



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

**ESCUELA DE INGENIERÍA ELECTRÓNICA EN
TELECOMUNICACIONES Y REDES**

**“ANÁLISIS DEL PROTOCOLO DUNDI, APLICADO AL DISEÑO DE
SISTEMAS DISTRIBUIDOS EN REDES DE VoIP”**

TESIS DE GRADO

Previa obtención del título de:

**INGENIERO ELECTRÓNICO EN TELECOMUNICACIONES Y
REDES**

Presentado por:

Patricio Renán Monar Tamayo

RIOBAMBA – ECUADOR

2013

A mis padres, por su dedicación, amor, apoyo y por brindarme la mejor herencia que alguien puede recibir, la educación; por haberme inculcado valores tan importantes, que han marcado la persona que ahora soy.

A mis profesores, por brindarme la mejor herramienta de trabajo para mi vida futura, el conocimiento, además de su grata amistad.

A mis amigos, que supieron sacar una sonrisa a cada uno de los días de mi vida politécnica, que supieron ser de gran ayuda en cada una de las nuevas experiencias que hemos adquirido.

NOMBRE	FIRMA	FECHA
Ing. Iván Menes Camejo DECANO FACULTAD DE INFORMÁTICA Y ELECTRÓNICA
Ing. Wilson Baldeón DIRECTOR DE LA ESCUELA DE INGENIERIA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES
Ing. Marcelo Donoso DIRECTOR DE TESIS
Ing. William Calvopiña MIEMBRO DEL TRIBUNAL
Lcdo. Carlos Rodríguez DIRECTOR DEPARTAMENTO DE DOCUMENTACIÓN

NOTA DE LA TESIS

“Yo, **PATRICIO RENÁN MONAR TAMAYO**, soy responsable de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la **ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**”.

Patricio Renán Monar Tamayo

ÍNDICE DE ABREVIATURAS

Se presentan las abreviaturas de uso frecuente en este documento, referentes en General a las redes de VoIP y en específico al protocolo DUNDI.

<u>Abreviatura</u>	<u>Descripción</u>
ADSL	Asymmetric Digital Subscriber Line
ADPCM	Adaptative Differential Pulse Code Modulation
ATAs	Adaptadores de Teléfonos Analógicos
BHCA	Busy Hour Call Attempts
CS-ACELP	Conjugate-Structure Algebraic-Code-Excited Linear Prediction
CQ	Custom Queuing
DID	Direct Inward Dialling
DTMF	Dual Tone Multi Frequency
DUNDI	Distributed Universal Number Discovery
CRTP	Compressed Real Time Protocol
ECCP	Elastix Call Center Protocol
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station
GIPS	Global IP Sound
GNU	GNU is Not Unix
GPA	Genera Peering Agreement
GPL	General Public License
GSM	Group Special Mobile
HTTP	Hypertext Transfer Protocol
IAX	Inter-Asterisk Exchange Protocol
IETF	Internet Engineering Task Force
ILBC	Internet Low Bitrate Codec
IP	Internet Protocol
ITU	International Telecommunication Union
LAN	Local Area Network
MCU	Multipoint Control Unit
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MoH	Music on Hold
MP3	Moving Picture Experts Group Audio Layer 3 Encoding Standard.
MMUSIC	Multimedia Session Control
PBX	Private Branch Exchange
PABX	Private Automatic Branch Exchange
PCM	Pulse Code Modulation
PQ	Priority Queuing

PSTN	Public Switched Telephone Network
RAS	Registro, Admisión, Situación
RDSI	Red Digital de Servicios Integrados.
RFC	Requests for Comments
SDP	Session Description Protocol
RTP	Real Time Protocol
RTC	Red Telefónica Pública Conmutada
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAC	User Agent Clients
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VBR	Variable Bit Rate
VoIP	Voice over IP
VPN	Virtual Private Network
WFQ	Weight Fair Queuing

ÍNDICE GENERAL

PORTADA	
AGRADECIMIENTO	
FIRMAS RESPONSABLES Y NOTA	
RESPONSABILIDAD DEL AUTOR	
ÍNDICE DE ABREVIATURAS	
ÍNDICE GENERAL	
ÍNDICE DE FIGURAS	
ÍNDICE DE TABLAS	
INTRODUCCIÓN	

CAPÍTULO I : MARCO REFERENCIAL

1.1. ANTECEDENTES	- 12 -
1.2. JUSTIFICACIÓN	- 13 -
1.3. OBJETIVOS	- 14 -
1.3.1. OBJETIVO GENERAL	- 15 -
1.3.2. OBJETIVOS ESPECÍFICOS	- 15 -
1.4. HIPÓTESIS	- 15 -

CAPÍTULO II: FUNDAMENTOS TEÓRICOS

2.1. VoIP	- 16 -
2.1.1. Introducción.....	- 16 -
2.1.2. Funcionalidad	- 17 -
2.2. Telefonía IP	- 17 -
2.2.1. Funcionamiento de la Telefonía IP	- 18 -
2.2.1.1.Digitalización de la voz	- 18 -
2.2.1.2.Paquetización de la voz.....	- 19 -
2.2.1.3.Enrutamiento de paquetes	- 20 -
2.2.1.4.Codificadores/Decodificadores de voz	- 20 -
2.3. Protocolos.....	- 22 -
2.3.1. Protocolos de Transporte	- 22 -
2.3.1.1.RTC.....	- 21 -
2.3.1.2RTCP.....	- 22 -

2.3.2. Protocolos de Señalización.....	- 23 -
2.3.2.1. Protocolo H323	- 22 -
2.3.2.2. Protocolo SIP	- 23 -
2.3.2.3. Protocolo IAX.....	- 24 -
2.4. Diseño de red.....	- 27 -
2.4.1. Topología Física.....	- 29 -
2.4.2. Topología Lógica.....	- 30 -
2.5. Sistemas Distribuidos	- 30 -
2.5.1. Evolución de los Sistemas Distribuidos	- 31 -
2.5.2. Ventajas de los Sistemas Distribuidos	- 32 -
2.6. Elastix.....	- 33 -
2.6.1. Dial Plan	- 34 -
2.7. Protocolo DUNDI	- 35 -
2.7.1. Funcionamiento	- 36 -
2.7.2. Características.....	- 37 -
2.7.3. Etapas de Transmisión.....	- 38 -
2.7.4. Archivos Configurables.....	- 39 -
2.7.5. Creación de Clave Pública.....	- 44 -

CAPÍTULO III: DISEÑO E IMPLEMENTACIÓN DE LA RED DE PRUEBA

3.1. Diseño de la red.....	- 46 -
3.2. Implementación de la red	- 49 -
3.3. Determinación del Costo de Implementación.....	- 50 -

CAPÍTULO IV: FUNCIONAMIENTO Y PRUEBAS DEL PROTOCOLO DUNDI EN EL AMBIENTE DE PRUEBA

4.1. Planteamiento de la Hipótesis	- 52 -
4.2. Variables de Estudio e Indicadores	- 53 -
4.3. Estimación de una muestra	- 53 -
4.4. Escenarios de prueba	- 54 -
4.4.1. Escenario de prueba 1	- 54 -
4.4.2. Escenario de prueba 2.....	- 58 -
4.4.3. Escenario de prueba 3.....	- 62 -

4.4.4. Escenario de prueba 4.....	- 65 -
4.4.5. Escenario de prueba 5.....	- 66 -
4.5. Evaluación de los resultados obtenidos.....	- 69 -
4.6. Demostración de la Hipótesis.....	- 74 -
4.7. Disponibilidad de la red	- 78 -
4.8. Seguridad de la red.....	- 79 -
4.9. Consumo de recursos	- 80 -

CONCLUSIONES

RECOMENDACIONES

RESUMEN

SUMMARY

GLOSARIO

ANEXOS

ANEXO 1

ANEXO 2

ANEXO 3

BIBLIOGRAFÍA

BIBLIOGRAFÍA DE INTERNET

ÍNDICE DE FIGURAS

Figura II.1. Muestreo y digitalización de Voz	19
Figura II.2. Estructura de un Paquete de VoIP.....	20
Figura II.3. Enrutamiento de paquetes en la red.	21
Figura II.4. Establecimiento y Finalización de una llamada IAX entre dos puntos.....	27
Figura II.5. Pasos para un correcto diseño de red	29
Figura II.6. Esquema General de los Componentes Elastix.....	34
Figura II.7. Configuración extensiones PBX_A	40
Figura II.8. Sintaxis sip.conf	41
Figura II.9. Configurando iax.conf.....	41
Figura II.10. dundi.conf PBX_A.....	43
Figura II.11. Claves generadas	45
Figura II.12. Copiando claves publicas entre servidores	45
Figura III.13. Esquema de análisis A	46
Figura III.14. Esquema de análisis B	47
Figura III.15. Esquema de análisis C	47
Figura III.16. Esquema de análisis D	48
Figura III.17. Esquema Físico del prototipo de prueba.....	49
Figura III.18. Esquema Lógico del prototipo de prueba	50
Figura IV.19. Delimitación del ancho de banda Escenario 2.	58
Figura IV.20. Delimitación del ancho de banda Escenario 3.	62
Figura IV.21. Delimitación del ancho de banda Escenario 4.	64
Figura IV.22. Delimitación del ancho de banda Escenario 5.	66
Figura IV.23. Curva de Probabilidad.....	78
Figura IV.24. Recursos del Sistema consumidos.	80
Figura IV.25. Consumo total del disco duro de la central telefónica.	81
Figura IV.26. Consumo de recursos en llamadas simultaneas.	81
Figura IV.27. Uso de los canales mostrados cronológicamente.....	82

ÍNDICE DE TABLAS

Tabla II.I. Características de Codecs	22
Tabla II.II. Archivos configurables en Asterisk	39
Tabla III.III. Costo de Equipos.	51
Tabla III.IV. Costo de Instalación.	51
Tabla III.V. Costo Total	51
Tabla III.VI. Variables e Indicadores.....	53
Tabla IV.VII. Tiempos de respuesta de consultas DUNDI sin tráfico. Escenario 1	55
Tabla IV.VIII. Tiempos de respuesta de consultas DUNDI con tráfico. Escenario 1	55
Tabla IV.IX. Tiempos de respuesta en re conexión sin tráfico. Escenario 1	56
Tabla IV.X. Tiempos de respuesta en re conexión con tráfico. Escenario 1	56
Tabla IV.XI. Tiempos de consulta en el enlace principal. Escenario 1	57
Tabla IV.XII. Tiempos de consulta en el enlace secundario. Escenario 1	57
Tabla IV.XIII. Tiempos de respuesta de consultas DUNDI sin tráfico. Escenario 2.....	59
Tabla IV.XIV. Tiempos de respuesta de consultas DUNDI con tráfico. Escenario 2.....	59
Tabla IV.XV. Tiempos de respuesta en re conexión sin tráfico. Escenario 2.....	60
Tabla IV.XVI. Tiempos de respuesta en re conexión con tráfico. Escenario 2.....	60
Tabla IV.XVII. Tiempos de consulta en el enlace principal. Escenario 2.....	61
Tabla IV.XVIII. Tiempos de consulta en el enlace secundario. Escenario 2.....	61
Tabla IV.XIX. Tiempos de respuesta de consultas DUNDI sin tráfico. Escenario 3	62
Tabla IV.XX. Tiempos de respuesta de consultas DUNDI con tráfico. Escenario 3.....	63
Tabla IV.XXI. Tiempos de respuesta en re conexión sin tráfico. Escenario 3	63
Tabla IV.XXII. Tiempos de respuesta en re conexión con tráfico. Escenario 3.....	64
Tabla IV.XXIII. Tiempos de consulta en el enlace principal. Escenario 3	64
Tabla IV.XXIV. Tiempos de consulta en el enlace secundario. Escenario 3	65
Tabla IV.XXV. Tiempos de respuesta de consultas DUNDI sin tráfico. Escenario 5.....	66
Tabla IV.XXVI. Tiempos de respuesta de consultas DUNDI con tráfico. Escenario 5	67
Tabla IV.XXVII. Tiempos de respuesta en re conexión sin tráfico. Escenario 5.....	67
Tabla IV.XXVIII. Tiempos de respuesta en re conexión con tráfico. Escenario 5	68
Tabla IV.XXIX. Tiempos de consulta en el enlace principal. Escenario 5	68
Tabla IV.XXX. Tiempos de consulta en el enlace secundario. Escenario 5.....	69
Tabla IV.XXXI. Tablas de comparación Paso 1 de todos los escenarios, sin tráfico.....	70
Tabla IV.XXXII. Tablas de comparación Paso 1 de todos los escenarios, con tráfico.	70
Tabla IV.XXXIII. Tablas de comparación Paso 2 de todos los escenarios, sin tráfico.	71
Tabla IV.XXXIV. Tablas de comparación Paso 2 de todos los escenarios, con tráfico.	72
Tabla IV.XXXV. Tablas de comparación Paso 3 de todos los escenarios, enlace directo... ..	73
Tabla IV.XXXVI. Tablas de comparación Paso 3 de todos los escenarios, con nodo intermedio .	74
Tabla IV.XXXVII. Tabla porcentaje de disponibilidad.	79
Tabla IV.XXXVIII. Tiempos de disponibilidad de la red.....	79

INTRODUCCIÓN

Voz sobre IP es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, Gateway y teléfonos estándares. En la actualidad los sistemas de Voz sobre IP son esenciales para la evolución del sector de las telecomunicaciones. A nivel empresarial VoIP ofrece ventajas como: reducción de costos en las llamadas y la implementación de servicios de telefonía adicionales.

Con este proyecto se busca potenciar las herramientas con las que disponemos actualmente, para trabajar sobre una red telefónica montada sobre IP, logrando la comunicación de varias pequeñas centrales telefónicas que usaran servidores de código abierto, en las mismas que emplearemos el protocolo DUNDI; este ambiente está diseñado para facilitar la distribución de los recursos que pueden ser utilizados para determinar los números de teléfono mediante el uso de un sistema *peer to peer* (punto a punto), sin necesidad de control o autoridad centralizada, no hay punto único de fallo, y no existe una jerarquía forzada.

Como resultado de las pruebas realizadas en el prototipo de prueba, se evidencia que la aplicación del protocolo DUNDI facilita la propagación del plan de marcado de un servidor a otro, reduciendo costos de operación, tiempos requeridos para configuración y recursos necesarios para ello, facilitando además la escalabilidad y rápida adaptación a los cambios que puedan surgir.

CAPÍTULO I

MARCO REFERENCIAL

1. FORMULACIÓN GENERAL DEL PROYECTO DE TESIS

1.1. ANTECEDENTES

La evolución de las comunicaciones hacia las telecomunicaciones ha provocado grandes cambios en la manera en la que se desarrolla nuestra vida, donde la tecnología crece a pasos cada vez más agigantados, facilitando muchas de las tareas involucradas dentro de un proceso de comunicación. Pasando por el telégrafo, el teléfono y el actual apogeo que tiene la Telefonía IP.

La importancia y desarrollo de las telecomunicaciones han permitido la aparición de nuevas tendencias tecnológicas en el transporte y administración de las conversaciones telefónicas. Se han adicionado muchos beneficios y servicios, brindando sistemas de comunicación integrales. Todos estos beneficios y nuevas tecnologías de transporte de información, están contenidos en la actualidad dentro de pequeñas centrales de telefonía, brindando iguales y mayores ventajas que las grandes y ya conocidas centrales telefónicas.

