o más comandos pueden encapsularse en otro.
- Puede utilizarse tanto en redes H.323 como SIP.

- **Desventajas:**

- Puede quedar desplazado por *MEGACO/H.248*, que no es más que una versión avanzada de MGCP con la misma filosofía.

Como se acaba de comentar, la evolución del MGCP desemboca en lo que se conoce como MEGACO (MEdia GATeway COntrol Protocol), definido por el IETF. Éste, lo que hace es una separación de funciones en las pasarelas. Así, se tendrá:

- **Pasarela física** (*MG, Media Gateway*)
- **Controlador de pasarela física** (*MGC, Media Gateway Controller*)
- **Pasarela de señalización** (*SG, Signalling Gateway*)

La función que realiza es la de especificar la comunicación entre las pasarelas (MGs) y sus controladores (MGCs), por lo que más bien es un protocolo de conexión y no

de señalización; siendo así un complemento perfecto para H.323 y SIP.

MEGACO está basado en un funcionamiento maestro/esclavo, utiliza mensajes de texto y funciona tanto en TCP como en UDP.

Además, al igual que SIP, permite el desarrollo de nuevos servicios más sencillos, a la vez que es más fiable y escalable que su predecesor.

Por todo lo citado en este apartado, MGCP/MEGACO quedan bastante lejos del objetivo de estudio de este proyecto, pues está más orientado a operadores de Telecomunicaciones, que a usuarios finales y/o empresas.

3.3.4 IAX

IAX (Inter-Asterisk eXchange protocol) es uno de los protocolos utilizado por Asterisk, un servidor PBX (centralita telefónica) de código abierto patrocinado por Digium. Es utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que también utilizan protocolo IAX.

El protocolo IAX ahora se refiere generalmente al IAX2, la segunda versión del protocolo IAX. El protocolo original ha quedado obsoleto en favor de IAX2.

3.3.4.1 Propiedades Básicas

IAX2 es robusto, lleno de novedades y muy simple en comparación con otros protocolos. Permite manejar una gran cantidad de codecs y un gran número de streams, lo que significa que puede ser utilizado para transportar virtualmente cualquier tipo de dato. Esta capacidad lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas.

IAX2 utiliza un único puerto UDP, generalmente el 4569, para comunicaciones entre puntos finales (terminales VoIP) para señalización y datos. El tráfico de voz es transmitido in-band, lo que hace a IAX2 un protocolo casi transparente a los cortafuegos y realmente eficaz para trabajar dentro de redes internas. En esto se diferencia de SIP, que utiliza una cadena RTP out-of-band para entregar la información.

IAX2 soporta Trunking (red), donde un simple enlace permite enviar datos y señalización por múltiples

canales. Cuando se realiza Trunking, los datos de múltiples llamadas son manejados en un único conjunto de paquetes, lo que significa que un datagrama IP puede entregar información para más llamadas sin crear latencia adicional. Esto es una gran ventaja para los usuarios de VoIP, donde las cabeceras IP son un gran porcentaje del ancho de banda utilizado.

3.3.4.2 Objetivos de IAX

El principal objetivo de IAX ha sido minimizar el ancho de banda utilizado en la transmisión de voz y vídeo a través de la red IP, con particular atención al control y a las llamadas de voz y proveyendo un soporte nativo para ser transparente a NAT. La estructura básica de IAX se fundamenta en la multiplexación de la señalización y del flujo de datos sobre un simple puerto UDP entre dos sistemas.

IAX es un protocolo binario y está diseñado y organizado de manera que reduce la carga en flujos de datos de voz. El ancho de banda para algunas aplicaciones se sacrifica en favor del ancho de banda para VoIP.

3.3.5 Asterisk

Es una aplicación de código abierto de una central telefónica (PBX). Como cualquier PBX, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP o bien a una RDSI tanto básicos como primarios.

Asterisk tiene licencia GPL. Mark Spencer de Digium inicialmente creó Asterisk y actualmente es su principal desarrollador junto con otros programadores han contribuido a corregir errores, añadir novedades y funcionalidades. Originalmente desarrollado para el sistema operativo Linux, Asterisk actualmente también funciona en BSD, MacOSX, Solaris y Microsoft Windows aunque la plataforma nativa (Linux) es la mejor soportada de todos.

Asterisk incluye muchas características anteriormente solo disponibles en caros sistemas propietarios PBX: buzón de voz, conferencias, IVR, distribución automático de llamadas, y otras muchas más. Los usuarios pueden crear nuevas funcionalidades escribiendo un dialplan en el lenguaje de script de Asterisk o añadiendo módulos escritos en lenguaje C o en cualquier otro lenguaje de programación soportado por Linux.

Para conectar teléfonos normales analógicos hace falta unas tarjetas telefónicas FXS o FXO fabricadas por Digium o por otros fabricantes, ya que para conectar el servidor a una línea externa no vale con un simple módem.

Quizá lo más interesante de Asterisk es que soporta muchos protocolos VoIP como pueden ser SIP, H.323, IAX. Asterisk puede interoperar con teléfonos IP actuando como un registrador y como gateway entre ambos.

Las compañías de telecomunicaciones de todo el mundo empiezan a utilizar Asterisk como sistema nativo de VoIP junto con SER (Sip Express Router) en lugar de otras marcas que ofrecen PBX propietarios como Alcatel, Cisco o Avaya.

3.3.5.1 Funcionalidades generales

Asterisk es capaz de trabajar con prácticamente todos los estándares de telefonía tradicional:

- Líneas analógicas
- Líneas digitales: E1, T1, accesos básicos.

Soporta casi todos los protocolos de VozIP:

- SIP.
- IAX/IAX2.
- MGCP.
- H.323.
- Cisco Skinny.

3.3.5.2 Esquema Conceptual

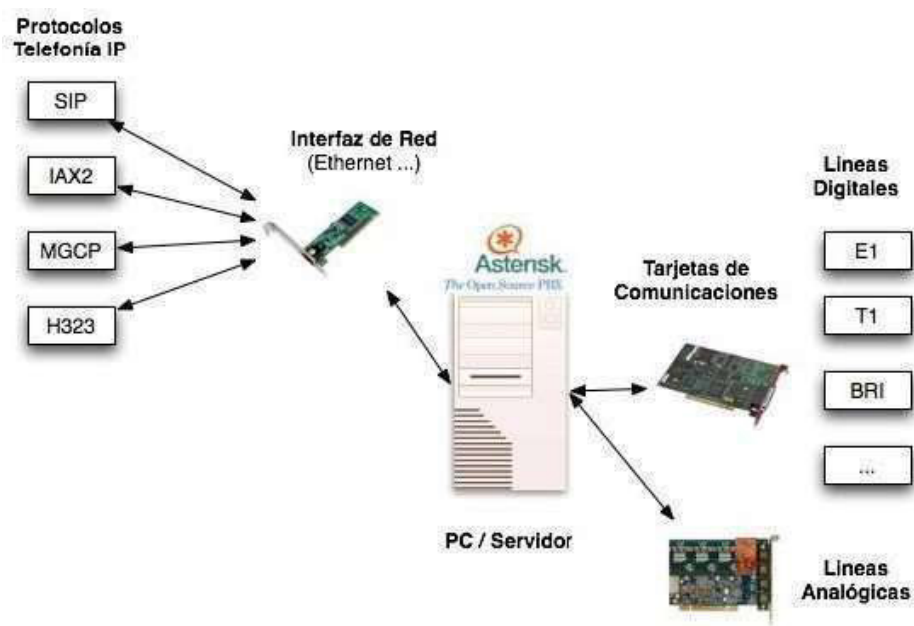


Figura 6 Esquema Conceptual del servidor Asterisk

3.3.5.3 Funcionalidades tipo centralita clásica

Algunas de las funcionalidades tipo centralita más comunes:

- Transferencia Ciega.
- Música en espera.
- Timbres Distintivos.

- Pickup de llamadas.
- Llamada en espera.
- Conferencias.
- Buzón de Voz .
- Colas de llamadas.
- Colas con Prioridad.
- Caller ID en espera.

3.3.5.4 Funcionalidades tipo centralita avanzada

- IVR: Interactive Voice Response, recepción y gestión de llamadas con menús interactivos.
- Buzón de Voz: Mensajes de Voz enviados por EMail, avisos por SMS, etc.
- Configuración en base de datos: Extensiones, usuarios, etc , pueden ser almacenados en BBDD (MySQL, MS SQL, ODBC * ...). Es posible gestionar la BBDD desde intranets/extranets, etc.

3.3.5.5 Funcionalidades Voz IP

- Soporte de todos los protocolos estándar:
 - SIP (Session Initiation Protocol).
 - H.323
 - MGCP (Media Gateway Control Protocol).

- IAX2 (Inter-Asterisk eXchange).
 - SCCP (Cisco Skinny).
 - Soporta 'bridging' entre tecnologías distintas.
 - Soporta transcodificación.
-
- Soporte de todos los codecs estándar:
 - ADPCM
 - G.711, G.723.1, G.726, G.729A/B (Con licencia).
 - GSM
 - ILBC
 - LineaR
 - LPC-10
 - Speex.

3.3.5.6 Problemas nativos de la Voz IP

Asterisk sufre, al igual que el resto de soluciones, de los problemas de la Voz IP:

- Latencia
- Jitter
- Ancho de banda

Algunos se pueden solucionar en cierta medida:

- Cambio dinámico de proveedor en base a su latencia.
- IAX2 Trunking para ahorrar cierto ancho de banda en los enlaces inter-asterisk.

3.3.5.7 Problemas de configuración (Complejidad)

Asterisk se configura normalmente como ficheros de texto, la sintaxis puede ser ligeramente 'obtusa'. Existen bastantes gestores e interfaces de usuario para configurarlo, pero no están del todo depurados para ser integrados conjuntamente.

3.3.5.8 Integración de Asterisk

Asterisk puede ser integrado de varias formas aquí algunas:

- Como centralita tradicional / centralita IP.
- Como pasarela transparente hacia VoIP en sistemas en producción actuales.
- Como plataforma para servicios telefónicos avanzados: gestión de incidencias, soporte, pedidos, pudiendo estar en cualquier punto con

conexión a Internet (buena conectividad recomendada).

3.3.5.9 Asterisk y la Telefonía Tradicional

3.3.5.9.1 Interfaces Analógicos

- **Puertos FXO:** Estas interfaces que integra el Asterisk es utilizado para conectarse con la RTPC o como extensión de una centralita tradicional analógica. Para establecer estas conexiones se pueden utilizar las tarjetas X100P y TDM400P de Digium o bien tarjetas TE110P o TE410P conectadas con bancos de Canales.
- **Puertos FXS:** Estas interfaces que integra el Asterisk es utilizado para que se puedan conectar extensiones analógicas al Sistema. Para establecer estas conexiones se pueden utilizar las tarjetas TDM400P de Digium o bien tarjetas TE110P o TE410P conectadas con Bancos de Canales.

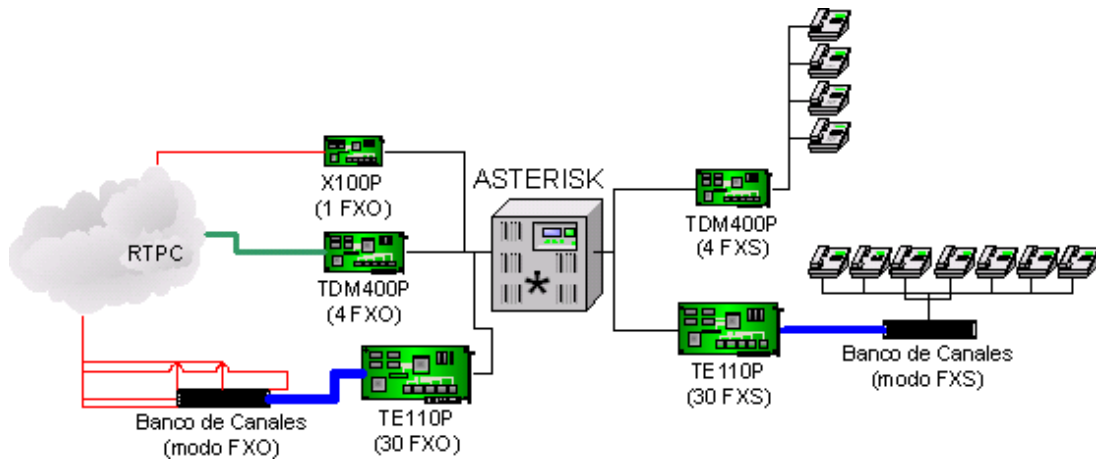


Figura 7 Servidor Asterisk enlazado a tarjetas FXO y FXS.