Por otra parte, tenemos la búsqueda continua por parte de las empresas de crear y desarrollar nuevos métodos, sistemas y/o nuevas tecnologías con el fin de reducir el costo

de la prestación de servicios y por ende las tarifas, sin comprometer con ello la fiabilidad, seguridad, integridad, etc. Con la que deben contar estos servicios. Costos que actualmente son elevados, debido a la alta inversión imperiosa, tanto en infraestructura y equipamiento necesario para permitir el acceso a la comunicación en distintas áreas, sin mencionar las altas tasas por interconexión que muchas telefónicas cobran.

El fenómeno de la Internet ha sido pieza clave para que podamos alcanzar esta meta, ya que gracias al constante desarrollo de las redes IP combinado con técnicas avanzadas de digitalización de voz y los protocolos de control y transmisión en tiempo real, han hecho que la telefonía sobre IP se convierta en un tema estratégico, ya que permite la calidad de servicio a bajo costo.

1.2. JUSTIFICACIÓN

Debido a que en la actualidad las centrales telefónicas basadas en VoIP han ido ganando territorio en el sector de la telefonía privada, gracias a sus prestaciones e innegables ventajas, frente a la implementación de centrales telefónicas tradicionales; y el costo que conllevan las mismas. A tal punto de que es muy común encontrarlas en muchos tipos de negocios, oficinas e instituciones.

Con esto surge la idea de establecer la comunicación entre estas centralitas a través de una red de datos como la Internet. Implementando el protocolo DUNDI para comunicar varias centrales ubicadas remotamente, vamos a facilitar la escalabilidad en la red de servidores y así permitir la comunicación entre estas terminales VoIP, unificando el plan de marcado de cada servidor PBX independiente, facilitando la configuración y comunicación entre los servidores.

Para implementar DUNDI en cada servidor es necesario:

- Crear un plan de marcación distinto para cada servidor.

- Configurar los archivos: *iax.conf*, *extensions.conf* y *dundi.conf*.
- Antes de comenzar es necesario conocer las direcciones IP y direcciones MAC de cada servidor.

Y así logramos la integración y comunicación entre diferentes centrales privadas, conectadas remotamente gracias al acceso que se tienen a la Internet. El valor agregado que tenemos con esto, es la reducción de costos, si se habría aplicado un sistema diferente, como son las centrales telefónicas tradicionales por ejemplo.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

- Analizar el comportamiento del protocolo DUNDI, aplicado al diseño de sistemas distribuidos en redes de VoIP.

1.3.2. OBJETIVOS ESPECÍFICOS

- Estudiar el protocolo DUNDI.
- Diseñar e implementar un prototipo de prueba.
- Evaluar el comportamiento del protocolo en el ambiente de prueba.
- Proporcionar una guía de implementación del protocolo DUNDI.

1.4. HIPÓTESIS

La puesta en marcha del protocolo DUNDI sobre una red de VoIP, facilitara la propagación del plan de marcado de cada servidor, a través de la red, entre varios servidores PBX ubicados remotamente.

CAPÍTULO II

FUNDAMENTOS TEÓRICOS

2.1. VoIP

2.1.1. Introducción

Voz sobre Protocolo de Internet, también llamado Voz sobre IP, Voz IP, VoIP, es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP. Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN.

Los Protocolos que se usan para enviar las señales de voz sobre la red IP se conocen como protocolos de Voz sobre IP o protocolos IP. El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo las redes de área local (LAN). Es muy importante diferenciar entre Voz sobre IP (VoIP) y Telefonía sobre IP.

VoIP es el conjunto de normas, dispositivos, protocolos, en definitiva la tecnología que permite comunicar voz sobre el protocolo IP.

Telefonía sobre IP es el servicio telefónico disponible al público, por tanto con numeración E.164, realizado con tecnología de VoIP.

El desarrollo en la Industria de las telecomunicaciones ha cambiado el uso de las redes actuales; los usuarios de las redes telefónicas convencionales cada día incrementan el uso de estas redes para la transmisión de información y datos, en lugar de usarlas para llamadas de voz, únicamente.

2.1.2. Funcionalidad

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

- Las llamadas telefónicas locales pueden ser automáticamente enrutadas a un teléfono VoIP, sin importar dónde se esté conectado a la red.
- Los agentes de call-center usando teléfonos VoIP pueden trabajar en cualquier lugar con conexión a Internet lo suficientemente rápida.
- Algunos paquetes de VoIP incluyen servicios extra por los que PSTN normalmente cobra un cargo extra, o que no se encuentran disponibles en algunos países, como son las llamadas de 3 a la vez, retorno de llamada, remarcación automática, o identificación de llamada.

“La tecnología de VoIP no es un servicio como tal, sino una tecnología”¹ que usa el Protocolo de Internet (IP) a través de la cual se comprimen y descomprimen de manera altamente eficiente paquetes de datos o datagramas, para permitir la comunicación de dos o más clientes a través de una red como la red de Internet. Con esta tecnología pueden prestarse servicios de Telefonía o Videoconferencia, entre otros.

2.2. Telefonía IP

¹<http://upcommons.upc.edu/pfc/bitstream/2099.1/7312/1/ProyectoFINAL.pdf>

La telefonía IP se refiere a la utilización de una red IP (privada o pública, como es Internet) por la que transmitimos los servicios de voz, fax y mensajería. Esta red IP puede ser utilizada para realizar las llamadas internas de la propia empresa, así como las llamadas externas, usando, por ejemplo, Internet en lugar de la red telefónica pública conmutada.

La VoIP es la tecnología usada para el funcionamiento de la telefonía IP. VoIP gestiona el envío de información de voz utilizando IP. La información analógica vocal se transforma en paquetes digitales diferenciados que se envían por la red. Los paquetes de información de voz viajan por la red IP, del mismo modo que los datos generados por una comunicación de correo electrónico, por ejemplo.

Por tanto, la telefonía IP es una aplicación inmediata de esta tecnología, de manera que permite la realización de llamadas telefónicas ordinarias sobre las redes IP u otras redes de paquetes, utilizando ordenadores personales, gateways, gatekeepers, unidades de multiconferencia o teléfonos normales. En general, soporta servicios de comunicación de voz, fax, de mensajes de voz, etc. que se transportan vía redes IP, como Internet, en lugar de ser transportados vía la red telefónica convencional.

2.2.1. Funcionamiento de la Telefonía IP

Realmente, se podría decir que la VoIP es simplemente la transferencia de las conversaciones de voz convertidas en datos sobre una red IP (pública o privada) que si dispone de un gran ancho de banda puede dar una buena calidad. Como ya se ha explicado, esta tecnología utiliza para su comunicación la conmutación de paquetes.

Como se puede intuir, en la telefonía IP el cambio fundamental se produce en la red de transporte, ya que ahora esta tarea se lleva a cabo por una red basada en el protocolo IP, como por ejemplo Internet. En cuanto a la red de acceso, puede ser la misma que en la telefonía convencional, físicamente hablando.

Los elementos necesarios para que se puedan realizar llamadas vocales a través de una red

IP depende en gran medida de qué terminal se utiliza en ambos extremos de la conversación. Éstos pueden ser terminales IP, como pueden ser los softphones, o no IP, que serían los teléfonos analógicos convencionales. Hay que señalar que en el caso de que uno de los terminales sea no IP, la comunicación pasará a través de una red de datos como por la RTC.

La telefonía IP en su proceso de funcionamiento, cumple con las siguientes etapas de manera general:

2.2.1.1. Digitalización de la Voz

Es el primer paso para cada conexión de VoIP, comprende la conversión de la señal analógica a digital. Este proceso involucra las fases de muestreo, cualificación y cuantificación de la señal. Los dispositivos utilizados en esta conversión son llamados CODECS los cuales además de realizar la conversión de la señal se encargan de comprimir la información y proporcionan la cancelación de eco.

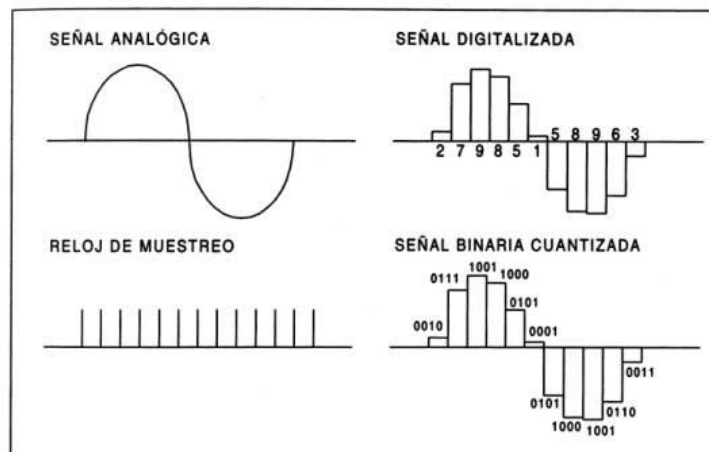


Figura II.1. Muestreo y digitalización de Voz²

La forma más fácil es tomar un muestreo de frecuencias con una proporción fija que sea lo suficientemente alta para captar todas las frecuencias necesarias, luego dividimos la fuerza de la señal en varios niveles. Por ejemplo, 8000 Hz y 256 niveles de muestreo es una

²<http://www.dte.us.es/personal/pfortet/P4TBC.pdf>

configuración fija muy común. La reducción de la frecuencia de muestreo puede ayudar un poco en la reducción de la asignación de ancho de banda de la aplicación de VoIP, pero en una pequeña proporción.

2.2.1.2. Paquetización de la Voz

Este proceso involucra encapsular la señal de voz digitalizada al formato de un paquete de IP, para posteriormente realizar la transmisión a través de la red de telefónica IP. Ahora, cada Payload de Voz comprimido por el Algoritmo hay que empaquetarlo y enviarlo a través de la red. Hay, al menos, cuatro empaquetamientos: RTP (Aplicación), UDP (Transporte), IP (Red) y Enlace/Link (típicamente Ethernet).

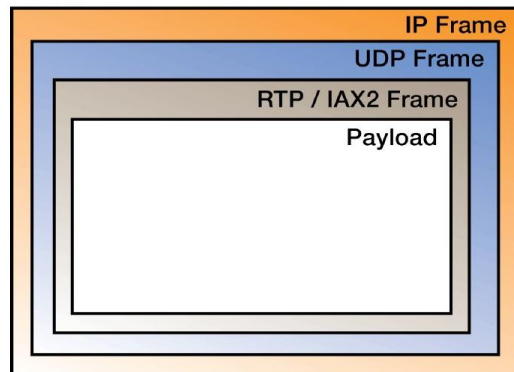


Figura II.2. Estructura de un Paquete de VoIP³

El Proceso de Empaquetamiento sugiere la Añadidura de una serie de Cabeceras, lo cual aumenta el Tamaño de los Paquetes enviados y por ende la Tasa de Bits consumida. La Compresión se puede entender en realidad como una técnica de compensación de 'Overhead' las cuales trabajan con Cabecera IPv4 (20 Bytes) \neq Cabecera IPv6 (40 Bytes).

Las Cabeceras añaden Control, pero cobran con más Tasa de Bits requerida. Como consecuencia la Tasa de Bits Real del Códec se aumenta considerablemente.

2.2.1.3. Enrutamiento de los Paquetes

³http://www.voztovoice.org/tmp/Codec-y-consumo-de-banda_CC54/Captura_thumb.png

Varios usuarios pueden utilizar simultáneamente la misma línea o realizar varias conversaciones al mismo tiempo, a diferencia de las redes telefónicas tradicionales. Cada paquete contiene la información de direccionamiento en la que se especifica la dirección del equipo origen y destino (parte de la cabecera del protocolo IP). Los paquetes dentro de una simple transmisión pueden tomar diversas vías desde el punto de origen al punto final de destino a través de una red de datos, esto se muestra en la *Figura II.3*.

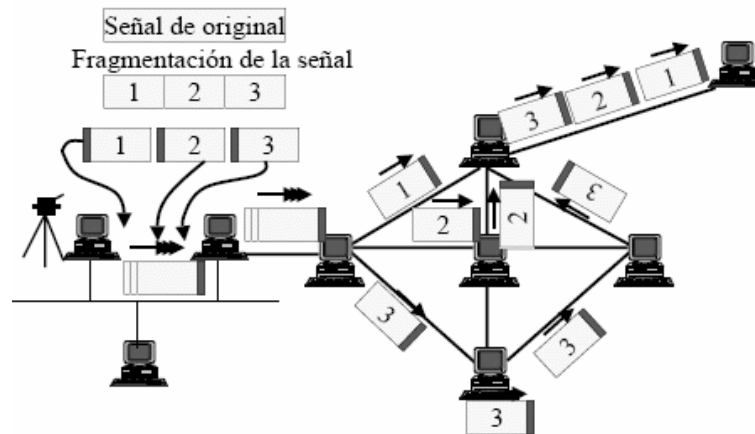


Figura II.3.Enrutamiento de paquetes en la red ⁴

2.2.1.4. Codificadores / Decodificadores de voz (CoDecs)

Los códecs son el medio por el cual una señal analógica puede ser convertida en una señal digital y ser transportada a través del Internet. El ancho de banda y el número de conversaciones simultáneas que se pueden transportar en una conexión en particular están directamente relacionados con el tipo de códec a ser implementado. Entre cada tipo de códec existen diferencias en requerimientos de ancho de banda, calidad y características de codificar el flujo de datos de la señal, como se muestra en la *Tabla II.1*.

⁴http://www.imaginar.org/ngn/manuales/P_protocolos_enrutamiento.pdf

Tabla II.I. Características de Códecs⁵

Codec	Compresión de Datos (Kbps)	Requerimientos de Licencia
G.711	64 Kbps	No
G.726	16, 24 o 32 Kbps	No
G.723.1	5.3 o 6.3 Kbps	Si*
G.729A	8 Kbps	Si*
GSM	13 Kbps	No
iLBC	13.3 Kbps o 15.2 Kbps	No
Speex	Variable entre 2.15 y 22.4 Kbps	No

* Existen versiones de prueba gratuitas.

2.3. Protocolos

Dentro del conjunto de protocolos de Voz sobre IP tenemos aquellos relacionados a los datos, estos son necesarios para llevar el tráfico de un usuario a otro. Y los protocolos de control relacionados al tráfico, necesarios para conectar y mantener el tráfico actual de usuario.

2.3.1. Protocolos de Transporte

2.3.1.1. RTP

Es un protocolo desarrollado por la IETF, el cual es empleado para transmitir información de audio y video a través del Internet en tiempo real. Este protocolo se encapsula dentro de datagramas UDP. Al trabajar bajo UDP no garantiza la entrega de todos los paquetes al igual que su llegada al destino en el instante adecuado. La capa de aplicación se encarga de superar estos fallos en la transmisión de información. RTP no trabaja con un puerto definido por lo general escoge un numero par elegido al azar.

RTP es el protocolo que se encarga de transportar la voz propiamente dicha. Una vez que SIP establece una llamada es RTP quien toma la posta para transportar la voz a su destino. Si un paquete de voz se pierde en el camino simplemente se rellenará ese espacio con un

⁵<https://comdigital.wikispaces.com/>

silencio. Lo que técnicamente se llama ruido confortable (*comfortnoise*). A pesar de encargarse de casi toda la labor de transportar la voz, RTP no está solo y tiene un protocolo de apoyo llamado RTCP.

En telefonía IP RTP se encarga de la digitalización y comprensión de la voz.

- *Reconocimiento*: identifica el tipo de información transmitida.
- *Secuenciación*: RTP implementa números de secuencia de paquetes IP para rearmar la información en el emisor y receptor, e indicar el instante donde se generó el paquete.
- *Multicasting*: Los paquetes de difusión múltiple utilizan RTP para enrutar conversaciones en múltiples usuarios.
- *Monitorización*: Controla la llegada de los paquetes al destino.

2.3.1.2. RTCP

Protocolo usado para enviar datos de control y de mediciones realizadas durante la transmisión. RTCP no es del todo indispensable pero proporciona valiosa ayuda al momento de transportar la voz de manera óptima. Para su transmisión se encapsulan dentro de mensajes RTP. La frecuencia de envío es aproximadamente cada cinco segundos. El puerto con el cual trabaja RTCP al igual que RTP no es definido, por ello escoge un número de puerto impar consecutivo en relación al seleccionado por RTP. RTCP no da ninguna clase de cifrado de flujo o de autenticación.

RTCP realiza el control de flujo RTP; es decir, permite obtener información básica sobre los participantes de la sesión y la calidad de servicio. El emisor y receptor de la comunicación intercambian estadísticas sobre paquetes perdidos y recibidos.

2.3.2. Protocolos de Señalización.

2.3.2.1. Protocolo H.323

El estándar H.323 es un conjunto de normas y protocolos recomendado por el ITU-T

diseñado para permitir transmisiones multimedia en LANs basadas en IP. Fue rápidamente adoptado por fabricantes de equipos para transmitir voz y videoconferencia sobre IP ya que define un modelo básico de llamada con servicios suplementarios (convergencia de voz, vídeo y datos en una sola red) y surgió en el momento adecuado.

Sus principales características son:⁶

- No garantiza una calidad de servicio (QoS).
- Es independiente de la topología de la red
- Admite pasarelas.
- Permite usar más de un canal (voz, vídeo, datos) al mismo tiempo.
- El estándar permite que las empresas añadan funcionalidades, siempre que implementen las funciones de interoperabilidad necesarias.

Los componentes principales del sistema H.323 son:

- *Terminales*: Equipamiento que utilizan directamente los usuarios. Se pueden implementar tanto por software como por hardware.
- *Gatekeepers*: Son el centro de toda organización VoIP y son el equivalente a las centralitas privadas o PBX. Normalmente se implementan por software.
- *Gateways*: Hacen de enlace con la red telefónica conmutada, actuando de forma transparente para el usuario.
- *MCUs*: se encargan de gestionar las multi-conferencias.

2.3.2.2. Protocolo SIP

Session Initiation Protocol es un protocolo desarrollado por el grupo de trabajo MMUSIC del 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 en línea y realidad virtual.

El protocolo SIP fue diseñado por el IETF con el concepto de "caja de herramientas", es

⁶<http://bibing.us.es/proyectos/abreproy/11252/fichero/2-H.323.pdf>

decir, el protocolo SIP se vale de las funciones aportadas por otros protocolos, que da por hechas y no vuelve a desarrollar. Debido a este concepto, SIP funciona en colaboración con otros muchos protocolos, entre ellos el protocolo SDP, que describe el contenido multimedia de la sesión, además está el RTP.

Las funciones básicas del protocolo incluyen:

- Determinar la ubicación de los usuarios, aportando movilidad.
- Establecer, modificar y terminar sesiones multipartitas entre usuarios.

El protocolo SIP adopta el modelo cliente-servidor y es transaccional. El cliente realiza peticiones (requests) que el servidor atiende y genera una o más respuestas. La petición inicial y todas sus respuestas constituyen una transacción. Los servidores, por defecto, utilizan el puerto 5060 en TCP y UDP para recibir las peticiones de los clientes SIP.

2.3.2.3. Protocolo IAX

El protocolo IAX es un protocolo de señalización creado por Mark Spencer, el mismo creador de Asterisk, con el objetivo de solucionar algunos problemas existentes con otros protocolos. En esencia IAX presenta tres ventajas muy interesantes sobre otras alternativas como SIP.

- Consume menos ancho de banda.
- Soluciona mejor problemas de NAT.
- Pasa más fácilmente a través de firewalls.

Estas ventajas resultan perfectas para troncalización entre dos servidores Elastix. En otras palabras, es recomendable el uso de IAX para interconectar dos o más servidores Elastix entre sí.

IAX es un protocolo binario, a diferencia de SIP que es un protocolo basado en texto. IAX usa UDP y normalmente usa el puerto 4569. Lo interesante de IAX es que por un solo

puerto transmite tanto la voz como la señalización y es esto lo que le permite resolver problemas de NAT y pasar a través de *firewalls* sin mayor inconveniente.

Además el protocolo permite la troncalización de varios canales de audio en el mismo flujo de datos. Es decir que en un mismo datagrama se pueden enviar varias sesiones al mismo tiempo, lo que significa una reutilización de datagramas.⁷

2.3.2.3.1. Fases de una llamada IAX

Una llamada IAX tiene tres fases:

- *Establecimiento de la llamada*: Para iniciar una llamada el equipo que la inicia (equipo A) le envía un mensaje *NEW* al equipo B y éste último responde con un mensaje *ACCEPT*. Luego de esto el equipo destino timbrará en espera de que el usuario conteste. Si esto sucede, el equipo B enviará un mensaje *ANSWER* al equipo A para notificar que el usuario contestó. *Figura II.4.*
- *Llamada en curso*: Si se contestó la llamada se inicia el intercambio de audio mediante unos paquetes llamados *frames*. Estos *frames* se envían dentro del mismo flujo de comunicación que la señalización inicial.
- *Colgad*: Para terminar la llamada cualquiera de las partes involucradas debe enviar un mensaje *HANGUP*.

Para intercambiar el audio entre los participantes de la llamada se utilizan dos tipos de *frames* llamados Full y Mini. También se les suelen llamar F y M. Una conversación está compuesta en su mayoría por *frames* tipo Mini cuya virtud es (como su nombre lo sugiere) ser ligeros. Esto quiere decir que tienen una cabecera pequeña (de 4 bytes), lo cual ayuda a ahorrar ancho de banda. De cuando en cuando se intercambian *frames* tipo Full, los cuales conllevan adicionalmente información de sincronización para mantener sincronizados a ambos puntos.

⁷ Gil Cabezas, Jesús., Protocolo IAX., Córdoba, Argentina., 209.

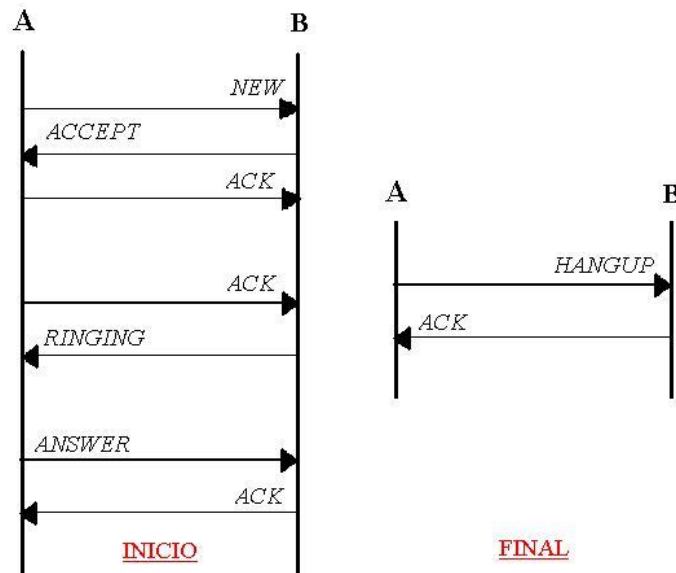


Figura II.4. Establecimiento y Finalización de una llamada IAX entre dos puntos.

2.4. Diseño de la red

Antes de decidirse por una plataforma se debe tener una clara idea de la naturaleza de sus problemas de comunicación. El diseño de red que se elija debe concordar con los problemas de comunicaciones que se está tratando de resolver. Para lo cual debemos plantearnos metas, dando respuesta a preguntas como: ¿Quién va a usar la red? ¿Qué tareas van a desempeñar los usuarios en la red? ¿Cuál es la relación Costo-Beneficio? Cuando esas respuestas sean respondidas, las prioridades serán establecidas y el proceso del diseño de la red será mucho más productivo. Estas prioridades se convertirán en las metas del diseño. Cuyos pasos se plasman en la *Figura II.5*.

- **Desempeño (performance):** Los tipos de datos procesados pueden determinar el grado de desempeño requerido. Si la función principal de la red es transacciones en tiempo real, entonces el desempeño asume una muy alta prioridad y el costo se eleva. En nuestro caso necesitamos un buen desempeño debido a que trabajamos con VoIP.
- **Volumen proyectado de tráfico:** Algunos equipos de interconexión como los puentes, concentradores pueden ocasionar cuellos de botella (bottle necks) en las redes con tráfico pesado. Cuando se está diseñando una red se debe de incluir el número

proyectado de usuarios, el tipo de trabajo que los usuarios harán, el tipo de aplicaciones que se correrán y el monto de comunicaciones remotas (www, ftp, telnet, VoIP, real audio, etc). Si bien un diseñador de red no puede predecir el futuro, éste debe de estar al tanto de las tendencias de la industria.

- **Expansión futura:** Las redes están siempre en continuo creciendo. Una meta del diseño deberá ser planear para el crecimiento de la red, para que las necesidades de la compañía no saturen la red en un futuro inmediato. Los nodos deberán ser diseñados para que estos puedan ser enlazados al mundo exterior. ¿Cuántas estaciones de trabajo puede soportar el sistema operativo de red? ¿El ancho de banda del medio de comunicación empleado es suficiente para futuro crecimiento de la red? ¿El equipo de comunicaciones tiene puertos disponibles para futuras conexiones?
- **Seguridad:** Permite proteger la red contra el robo y el uso incorrecto de información confidencial de la empresa y ofrecen protección contra ataques maliciosos de virus y gusanos de Internet. La seguridad de la red no se basa en un método concreto, sino que utiliza un conjunto de barreras, incluso si falla una solución, se debe mantener otros planes de contingencia. De esta manera se garantiza el funcionamiento de todas las máquinas de la red de manera óptima y que todos los usuarios de estas máquinas posean los derechos que les sean concedidos. Aquí entran preguntas como: ¿Estarán encriptados los datos? ¿Qué nivel de seguridad en los *passwords* es deseable?
- **Redundancia:** Las redes robustas requieren redundancia, si algún elemento falla, la red deberá seguir operando por sí misma. Un sistema tolerante a fallas debe estar diseñado en la red, de tal manera que, si un servidor falla, un segundo servidor de respaldo entrará a operar inmediatamente. La redundancia también se aplica para los enlaces externos de la red. Los enlaces redundantes aseguran que la red siga funcionando en caso de que un equipo de comunicaciones falle o el medio de transmisión en cuestión. Es común que compañías tengan enlaces redundantes, si el enlace terrestre falla (por ejemplo, una línea privada), entra en operación el enlace vía satélite o vía microondas. Es lógico que la redundancia tenga un mayor costo, pero a veces es inevitable.
- **Compatibilidad: hardware & software** La compatibilidad entre los sistemas, tanto en *hardware* como en *software* es una pieza clave también en el diseño de una red. Los

sistemas deben ser compatibles, para que estos, dentro de la red puedan funcionar y comunicarse entre sí, por lo que el diseñador de la red, deberá tener cuidado de seleccionar protocolos, sistemas operativos de red, aplicaciones estándar. Así como deberá tener a la mano el *conversor* de un formato a otro.

- **Costo:** El costo que implica diseñar, operar y mantener una red, quizá es uno de los factores por los cuales las redes no tengan la seguridad, redundancia, proyección a futuro y personal adecuado. Seguido ocurre que las redes se adaptan al escaso presupuesto y todas las metas del diseño anteriores no se puedan implementar.

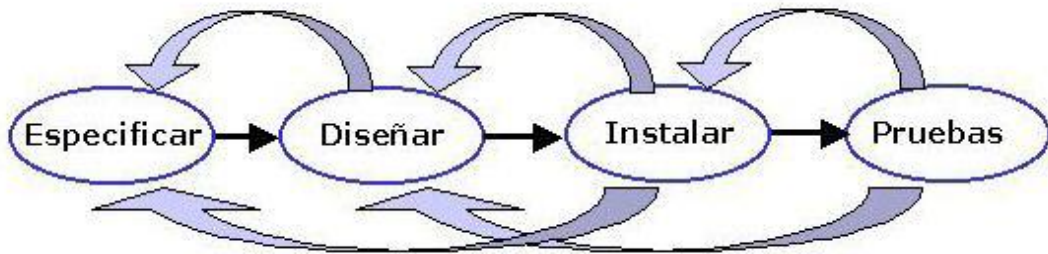


Figura II.5. Pasos para un correcto diseño de red.

2.4.1. Topología Física⁸

Constituye la parte palpable de la red, el diseño que se elija va a depender de la naturaleza del problema que se esté tratando de resolver.

La topología física se define como la cadena de comunicación que los nodos que conforman una red usan para comunicarse. La topología de red la determina únicamente la configuración de las conexiones entre nodos. La distancia entre los nodos, las interconexiones físicas, las tasas de transmisión y/o los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma.

Estas pueden denominarse de diferente manera, dependiendo de su organización:

- **Topología de Bus:** Es una topología de red en la que todas las estaciones están

⁸ <http://www.bloginformatico.com/topologia-de-red.php>

conectadas a un único canal de comunicaciones por medio de unidades interfaz y derivadores. Las estaciones utilizan este canal para comunicarse con el resto.

- **Topología de estrella:** Este tipo de red consiste en conectar todas las computadoras a un punto central, en el que todas las comunicaciones tienen que hacerse a través de ese punto. Este tipo de red es muy utilizada en las redes locales.
- **Topología de Anillo:** En esta topología las computadoras van conectadas en serie y la última se conecta con la primera formando un anillo. Solo se encuentra en redes muy antiguas, ya que actualmente no se usa para crear redes debido a su poca funcionalidad comparada con otras topologías.
- **Topología de Árbol o Jerárquica:** Puede verse como una combinación de varias topologías en estrella. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol.
- **Topología de Malla:** Topología de red en la que cada nodo está conectado a uno o más de los otros nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada nodo tiene sus propias conexiones con todos los demás nodos.

2.4.2. Topología lógica

Es la forma de conseguir el funcionamiento de una topología física cableando la red de una forma más eficiente.

Existen topologías lógicas definidas:

- **Topología anillo-estrella:** implementa un anillo a través de una estrella física.
- **Topología bus-estrella:** implementa una topología en bus a través de una estrella física.