3.3.5.9.2 Interfaces Digitales

La Red Digital de Servicios Integrados (RDSI) utiliza, en principio, dos tipos de capacidades de acceso. El acceso Básico (2 Canales de voz + 1 de señalización) y el acceso Primario (30 canales de Voz + 1 de señalización). Estas interfaces son integradas dentro de Asterisk con las tarjetas de Digium TE110P y TE410P para acceso primarios y por las tarjetas QuadBRI y OctoBRI de Junghanns, las Tarjetas Diva Server de Eicon, las Fritz de AVM así como aquellas tarjetas RDSI con chipset HFC-S para accesos básicos.

Además del tipo de señalización, los interfaces RDSI pueden funcionar en modo NT(Network Termination) o TE(Terminal Equipment).

- **Modo TE:** En Este modo, Asterisk puede conectarse con interfaces RDSI (BRI o PRI) o con Centrales Digitales Tradicionales que tengan conexión RDSI de foma esclava.
- **Modo NT:** En este modo el Asterisk puede conectarse con Centrales Digitales Tradicionales que tengan conexión RDSI de forma Maestro o con extensiones Digitales.

Existen dos tipos de interfaces RDSI: BRI (o Básico) y el RDSI/PRI (o Primario):

- **RDSI/BRI (Basic Rate Interface)** normalmente es de uso doméstico o utilizado por pequeñas empresas, reemplazando los accesos telefónicos tradicionales. El RDSI/BRI está compuesto de dos canales de datos (Canales B) de 64 Kbps, y un canal de señalización (Canal D) de 16 Kbps. Cada canal B puede ser utilizado tanto para voz (enlace telefónico) como para datos (acceso a red

corporativa, Internet). En una única línea RDSI, es posible conectar varios dispositivos RDSI, siendo permitido, la utilización simultánea de apenas dos de ellos. (Ejemplo Fax+Teléfono, acceso Internet+Teléfono) Los dos canales pueden ser agrupados, resultando un único canal de 128 para datos.

Para conectar equipos NO-RDSI (fax, teléfono, modem convencional, etc.) a una línea RDSI es necesario utilizar un Adaptador de Terminal (TA- Terminal adapter). Los equipos NO-RDSI son conectados al adaptador de Terminal, que a su vez es conectado al al terminal de red. Algunos modelos de terminal de red poseen adaptadores de terminal incluidos. Enn este caso los equipos NO-RDSI pueden ser conectados directamente al terminal de red.

- **RDSI/PRI (Primary Rate Interface)** normalmente es utilizado por empresas de proveedores de acceso a Internet. La Red Digital de Servicios Integrados, en su acceso básico, provee al usuario de 2 canales de comunicación digital de 64Kbits/s (canales B) y uno de control de

16Kbits/s (canal D) sobre las líneas telefónicas convencionales (el par de cobre que soporta actualmente la RTB). La RDSI se encuentra integrada en la red telefónica convencional, de tal forma que soporta de forma nativa el establecimiento de llamadas hacia/desde cualquier abonado que disponga de RTB.

CAPITULO IV

4. MARCO METODOLOGICO

4.1 Tipo de Investigación

El tipo de Investigación utilizada en el presente trabajo parte de los conceptos fundamentales sobre la tecnología de VoIP y sus protocolos de enrutamiento, buscando así implementar soluciones a partir de esta tecnología que nos permitan resolver situaciones y necesidades concretas en la empresa.

El estudio responde a fines prácticos y concretos. Se busca el contribuir a mejorar la aplicación de estas tecnologías a favor de la economía de la empresa. La empresa esta inmersa en un contexto de avance tecnológico y de competitividad en el mercado por lo cual una de sus principales preocupaciones es la de reducción de costos en cuanto a comunicaciones.

La atención a este tipo de requerimiento se dio debido al constante aumento respecto a las comunicaciones y a su vez al costoso mantenimiento que implica tener una central telefónica tradicional, para lo cual valiéndonos de la metodología y de aplicando los resultados de la investigación es que brindamos una solución al respecto implantando un sistema de telefonía IP para la reducción de costos en cuanto a comunicaciones internas y externas.

Para este tipo de Investigación se preciso estar actualizado en los temas de redes y de la tecnología VoIP, así como también de los codecs, protocolos y hardware asociado con la infraestructura de redes y telefonía, lo cual nos permite alcanzar el objetivo de ayudar de manera concreta a la empresa a lograr su cometido, la reducción de costos en comunicaciones.

4.2 Universo o Población

4.2.1 Determinación del Universo

La población para la aplicación de la presente investigación sobre la implantación del Sistema de Telefonía IP queda especificada de la siguiente manera: “Todas las empresas que posean una infraestructura de red por mínima o pequeña que parezca.”

4.2.2 Determinación de la Muestra

La muestra para la aplicación del presente trabajo de investigación queda limitada a la empresa CDSOft SA en la cual se implantara el sistema propuesto.

CAPITULO V

5. IMPLANTACION METODOLOGICA Y TECNOLOGICA

5.1 Descripción de la situación actual de la empresa:

La empresa CDSoft S.A. Es una organización que se desempeña en el desarrollo e implementación de software y del diseño de imagen institucional, cuenta con una amplia cartera de clientes en el ámbito local, nacional, e internacional. En la actualidad la empresa cuenta con un sistema de comunicaciones tradicionales de 2 líneas telefónicas (troncales), una central telefónica y 8 anexos distribuidos en toda la empresa.

La organización mensualmente realiza un gasto elevado en comunicaciones debido a las constantes llamadas a los clientes para la coordinación de los proyectos que la empresa desarrolla. La gran mayoría de proyectos desarrollados son para clientes a nivel nacional y algunos últimamente a nivel internacional, el grado de comunicación que estos demandan es elevado. Así mismo los demás servicios que la empresa ofrece a sus clientes después de la implantación de los proyectos que requiere de un monitoreo constante

y demanda una comunicación fluida entre los usuarios de los sistemas y la empresa.

Ocasionalmente los clientes muestran cierto grado de incomodidad debido a que la comunicación entre los encargados del desarrollo de los proyectos por parte del cliente y los integrantes del equipo de proyecto por parte de la empresa no tienen una comunicación adecuada debido a que la central telefónica tradicional con la que cuentan esta saturada o simplemente por que el personal no se encuentra o esta ocupado.

La empresa cuenta con una red de datos estructurada que cumple con los estándares requeridos además cada empleado cuenta con su computadora personal asignada y su respectivo anexo telefónico, La empresa cuenta con una conexión a Internet Speedy Business al 10% en el plan de 2000 (2048/512Kbps). La organización periódicamente le da mantenimiento a su red de datos y a su central telefónica para lo cual adquiere los servicios de una empresa que se encargue de todo el mantenimiento y también de la extensión de su red de datos así como la instalación de los nuevos puntos de red o de la implantación de más anexos telefónicos.

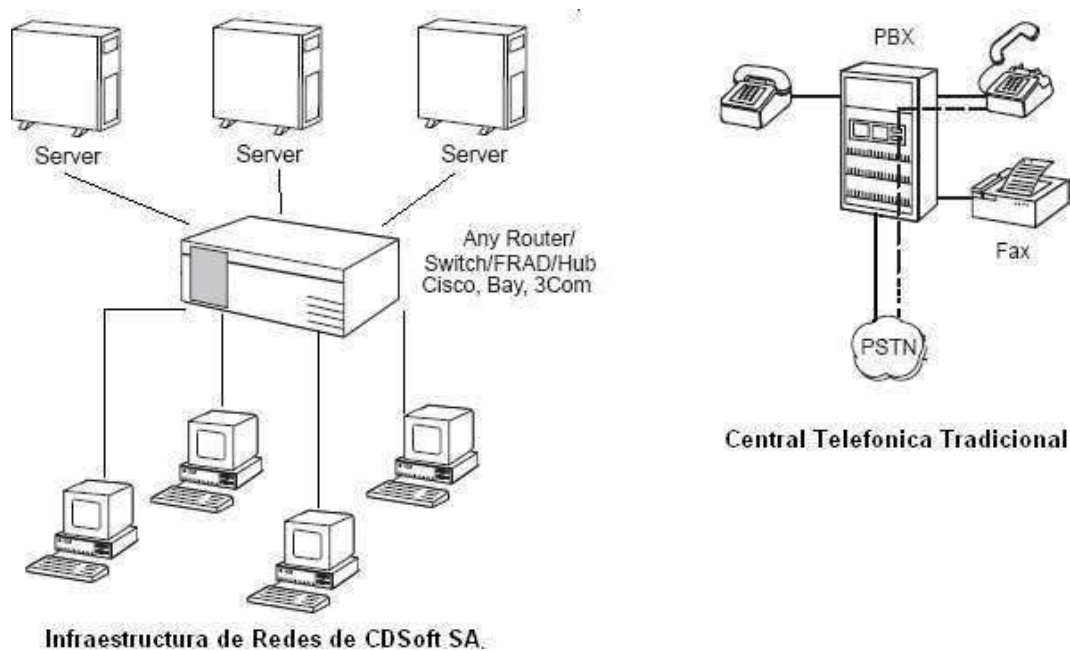


Figura 8 Estructura Actual de Voz y Datos de CDSOFT S.A.

La central telefónica con la que cuenta la empresa es un PBX Matra Nortel 6501-C la cual nos permite de 6 – 40 puertos y/o extensiones.

Luego de haber configurado el servidor asterisk y los terminales IP así como también todas las extensiones necesarias para el funcionamiento entre ellas nuestra infraestructura quedaria como lo muestra la Figura .

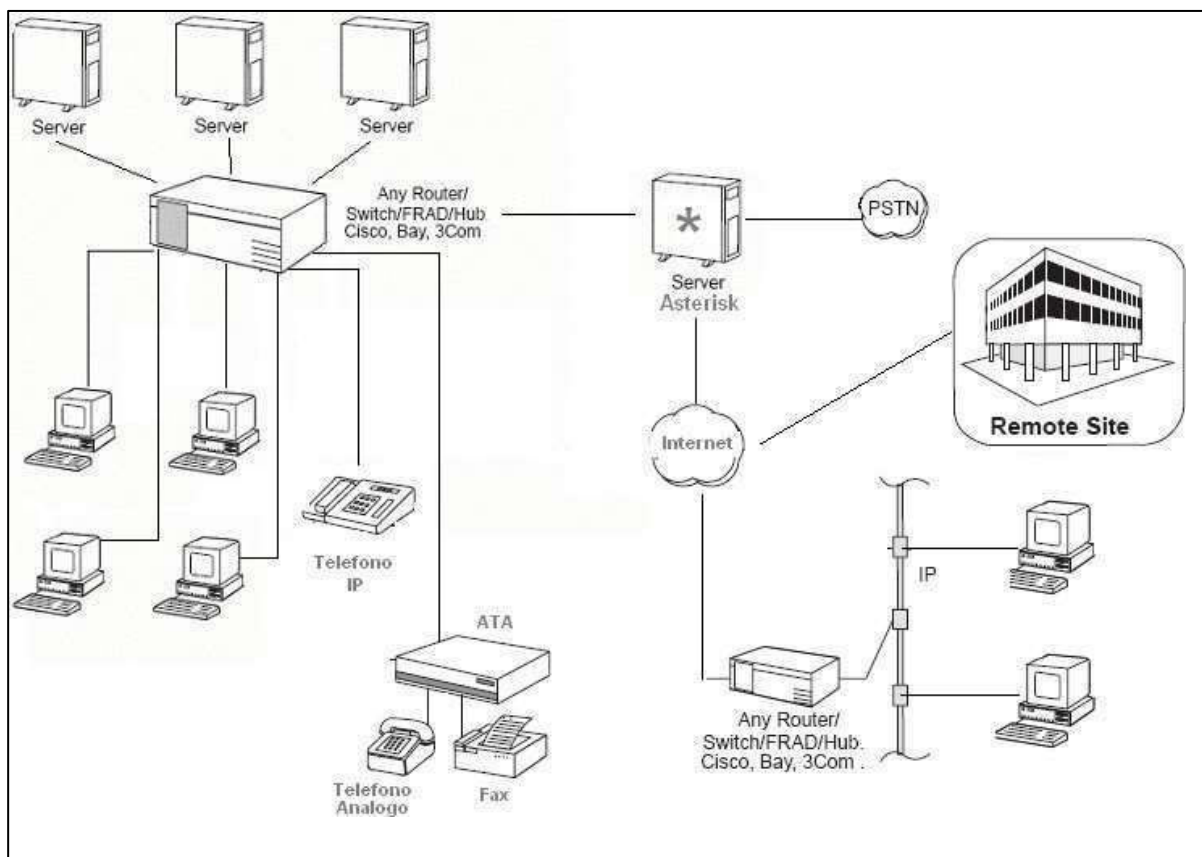


Figura 9 Infraestructura al Final de la Implantación de Asterisk como IP PBX

5.2 Modelo de Implantación de la Solución.

La solución que presentamos en el presente proyecto es la implementación de un Sistema de Telefonía IP sobre una plataforma Linux CentOS con el software Open Source Asterisk el cual nos sirve como administrador de los servicios de la centralita, donde el principal objetivo es el de utilizar los recursos actuales de infraestructura de red y la tecnología para reducir los costos de comunicación en la empresa CDSOft S.A.