2.5. Sistemas Distribuidos

"Sistemas cuyos componentes hardware y software, que están en ordenadores conectados en red, se comunican y coordinan sus acciones mediante el paso de mensajes, para el logro de un objetivo. Se establece la comunicación mediante un protocolo prefijado por un esquema cliente-servidor".⁹

Características:

- **Concurrencia.-** Esta característica de los sistemas distribuidos permite que los recursos disponibles en la red puedan ser utilizados simultáneamente por los usuarios y/o agentes que interactúan en la red.
- **Carencia de reloj global.-** Las coordinaciones para la transferencia de mensajes entre los diferentes componentes para la realización de una tarea, no tienen una temporización general, está más bien distribuida a los componentes.
- **Fallos independientes de los componentes.-** Cada componente del sistema puede fallar independientemente, con lo cual los demás pueden continuar ejecutando sus acciones. Esto permite el logro de las tareas con mayor efectividad, pues el sistema en su conjunto continua trabajando.

2.5.1. Evolución de los Sistemas Distribuidos

A lo largo de los años, desde la aparición del concepto de sistemas distribuidos han existido diferentes maneras de llevarlos a la práctica. Así tenemos:

- **Procesamiento central (Host).-** Uno de los primeros modelos de ordenadores interconectados, llamados centralizados, donde todo el procesamiento de la organización se llevaba a cabo en una sola computadora, normalmente un Mainframe, y los usuarios empleaban sencillos ordenadores personales.

Los problemas de este modelo son: -Cuando la carga de procesamiento aumentaba se tenía que cambiar el hardware del Mainframe, lo cual es más costoso que añadir más computadores personales clientes o servidores que aumenten las capacidades. - El otro

⁹ <http://www.monografias.com/trabajos16/sistemas-distribuidos/sistemas-distribuidos.shtml>

problema que surgió son las modernas interfaces gráficas de usuario, las cuales podían conllevar a un gran aumento de tráfico en los medios de comunicación y por consiguiente podían colapsar.

- **Grupo de Servidores.-** Otro modelo que entró a competir con el anterior, también un tanto centralizado, son un grupo de ordenadores actuando como servidores, normalmente de archivos o de impresión, poco inteligentes para un número de Minicomputadores que hacen el procesamiento conectados a una red de área local. Presentado problemas como: -Podría generarse una saturación de los medios de comunicación entre los servidores poco inteligentes y los minicomputadores.
- **La Computación Cliente Servidor.-** Este modelo, que predomina en la actualidad, permite descentralizar el procesamiento y recursos, sobre todo, de cada uno de los servicios y de la visualización de la Interfaz Gráfica de Usuario. Esto hace que ciertos servidores estén dedicados solo a una aplicación determinada y por lo tanto ejecutarla en forma eficiente.

2.5.2. Ventajas de los Sistemas Distribuidos

Con respecto a Sistemas Centralizados:

- La economía, pues es mucho más barato, añadir servidores y clientes cuando se requiere aumentar la potencia de procesamiento.
- El trabajo en conjunto. Por ejemplo: en una fábrica de ensamblado, los robots tienen CPUs diferentes y realizan acciones en conjunto, dirigidos por un sistema distribuido.
- Tienen una mayor confiabilidad. Al estar distribuida la carga de trabajo en muchas máquinas la falla de una de ellas no afecta a las demás, el sistema sobrevive como un todo.
- Capacidad de crecimiento incremental. Se puede añadir procesadores al sistema incrementando su potencia en forma gradual según sus necesidades.

Con respecto a PCs Independientes:

- Se pueden compartir recursos, como programas y periféricos, muy costosos. Ejemplo: Impresora Láser, dispositivos de almacenamiento masivo, etc.

- Al compartir recursos, satisfacen las necesidades de muchos usuarios a la vez. Ejemplo: Sistemas de reservas de aerolíneas.
- Se logra una mejor comunicación entre las personas. Ejemplo: el correo electrónico.
- Tienen mayor flexibilidad, la carga de trabajo se puede distribuir entre diferentes ordenadores.

2.6. Elastix

Para el montaje y configuración de nuestra red, vamos a utilizar la distro Elastix, debido a sus grandes prestaciones y simplicidad al momento de usarlo.

Elastix fue creado y actualmente es mantenido por la compañía ecuatoriana Palosanto Solutions. Elastix es una interfaz libre de Servidor de Comunicaciones Unificadas que integra en un solo paquete: VoIP PBX, fax, mensajería instantánea, correo electrónico, colaboración¹⁰.

Elastix implementa gran parte de su funcionalidad sobre cuatro programas de software muy importantes como son Asterisk, Hylafax, Openfire y Postfix. Estos brindan las funciones de PBX, Fax, Mensajería Instantánea y Correo electrónico respectivamente. La parte de sistema operativo se basa en CentOS, una popular distribución Linux orientada a servidores.

A través de sus versiones se han añadido varias funcionalidades las cuales incluyen un módulo de Call Center, el cual se comunica con una consola de agente a través de un protocolo propietario, denominado ECCP. El protocolo es de código abierto y permite además la comunicación con consolas desarrolladas por terceros diseñadas para actuar como agente o supervisor.

¹⁰ **Edgar Landívar.**, Comunicaciones Unificadas con Elastix., Volumen 1., 2008

La interface Web de Elastix es una aplicación completa de administración del servidor de comunicaciones unificadas escrita en su mayoría en lenguaje PHP.

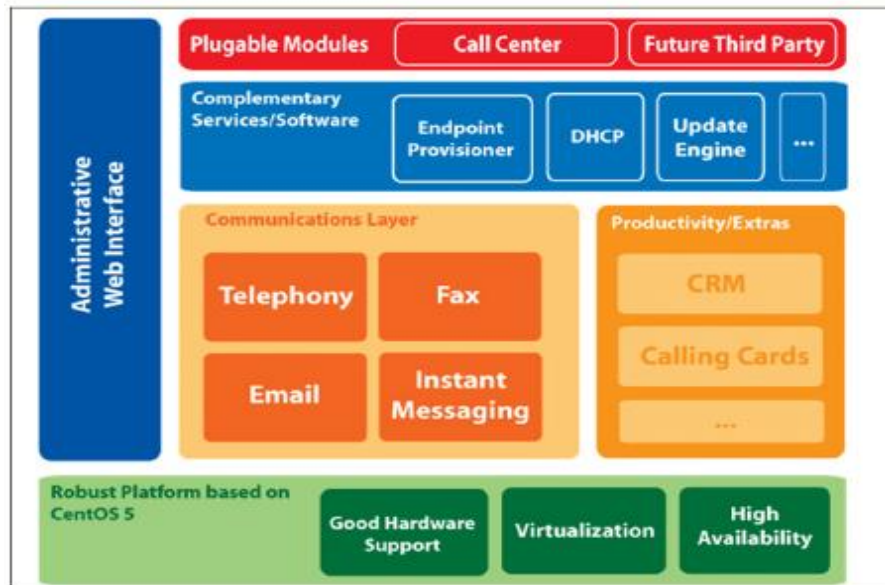


Figura II.6. Esquema General de los Componentes Elastix ⁽¹¹⁾.

2.6.1. Dial Plan

Constituye la configuración de la central Asterisk, es decir su comportamiento Lógico. El dialplan o plan de marcado, por tanto indica el itinerario que sigue una llamada desde que entra o sale del sistema hasta que llega a su destino.

El plan de marcado en Asterisk reside principalmente en el archivo extensions.conf. Desde este archivo se incluyen otros importantes que contienen también porciones del plan de marcado. Los principales son:

- extensions_additional.conf
- extensions_custom.conf

¹¹Edgar Landívar, Comunicaciones Unificadas con Elastix. Volumen 1

Todos estos archivos del plan de marcado están escritos en texto plano en un formato definido por Asterisk. Estos archivos se encuentran divididos en secciones llamadas contextos. Más adelante explicaremos más detalladamente cada archivo interviniente.

2.6.1.1. Contexto (Context)

El plan de marcado se divide en uno o varios contextos. Un contexto es una colección de extensiones. Los contextos existen para programar las funcionalidades de marcado de acuerdo a los requerimientos del usuario, tales como: diferenciar donde se encuentra una llamada, aplicar políticas de seguridad y acceso, proceso de registro de los teléfonos IP, etc.

Básicamente los contextos sirven para formar una agrupación lógica de plan de marcado. Los contextos también pueden incluir otros contextos mediante la cláusula "include" o redirigir el hilo de ejecución del plan de marcado a otros contextos dependiendo de condiciones. Un contexto también puede agrupar la lógica necesaria para la aplicación de reloj despertador. En general prácticamente todo en el plan de marcado se encuentra agrupado en contextos. Los contextos son los agrupadores u organizadores del plan de marcado. Cada contexto debe llevar un nombre único y este nombre va encerrado entre los símbolos [y].

Contextos reservados: Hay dos nombres de contextos que están reservados para un propósito especial y son [general] y [globals].

2.6.1.2. Aplicación

En las aplicaciones radica el verdadero poder del plan de marcado en Asterisk. Para hacer una analogía, las aplicaciones son el equivalente a las funciones de un lenguaje de programación. Las aplicaciones nos permitirán contestar una llamada o colgarla, reproducir música en espera, saltar a otros contextos entre otras muchas cosas.

2.7. Protocolo DUNDI

DUNDI por sus siglas en inglés significa Distributed Universal Number Discovery, es un protocolo que nos permite buscar y compartir planes de marcación entre servidores IP-PBX, como lo es Asterisk, por medio de un sistema par a par que se utiliza para localizar gateways de Internet para servicios de telefonía. Debido a que es una red par a par no existen roles fijos de cliente-servidor. Por este motivo a diferencia de los sistemas centralizados, como el estándar ENUM, DUNDI se distribuye de manera completa a lo largo de toda la red sin ninguna autoridad centralizada.

El protocolo fue inventado por Mark Spencer, quién también hizo el IP-PBX Asterisk por lo que ambos sistemas son compatibles entre sí y los comandos de búsqueda se pueden hacer directamente desde la línea de comandos de Asterisk.¹²

2.7.1. Funcionamiento

Antes de implementar DUNDI debemos saber cómo funciona, para esto imaginemos a DUNDI como un gran directorio telefónico que le permite a preguntar a los demás equipos si conoce alguna ruta alterna para realizar la llamada ya sea esta hacia una extensión o hacia algún teléfono de red telefónica pública conmutada.

Cada cliente DUNDI tiene que conocer al menos a otro cliente DUNDI o par dentro de la red. En la configuración de DUNDI el número de búsquedas consecutivas entre pares en la red para llegar al destino deseado se puede limitar utilizando el TTL.

El $TTL = 1$ significa que sólo se puede pedir búsquedas a los compañeros conocidos. El $TTL = n$ significa que al compañero al cual se pide la búsqueda puede redirigir la búsqueda a otros compañeros conocidos por él, solo con un TTL de $n-1$.

Por ejemplo, supongamos que estamos dentro de un red DUNDI y deseamos comunicarnos con la extensión 555 la cual no pertenece de manera local, entonces nuestro servidor “A”

¹² MULLINIX, J., DUNDi configuration., Cohutta – EEUU.,

preguntara a los otros equipos que dentro de la red si conocen a la extensión 555, suponiendo que el servidor “B” es uno de los equipos conectados con nuestro servidor, este también preguntara a el resto de equipos si conoce la extensión. Así directa o indirectamente esta consulta se hará a todos los equipos pertenecientes a la red DUNDI. La centralita que contenga esa extensión será la encargada de emitir una respuesta y será algo parecido a “IAX2/usuario:clave@1.2.3.4/555”.

Finalmente el equipo que hizo la consulta utilizará esa información para llamar efectivamente a la extensión 555. Además la respuesta es guardada por todos los equipos para de esta manera en la siguiente oportunidad que se efectúe otra llamada a la misma extensión, los equipos seleccionan la mejor ruta. Este aprendizaje de rutas ayuda a la red a incrementar su tiempo de respuesta y a reducir la carga de información. Hay que tener en cuenta que la información guardada tiene un tiempo límite de validez, sin embargo la solución a esto es declarar el argumento switch => dentro del archivo extensions.conf.

2.7.2. Características

DUNDI permite configurar una red redundante al eliminar puntos centrales de falla. En el caso que un Servidor PBX deje de funcionar, la llamada será enrutada por otras rutas para llegar a su destino sin ser descartada.

DUNDI da la posibilidad de añadir nuevas extensiones a los planes de marcación de forma dinámica, función requerida para dar movilidad a los usuarios a través de la red.

DUNDI no consume mayor ancho de banda para proporcionar seguridad y privacidad. DUNDI utiliza RSA y AES para el cifrado y la autenticación de la información.

DUNDI se puede utilizar dentro de una empresa para crear una completa PBX asociada, con ningún punto de falla central; también ofrece la posibilidad de agregar arbitrariamente nuevas extensiones, gateways u otros recursos en una red confiable de servidores de

comunicación, donde cualquier creación, movimiento, cambio, falla o nuevas rutas; son absorbidas automáticamente dentro de la nube sin tener que realizar ninguna configuración adicional.

DUNDI también puede utilizar todo el Internet para formar una red E.164 confiable que permita a los proveedores de servicios habilitar números de teléfono reales a través de Internet. Esto permite tener el control de los números sin necesidad de un cargo adicional y transparente para el usuario. Un uso responsable y una correcta creación de políticas nos ayudarían a prevenir llamadas VoIP tipo “spam”.

DUNDI por sí mismo no es un protocolo de señalización de VoIP ni tampoco un medio de comunicación. En lugar de ello, DUNDI publica rutas por las cuales se accede a través de protocolos estándar como IAX, SIP y H.323. El protocolo DUNDI utiliza por defecto el puerto 4520/UDP. Habrá que abrirlos en los firewalls. Es independiente de IAX, es decir, la cadena de conexión devuelta en una consulta puede hacer referencia a cualquier tipo de canal (IAX2, SIP, H323, etc.), aunque normalmente se usa el IAX2.

2.7.3. Etapas de Transmisión

2.7.3.1. Transacción:

Una transacción DUNDI es un diálogo completo en el protocolo DUNDI de una PBX (nodo) a otra. Cada mensaje contiene dos números de transacción un origen y un destino para que un mensaje recibido pueda ser identificado únicamente por el número de transacción de manera aislada

2.7.3.2. Retransmisión:

Una solicitud DUNDI puede ser retransmitida hasta 10 veces a intervalos de tiempo que serán decididas por el implementador, pero no más de 1 segundo. Si un mensaje no se

reconoce después de 10 retransmisiones o 10 segundos, la operación deberá ser considerada cerrada, sin mensajes adicionales que se transmiten o se esperan.

2.7.3.3. Registro:

El registro se utiliza para un par DUNDI, por lo general con una ubicación dinámica o una dirección traducida, para registrar su presencia a otros pares DUNDI. Las aplicaciones también pueden recibir parámetros. Por ejemplo a la aplicación Dial() habrá que indicarle qué número marcar para que pueda realizar su labor.

2.7.4. Archivos Configurables.

Dentro de Asterisk existen un sinnúmero de archivos que nos permiten administrar cada una de las características que esta plataforma nos ofrece al momento de montar nuestra propia central telefónica. Estos archivos nos permitirán acoplar cada una de estas características acorde a nuestras necesidades. Basaremos nuestro estudio en los archivos involucrados al momento de configurar DUNDI.

Tabla II.II. Archivos configurables en Asterisk

Archivo	Descripción
extensions.conf	Aquí reside el plan de marcado. En Elastix este archivo incluye otros más para organizar el plan de marcado de mejor manera. Estos archivos adicionales empiezan con la cadena extensions_
sip.conf	Aquí se definen los end points SIP
iax.conf	Aquí se definen los end points IAX

2.7.4.1. extensions.conf

Es el propio Dial-plan de Asterisk. Le permite a la central telefónica determinar las acciones a tomar en función, básicamente, de lo que ha marcado el usuario desde el cliente

de telefonía IP. Se le denomina el “corazón” de Asterisk, pues gracias a este archivo es que esta solución de telefonía IP goza de tanta flexibilidad y funcionalidad, sin olvidar el gran aporte que le da la existencia de aplicaciones y funciones que pueden utilizarse dentro del plan de marcado.



```
<< Back File: extensions_custom.conf Save Reload Asterisk
; This file contains the contexts the agents login for the module call center.
; and contains the context conferences for module conferences of elastix 1.0.

[vozcom-local]
exten => _0057.,1,Dial(SIP/justvoip/${EXTEN})
exten => _30X,1,Dial(SIP/${EXTEN},15)
exten => _30X,n,GotoIf(["${DIALSTATUS}" = "BUSY"]?busy:unavail)
exten => _30X,n(busy),Voicemail(${EXTEN}@default,b)
exten => _30X,n,Hangup
exten => _30X,n(unavail),Voicemail(${EXTEN}@default,u)
exten => _30X,n,Hangup
```

Figura II.7. Configuración extensiones PBX_A.

La configuración del archivo extensions_custom.conf es similar en los tres servidores, la única diferencia se muestra al momento de declarar las extensiones, en la PBX_A tenemos la extensión 1XX, en la PBX_B 2XX y en la PBX_C las 3XX; las declaraciones se hacen de esta manera debido al rango que cubren nuestras extensiones, de esta manera simplificamos la declaración de todas nuestras extensiones en una sola línea de código, en la que el signo X toma un valor del 0 al 9. Véase la *Figura II.7*.

El resultado final de las configuraciones de los archivos necesarios para el funcionamiento de DUNDI se adjunta en el ANEXO 3.

2.7.4.2. sip.conf

Este archivo sirve para configurar todo lo relacionado con el protocolo SIP y añadir nuevos usuarios o conectar con proveedores SIP. El fichero sip.conf comienza con una sección [general] que contiene la configuración por defecto de todos los usuarios y "peers" (proveedores). Se puede sobrescribir los valores por defecto en las configuraciones de cada usuario o peer.

Cada extensión está definida por un *user* o usuario, un *peer* o proveedor o un *friend* o amigo y viene definida con un nombre entre corchetes [].

```
1 [general]
2 register => USERID:PW@sip.voipon.co.uk/USERID
3
4 [voipon]
5 type=friend
6 username=USERID
7 secret=PW
8 fromuser=USERID
9 host=sip.voipon.con.uk
10 dtmfmode=rfc2833
11 fromdomain=sip.voipon.co.uk
12 context=default
13 insecure=very
```

Figura II.8. Sintaxis sip.conf¹³

2.7.4.3. iax.conf

En este archivo se definen todos los enlaces que se realizaran usando el protocolo IAX. Al igual que en SIP, se pueden definir: Variables generales de IAX, Clientes IAX, Servidores IAX.

IAX soporta nativamente autenticación con clave publica/privada, al definir un peer se puede autenticar, además soporta nativamente “trunking”, es decir, enviar por un mismo flujo varias llamadas



Figura II.9. Configurando iax.conf

Añadimos estas líneas a cada servidor. Todo esto es hecho con una configuración IAX2. Ahora todo PBX tiene un canal para dirigir sus llamadas.

- El contexto *[priv]* es solo un nombre, podría ser cualquier nombre siempre que se use

¹³ Fuente Propia

el mismo en el archivo `dundi.conf`

- El tipo `type=friend` permite un canal en doble sentido entre servidores.
- El `dbsecret=dundi/secret` es la contraseña utilizada para la información de localización se envía a las solicitudes entre servidores. El protocolo DUNDI genera una nueva contraseña secreta a cada hora y almacena la contraseña en la base de datos de Asterisk local.
- El `context=incomingdundi` es el punto de entrada en el plan de marcado donde ingresarán las llamadas. Debe también existir un contexto `[incomingdundi]` en el archivo `extensions.conf` para que exista una ruta de enrutamiento para las extensiones. Aquí debe existir un `Goto o include=internal` para que una nueva llamada pueda ser procesada apropiadamente. Este contexto podría tener cualquier nombre o podría ser cualquier contexto actual, aquí es donde vienen las llamadas entrantes.

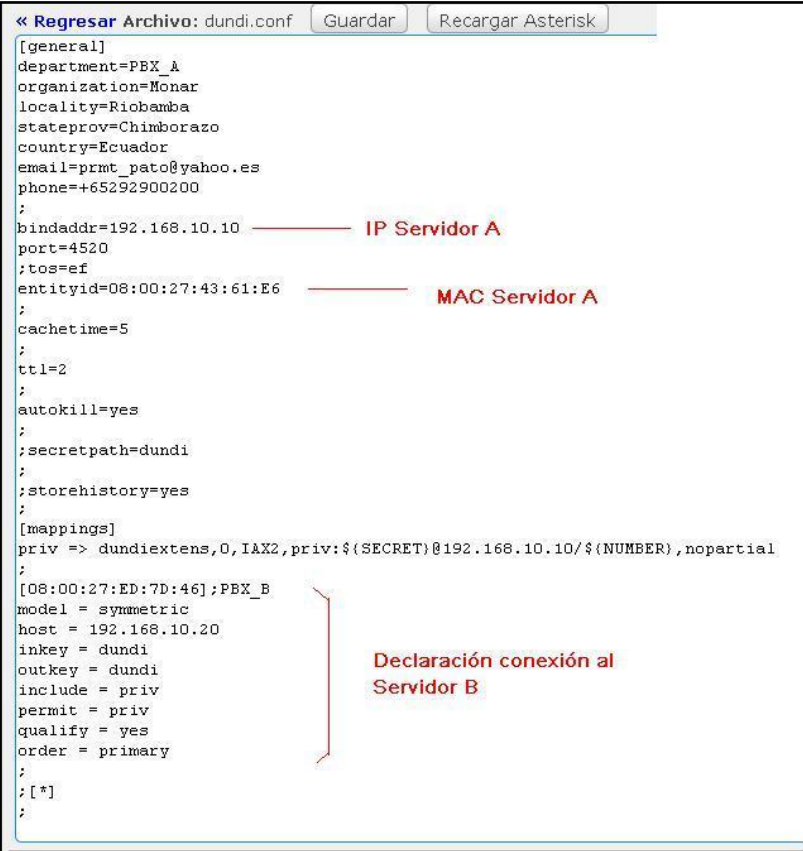
2.7.4.4. **dundi.conf**

Ahora vamos a ver la configuración específica `dundi.conf`. Aquí es donde configuramos nuestra relación de pares DUNDI entre servidores y las respuestas que se envían. DUNDI utiliza su propio protocolo en el puerto UDP 4520 para intercambiar mensajes de consulta DUNDI. DUNDI no se comunica a través de consultas o respuestas IAX, las llamadas pasan a través de la `[priv]` del canal IAX. Para probar esto se comenta el contexto `[priv]` de `iax.conf`, vuelva a cargar con `chan_iax.so` y se verifica que todavía puede tener consultas.

Iniciamos la declaración de las configuraciones para el `PBX_A`. Como vemos, la primera parte `[general]` consiste en indicar quiénes somos y la información de contacto. Esto permitirá a otros nodos de la red conocernos. Esta información es muy importante a la hora de interconexión con servidores externos a la organización. En el Asterisk

CLI>dundiquery {entityID}

Recuperará esta información de un punto remoto para el contacto.



The image shows a screenshot of a text editor displaying the configuration file `dundi.conf`. The file is divided into sections: `[general]`, `[mappings]`, and `[08:00:27:ED:7D:46];PBX_B`. Annotations in red text with lines pointing to specific configuration values are present:

- `bindaddr=192.168.10.10` is annotated as **IP Servidor A**.
- `entityid=08:00:27:43:61:E6` is annotated as **MAC Servidor A**.
- The entire `[08:00:27:ED:7D:46];PBX_B` section is annotated as **Declaración conexión al Servidor B**.

```
<< Regresar Archivo: dundi.conf Guardar Recargar Asterisk
[general]
department=PBX_A
organization=Monar
locality=Riobamba
stateprov=Chimborazo
country=Ecuador
email=prmt_pato@yahoo.es
phone=+65292900200
;
bindaddr=192.168.10.10
port=4520
;tos=ef
entityid=08:00:27:43:61:E6
;
cachetime=5
;
ttl=2
;
autokill=yes
;
secretpath=dundi
;
storehistory=yes
;
[mappings]
priv => dundiextens,0, IAX2,priv:${SECRET}@192.168.10.10/${NUMBER},nopartial
;
[08:00:27:ED:7D:46];PBX_B
model = symmetric
host = 192.168.10.20
inkey = dundi
outkey = dundi
include = priv
permit = priv
qualify = yes
order = primary
;
;[*]
;
```

Figura II.10. dundi.conf PBX_A

- El *entityid* es un parámetro importante. Es nuestra identificación en la red, y debe ser única. Si no lo definimos, se usará la dirección MAC de la primera interfaz de red, pero para más seguridad conviene definirlo.
- *Cachetime* le dice a la centralita extremo cuánto tiempo se debe almacenar en caché el resultado de la consulta en su caché local.

No necesitaremos conocer “personalmente” a todos los nodos de la red. Nuestros vecinos pueden propagar nuestras consultas a los suyos, y así sucesivamente hasta que el *ttl* llegue a 0. Poniendo *ttl=2* limitaremos la profundidad de las consultas, reduciendo el tiempo de espera y evitando exista un loop o bucle sin fin.

En la sección *[mappings]* es clave. Por un lado definimos los recursos que vamos a usar,

por otro indicaremos los números que nuestra centralita publicará.

```
priv => dundiextens,0,IAX2,priv:${SECRET}@192.168.10.10/${NUMBER},nonpartial
```

- **priv:** Este es el nombre del recurso, lo usaremos solamente para buscar extensiones en la red, en los diferentes servidores. Es el destino que se distribuye cuando hay una consulta de un número. Y sus variables son sustituidas automáticamente. *\${NUMBER}*: El numero está siendo buscado; *\${IPADDR}*: La dirección IP desde donde se conecta; *\${SECRET}*: La actual clave secreta creada al azar y que está siendo usada al momento.
- **nonpartial:** no se harán búsquedas por números que no sean completos.
- **dundiextens:** Es el contexto donde tenemos definidas nuestras extensiones. Cuando otro nodo busque una extensión que tenemos definida en este contexto, responderemos.
- **0:** Es el peso de nuestra respuesta. Cuando menor sea más peso (prioridad). Es útil en otro tipo de recursos. A la hora de buscar rutas de menor coste para las llamadas.
- **IAX2:** Simplemente indica el tipo de canal. Puede ser SIP, H323 o cualquier otro.

Cuando una solicitud [priv] de búsqueda DUNDI entra, esta central anuncia las extensiones presentes en el contexto [dundiextens] contenido en el dialplan (extensions.conf) y si la extensión consultada existe aquí, esta central le devolverá la información de contacto.

Las comunicaciones entre nodos van encriptados usando clave pública/privada. Deberemos generarlas previamente y almacenarlas en */var/lib/asterisk/keys*. El parámetro *inkey* indica la clave a usar en las consultas que nos hace el nodo, y *outkey* la que emplearemos nosotros cuando enviemos nuestras consultas.

2.7.5. Creación de Clave Pública.

Usamos el mismo inkey/outkey para PBX _A, B y C. El compartir la misma clave a través de la prueba de servidores es mucho más fácil que hacer el seguimiento de un conjunto de

claves para cada servidor. Para generar las claves:

```
[root@PBX_A ~]# cd /var/lib/asterisk/keys/
[root@PBX_A keys]# astgenkey -n priv

This script generates an RSA private and public key pair
in PEM format for use by Asterisk. You will be asked to
enter a passcode for your key multiple times. Please
enter the same code each time. The resulting files will
need to be moved to /var/lib/asterisk/keys if you want
to use them, and any private keys (.key files) will
need to be initialized at runtime either by running
Asterisk with the '-i' option, or with the 'init keys'
command once Asterisk is running.

Press ENTER to continue or ^C to cancel.

Generating SSL key 'priv':
Generating RSA private key, 1024 bit long modulus
.....+++++
..+++++
e is 65537 (0x10001)
writing RSA key
Key creation successful.
Public key: priv.pub
Private key: priv.key
[root@PBX_A keys]# _
```

Figura II.11. Claves generadas.

No ponga una contraseña en las llaves. Esto va a generar 2 archivos (priv.key y priv.pub)

Copie las nuevas claves priv a la centralita B y C para el directorio /var/lib/asterisk/directorios de las claves. Es necesario tener el paquete OpenSSL instalado en el sistema para generar las claves. Como se dijo en este documento vamos a configurar un par entre PBX_A con B, PBX_B con A y C, y PBC_C con B.

```
[root@PBX_A keys]# scp priv.pub root@192.168.10.20:/var/lib/asterisk/keys/
The authenticity of host '192.168.10.20 (192.168.10.20)' can't be established.
RSA key fingerprint is 55:0b:02:79:53:15:51:75:ff:9c:e9:23:eb:92:ef:49.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.20' (RSA) to the list of known hosts.

root@192.168.10.20's password:
priv.pub                               100% 272      0.3KB/s  00:00
[root@PBX_A keys]# _
```

Figura II.12. Copiando claves publicas entre servidores.

CAPÍTULO III

DISEÑO E IMPLEMENTACIÓN DE LA RED DE PRUEBA

3.1. Diseño de la red.

Para el proceso de diseño y montaje de la red, iniciamos las pruebas con dos nodos y una topología física en bus. Con un enlace ideal, por el cual solo viajará tráfico de voz. Con un ancho de banda de 100Mbps, que es la capacidad máxima de la tarjeta de red.



Figura III.13. Esquema de análisis A.

El funcionamiento es correcto, existe comunicación entre los dos servidores, hay un intercambio de datos (dial plan) entre los dos puntos. El único problema que se puede presentar aquí, sería la caída de uno de los dos nodos, o en su caso del enlace de comunicación. Como medida preventiva podemos tener dos enlaces de comunicación, para garantizar redundancia, por el cual además también podemos aplicar un balance de carga.

Continuando con el análisis para el diseño óptimo de nuestra red aumentamos un nodo, utilizando la misma topología en bus. Y las mismas características del modelo uno.