5.2.1 Los medios físicos, características y equipamiento necesarios para la implantación

El equipamiento necesario estará definido por la infraestructura de red actual de CDSOFT S.A.

Implantaremos unos cuantos teléfonos IP que se conectan a una red LAN (típicamente Ethernet) y bastará con enchufar uno de estos a una boca Ethernet. En este caso no hubo que cablear ya que todo dependía de los puntos de red existentes dentro de la red actual, en otras condiciones tendrá mayor capacidad de crecimiento y menor coste de instalación (salvo, claro está, en el caso en que la proliferación de teléfonos IP nos obligara a potenciar drásticamente los equipos de interconexión LAN y cablear mas puntos de red).

Posteriormente, el encaminamiento de las llamadas por la WAN ya será misión del router o de la PBX, esto dependerá de si la empresa desea seguir con la PBX actual (Matra Nortel 6501-C).

La organización puede adoptar este sistema abandonando rápidamente sus servicios antiguos. O puede también seguir aprovechando sus sistemas de

voz y realizar una migración gradual hacia una infraestructura de IP, agregando funciones y características a su propio ritmo. Los sistemas IP pueden coexistir con los sistemas heredados: es lo que se conoce como “solución híbrida”.

A continuación se describirán los distintos componentes que fueron necesarios para implementar el sistema de Telefonía IP sobre plataforma Linux y Asterisk.

5.2.1.1 Terminales IP

Hablando en terminología tradicional son extensiones telefónicas que se conectan sobre la red de datos LAN. Pueden ser:

- Terminales IP específicos (Teléfonos IP)
- Terminales propietarios con un adaptador IP(Teléfonos Análogos conectados a un ATA)
- PCs multimedia con conexión a la red (SoftPhone).

Estos terminales realizan la función de compresión y paquetización en tiempo real (así

como el proceso inverso en el caso de recepción de una llamada).

Un terminal IP que este diseñado de acuerdo a H.323 puede soportar:

- G.711, G.723 y/o G.729 para la compresión/descompresión de audio.
- H.261 y/o H.263 para la compresión de vídeo (definida también en H.323)
- T.120 para la transmisión de datos que incluye los T.12x (ver en descripción general de H.323, apartado 3.2)
- H.245 para la negociación de parámetros y capacidades en la llamada.
- Q.931 (definida en RDSI) para señalización y establecimiento de llamada.
- H.225, como interfaz de acceso al *gatekeeper* (para encaminamiento de llamadas) mediante mensajes RAS (*Registration, Admisión, Status*) usándose E.164³ para establecer la correspondencia de IP con el número telefónico Además, H.225 describe los medios por los cuales, audio, vídeo, datos y control son

³ E.164 es la normativa actual de numeración/direccionamiento de RDSI, lo cual facilita la interoperabilidad de extensiones IP y analógicas o digitales tradicionales

asociados, codificados y paquetizados para su transmisión por el medio.

5.2.1.2 Red LAN

Como se utilizan terminales IP en la red LAN es preciso indicar que para conectarlos solo necesitamos utilizar la misma infraestructura de red.

Las redes LAN de un tamaño considerable, con multitud de elementos de interconexión (switches, hubs...) pueden ser problemáticas en cuanto al retardo que puedan generar, ya sea porque un alto índice de ocupación aumente las colisiones o porque las colas de acceso de los switches estén con un elevado número de datos esperando a ser conmutados (lo que impone un retardo que puede ser desastroso para la VoIP).

5.2.1.3 Red WAN

Técnicamente hoy en día en CDSOFT S.A. es posible utilizar VoIP sobre WAN, suponiendo

que existe ancho de banda disponible sobre ella. Para lo cual solo tendría que contactarse con un proveedor que le permita salir a llamadas por Internet.

Para esto cada tipo de red y cada operador suele indicar en el contrato los siguientes parámetros determinan la calidad de servicio.

- Tipo de tráfico (Tráfico de voz y datos)
- Ráfagas (entre 250 Kb/s – 800 Kb/s)
- Ancho de Banda. (Mínimo 256 kbps)
- Latencias, Retardos. (aceptable por debajo de los 150 ms)
- *Jitter*(Lo ideal es q esta diferencia se encuentre entre los 20ms a 25ms)
- Pérdida de paquetes(de orden 0.3% en las redes)

Existen diversos mecanismos para garantizar la calidad de servicio en la red. La filosofía básica de dichos mecanismos se basa en hacer posible que cada aplicación pueda, en un momento dado, “reclamar” de la red una garantía

de que los recursos que necesita estén disponibles.

5.2.1.4 Servidor Linux con Asterisk

Se implemento el servidor Asterisk en una PC de las siguientes características:

- Procesador Pentium IV de 3.0 Ghz.
- Placa Intel D915GEV
- 512 de Memoria Ram DDR
- Disco Duro de 80 GB con tecnología SATA.
- Tarjeta PCI TDM400P TDM04B Digium Direct con 4 puertos FXO.
- Tarjeta de Red D-link 10/100.

A este servidor se le instalo el software Asterisk@Home version1.5, el cual contiene el sistema operativo Linux CentOS, además de aplicaciones como freepbx, Asterisk recording interface, A2billing, Sugar CRM, herramientas para configuración de teléfonos Cisco, etc. En el presente solo tocaremos las configuraciones básicas con las características principales de una central telefónica y algunas de sus características

avanzadas como herramienta mejorada o como una central telefónica mejorada.

En el servidor se instalo una tarjeta PCI TDM400P que tiene una función similar a la de un MODEM especialmente dedicada a gestionar el tráfico de voz. La tarjeta seleccionada fue el modelo TDM04B que tiene 4 puertos para conectar Líneas Telefónicas que son los puertos FXO.



Figura 10 Tarjeta FXO TDM400P

Existen además de la tarjeta mencionada, otras con la misma función de ofrecer puertos FXS o FXO dependiendo mucho de lo que se requiera a la hora de la implementación mencionaremos algunos de los modelos y sus principales características, con el fin de dar un

alcance de el hardware con el que puedan contar para futuras implementaciones.

- **Tarjeta Digium TDM20B:** Posee 2 módulos FXS, interfase PCI, y compatible con los protocolos SIP, IAX, H.323.
- **Tarjeta Digium TDM30B:** Posee 3 módulos FXS, interfase PCI, y compatible con los protocolos SIP, IAX, H.323.
- **Tarjeta Digium Wildcard TDM2401B:** Posee 4 módulos FXO, interfase PCI, incluye todas las características sofisticadas de un sistema de teléfono high-end del negocio.

La instalacion de estas tarjetas en el servidor asterisk es de facil configuración solo basta insertarlas en un slot PCI y confirara los driver que vienen con el hardware, asi mismo la capacidad de cuantas tarjetas podemos poner en nuestro servidor dependera de la cantidad de slots PCI disponibles que tengamos en nuestro servidor, esto tambien dependera mucho de la

cantidad de líneas que tengamos en nuestra organización.

Cabe señalar que para las terminales PC se utilizo Softphone en este caso el X-lite donde después de una simple configuración ya se podía tener todas las bondades de nuestra central telefónica implantada. La instalación de este softphone X-lite no afecto en nada a los usuarios que trabajan sobre el sistema operativo Windows al momento de usarla como teléfono solo basto agregar a las PCs los auriculares y micrófonos necesarios para la comunicación.

Desde cualquier PC que cuente con el Sistema Operativo Windows se puede acceder al modulo de administración del IP PBX, a través de un navegador, cabe señalar que este modulo contiene un usuario y password de seguridad.

5.2.2 Configuración del Servidor Asterisk

A continuación explicaremos como se desarrollo el proceso de configuración del paquete asterisk@home

que incluye asterisk y la herramienta de configuración GUI basada en la Web.

Los componentes que configuramos fueron los siguientes: el IP PBX, los terminales y el servicio de portal que le permita llamar a cualquier persona a través de RTB.

5.2.2.1 IP PBX

En la PC que nos proporciona la organización la usamos como servidor para instalar el IP PBX, a la cual se le instala el Asterisk@home que es un paquete que consiste en muchos componentes mayores. Estos fueron desarrollados y soportados independientemente. El origen del nombre se da por que la parte ‘Asterisk’ es una base IP PBX, y la parte ‘@home’ que consiste en aplicaciones, un sistema de provisión, un instalador, un sistema de operación, que juntos hacen un paquete completo.

En el dicho equipo se implantará la centralita telefónica se hará iniciar el equipo desde el CD de Instalación Asterisk@home, Esto

formateara el disco duro y cargara todo desde el sistema operativo, luego esperara que todo cargue y compile, esto tomara 20 minutos dependiendo de la rapidez de la computadora, al finalizar la instalación retiramos el CD y reiniciamos desde el disco duro.

Una vez reiniciado el equipo, este nos mandará al prompt en el cual nos pedirá un usuario y password para lo cual se insertara lo siguiente:

```
Username      :      root
Password      :      password
```

Si queremos cambiar el password inicial solo debemos digitar el comando ***passwd*** con el cual se le solicitara ingresar un nuevo password y reconfirmar.

Al término de la instalación la maquina recibió una dirección IP que debemos cambiar para esto es necesario, ejecutar el comando: ***netconfig*** que exhibirá la información de la configuración. Se debe cambiar los siguientes datos (en el caso de la implantación en la

empresa CDSOft S.A. quedo registrado de la siguiente manera):

IP address	:	192.168.0.40
Netmask	:	255.255.255.0
Gateway	:	192.168.0.1
DNS Server	:	192.168.0.1

Al terminar de realizar los cambios se reinicia la PC para que los cambio tengan efecto. Después de reiniciar la PC loguearse una ves mas, Una vez terminado con estos cambios se puede seguir con la configuración a través de la Web. Para lo cual desde el navegador Web de cualquiera de las PC en la red de CDSOft S.A. ingresamos a la IP designada al servidor en el caso planteado será de la siguiente manera ***http://192.168.0.40*** en donde visualizaremos lo siguiente:



Figura 11 Interfaz grafica de Configuración del Asterisk

Para empezar a configurar las extensiones así como las demás opciones entraremos a la opción **Asterisk Managemenet Portal** o mas conocido como **AMP**, para lo cual también accederemos a esta opción mediante un login y un password.

Username : maint
Password : password

Ingresados correctamente los datos se debería acceder a la pantalla principal AMP.