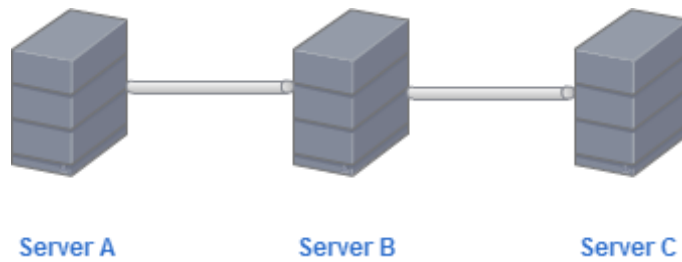


Figura III.14. Esquema de análisis B.

El funcionamiento del protocolo es correcto, el Servidor B sirve como canal de comunicación entre A y C, transmitiendo las consultas DUNDI. Aquí ya se evidencian las desventajas de la topología en bus, debido a que la caída de un nodo o una línea de comunicación dejarían a la red completa fuera de servicio. Por tanto descartamos esta topología. Para solventar este problema se puede adicionar un enlace de comunicación entre A y C, aumentando de esta manera los costos pero a cambio logramos redundancia en la red. Convirtiéndose en una red en anillo.

Ahora añadimos un nodo más a la red, pero esta vez cambiamos la topología usada por una red en malla, continuamos con el ancho de banda inicial, es decir; un enlace ideal, por el cual solo pasará tráfico de voz. Como se ve en la *Figura III.15*.

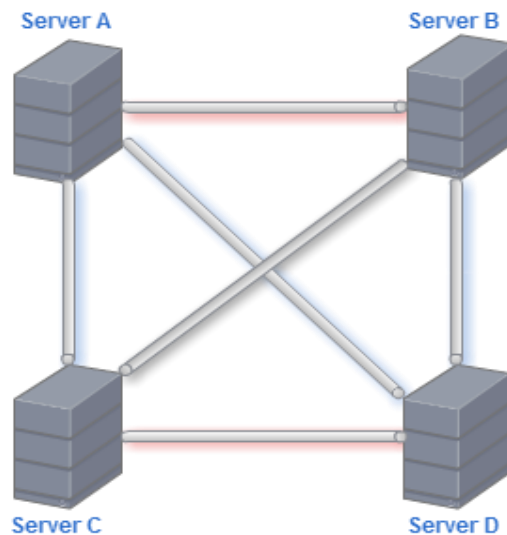


Figura III.15. Esquema de análisis C.

La principal ventaja de esta topología sería la redundancia total, al existir un enlace directo entre cada nodo hacia cada uno de los otros nodos en la red, y varias rutas secundarias. La desventaja de contar con esta red vendría a ser el costo de montaje y operación. Pues si queremos escalar la red el número de enlaces aumenta considerablemente según la fórmula.

$$N = \sum_{k=1}^{n-1} (k)$$

Donde

N = número total de enlaces.

n = número de nodos en la red.

En la actualidad son muy pocas las empresas que implementan este tipo de redes con redundancia total, dado el alto costo que implica. Lo que si se acostumbra es contar con al menos un enlace de backup para cada nodo de la red, o más de uno en caso de que la necesidad de comunicación sea imperiosa.

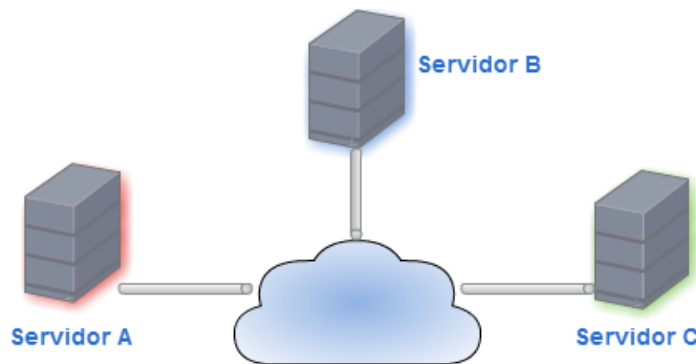


Figura III.16. Esquema de análisis D.

Otro modelo de red muy usado es el de estrella física y bus lógica. “La razón para la configuración de estrella es doble. Primeramente, esto refleja la estructura organizacional y flujo de datos de los negocios, con administración centralizada y funciones locales. Secundariamente, esto es impuesto por la tecnología de las líneas alquiladas”.¹⁴ “Ya que es el más extendido y los WANs de la estrella son más confiables que los WANs punto- a-punto

¹⁴ <http://www.monografias.com/trabajos11/frame/frame.shtml>

o del anillo”.¹⁵ Además, este modelo es el más cercano a la realidad, ya que la mayor parte de empresas no cuentan con infraestructura propia y subcontratan los servicios de un carrier para transmitir sus datos, ya sea a través de enlaces dedicados o Internet, entre ellas tenemos ADSL, Cable Módems, el RDSI o Fram Relay. Esta red se ve representada en la *Figura III.16*.

3.2. Implementación de la red

Para tener un diseño lo más cercano a la realidad vamos a trabajar con una red estrella física, que será de manera lógica una red en anillo. En la cual conectaremos tres servidores, debido a que en la mayoría de casos en los que se demuestra la configuración de DUNDI se usan dos servidores como en el caso de *JR Richardson* en su publicación web titulada “DUNDI, So Easy A Caveman Could Do It”¹⁶, también tenemos la publicación de *Julián J. Menéndez* “Usando la red DUNDI en Asterisk”.¹⁷ Para nuestro prototipo de prueba inicial tendríamos el siguiente esquema físico. *Figura III.17*.

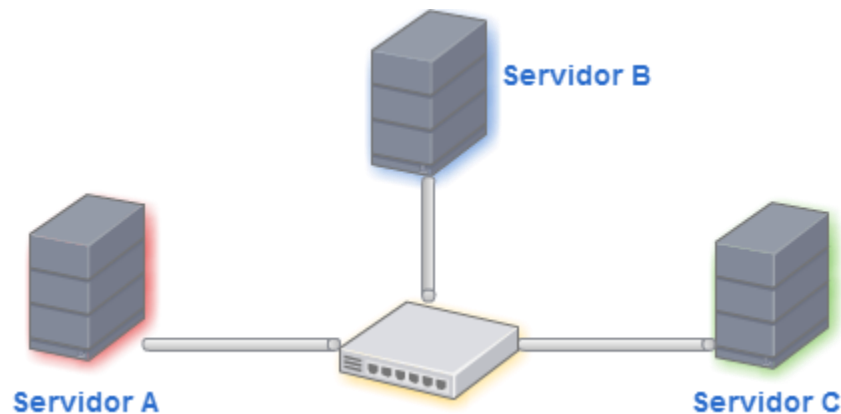


Figura III.17. Esquema Físico del prototipo de prueba.

Una vez instalados los servidores, y configurados los peers DUNDI, así como los diferentes archivos involucrados dentro de este protocolo; nuestra red lógica tendría el siguiente esquema, como se muestra en la *Figura III.18*, donde podemos ver que tenemos tres

¹⁵ <http://es.scribd.com/doc/73926343/Diseno-de-la-RED-WAN>

¹⁶ http://www.voip-info.org/storage/users/813/47813/images/1654/DUNDi_So_Easy.pdf

¹⁷ <http://www.julianmenendez.es/usando-dundi-asterisk/>

servidores, cada uno con un plan de marcado diferente, en cada servidores limitaremos el numero de extensiones a 10. De las cuales vamos a trabajar con tres en cada servidor, para realizar las llamadas y tomar los datos.

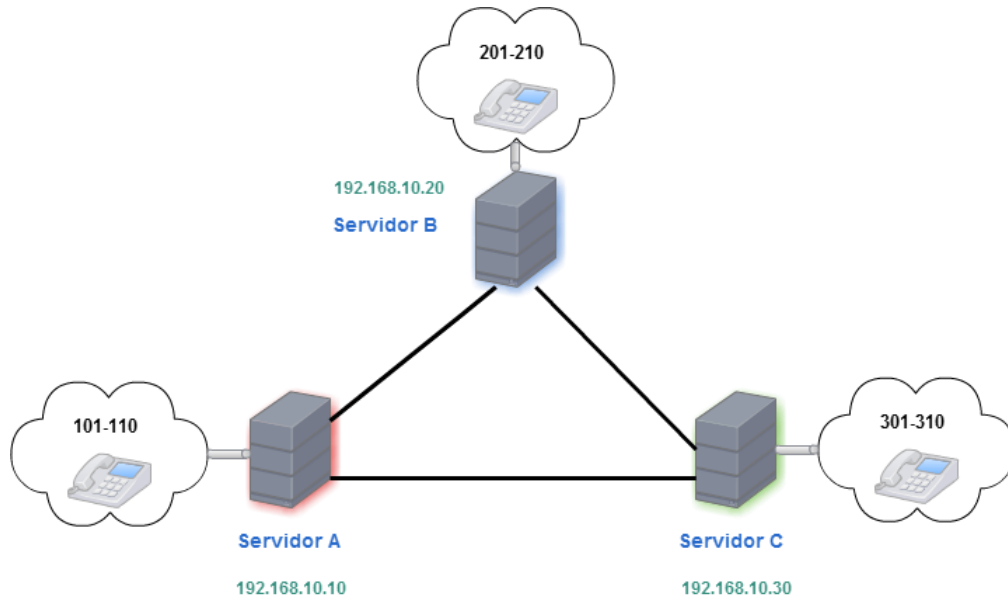


Figura III.18. Esquema Lógico del prototipo de prueba.

3.3. Determinación del Costo de Implementación

La información necesaria para elaborar las tablas de estimación de costos se obtuvieron después de realizar varias proformas en diferentes empresas. Buscando satisfacer las diferentes necesidades, considerando la funcionalidad del equipo y el precio.

Los principales elementos a considerar en la estimación de costos son:

- Compra de Equipos.
- Instalación.
- Calibración y Puesta en marcha.

Costo de Equipos y Características

Tabla III.III. Costo de Equipos.

Equipo	Descripción	Precio
1 PC	S. O : Genuine Windows ® 7 Home Premium Procesador: Intel, Dual Core G640, 2.8GHz Memoria: 8GbDDR3 SDRAM Tarjeta Grafica: Intel HD Graphics Disco Duro: 500Gb, Serial ATA, 5400 rpm DVD-RAM / ± R / ± RW. Wifi, Ethernet gigabit, webcam, micrófono. Teclado, mouse, cargador CA	\$492.78 inc IVA

Costos de Instalación

Tabla III.IV. Costo de Instalación.

Descripción	Detalles	Precio
Servidores PBX	Virtualizacion 3 PBX dentro de una misma PC. Y posterior configuración	\$300
Softphones	Se instalan y configuran 3 teléfonos por cada servidor para realizar las pruebas.	\$100
Software adicional	Se instala y configura Software de virtualizacion, mismo que es de distribución gratuita. Y se configura una red virtual dentro de este.	\$50
TOTAL		\$450.00

Costo Total del Proyecto

Tabla III.V. Costo Total.

Descripcion	Precio
Equipos	\$492,78
Instalacion	\$450,00
TOTAL	\$942,78

CAPÍTULO IV

FUNCIONAMIENTO Y PRUEBAS DEL PROTOCOLO DUNDI EN EL AMBIENTE DE PRUEBA

4.1. Planteamiento de la Hipótesis

La puesta en marcha del protocolo DUNDI sobre una red de VoIP, facilitará la propagación del plan de marcado de cada servidor, a través de la red, entre varios servidores PBX ubicados remotamente.

Para el desarrollo del análisis y demostración de la hipótesis, trabajaremos con el Método Comparativo de los datos obtenidos a través de la Experimentación y Observación a lo largo de los diferentes escenarios que se van a simular durante el proyecto.

Las variables que influyen directamente en la demostración de nuestra hipótesis son el número de servidores, el enlace físico a través del cual están conectados, el Ancho de Banda, y los servicios que correrán a través de estos enlaces. Siendo menos relevantes el número de extensiones y el total de llamadas, ya que estas variables entran en juego después que el protocolo DUNDI a realizado la comunicación y el intercambio de mensajes.

Al tener los servicios virtualizados no podemos variar el medio físico de comunicación, pero como sabemos, la mayor parte de las empresas trabajan a través de un carrier,

utilizando mayormente una conexión por cable (líneas telefónica o coaxial), seguido por enlaces de fibra óptica y en un menor porcentaje a través de enlaces inalámbricos o satelitales.

4.2. Variables de Estudio e Indicadores

Lo que nosotros sí podemos controlar es el Ancho de Banda, el cual variaremos para realizar las pruebas, para lo cual consideramos existe una división del ancho de banda con el que cuenta la organización, teniendo una porción exclusiva para el paso de datos de VoIP.

Ahora vamos a definir nuestras variables de estudio.

Tabla IV.VI. Variables e Indicadores.

Objetivo Específico	Variable	Dimensión	Indicador
Estudiar el protocolo DUNDI.	El protocolo DUNDI.	Programación. (Configuración Software)	-Tiempo necesario para configurar. -Tiempo para realizar cambios y aplicarlos.
Diseñar e implementar un prototipo de prueba.	Prototipo de prueba. (topología de red)	-Topología Física -Topología Lógica. -Hardware. -Software. -Ancho de Banda.	-Facilidad y factibilidad de implementación -Seguridad de la red. -Costo necesario
Evaluar el comportamiento del protocolo en el ambiente de prueba	Comportamiento del protocolo en el ambiente de prueba	Tiempo	-Retardo en las conexiones -Retardo en las consultas. -Tiempo necesario para realizar una llamada. -Tiempos de Uptime.
		Recursos	-Consumo de recursos(memoria Física, lógica, RAM, Disco Duro)

4.3. Estimación de una muestra

Debido a que tenemos una población infinita, pues desconocemos la cantidad de servidores que implementan DUNDI en la práctica y por ende el total de consultas que se realizan en un determinado tiempo. Vamos a tomar una muestra aleatoria de 10 datos de cada una de las pruebas a realizar, tratando de evitar que ésta sea sesgada. Para posteriormente compararlas y tomar una decisión en base a esto.

En general, resulta muy difícil comprobar si una determinada muestra es o no aleatoria, cosa que sólo puede hacerse considerando otro tipo de muestreos aleatorios robustos que permitan decir si la primera muestra era aleatoria o no.

Para nuestro estudio contamos con tres servidores, para realizar las pruebas vamos a seguir el siguiente proceso, el mismo que se repetirá un número de 10 veces para cada caso y así obtener datos que nos permitan realizar el análisis de resultados:

Paso 1: Primero vamos a variar el ancho de banda en el prototipo de prueba *Fig. III.18*. Y realizamos consultas DUNDI entre dos servidores cercanos, con y sin tráfico.

Paso 2: Posteriormente se incorporará un nuevo servidor a la red y se medirá el tiempo que toma DUNDI para propagar las extensiones de este nodo a los demás. Esto se hará:

- Sin tráfico en la red.
- Con varias llamadas simultáneas (todas las que las extensiones nos permitan).

Paso 3: Realizaremos un proceso similar al anterior, pero en este caso, vamos a simular la caída de un enlace, forzando a DUNDI a redirigir las llamadas por otra ruta, para luego comparar los tiempos de respuesta entre los dos casos.

4.4. Escenarios de prueba

4.4.1. Escenario de prueba 1

Paso 1: Iniciamos con dos servidores en marcha (A y B) de la *Fig. III.18*., sin ninguna delimitación en el ancho de banda, es decir trabajaremos con la capacidad máxima de la

tarjeta de red (10/100 Mbps), comprobamos la conexión entre los servidores. Realizamos consultas desde A hacia B a intervalos de tiempo regulares y tabulamos los datos obtenidos.