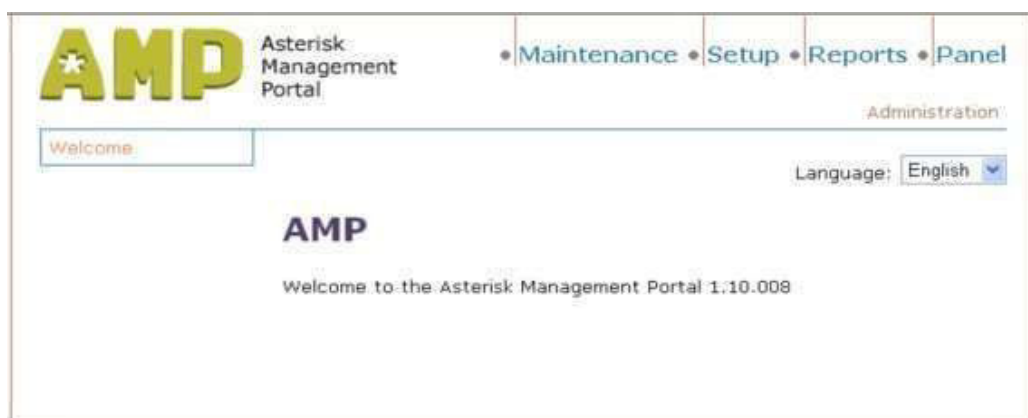


Figura 12 Pantalla principal del AMP

Ingresamos en la opción **Setup** para entrar en la pantalla de configuración personal.



Figura 13 Menú de Opciones de Setup del AMP

5.2.2.1.1 Configurar Troncales (Trunks):

Para empezar configuraremos la salida de llamadas a través de un proveedor de servicios VoIP.

Ingresamos ahora a la opción **Trunks** y luego **Add SIP Trunk**. Se vera una forma de espacio SIP trunk.

Trunk.” You see a blank SIP trunk form.

AMP Asterisk Management Portal

Maintenance • Setup • Reports • Panel

Setup:

Add SIP Trunk

General Settings

Outbound Caller ID: 7237570239

Maximum channels: 1

Outgoing Dial Rules

Dial Rules:

Clean & Remove duplicates

Dial rules wizards: (pick one)

Outbound Dial Prefix:

Outgoing Settings

Trunk Name: BroadVoice

PEER Details:

```
host=***provider ip address***
username=***userid***
secret=***password***
type=peer
```

Figura 14 Pantalla de Configuración de Trunk

En esta sección completamos las partes mas importantes de SIP/Trunk, se configura el proveedor de la organización que es Broadvoice solo para servicio saliente.

Outbound caller ID : 7237570239

Max channels : 1

En “outcoming setting” llenar con lo siguiente:

Host	:	Direc IP del Proveedor
UserName	:	UserId o Id de Usuario
Secret	:	Password o clave Type
	:	peer

Una vez que toda la información sea integrada, se puede hacer clic en el botón ***submit***, después de ello una línea roja aparecerá en la parte superior de la pantalla, para poder aplicar tus cambios debes hacer clic en esta línea con la finalidad de recargar los archivos del Asterisk.

5.2.2.1.2 Configurar Extensiones

Ahora es el momento de definir las extensiones. Para lo cual definiremos 2 extensiones como ejemplo de aplicación, numero 200 en la oficina principal y numero 201 en la estación 1. Ingresamos a la opción ***Extensions*** a la izquierda, y luego

Add An Extension veremos la pagina de siguiente.

AMP Asterisk Management Portal

Maintenance • Setup • Reports • Panel

Setup

Add an Extension

Account Settings:

phone protocol: SIP rfc2833

extension number: 200

extension password: 123456

full name: Oficina

Record INCOMING: ☐ Always ☐ Never ☒ On-Demand

Record OUTGOING: ☐ Always ☐ Never ☒ On-Demand

Voicemail & Directory: Enabled

voicemail password: 123456

email address: oficina@ejemplo.com

pager email address: oficina@ejemplo.com

email attachment: ☐ yes ☒ no

Play CID: ☐ yes ☒ no

Play Envelope: ☐ yes ☒ no

Add Extension	
"basement" <200>	
"study" <201>	
7327570239	

Figura 15 Pantalla de configuración de extensiones

La información que completaras será la siguiente:

Extension : 200

Password : 123456

Full name : Oficina

Voice Mail Password : 1234
Email Address : <email>

Cuando se termina de adicionar la extensión, se pueden ver los detalles de esta misma haciendo click en el nombre al lado derecho de la interfase AMP (como se aprecia en la figura 14).

Para la extensión siguiente se haran los mismos pasos Add Extension y configuramos con los datos siguientes:

Extension : 201
Password : abcdef
Full name : Estacion
Voice Mail Password : 1234
Email Address : <email>

De esta manera podemos seguir configurando las extensiones que deseemos. Recordar que para que los cambios surtirán efecto luego de presionar submit.

5.2.2.2 Configuración de Terminales IP

En este punto, vamos a tratar sobre la configuración de los terminales IP, para esto utilizaremos un software denominado X-lite que es un SoftPhone que nos permite recepcionar o realizar llamadas a través del Sistema de Telefonía IP implantada que tienen como pasarela el servidor Asterisk.

Como ya tenemos configuradas las extensiones en Asterisk (extensiones 200 y 201), lo único que queda por hacer es lo siguiente, instalamos el software en cada una de las pcs, ejecutamos el X-Lite.



Figura 16 Mascara de X-Lite SoftPhone

Luego se configurara de la siguiente manera:

Damos clic en la opción Menú luego en System Settings , seguidamente Sip Proxy y por ultimo Default, apareciéndonos una ventana como lo muestra la Figura 16, donde ingresaremos los siguientes datos:

User name	:	200
Authorization user	:	200
Password	:	123456

Domain/Realm : 192.168.0.40
SIP Proxy : 192.168.0.40

Esta configuración sería para la PC que se encuentra en la oficina principal.



Figura 17 Pantalla de X-Lite Configuración

Cuando este configurado el X-Lite lo único que debemos hacer es cerrar el menú y volver a la pantalla principal del SoftPhone en donde podremos constatar que muestre el mensaje 'logged in' (loggado) como se muestra en la Figura 17.



Figura 18 Pantalla de SoftPhone Configurado correctamente

Configurado esto en nuestras terminales IP, ya podemos realizar las comunicaciones deseadas entre anexos.

5.3 Ventajas obtenidas al implantar Asterisk como PBX

Al implementar y configurar asterisk como una central telefónica se tiene diversas ventajas con respecto a las centrales telefónicas tradicionales como:

5.3.1 Ahorro de costos.

La ventaja más importante es la reducción de los gastos mensuales que la empresa periódicamente

obtenía en materia de telecomunicaciones. Debido a que la implantación de una central telefónica basada en telefonía IP es más económica (aproximadamente un 50% de reducción de gastos en el caso de llamadas internacionales), lo que supone un gran ahorro en las llamadas internacionales. Las llamadas internas entre los distintos usuarios de la empresa son gratuitas.

Cabe resaltar como muestra la tabla 5, que no para todos los destinos el costo de llamada por minuto es un ahorro, debido a que en nuestro país no existen todavía proveedores nacionales de VoIP porque esta tecnología aun esta en sus comienzos en nuestro país.

En el caso de llamadas a nivel local por decir hay un pequeño desbalance con respecto a la tarificación debido a que este proveedor para conectarnos una llamada a nivel local hace una conexión desde su sitio origen (España) hasta el lugar destino (Perú), por lo cual el costo es un poco más elevado pero no es mucha la diferencia.

Servicio	COSTO X MINUTO					
	Fijo local	Nacional	Nacional a cualquier Celular	Móvil Movistar	Móvil Claro	Nextel
Telefonía Tradicional	S/. 0.13	S/. 0.740	S/. 1.6950	S/. 0.9702	S/. 0.9702	S/. 1.1502
VOIP (PeopleCall)	S/. 0.135	S/. 0.475	S/. 1.1308	S/. 0.8308	S/. 0.8308	S/. 0.8308

Tabla 5 Tabla de costos de llamadas x Minuto

En la tabla 6 podemos ver con mayor detalle el ahorro de las llamadas por VoIP a nivel internacional para lo cual hemos tomado algunos destinos que utiliza para comunicarse la empresa CDSOFT S.A.

Servicio	USA		Colombia		España		Venezuela	
	Fijo	Móvil	Fijo	Móvil	Fijo	Móvil	Fijo	Móvil
Telefonía Tradicional	2.431		2.431		2.431		2.431	
VOIP (PeopleCall)	0.1188	0.2432	0.2826	0.3687	0.0942	0.6555	0.3687	0.7948

Tabla 6 Tabla detallada de destinos tarificada por minuto

Las tarifas tomadas de la telefonía tradicional son en horarios Diurno de 08:00 – 20:00 y en lo que respecta a las llamadas locales se está tomando el cargo por establecimiento de llamada (1 minuto equivalente a S/0.065) las de PEOPLECALL son de 00:00 – 24:00

Como se puede apreciar en las tablas los precios en telefonía tradicional en comparación con las compañías de telefonía IP son muy contrastantes

5.3.2 Productividad.

En general, las mejoras en productividad derivaban de que ya no se pierde tiempo en tomar y recoger mensajes, y que es mucho más fácil ponerse en contacto con las personas. Estas funciones, junto con la capacidad de redirigir las llamadas de voz en función de la identificación del usuario, dieron lugar a una mayor capacidad de respuesta de cara al cliente.

Una de las ventajas clave de VoIP es que el número de teléfono de cada persona es suyo exclusivamente. Este número se vincula a una ubicación física únicamente cuando el usuario inicia una sesión. Esto significa que las llamadas sobre IP se encaminan directamente a un empleado, esté donde esté, siempre que esté conectado a la red. Esto incluye la oficina en casa conectada a la red principal a través de una conexión IP VPN segura, con banda ancha.

5.3.3 Optimización de Recursos.

Al realizar la convergencia de la red de voz y datos se redujo los costos de mantenimiento, ya que la empresa sólo pagaría por el mantenimiento de una única

red de voz y datos, en lugar de dos redes diferentes. Además, los costos de los traslados, nuevos usuarios y cambios que eran un proceso pesado cuando se utiliza un sistema basado en telefonía tradicional que implicaba un acceso físico a la centralita, se redujeron casi a cero con la implantación de asterisk ya que se pueden realizar de forma remota, con una herramienta de autogestión de usuario basada en la Web o desde una única consola con funciones complejas.

5.3.4 Compatibilidad con el Tele trabajo.

Dado que los usuarios están accesibles desde cualquier lugar, siempre que se puedan conectar a la red corporativa, es muy fácil practicar el teletrabajo. Basta con que el empleado inicie una sesión en un teléfono IP y recibirá automáticamente acceso a los servicios de voz. Esto significa que la empresa puede tener un único sistema telefónico, en lugar de una mezcla de equipos en la oficina y líneas únicas para aquéllos que trabajen desde casa, lo que da una imagen más profesional. Además, los empleados tienden a utilizar menos sus teléfonos móviles, lo que también reduce los costes.

5.3.5 Calidad de Servicio a los clientes.

En general, los clientes obtendrán un mejor trato y una mejor comunicación efectiva con los integrantes del equipo de desarrollo de los proyectos y los encargados en el monitoreo de los sistemas implantados, que se ejecutaron en la empresa mejorando y elevando la calidad del servicio y el aumento de la producción por parte de los empleados de la organización.

5.4 Costos de Implantación y beneficios

5.4.1 Beneficios de Asterisk frente a lo tradicional

- Desplegar automáticamente la ficha del cliente en la pantalla del ordenador al recibir una llamada suya.
- Creación aplicaciones basadas en menús de voz que permitan por ejemplo a sus clientes conocer el estado de sus pedidos con una llamada de teléfono, todo de manera automática.
- Realizar llamadas internacionales a bajo coste a cualquier destino a precios en torno a los dos céntimos de euro el minuto (S/. 0,015 x min).
- Realizar llamadas gratuitas a sus delegaciones, desde su teléfono directamente a la extensión que desee.

- Buzones de voz ilimitados con recepción de los recados por email, operadora virtual, desvíos, extensiones móviles a cualquier lugar con acceso a Internet y muchas otras prestaciones de telefonía avanzada.

Las soluciones de telecomunicaciones basada en Asterisk son económicas, robustas, potentes, flexible y protegen la inversión.

5.4.2 Económico

Asterisk es más económico principalmente por dos motivos, por qué utiliza equipos estándar y está basado en código abierto.

Los servidores y los teléfonos usados son estándar, los producen multitud de fabricantes, que compiten entre ellos en prestaciones y precio. En el caso de una centralita IP propietaria, la empresa está obligada a adquirir un hardware concreto a un precio establecido a un solo fabricante. Los teléfonos estándar no funcionan o lo hacen parcialmente, y únicamente se pueden comprar al fabricante de la centralita.

Asterisk es de código abierto, por lo que se obtienen gratuitamente el código fuente y todas las futuras actualizaciones. Todas las prestaciones que en otra centralita son de pago, en Asterisk vienen incorporadas, sólo hay que configurarlas y ponerlas en producción. A Asterisk puede conectar cuantos teléfonos quiera mientras el servidor tenga potencia para gestionarlos, no pagará ninguna licencia por cada extensión, ni por cada buzón de voz asociado a la extensión, etc.

5.4.3 Robusto

Asterisk se ejecuta sobre servidores Linux, sistema operativo de gran robustez y estabilidad. Para soluciones a prueba de fallos, AIX Telecom instala clústers de alta disponibilidad con dos servidores para asegurar un servicio de telefonía sin interrupciones.

5.4.4 Potente

Asterisk se ha diseñado para realizar todo lo que un sistema tradicional de telefonía puede hacer, y más, mucho mas.

- Desvíos, grupos de llamadas y demás aplicaciones de la telefonía básica.
- Buzones de voz con consulta desde web o envío al correo electrónico del mensaje como un archivo de sonido adjunto.
- Música en espera.
- Multi-conferencias de voz.
- Aplicaciones interactivas de voz (IVR).
- Gestión de colas de llamadas.
- Identificación de llamadas.
- Registro de llamadas a base de datos (CDR)
- Selección dinámica del operador (rutas de bajo coste).
- Call center básico (aplicaciones de terceros para soluciones a gran escala).
- Marcación predictiva, etc.

5.4.5 Flexible

Asterisk se configura y adapta a la medida de cada organización como ninguna otra centralita del mercado.

Debido a su sistema de configuración a bajo nivel, la centralita prácticamente se programa a medida para cada cliente, permitiendo adaptarla para cubrir prácticamente todas las necesidades de su empresa, hasta el mínimo detalle.

Gran capacidad de integración con el resto de sistemas y de aplicaciones de su organización, sobre el núcleo de conmutación de Asterisk, se pueden conectar 4 diferentes interfaces de programación que pueden desarrollar aplicaciones a medida, integrarlo con sus sistemas, bases de datos, o integrar aplicaciones comerciales como Call centers.

5.4.6 Protege la inversión

La elección de una centralita IP basada en Asterisk tiene una ventaja importante más, protege la inversión. La inversión en software y equipos que se realiza por parte de la empresa no depende de la continuidad que un fabricante quiera dar al producto que ha comprado. Utilizando Asterisk la empresa puede aprovechar de nuevo los servidores y al ser el software de código abierto, dispone del código fuente y de los ficheros de configuración para modificarlo si lo necesita.

5.5 Especificaciones de Seguridad

En el tema de seguridad se tiene que considerar muchos aspectos ya que desafortunadamente, las nuevas tecnologías traen también consigo detalles a tener en cuenta con respecto a la seguridad.

Al optar por la convergencia de Voz y Datos, las señales analógicas de voz son digitalizadas, comprimidas en paquetes y enviadas a través de la red de datos. Los algoritmos avanzados de compresión reducen el ancho de banda necesario para una llamada de voz de calidad. Debido a esto tenemos que preocuparnos más por el resguardo de la red, ya que por ahí no solo circula documentación e información valiosa si no también otro tipo de recurso tanto o más importante.

En la seguridad de la transmisión y la calidad, el silencio y el ruido de fondo en la transmisión pueden ser eliminados, el despliegue de la voz sobre IP reduce el coste y mejora la escalabilidad empleando componentes de redes de datos estándares (routers, switches, etc.), en vez de los costosos y complicados switches para teléfonos. Ahora el mismo equipo que dirige las redes de datos puede manejar una red de voz esto conlleva a realizar una planificación mas

detallada y especializada en el mantenimiento de la infraestructura de la red de datos.

En el proceso de ahorrar dinero (objetivo del proyecto) e incrementar la eficacia, dos porciones cruciales de la infraestructura de cualquier empresa, voz y datos, fueron combinadas. Los servidores de VoIP actuaran como puertas de enlace; así, routers especiales, teléfonos, nuevos protocolos y sistemas operativos están ahora entremezclándose con esta nueva tecnología.

5.5.1 Amenazas

Existen numerosas amenazas que conciernen a las redes VoIP; muchas de las cuales no son muy obvias para la mayoría de los usuarios. Los dispositivos de redes, los servidores y sus sistemas operativos, los protocolos, los teléfonos y su software, todos son componentes vulnerables.

En este sentido la información sobre una llamada es tan valiosa como el contenido de la voz. Por ejemplo, una señal comprometida en un servidor puede ser usada para configurar y dirigir llamadas, del siguiente modo: una lista de entradas y salidas de llamadas, su duración y sus parámetros. Usando esta información, un atacante puede obtener un mapa detallado de todas las

llamadas realizadas en tu red, pudiendo crear grabaciones completas de conversaciones y datos de usuarios.

La conversación es en sí misma un riesgo y el objetivo más obvio de una red VoIP. Consiguiendo una entrada en una parte clave de la infraestructura, como una puerta de enlace de VoIP, un atacante puede capturar y volver a montar paquetes con el objetivo de escuchar la conversación. O incluso peor aún, grabarlo absolutamente todo, y poder retransmitir todas las conversaciones sucedidas en tu red.

Las llamadas son también vulnerables al “secuestro”. En este escenario, un atacante puede interceptar una conexión y modificar los parámetros de la llamada. Se trata de un ataque que puede causar bastante temor, ya que las víctimas no notan ningún tipo de cambio. Las posibilidades incluyen la técnica de spoofing o robo de identidad, y redireccionamiento de llamada, haciendo que la integridad de los datos estén bajo un gran riesgo.

La enorme disponibilidad de las redes VoIP es otro punto sensible. En la telefonía RTB, la

disponibilidad era raramente un problema. Pero es mucho más sencillo hackear una red VoIP. Todos estamos familiarizados con los efectos demoledores de los ataques de denegación de servicio. Si se dirigen a puntos clave de la red, podrían incluso destruir la posibilidad de comunicación vía voz o datos.

Los teléfonos y servidores son blancos de ataques por sí mismos. Aunque sean de menor tamaño o nos parezcan simples teléfonos, son en base, ordenadores con software. Obviamente, este software es vulnerable con los mismos tipos de bugs o agujeros de seguridad que pueden hacer que un sistema operativo pueda estar a plena disposición del intruso. El código puede ser insertado para configurar cualquier tipo de acción maliciosa dentro del dispositivo.

5.5.2 Recomendaciones de Seguridad

Hemos enumerado algunas de las amenazas o graves problemas de seguridad. Afortunadamente, los riesgos que comporta usar el protocolo VoIP no son muy diferentes de los que nos podemos encontrar en las redes IP. Desafortunadamente, en los diseños iniciales de hardware para voz, software y protocolos, la seguridad no es un punto fuerte.

Listaremos consideraciones que pueden protegernos de las amenazas sobre esta tecnología.

5.5.2.1 Encriptación

Lo primero que debemos tener en mente a la hora de implantar VoIP es la encriptación. Aunque lógicamente no es sencillo capturar y decodificar los paquetes de voz, puede hacerse. Y encriptar es la única forma de prevenirse ante un ataque, una consideración muy importante de esta opción es que nos ocasionara utilizar mas ancho de banda.

Por tanto debemos considerar el ancho de banda que tenemos actualmente en la organización pero existen múltiples métodos de encriptación o posibilidades de encriptación: VPN (virtual personal network), el protocolo Ipsec (IP segura) y otros protocolos como SRTP (secure RTP).

El objetivo de cualquier forma, es elegir un algoritmo de encriptación rápido, eficiente, y

emplear un procesador dedicado de encriptación. Esto debería aliviar cualquier atisbo de amenaza. Otra opción podría ser QoS (Quality of Service); los requerimientos para QoS asegurarán que la voz se maneja siempre de manera oportuna, reduciendo la pérdida de calidad.

5.5.2.2 Configuración Adecuada de los componentes

El proceso de seguridad de todos los elementos que componen la red VoIP: servidores de llamadas, routers, switches, centros de trabajo y teléfonos. Es imperativo. Se Necesita configurar cada uno de los dispositivos para asegurarse de que están en línea con las demandas en términos de seguridad. Los servidores pueden tener pequeñas funciones trabajando y sólo abiertos los puertos que sean realmente necesarios. Los routers y switches deberían estar configurados adecuadamente, con acceso a las listas de control y a los filtros. Todos los dispositivos deberán estar actualizados en términos de parches y actualizaciones. Se trata del mismo tipo de precauciones que se podría tomar cuando añadimos nuevos elementos a la red de datos;

únicamente habrá que extender este proceso a la porción que le compete a la red VoIP.

5.5.2.3 Disponibilidad de la Red

La disponibilidad de la red es muy preocupante, una pérdida de potencia puede provocar que la red se caiga y los ataques DdoS son difíciles de contrarrestar. Aparte de configurar con propiedad el router, hay que tener en cuenta que los ataques no solo irán dirigidos a los servicios de datos, sino también a los de voz.

5.5.2.4 Utilización de un Firewall y un IDS

Por último, se puede emplear un firewall y un IDS (Intrusion Detection System) para ayudar a proteger la red de voz. Los firewalls de VoIP son complicados de manejar y tienen múltiples requerimientos. Los servidores de llamada están constantemente abriendo y cerrando puertos para las nuevas conexiones. Este elemento dinámico hace que su manejo sea más dificultoso. Pero el costo está lejos de verse oscurecido por la cantidad de beneficios, así que hay que utilizar

algo de tiempo para ir perfeccionando los controles de acceso. Un IDS monitoriza la red para detectar cualquier anomalía en el servicio o un abuso potencial. Las advertencias son una clave para prevenir los ataques posteriores.

Según los ejecutivos de gigantes organizaciones como Nortel Networks, Cisco Systems o Alcatel, las empresas tendrán que protegerse más que nunca de los ataques DoS, gusanos e incluso spam de VoIP. "Como cualquier red IP, la seguridad es una cuestión permanente. No estás protegido ni desprotegido, simplemente entras en un proceso de seguridad que nunca acaba. Siempre hay que estar preparados para el próximo problema que pueda surgir."

Las organizaciones creen que podrán acorazar sus redes adecuadamente para que sean tan seguras como las tradicionales. El problema de estas redes podrían ser los agujeros de seguridad del software. "Se Pueden tener de seguridad el 99,999% pero en un simple error que

haya en el software, la red puede dejar de funcionar.

5.6 Posibles escenarios de Instalación con Asterisk

A continuación presentaremos otros escenarios de los muchos que se podrían dar en cada organización, dependiendo el uso que se le quiera dar mediante la implementación del Asterisk. Los casos a describir serán los siguientes:

- Centralita Nueva con conexiones y extensiones de varios tipos
- Pasarela para dotar a una centralita tradicional de servicios nuevos
- Pasarela para dotar a una centralita tradicional de nuevas extensiones
- Varias Oficinas con un Asterisk Centralizado
- Varias Oficinas con Sistemas Asterisk interconectados

Los otros casos de uso pueden ser muchos más solo se presentaran algunos casos de ejemplo. Asterisk está preparado para cubrir prácticamente todas las necesidades de comunicaciones existentes y lo más importante, es siempre actualizable para nuevos servicios que se vayan añadiendo. La videoconferencia, el envío de SMS mediante la línea Fija. Servicios Automáticos de respuesta interactiva y demás aplicaciones cubren prácticamente todas las necesidades existentes en el sector de las Comunicaciones.