Tabla IV.VII. Tiempos de respuesta de consultas DUNDI sin tráfico. Escenario 1.

Prueba	Tiempo (ms)
1 ^o	7
2 ^o	8
3 ^o	5
4 ^o	1
5 ^o	4
6 ^o	3
7 ^o	4
8 ^o	1
9 ^o	4
10 ^o	9
Promedio	4.6 ms

Tabla IV.VIII. Tiempos de respuesta de consultas DUNDI con tráfico. Escenario 1.

Prueba	Tiempo (ms)
1 ^o	10
2 ^o	20
3 ^o	27
4 ^o	6
5 ^o	11
6 ^o	31
7 ^o	5
8 ^o	6
9 ^o	11
10 ^o	4
Promedio	13.1 ms

Paso 2. Procedemos a añadir a la red el tercer servidor (C) y medimos el tiempo que tarda el servidor A en obtener comunicación con C. En este caso sin tráfico en la red.

Tabla IV.IX. Tiempos de respuesta en re conexión sin tráfico. Escenario 1.

Prueba	Tiempo (s)
1°	13
2°	25
3°	22
4°	10
5°	17
6°	21
7°	8
8°	15
9°	18
10°	19
Promedio	16.8 s

Ahora realizaremos varias llamadas simultáneas para inyectar tráfico en la red.

Tabla IV.X. Tiempos de respuesta en re conexión con tráfico. Escenario 1.

Prueba	Tiempo (s)
1°	17
2°	18
3°	20
4°	10
5°	24
6°	23
7°	13
8°	12
9°	11
10°	24
Promedio	17.2 s

Como podemos ver los tiempos son muy variables, debido a que DUNDI realiza consultas periódicas de un servidor a otro, es decir, si al agregar el nuevo nodo coincidimos con el envío de una solicitud DUNDI el tiempo de respuesta será menor. Si al contrario añadimos el nodo justo después de que se ha dado el broadcast, el tiempo de respuesta será máximo.

Paso 3. Esta vez trabajaremos con los tres servidores, al tener redundancia existen dos vías de comunicación entre servidores continuos, una directa y otra indirecta a través de un tercer servidor. La prueba que realizaremos consiste en simular la caída de la línea de comunicación principal obligando a DUNDI a redirigir la llamada por la vía alterna.

Tabla IV.XI. Tiempos de consulta en el enlace principal. Escenario 1.

Prueba	Tiempo (ms)
1 ^o	14
2 ^o	11
3 ^o	17
4 ^o	9
5 ^o	8
6 ^o	6
7 ^o	9
8 ^o	15
9 ^o	6
10 ^o	8
Promedio	10.3 ms

Tabla IV.XII. Tiempos de consulta en el enlace secundario. Escenario 1.

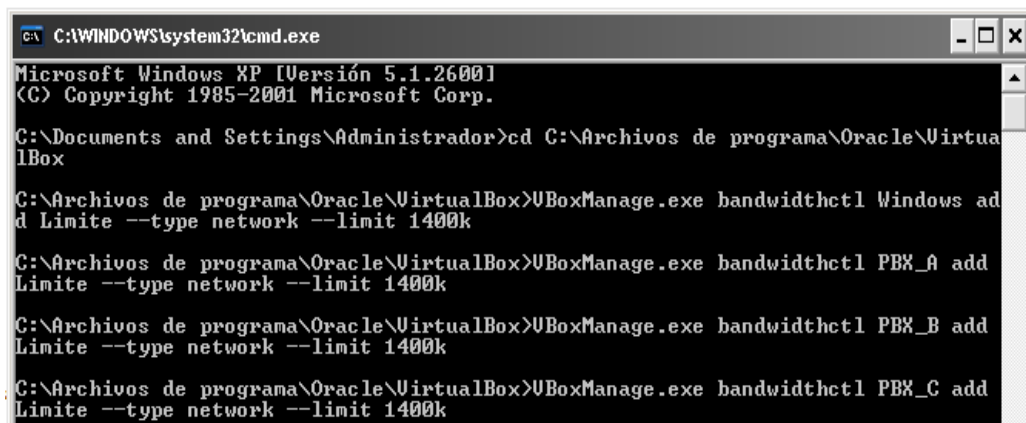
Prueba	Tiempo (ms)
1 ^o	12
2 ^o	15
3 ^o	12
4 ^o	9
5 ^o	7
6 ^o	28
7 ^o	15
8 ^o	27
9 ^o	9
10 ^o	20
Promedio	15.4 ms

De esta manera vamos a comparar el tiempo de la consulta entre un enlace principal y el secundario, con los datos de las *Tablas IV.XII* y *IV.XIII*. Dentro de las dos líneas de comunicación tenemos tráfico de voz.

La diferencia que existe en los dos casos es muy pequeña, esta diferencia se debe a que al pasar la consulta a través del enlace secundario, se suman los tiempos de procesamiento del servidor intermedio y los retardos de las líneas de comunicación. Por tanto, este tiempo es dependiente, no solo del medio que se utilice, sino también del número de servidores por el cual deba pasar la información para lograr comunicar al punto inicial con el destino.

4.4.2. Escenario de prueba 2

Paso 1: Esta vez iniciamos con la delimitación del tráfico. Simulamos un canal de 10Mbps entre cada nodo. Además, como se explico en el capítulo anterior, también asumimos que existe una división del canal y hay un ancho de banda dedicado solo para el tráfico de VoIP, el cual es del 14% del total, ya que ese es el porcentaje de uso de VoIP a nivel de Latinoamérica del total de uso del Internet.¹⁸ Por lo tanto tendremos un canal de 1.4Mbps como canal dedicado y exclusivo para el tráfico de VoIP.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador>cd C:\Archivos de programa\Oracle\VirtualBox
C:\Archivos de programa\Oracle\VirtualBox>VBoxManage.exe bandwidthctl Windows add Limite --type network --limit 1400k
C:\Archivos de programa\Oracle\VirtualBox>VBoxManage.exe bandwidthctl PBX_A add Limite --type network --limit 1400k
C:\Archivos de programa\Oracle\VirtualBox>VBoxManage.exe bandwidthctl PBX_B add Limite --type network --limit 1400k
C:\Archivos de programa\Oracle\VirtualBox>VBoxManage.exe bandwidthctl PBX_C add Limite --type network --limit 1400k
```

Figura IV.19. Delimitación del ancho de banda Escenario 2.

Paso 1: Con la delimitación del ancho de banda en 1.4Mbps realizaremos las mismas pruebas que se dieron en el escenario de pruebas 1.

¹⁸ <http://www.tendenciasdigitales.com/1461/infografia-usos-de-internet-en-latinoamerica-2012/>

Tabla IV.XIII. Tiempos de respuesta de consultas DUNDI sin tráfico. Escenario 2.

Prueba	Tiempo (ms)
1°	6
2°	12
3°	5
4°	6
5°	8
6°	6
7°	5
8°	6
9°	8
10°	10
Promedio	7.2 ms

Tabla IV.XIV. Tiempos de respuesta de consultas DUNDI con tráfico. Escenario 2.

Prueba	Tiempo (ms)
1°	64
2°	33
3°	12
4°	22
5°	10
6°	12
7°	8
8°	7
9°	22
10°	21
Promedio	21.2 ms

Paso 2. Procedemos a añadir a la red el tercer servidor (C) y medimos el tiempo que tarda el servidor A en obtener comunicación con C. En este caso sin tráfico en la red.

Tabla IV.XV. Tiempos de respuesta en reconexión sin tráfico. Escenario 2.

Prueba	Tiempo (s)
<i>1°</i>	12
<i>2°</i>	10
<i>3°</i>	9
<i>4°</i>	7
<i>5°</i>	14
<i>6°</i>	6
<i>7°</i>	7
<i>8°</i>	9
<i>9°</i>	11
<i>10°</i>	7
Promedio	9.2 s

Ahora realizaremos varias llamadas simultáneas para inyectar tráfico en la red.

Tabla IV.XVI. Tiempos de respuesta en reconexión con tráfico. Escenario 2.

Prueba	Tiempo (s)
<i>1°</i>	12
<i>2°</i>	11
<i>3°</i>	18
<i>4°</i>	16
<i>5°</i>	17
<i>6°</i>	19
<i>7°</i>	15
<i>8°</i>	20
<i>9°</i>	9
<i>10°</i>	12
Promedio	14.9 s

Los tiempos con la delimitación del ancho de banda no reflejan cambios significativos, hasta ahora se mantienen dentro del rango del escenario de pruebas 1.

Paso 3. Añadimos el tercer servidor a la red, y tomamos los datos de los tiempos de consulta para compararlos entre la línea principal de comunicación y la secundaria, simulando la caída de la línea principal. De esta manera vamos a comparar el tiempo de la consulta entre un enlace principal y el secundario.

Tabla IV.XVII. Tiempos de consulta en el enlace principal. Escenario 2.

Prueba	Tiempo (ms)
1 ^o	11
2 ^o	7
3 ^o	8
4 ^o	6
5 ^o	19
6 ^o	15
7 ^o	12
8 ^o	8
9 ^o	12
10 ^o	6
Promedio	10.4 ms

Tabla IV.XVIII. Tiempos de consulta en el enlace secundario. Escenario 2.

Prueba	Tiempo (ms)
1 ^o	28
2 ^o	10
3 ^o	10
4 ^o	9
5 ^o	9
6 ^o	19
7 ^o	10
8 ^o	4
9 ^o	18
10 ^o	28
Promedio	14.5 ms

Al igual que el caso anterior, existe una pequeña diferencia entre los tiempos de consulta de la línea principal y la línea secundaria, debido a los motivos ya expuestos.

4.4.3. Escenario de prueba 3

Paso 1: Para este escenario vamos a simular un canal de 5Mbps entre cada nodo. Por tanto una vez hecha la división del ancho de banda y configurado el canal exclusivo de VoIP tendríamos un canal de 700Kbps, que es el 14% del total, por la razón que se explico en el escenario anterior.

```
C:\Archivos de programa\Oracle\VirtualBox>
C:\Archivos de programa\Oracle\VirtualBox>UBoxManage.exe bandwidthctl PBX_C set
Limite --limit 700k
C:\Archivos de programa\Oracle\VirtualBox>UBoxManage.exe bandwidthctl PBX_B set
Limite --limit 700k
C:\Archivos de programa\Oracle\VirtualBox>UBoxManage.exe bandwidthctl PBX_A set
Limite --limit 700k
C:\Archivos de programa\Oracle\VirtualBox>UBoxManage.exe bandwidthctl Windows se
t Limite --limit 700k
```

Figura IV.20. Delimitación del ancho de banda Escenario 3.

Con la delimitación del ancho de banda en 700Kbps realizaremos las mismas pruebas que se dieron en el escenario de pruebas 1.

Tabla IV.XIX. Tiempos de respuesta de consultas DUNDI sin tráfico. Escenario 3.

Prueba	Tiempo (ms)
1º	5
2º	6
3º	8
4º	24
5º	7
6º	8
7º	10
8º	5
9º	7
10º	26
Promedio	10.6 ms

Tabla IV.XX. Tiempos de respuesta de consultas DUNDI con tráfico. Escenario 3.

Prueba	Tiempo (ms)
1 ^o	19
2 ^o	21
3 ^o	4
4 ^o	23
5 ^o	13
6 ^o	11
7 ^o	15
8 ^o	17
9 ^o	23
10 ^o	9
Promedio	15.5 ms

Paso 2. Procedemos a añadir a la red el tercer servidor (C) y medimos el tiempo que tarda el servidor A en obtener comunicación con C. En este caso sin tráfico en la red.

Tabla IV.XXI. Tiempos de respuesta en re conexión sin tráfico. Escenario 3.

Prueba	Tiempo (s)
1 ^o	13
2 ^o	15
3 ^o	5
4 ^o	10
5 ^o	6
6 ^o	11
7 ^o	17
8 ^o	16
9 ^o	13
10 ^o	20
Promedio	12.6 s

Ahora realizaremos varias llamadas simultáneas para inyectar tráfico en la red y realizar las mismas pruebas.

Tabla IV.XXII. Tiempos de respuesta en reconexión con tráfico. Escenario 3.

Prueba	Tiempo (s)
<i>1º</i>	20
<i>2º</i>	15
<i>3º</i>	14
<i>4º</i>	11
<i>5º</i>	18
<i>6º</i>	6
<i>7º</i>	6
<i>8º</i>	9
<i>9º</i>	15
<i>10º</i>	17
Promedio	13.1 s

Hasta ahora el ancho de banda ha sido idóneo, mostrando cambios poco significativos entre las consultas con tráfico y aquellas con el canal libre.

Paso 3. Añadimos el tercer servidor a la red, y tomamos los datos de los tiempos de consulta para compararlos entre la línea principal de comunicación y la secundaria, simulando la caída de la línea principal.

Tabla IV.XXIII. Tiempos de consulta en el enlace principal. Escenario 3.

Prueba	Tiempo (ms)
<i>1º</i>	22
<i>2º</i>	4
<i>3º</i>	28
<i>4º</i>	24
<i>5º</i>	15
<i>6º</i>	13
<i>7º</i>	23
<i>8º</i>	7
<i>9º</i>	17
<i>10º</i>	16
Promedio	16.9 ms

Tabla IV.XXIV. Tiempos de consulta en el enlace secundario. Escenario 3.

Prueba	Tiempo (ms)
1°	18
2°	15
3°	15
4°	12
5°	14
6°	28
7°	34
8°	12
9°	14
10°	12
Promedio	17.4 ms

En relación a los escenarios anteriores, ya existe un aumento en cuanto al tiempo que toma realizar una consulta, pero la diferencia entre los datos obtenidos con flujo de tráfico en la red y aquellos con el canal libre, aún es pequeña.

4.4.4. Escenario de prueba 4

Paso 1: Este sería nuestro último escenario, trabajamos con un canal de 1Mbps entre cada nodo. Por tanto, una vez hecha la división del ancho de banda y configurado el canal exclusivo de VoIP tendríamos un canal de 140Kbps.

```
C:\Archivos de programa\Oracle\VirtualBox>
C:\Archivos de programa\Oracle\VirtualBox>UBoxManage.exe bandwidthctl Windows set
Limite --limit 140k

C:\Archivos de programa\Oracle\VirtualBox>UBoxManage.exe bandwidthctl PBX_A set
Limite --limit 140k

C:\Archivos de programa\Oracle\VirtualBox>UBoxManage.exe bandwidthctl PBX_B set
Limite --limit 140k

C:\Archivos de programa\Oracle\VirtualBox>UBoxManage.exe bandwidthctl PBX_C set
Limite --limit 140k
```

Figura IV.21. Delimitación del ancho de banda Escenario 4.

Al momento de realizar las pruebas se tiene cortes en la conexión, aún sin tráfico de VoIP. Y los tiempos de latencia son extremadamente altos, por lo cual es imposible realizar más

pruebas. Debido a esto se toma la decisión de elevar el ancho de banda a 256Kbps para realizar nuevas pruebas.

4.4.5. Escenario de prueba 5

Paso 1: Delimitamos el canal a 256Kbps para realizar nuevas pruebas.