5.6.1 Centralita Nueva con conexiones y extensiones de varios tipos

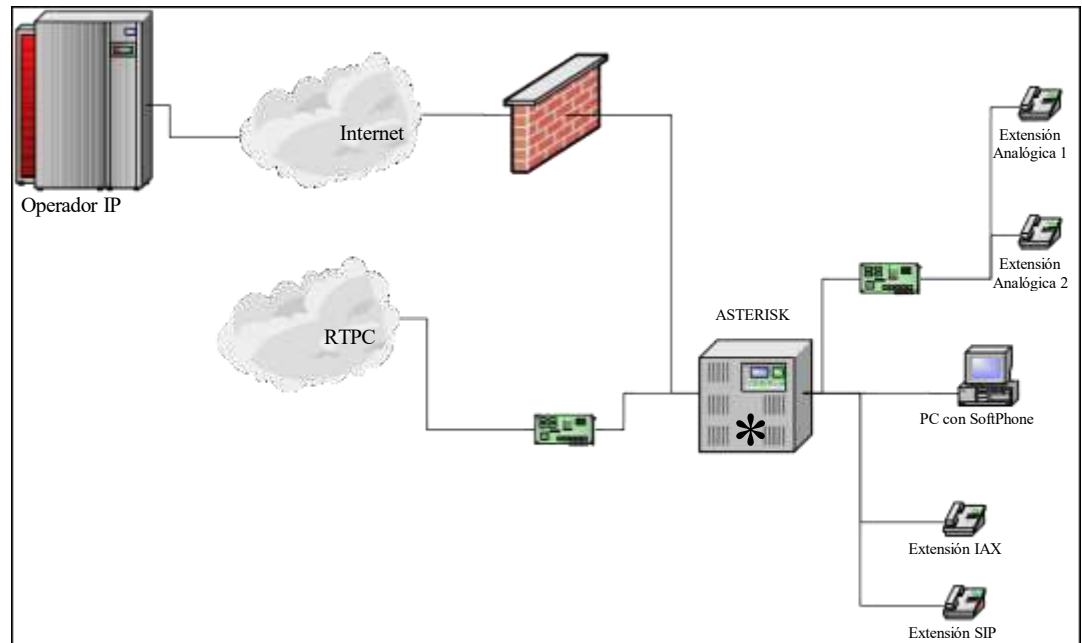


Figura 19 Implantación de Asterisk Escenario 1

5.6.2 Pasarela para dotar a una centralita tradicional de servicios nuevos

Posibles servicios: Conexión con Operador IP, Buzón de Voz a email, Sistema automático de respuesta, etc.

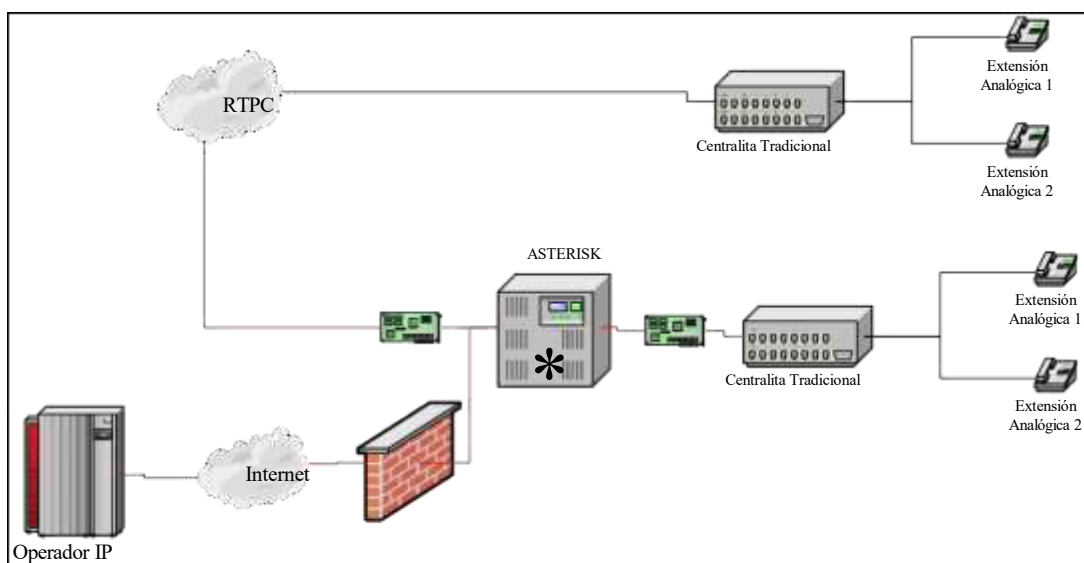


Figura 20 Implantación de Asterisk Escenario 2

5.6.3 Pasarela para dotar a una centralita tradicional de nuevas extensiones

Para poder hacer esto la centralita tradicional debería poder programarse para ello.

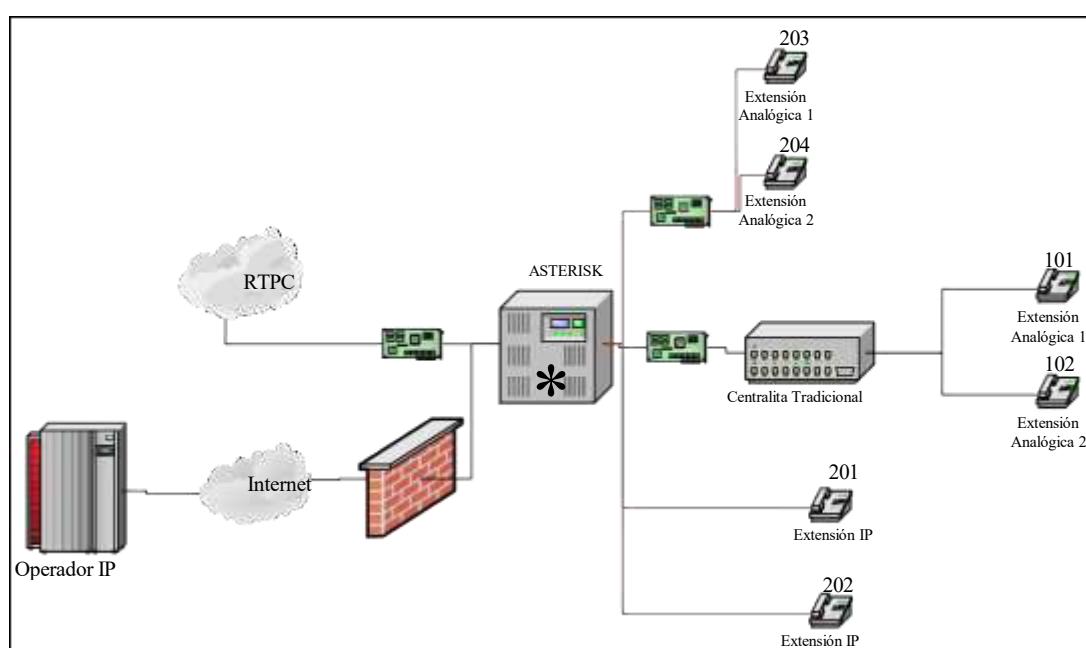


Figura 21 Implantación de Asterisk Escenario 3

5.6.4 Varias Oficinas con un Asterisk Centralizado

De esta forma, además de comunicaciones entre Sedes, toda las sedes pueden hacer llamadas al exterior a través de la central Asterisk. Las extensiones externas podrán seguir el protocolo SIP o el Protocolo IAX.

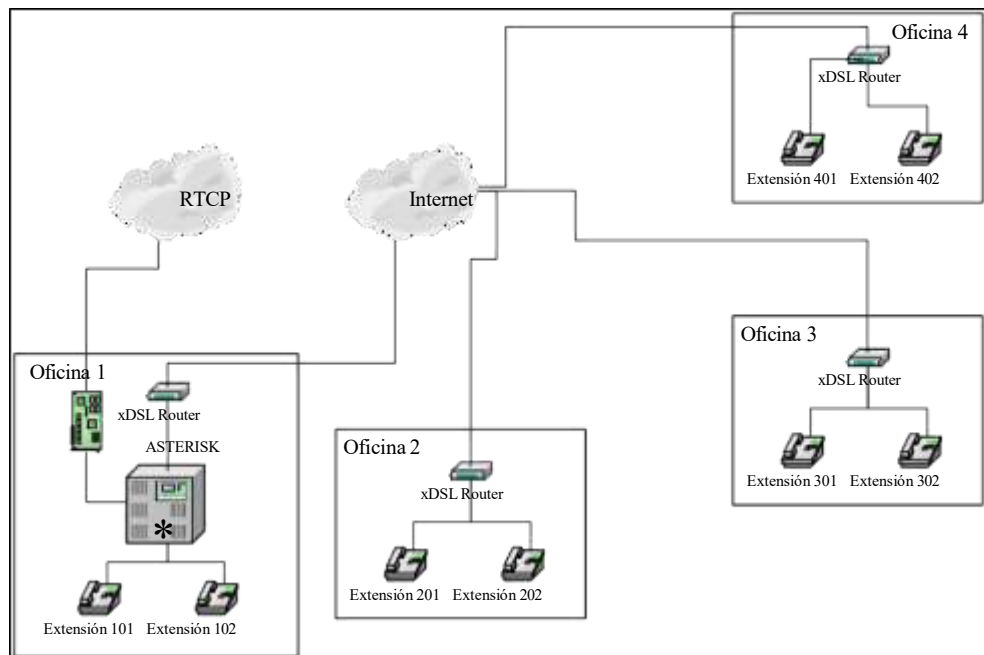


Figura 22 Implantación de Asterisk Escenario 4

5.6.5 Varias Oficinas con Sistemas Asterisk interconectados

Todos los Asterisk Pueden utilizar los otros Asterisk para hablar con números de las provincias donde se encuentran. Entre ellos se pueden conectar mediante IAX o SIP, e incluso se puede montar un plan de numeración único entre todos.

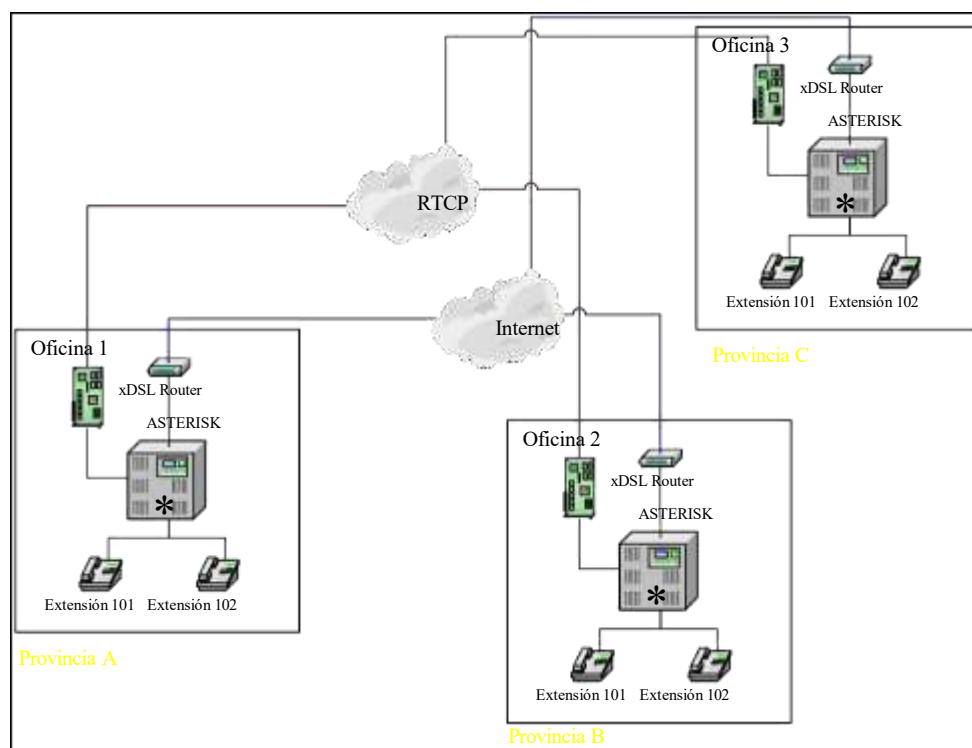


Figura 23 Implantación de Asterisk Escenario 5

CAPITULO VI

6. CONCLUSIONES

- La Telefonía IP es una tecnología aún en auge a nivel Latinoamérica que tendrá mucho que decir en los próximos años. Dentro de la cual, hay que comentar que si bien H.323 es la apuesta tradicional, y SIP aún presenta algunos riesgos tenemos en IAX2 un protocolo más flexible, de mayor compatibilidad y flexibilidad.
- Los avances en la tecnología de redes aseguran una fiabilidad y una calidad en la voz comparable a la de las centralitas tradicionales.
- La aceptación de la voz sobre IP se puede comparar con la de las LAN inalámbricas, hace apenas un año: los primeros en utilizarla están muy satisfechos. Las empresas de análisis están de acuerdo en que el mercado de VoIP está destinado a un enorme crecimiento en los próximos años.

- El open source llega también a la VoIP, posibilitando la utilización a un reducido coste de la tecnología, apropiado para empresas con pocos recursos, o como demostración para empresas que teman arriesgar su dinero al invertir en VoIP.
- En general, la cuestión que se deben plantear las empresas que desean implantar la tecnología de VoIP no es “si deberían hacerlo”, sino “cuándo y cómo hacerlo”.

GLOSARIO DE TERMINOS

A

ANCHO DE BANDA: Este término se utiliza para los métodos en donde dos o más señales comparten un medio de transmisión.

ASTERISK: Aplicación de código abierto de una central telefónica (PBX).

B

BEST-EFFORT: Es un modelo simple de servicio, en el cual, una aplicación envía información cuando ella lo desea, en cualquier cantidad, sin ningún permiso requerido, y sin informar previamente a la red.

BRI: (Basic Rate Interface) Interfaz de razón básica. Servicio ISDN que proporciona dos canales B más un canal de datos. La BRI es adecuada para negocios pequeños.

BRIDGING: Aprendizaje de Direcciones, aprende automáticamente las direcciones MAC de los dispositivos situados en su mismo segmento LAN local.

C

CALLER ID: Identificador de llamadas

CODEC: es una abreviatura de **Codificador-Decodificador**. Describe una especificación implementada en software, hardware o una combinación de ambos, capaz de transformar un archivo con un flujo de datos (*stream*) o una señal.

D

DARPA: Defense Advanced Research Projects Agency es una agencia del Departamento de Defensa de los Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar

DHCP: Protocolo de configuración dinámica de servidores (Dynamic Host Configuration Protocol). Es un protocolo de red en el que un servidor provee los parámetros de configuración a las computadoras conectadas a la red, incluye un mecanismo de asignación de direcciones de IP. **DIFFSERV:**(Differentiated Services). El usuario marca los paquetes con un determinado nivel de prioridad; los routers van agregando las demandas de los usuarios y propagándolas por el trayecto

DTMF: (Dual-Tone Multi-Frequency), sistema de marcación por tonos, también llamado sistema multifrecuencial.

F

FXO: (Foreign Exchange Office), es un dispositivo de computador que permite conectar éste a la RTB, y mediante un software especial, realizar y recibir llamadas de teléfono

FXS: (Foreign Exchange Station) sirven para conectar teléfonos analógicos normales a un computador, y mediante un software especial, realizar y recibir llamadas hacia el exterior, o hacia otros interfaces FXS

G

GATEWAY: Puerta de enlace, un nodo en una red informática que sirve de punto de acceso a otra red

GSM: (Sistema Global para las Comunicaciones Móviles), formalmente conocida como "**Group Special Mobile**" (GSM, Grupo Especial Móvil) es un estándar mundial para teléfonos móviles digitales.

I

IAx: (*Inter-Asterisk eXchange protocol*) es uno de los protocolos utilizado por Asterisk, utilizado para manejar conexiones VoIP

IETF: (Internet Engineering Task Force, en castellano Grupo de Trabajo en Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet

ISDN: RDSI

INTSERV: (Integrated Services) y protocolo RSVP. El usuario solicita de antemano los recursos que necesita; cada router del trayecto ha de tomar nota y efectuar la reserva solicitada.

IP: Sus siglas en inglés *Internet Protocol*) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

ITU: Unión Internacional de Telecomunicaciones es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.

IVR: Es el acrónimo de Interactive Voice Response, que se traduce como Respuesta de Voz Interactiva. Consiste en un sistema telefónico que es capaz de recibir una llamada e interactuar con el humano a través de grabaciones de voz. Es la típica máquina que nos responde para saber la hora o cuando llamamos al banco.

J

JITTER: Variación en los tiempos de llegada entre los paquetes.

L

LATENCIA: Lapso necesario para que un paquete de información viaje desde la fuente hasta su destino. La latencia y el ancho de banda, juntos, definen la capacidad y la velocidad de una red.

M

MIPS: Es el acrónimo de "millones de instrucciones por segundo". Es una forma de medir la potencia de los procesadores.

MPLS: (siglas de Multiprotocol Label Switching) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

P

PBX: Private Branch eXchange o Private Business eXchange. Es una central telefónica que es utilizada para negocios privados.

PSTN: RTB

Q

QoS: (*Quality of Service*, Calidad de Servicio) garantiza que se transmitirá cierta cantidad de datos en un tiempo dado

R

RDSI: Red Digital de Servicios Integrados, es una red que procede por evolución de la red telefónica existente, que ofrece conexiones digitales de extremo a extremo permite la integración de multitud de servicios en un único acceso.

RTB: Red Telefónica Básica (RTB; también llamada Red Telefónica Conmutada o RTC) es una red de teléfono diseñada primordialmente para la transmisión de voz, aunque pueda también transportar datos, por ejemplo en el caso del fax o de la conexión a Internet a través de un módem acústico **RTP:** Son las siglas de Real-time Transport Protocol (Protocolo de Transporte de Tiempo real). Es un protocolo de nivel de aplicación utilizado para la transmisión de información en tiempo real, como por ejemplo audio y video en una videoconferencia.

S

SER: Sip Express Router

SIP: (Protocolo de Inicialización de Sesiones) es un protocolo desarrollado por el IETF con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos online y realidad virtual.

STREAM: es un término que describe una estrategia sobre demanda para la distribución de contenido multimedia a través del Internet.

T

TRUNKING: El Trunking es una función para conectar dos switches, routers o servidores, del mismo modelo o no, mediante 2 cables en paralelo en modo Full-Duplex. Así se consigue un ancho de banda del doble para la comunicación entre los switches. Esto permite evitar cuellos de botella en la conexión de varios segmentos y servidores.

U

UDP: User Datagram Protocol es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión.

V

VOCODER: Nombre derivado de voice coder- codificador de voz, es un analizador y sintetizador de voz

VOFR: Voz sobre Frame Relay.

VOIP: Voz sobre IP

REFERENCIAS BIBLIOGRÁFICAS

A. TANEMBAUM

1997 “Redes de computadores”. 3ª Ed. Prentice-Hall.

Asterisk - Es

2006 Asterisk en Español.

<http://www.asterisk-es.org/modules/news/>

2006 - 06 - 06

ARTUÑEDO GUILLÉN, David

2003 “Transparencias del curso de Telefónica I+D: Voz sobre IP”..

Boecillo.

BULMA

2005 Servidor de VOIP con Asterisk@home

<http://bulma.net/body.phtml?nIdNoticia=2234>

2005 - 09 - 12

CAPATRES

2006 Voz sobre IP: Asterisk y Capa Tres

<http://www.capatres.com/voz-sobre-ip.html>

2006 – 02 – 16

CISCO SYSTEMS, INC

2006 Cisco - Understanding Codecs.

<http://www.cisco.com/warp/public/788/voip/codeccomplexity.html>:

2006 – 01 - 15

DANG Luan, JENNINGS Cullen, KELLY David.

2002 “Practical VoIP Using Vocal: 1st ed” Ed: O’Reilly.

DAVIDSON Jonathan, PETERS James

2000 “Voice Over IP Fundamentals” Ed: Cisco Press.

E-Ghost Phpwiki

2005 Soluciones Voz IP con software libre.

<http://www.e->

[ghost.deusto.es/docs/2006/conferencias/voip_asterisk_irontec_Enpr](http://ghost.deusto.es/docs/2006/conferencias/voip_asterisk_irontec_EnpresaDigitala.pdf)

[esaDigitala.pdf](http://ghost.deusto.es/docs/2006/conferencias/voip_asterisk_irontec_EnpresaDigitala.pdf)

2005 - 09 - 12

HUIDOBRO MOYA J.M., ROLDÁN MARTÍNEZ D.

2003 “Integración de voz y datos: call centers, tecnología y aplicaciones”.

Ed: McGraw Hill.

IRONTEC

2005 Asterisk – El Futuro de la Telefonía.

http://www.irontec.com/files/voip/AsteriskTFOT_irontec.pdf

2005 – 03 - 19

IRONTEC

2005 Internet y Sistemas sobre GNU / Linux :: Voz sobre IP VoIP

www.irontec.com/voipProductos.html

2005 – 03 - 19

LINUX RED HAT

2006 Red Hat | The Open Source Leader: www.redhat.com: 2006

- 05 - 24

NECOMPLUS

2006 Asterisk - centralita telefónica PBX.

<http://www.necomplus.com/jsp/index2.jsp?pagina=asterisk&menu=ok> 2006

- 03 - 10

RAD-COM

2005 Protocols.com: | WAN, LAN, ATM |Ftp, Http, ICMP, UDP |

Telecommunications. www.protocols.com: 2005 - 07 - 25

RYDSA

2005 Comunidad VoIP. http://www.rydsa.com.ar/voip_info6.htm

2005 - 02 - 03

TIENDA LINUX.COM

2005 Asterisk Colombia / Telefonía IP (VoIP y PBX) con Linux.

<http://soporte.tiendalinux.com/portal/Portfolio/IPTelephony/>:

2005 - 11 - 19

PC - MAGAZINE

2006 IP: comunicación mágica.

<http://www.esmas.com/pcmagazine/noticias/533695.html>

2006 - 06 - 06

RECURSOS VoIP

2006 Voz sobre IP: Telefonía IP, Videoconferencia

<http://www.rekursosvoip.com/>

2006 - 03 - 17

UNITRONICS COMUNICACIONES

2006 Documentación y conocimiento.

http://www.comunicaciones.unitronics.es/html/documentacion_servicios.html:

2006 - 02 - 25.

VoIP PARA NOVATOS

2006 Cómo probar VozIP y no morir en el intento.

<http://www.voipnovatos.es/index.php?itemid=21&catid=6>.

2006 - 02 - 05

VOVIDA

2005 Vovida.org - Your Source for Open Source Communication.

www.vovida.org : 2005 – 07 - 18

ANEXOS

Anexo N° 1

RSVP/IntServ:

A.1.1 Introducción:

Veamos un repaso de protocolos que permiten asegurar QoS.

- **RSVP** (*Resource Reservation Protocol*). Este protocolo permite que un *host* o un *router* aseguren la reserva de ancho de banda a lo largo de la red IP. Es del tipo orientado al receptor (el receptor solicita la reservación) y es útil para aplicaciones de tipo *simplex* (unidireccional). Puede funcionar como *unicast* o *multicast*. Se particularizará en él a continuación.
- **RTP** (*Real-time Transport Protocol*). Se utiliza sobre el protocolo UDP para VoIP

- **RTCP** (*Real-Time Transport Control Protocol*). Este protocolo se utiliza para control de calidad de servicio sobre aplicaciones que trabajan sobre RTP.
- **IGMP** (*Internet Group Management Protocol*). Este protocolo se utiliza para aplicaciones del tipo *multicast* cuando se requiere distribuir la misma información sobre un grupo de usuarios y reduciendo así el ancho de banda ocupado. Se emite un mismo paquete con dirección *multicast* en lugar de uno para cada dirección *unicast*.

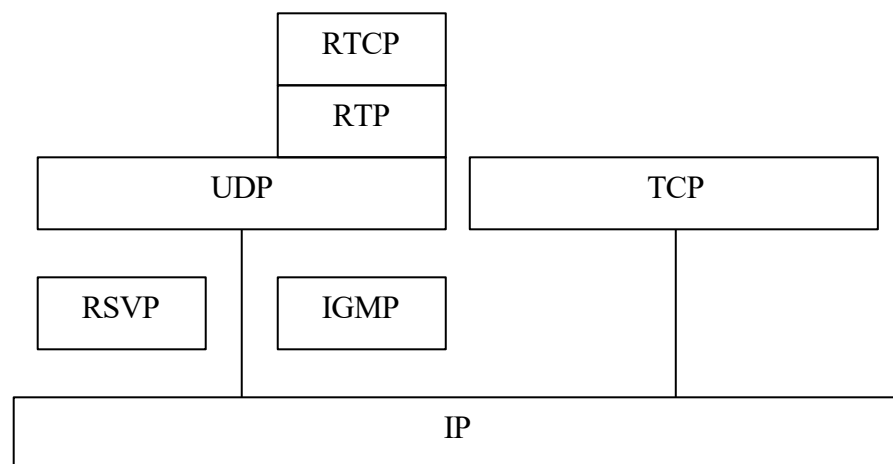


Figura A.1.- Esquema de los protocolos para asegurar la QoS por medio de RSVP

A.1.2.- El protocolo RSVP

Se procede a analizar RSVP (RFC-2205) viendo cómo se sirve de los protocolos mencionados en la introducción anterior.

Los servicios de nivel de aplicación (por Ej., HTTP) en Internet, como ya se ha mencionado, son con calidad "*best effort*"; es decir, no prevén una calidad de servicio. Esto tiene como consecuencia una latencia variable y *jitter* sobre la información del tipo tiempo-real (audio o vídeo). RSVP permite la reserva de ancho de banda para asegurar una **QoS extremo a extremo**. Para ello, el protocolo RSVP trabaja en conjunto con el protocolo de transporte **RTP** para servicios de voz y vídeo en tiempo-real.

Existen dos formas de reservar ancho de banda: estática y dinámica. La reserva estática permite asignar un porcentaje fijo del canal de comunicación a cada tipo de protocolo (por ejemplo, 10% a HTTP, 15% a FTP, 3% a *Telnet*, etc). El protocolo RSVP permite reservar el ancho de banda en forma dinámica para asegurar una calidad de servicio **QoS** en las redes IP. La **QoS** permite garantizar el servicio en forma CAR similar al CIR de *Frame Relay*.

El protocolo RSVP se define para los servicios integrados (*Guaranteed*) en Internet. Es utilizado por el *host* para solicitar una QoS al *router* para una aplicación particular y es usado por el *router* para establecer un ancho de banda con todos los nodos intermedios del trayecto.

RSVP no es un protocolo de *routing* y sólo se utiliza para reservar ancho de banda y *buffer*. En el modelo de capas, el protocolo RSVP ocupa la función de la capa 3 sobre IP, de la misma forma que los protocolos de *routing* (OSPF y BGP), de *multicast* (IGMP), de gestión (ICMP) y de transporte (TCP y UDP). Una sesión manejada por el protocolo RSVP está definida mediante tres direcciones: la dirección IP de destino (receptor), el identificador de protocolo y el puerto de UDP.

Está definido para operar en forma de *unicast* o *multicast*. En el caso de operar con protocolo *multicast*, primero se establece el enlace mediante IGMP (para establecer el grupo) y luego mediante RSVP (para establecer la reserva). Por otro lado, el RSVP es un protocolo de carácter unidireccional. Está orientado al receptor; en el sentido que es el receptor el que solicita la reserva y la interrumpe.

La QoS es implementada por un mecanismo de flujo de datos denominado "control de tráfico". Este mecanismo incluye 3 etapas:

- La clasificación del paquete para determinar la QoS y la ruta de cada paquete.
- El control de admisión para asegurar la disponibilidad de la reservación y
- El proceso de determinación temporal de emisión (*Packet Scheduler*).

El requerimiento de reservación es iniciado por el *host* receptor y pasa por los distintos *routers* de la red. Si algún mecanismo intermedio falla, se genera un reporte de error.

Este protocolo mantiene en forma "*soft*" el estado de los *routers* y *host*, entregando un soporte dinámico para cambios de miembros y adaptación automática de cambios de *routing*. No es un protocolo de *routing*, pero depende de los mismos.

El paquete RSVP (Reservation Protocol) se compone de los siguientes campos:

<i>VRS</i>	<i>Flags</i>	<i>Msg Type</i>	<i>Checksum</i>
<i>Send-TTL</i>		<i>RSV</i>	<i>Length</i>
<i>Messages</i>			

Figura A.2. Campos que componen el paquete de RSVP (*Reservation Protocol*)

- **VRS:** 4 *bits*. Versión del protocolo (actualmente la versión 1).
- **Flags:** 4 *bits*. No se han definido bits de *flag* hasta el momento.
- **Msg Type:** 1 *Byte*. Identifica el tipo de mensaje que ocupa el campo de longitud variable al final del paquete. Se dispone de los siguientes casos: *Path*, *Reser*, *PathErr*, *ResvErr*, *PathTear*, *ResvTear*, *ResvConf*.
- **Checksum:** 2 *Bytes*. Chequeo de paridad del protocolo RSVP.
- **Send-TTL:** 1 *Byte*. Se trata del tiempo de vida de IP con que se emite el paquete de RSVP.
- **RSV:** 1 *Byte*. No usado.
- **Length:** 2 *Bytes*. Longitud total del mensaje en *bytes* incluyendo la longitud variable.
- **Messages:** Nx4 *Bytes*. Mensaje de longitud variable en palabras de 32 *bits*.

- **.Resv:** mensaje emitido paso-a-paso desde el receptor al emisor para reservación de ancho de banda.
- **.Path:** mensaje emitido en forma regular para cada flujo de datos del emisor al receptor. No se enruta mediante RSVP asegurar la llegada al receptor mediante las direcciones IP.
- **-Teardown:** mensajes (*Path and Reservation*) usados para desarmar el camino y la reservación efectuada.
- **-Error:** reporta errores en el procesamiento del mensaje *Path* o *Resv*.
- **-Resv Conf:** mensaje emitido como respuesta al *Resv*.

Entre los principales inconvenientes de RSVP conviene destacar:

- Excesiva complejidad.
- Poca escalabilidad.
- Ineficiencia debido al *soft-state*.
- Tratamiento por paquete.

Anexo N° 2

MPLS

MPLS surge con el objetivo de solucionar los problemas de gestión de dos redes paralelas que supone IP o ATM integrando de una manera sencilla y efectiva lo mejor de cada solución (la “inteligencia en el encaminado de IP” y la rapidez de conmutación de ATM), por lo que se presenta como una alternativa interesante para la gestión de *backbones* de operador.

La idea de MPLS es una estandarización del IETF (Internet Engineering Task Force) de las distintas propuestas propietarias de conmutación multi-nivel que surgieron con la idea de mejorar las prestaciones de IP o ATM, porque aunque en principio MPLS es independiente de la red de transporte, se suele utilizar ATM para ello.

MPLS divide claramente dos funciones principales como son el control (routing) y el envío (forwarding).

El envío se implementa mediante el intercambio de etiquetas con significado local en los caminos virtuales (llamados LSP), cuya filosofía es similar a los PVCs de Frame Relay y ATM.

En la entrada a la red MPLS, un “router especial” añade una etiqueta MPLS (de 32 bits) a cada paquete IP según distintos posibles criterios (la dirección IP de destino, el router o interfaz de origen, con lo que la creación de VPNs es inmediata y sencilla). A la salida de la red MPLS, dicha etiqueta es removida y se continúa encaminando el paquete IP de manera convencional.

Posteriormente los routers del interior de la red MPLS (llamados LSR, Label Switching Router), leen esa etiqueta y según la interfaz de entrada, acceden a una tabla que les indica la nueva etiqueta del paquete (recordemos el significado local) y la interfaz de salida correspondiente.

La construcción de estas tablas en los LSR se realiza con protocolos estándar IGP (por ejemplo OSPF) y la distribución de las etiquetas que configuran el LSP se realiza de manera particular no estandarizada según el operador (una opción que tiene muchas opciones de convertirse en el estándar es el RSVP con modificaciones para adaptarse a MPLS).

La impresión de funcionamiento global de MPLS es que en el interior de la red MPLS hay un único salto entre los routers de entrada y salida, dando por tanto la impresión de una topología mallada de circuitos punto a punto.

Y en cuanto a los paquetes IP, no hay problema pues el encaminamiento en el interior de la red se realiza a través de las etiquetas MPLS y no se utilizan los campos de protocolo IP.

En cuanto a las clases de servicio hay que mencionar que MPLS está diseñado para poder cursar servicios diferenciados, según el modelo DiffServ del IETF (ver apéndice A.1), ya que en la cabecera MPLS hay un campo CoS que permite tratar en el interior del backbone el paquete IP de manera diferente según su valor (lo que significará que tendrá una distinta etiqueta MPLS y podrá ser encaminado por una ruta “privilegiada” con distinto nivel de servicio). Es misión del router de entrada asignar correctamente este valor CoS (configurable según el puerto origen, destino, campo TOS/DiffServ del paquete IP, etc.)

INDICE DE TABLAS

TABLA 1 EFECTOS DEL TIPO DE CÓDEC, TAMAÑO DE LA MUESTRA, USO DE CRTP EN EL ANCHO DE BANDA	31
TABLA 2. RANGOS DE LOS TAMAÑOS DE PAQUETE POSIBLES PARA LOS DISTINTOS CODECS	32
TABLA 3. PUNTUACIONES MOS DE LOS DISTINTOS FORMATOS DE COMPRESIÓN	68
TABLA 4 EFECTO MOS _{LE} SOBRE EL RETARDO	69

INDICE DE FIGURAS

FIGURA 1 CABECERAS RTP, UDP E IP	40
FIGURA 2 FUNCIONAMIENTO DE cRTP	43
FIGURA 3 PILA DE PROTOCOLOS EN VoIP	76
FIGURA 4 DESCRIPCIÓN BÁSICA DE UNA RED BASADA EN EL ESTÁNDAR H.323. COMUNICACIÓN ENTRE LOS DIFERENTES COMPONENTES: TERMINAL, GATEWAY, GATEKEEPER, MCU Y ROUTER	77
FIGURA 5 ESQUEMA GENERAL DE UNA RTC OPERANDO CON CUALQUIER RED IP CON ELEMENTOS H.323	78
FIGURA 6 ESQUEMA CONCEPTUAL DEL SERVIDOR ASTERISK	94
FIGURA 7 SERVIDOR ASTERISK ENLAZADO A TARJETAS FXO Y FXS	99
FIGURA 8 ESTRUCTURA ACTUAL DE VOZ Y DATOS DE CDSOFT S.A	108
FIGURA 9 INFRAESTRUCTURA AL FINAL DE LA IMPLANTACIÓN DE ASTERISK COMO IP PBX	109
FIGURA 10 TARJETA FXO TDM400P	116
FIGURA 11 INTERFAZ GRÁFICA DE CONFIGURACIÓN DEL ASTERISK	121
FIGURA 12 PANTALLA PRINCIPAL DEL AMP	122
FIGURA 13 MENÚ DE OPCIONES DE SETUP DEL AMP	123
FIGURA 14 PANTALLA DE CONFIGURACIÓN DE TRUNK	124
FIGURA 15 PANTALLA DE CONFIGURACIÓN DE EXTENSIONES	126
FIGURA 16 MÁSCARA DE X-LITE SOFTPHONE	129
FIGURA 17 PANTALLA DE X-LITE CONFIGURACIÓN	130

FIGURA 18 PANTALLA DE SOFTPHONE CONFIGURADO CORRECTAMENTE.....	131
FIGURA 19 IMPLANTACIÓN DE ASTERISK ESCENARIO 1	150
FIGURA 20 IMPLANTACION DE ASTERISK ESCENARIO 2	151
FIGURA 21 IMPLANTACION DE ASTERISK ESCENARIO 3	151
FIGURA 22 IMPLANTACIÓN DE ASTERISK ESCENARIO 4	152
FIGURA 23 IMPLANTACION DE ASTERISK ESCENARIO 5	153