```
C:\Archivos de programa\Oracle\VirtualBox>
C:\Archivos de programa\Oracle\VirtualBox>UBoxManage.exe bandwidthctl Windows set
Limite --limit 256k
C:\Archivos de programa\Oracle\VirtualBox>UBoxManage.exe bandwidthctl PBX_A set
Limite --limit 256k
C:\Archivos de programa\Oracle\VirtualBox>UBoxManage.exe bandwidthctl PBX_B set
Limite --limit 256k
C:\Archivos de programa\Oracle\VirtualBox>UBoxManage.exe bandwidthctl PBX_C set
Limite --limit 256k
```

Figura IV.22. Delimitación del ancho de banda Escenario 5.

Con esta nueva delimitación, el ancho de banda le permite a DUNDI realizar las consultas y se eliminan por completo los cortes, pudiendo realizar las pruebas.

Tabla IV.XXV. Tiempos de respuesta de consultas DUNDI sin tráfico. Escenario 5.

Prueba	Tiempo (ms)
1º	5
2º	19
3º	8
4º	4
5º	13
6º	8
7º	7
8º	3
9º	8
10º	5
Promedio	8 ms

En este experimento sin tráfico en la red, el tiempo de las consultas se mantiene estable en relación a los otros escenarios con las mismas características del experimento, es decir, no ha existido un cambio perceptible.

Tabla IV.XXVI. Tiempos de respuesta de consultas DUNDI con tráfico. Escenario 5.

Prueba	Tiempo (ms)
1°	137
2°	195
3°	277
4°	79
5°	203
6°	150
7°	104
8°	152
9°	120
10°	96
Promedio	151.3 ms

Aquí ya existe una notable diferencia en relación a los otros escenarios. DUNDI se encuentra trabajando al límite con esta capacidad del ancho de banda. Los tiempos de respuesta se dispararon de dos a tres dígitos.

Paso 2. Procedemos a añadir a la red el tercer servidor (C) y medimos el tiempo que tarda el servidor A en obtener comunicación con C. En este caso sin tráfico en la red.

Tabla IV.XXVII. Tiempos de respuesta en re conexión sin tráfico. Escenario 5.

Prueba	Tiempo (s)
1°	7
2°	5
3°	8
4°	6
5°	5
6°	6
7°	8
8°	11
9°	12
10°	6
Promedio	7.4 s

Tabla IV.XXVIII. Tiempos de respuesta en re conexión con tráfico. Escenario 5.

Prueba	Tiempo (s)
1°	8
2°	12
3°	6
4°	7
5°	8
6°	7
7°	8
8°	6
9°	5
10°	6
Promedio	7.3 s

El porcentaje de red usado por DUNDI es bajo, logrando trabajar incluso con un ancho de banda de 256Kbps y presencia de tráfico.

Paso 3. Añadimos el tercer servidor a la red, y comparamos los tiempos de consulta del servidor A hacia C, primero con un enlace directo, y luego a través del nodo C. Inyectando tráfico en la red en los dos casos. Con el ancho de banda del escenario.

Tabla IV.XXIX. Tiempos de consulta en el enlace principal. Escenario 5.

Prueba	Tiempo (ms)
1°	110
2°	98
3°	58
4°	89
5°	37
6°	91
7°	112
8°	90
9°	58
10°	87
Promedio	83 ms

Tabla IV.XXX. Tiempos de consulta en el enlace secundario. Escenario 5.

Prueba	Tiempo (ms)
1°	108
2°	110
3°	83
4°	147
5°	116
6°	122
7°	105
8°	277
9°	118
10°	165
Promedio	135.1 ms

En este escenario los tiempos se incrementaron considerablemente tanto con tráfico como sin él, dado lo limitado del ancho de banda. También existieron cortes en la señal, pues DUNDI cancela las solicitudes si los tiempos de respuesta son mayores a 1 segundo. El margen de tiempo entre las respuestas con tráfico y sin él, ya es mayor con un ancho de banda de 256Kbps. Existiendo problemas en momentos debido a la saturación del enlace.

4.5. Evaluación de los resultados obtenidos

Primero analizamos los datos obtenidos en el *Paso 1* de todos los escenarios y comparamos sus promedios. Estos datos muestran los retardos de tiempos de consultas DUNDI dentro de la red con tráfico y sin él, entre nodos adjuntos. Para cada escenario se ensayó un ancho de banda diferente, éstos fueron los datos obtenidos:

Tabla IV.XXXI. Tablas de comparación Paso 1 de todos los escenarios, sin tráfico.

Prueba	Escenario 1	Escenario 2	Escenario 3	Escenario 4	Escenario 5
1°	7	6	5	1028	5
2°	8	12	6	2013	19
3°	5	5	8	-	8
4°	1	6	24	-	4
5°	4	8	7	-	13
6°	3	6	8	-	8
7°	4	5	10	965	7
8°	1	6	5	-	3
9°	4	8	7	-	8
10°	9	10	26	365	5
Promedios	4.6 ms	7.2 ms	10.6 ms	-	8 ms

Existe un ligero retardo en los tiempos de respuesta de las consultas DUNDI conforme disminuía el ancho de banda. Los tiempos son mucho menores solo en el caso de tener banda abierta, es decir; trabajar con la capacidad máxima de la tarjeta de red. Una vez que se delimitó el ancho de banda, los tiempos se estabilizaron en un rango de 10ms con una variación promedio de ± 2 ms. El único caso que presento cambios radicales, fue al momento de trabajar con un ancho de banda de 140Kbps, aquí se presentaron problemas de comunicación, grandes retardos de tiempo y cortes en la conexión.

Tabla IV.XXXII. Tablas de comparación Paso 1 de todos los escenarios, con tráfico.

Prueba	Escenario 1	Escenario 2	Escenario 3	Escenario 4	Escenario 5
1°	1° 10	64	19	-	137
2°	2° 20	33	21	-	195
3°	3° 27	12	4	-	277
4°	4° 6	22	23	-	79
5°	5° 11	10	13	-	203
6°	6° 31	12	11	-	150
7°	7° 5	8	15	-	104
8°	8° 6	7	17	-	152
9°	9° 11	22	23	-	120
10°	10° 4	21	9	-	96
Promedio	13.1 ms	21.2 ms	15.5 ms	-	151.3 ms

Con un ancho de banda moderado y presencia de tráfico en la red, los tiempos de las consultas son estables. Una vez que reducimos el ancho de banda a 256Kbps, los tiempos de retardo para las consultas se dispararon, pasando los datos de números de dos a tres dígitos, existiendo una clara diferencia con el caso en el que no existía presencia de tráfico en la red. Para el escenario de 140Kbps, las consultas se pierden totalmente, debido a que sus tiempos de respuesta son muy altos y DUNDI automáticamente cancela todas las solicitudes cuya respuesta tarda más de 1000ms.

Con estos datos podemos concluir que los paquetes enviados por DUNDI para realizar el intercambio de información, tienen un consumo de ancho de banda bastante moderado pudiendo trabajar con comodidad con un ancho de banda igual o superior a los 256Kbps con tráfico de voz corriendo por la red, sin presentar problemas o cortes en la comunicación.

Continuando cronológicamente con el análisis de los datos, pasamos a la comparación de los datos obtenidos en el *Paso 2* de los 5 escenarios de prueba. Datos que reflejan el tiempo que tarda DUNDI en reconocer e ingresar un nuevo nodo a la red.

Tabla IV.XXXIII. Tablas de comparación Paso 2 de todos los escenarios, sin tráfico.

<i>Prueba</i>	<i>Escenario 1</i>	<i>Escenario 2</i>	<i>Escenario 3</i>	<i>Escenario 4</i>	<i>Escenario 5</i>
<i>1°</i>	<i>1°</i> 13	12	13	-	7
<i>2°</i>	<i>2°</i> 25	10	15	-	5
<i>3°</i>	<i>3°</i> 22	9	5	-	8
<i>4°</i>	<i>4°</i> 10	7	10	-	6
<i>5°</i>	<i>5°</i> 17	14	6	-	5
<i>6°</i>	<i>6°</i> 21	6	11	-	6
<i>7°</i>	<i>7°</i> 8	7	17	-	8
<i>8°</i>	<i>8°</i> 15	9	16	-	11
<i>9°</i>	<i>9°</i> 18	11	13	-	12
<i>10°</i>	<i>10°</i> 19	7	20	-	6
Promedio	16.8 s	9.2 s	12.6 s	-	7.4 s

En este experimento obtenemos promedios muy variables, los cuales no dependen directamente del ancho de banda de los enlaces entre nodos. A excepción del escenario 4, donde el ancho de banda fue demasiado limitado para que DUNDI pueda trabajar, existiendo cortes y pérdida de comunicación.

Como ya se dijo, este dato más bien es dependiente del periodo entre consultas DUNDI, por que, cada cierto tiempo el protocolo genera mensajes de registro para verificar la presencia de cambios en la red, entonces; si el momento de agregar el nuevo nodo a la red coincide con una consulta DUNDI, el tiempo de registro del nuevo servidor y en consecuencia la respuesta del mismo, darán como resultado un menor tiempo. Si al contrario el servidor es agregado exactamente después de un broadcast DUNDI, el tiempo de respuesta será máximo.

Tabla IV.XXXIV. Tablas de comparación Paso 2 de todos los escenarios, con tráfico.

<i>Prueba</i>	<i>Escenario 1</i>	<i>Escenario 2</i>	<i>Escenario 3</i>	<i>Escenario 4</i>	<i>Escenario 5</i>
<i>1°</i>	<i>1°</i> 17	12	20	-	8
<i>2°</i>	<i>2°</i> 18	11	15	-	12
<i>3°</i>	<i>3°</i> 20	18	14	-	6
<i>4°</i>	<i>4°</i> 10	16	11	-	7
<i>5°</i>	<i>5°</i> 24	17	18	-	8
<i>6°</i>	<i>6°</i> 23	19	6	-	7
<i>7°</i>	<i>7°</i> 13	15	6	-	8
<i>8°</i>	<i>8°</i> 12	20	9	-	6
<i>9°</i>	<i>9°</i> 11	9	15	-	5
<i>10°</i>	<i>10°</i> 24	12	17	-	6
Promedio	17.2 s	14.9 s	13.1 s	-	7.3 s

En este caso también se nota la variabilidad de los resultados, debido a las razones expuestas en la tabla anterior. Así mismo podemos ver que el tiempo de respuesta entre la red con tráfico y sin él, dentro de los mismos escenarios tiene poca variación, y una vez delimitado el ancho de banda, no se presentan problemas en las consultas.

En conclusión, el protocolo nos entrega una red totalmente escalable, donde la facilidad de

programación y rapidez de integración en la red son sus principales ventajas; que a su vez, ofrece una muy buena respuesta ante fallas, siendo los tiempos de respuesta mínimos.

Analizamos ahora los datos obtenidos en el **Paso 3**, el cual consiste en una comparación del tiempo que toma una consulta DUNDI, entre dos nodos conectados directamente y con un nodo de por medio para realizar la consulta.

Tabla IV.XXXV. Tablas de comparación Paso 3 de todos los escenarios, enlace directo.

Prueba	Escenario 1	Escenario 2	Escenario 3	Escenario 4	Escenario 5
1°	14	11	22	-	110
2°	11	7	4	-	98
3°	17	8	28	-	58
4°	9	6	24	-	89
5°	8	19	15	-	37
6°	6	15	13	-	91
7°	9	12	23	-	112
8°	15	8	7	-	90
9°	6	12	17	-	58
10°	8	6	16	-	87
Promedio	10.3 ms	10.4 ms	16.9 ms	-	83 ms

En esta tabla tenemos una respuesta estable entre el escenario 1 y 2, donde los anchos de banda eran bastante grandes, siendo las diferencias de tiempo mínimas. Pero una vez que se delimita el ancho de banda por debajo de 1Mbps, ya se nota un aumento en el retardo de las consultas, aunque no significativo, si muestra que al protocolo le costó algo más de tiempo realizar su trabajo dentro de la red con tráfico. Sin perder comunicación en ningún momento.

Tabla IV.XXXVI. Tablas de comparación Paso 3 de todos los escenarios, con nodo intermedio.

<i>Prueba</i>	<i>Escenario 1</i>	<i>Escenario 2</i>	<i>Escenario 3</i>	<i>Escenario 4</i>	<i>Escenario 5</i>
<i>1°</i>	<i>1°</i> 12	28	18	-	108
<i>2°</i>	<i>2°</i> 15	10	15	-	110
<i>3°</i>	<i>3°</i> 12	10	15	-	83
<i>4°</i>	<i>4°</i> 9	9	12	-	147
<i>5°</i>	<i>5°</i> 7	9	14	-	116
<i>6°</i>	<i>6°</i> 28	19	28	-	122
<i>7°</i>	<i>7°</i> 15	10	34	-	105
<i>8°</i>	<i>8°</i> 27	4	12	-	277
<i>9°</i>	<i>9°</i> 9	18	14	-	118
<i>10°</i>	<i>10°</i> 20	28	12	-	165
Promedio	15.4 ms	14.5 ms	17.4 ms	-	135.1 ms

En relación al envío de consultas de manera directa el incremento de tiempo es pequeño, y es explicable, debido a que al pasar una consulta por un nodo extra en este caso, al tiempo de retardo en la red, se suma el tiempo de procesamiento del servidor que enrutó la petición hacia el destino. Tiempo que será proporcional al número de nodos por los cuales deba pasar esta consulta, lo que quiere decir que, a más nodos, mayor el tiempo de retardo.

Este tiempo se mantuvo uniforme, dentro del mismo rango, hasta que el ancho de banda se redujo a 256Kbps, donde al protocolo le costó realizar sus consultas y transacciones a través de la red saturada de tráfico, pero sin perder en ningún momento el hilo de la comunicación.

Por tanto el protocolo puede trabajar de manera óptima con un ancho de banda igual o mayor a 256Kbps, siendo recomendable contar con por lo menos 500Kbps y un canal dedicado solo para el tráfico de voz, en aquellos casos que el servicio de VoIP dentro de la red sea preferencial y muy importante para el desarrollo de los labores de la empresa.

4.6. Demostración de la hipótesis.

Vamos a normalizar nuestro estudio estadísticos mediante una distribución muestral, en

este caso Distribución de Probabilidad Normal, con la cual es posible determinar parámetros de una población a través de sus valores estadísticos. Normalmente, no se indica un valor único para el parámetro desconocido, sino un rango de valores denominado, intervalo de confianza. Dado que tenemos una muestra pequeña en relación a la población que puede existir y es aquella que más se aproxima a fenómenos reales. Trabajaremos con un nivel de confianza del 99%, con los datos de la Tabla IV.XXX

Iniciamos calculando los valores necesarios. Como son **Media Aritmética**

$$X = \frac{1}{N} \sum_{i=1}^{18} X_i$$

$$X = \frac{1}{10} (1351)$$

$$X = 135,1$$

Ahora calculamos la **Desviación Estándar**

$$\sigma = \sqrt{\frac{1}{N-1} \sum_{i=1}^N (x_i - \bar{x})^2}$$

$$\sigma = \sqrt{\frac{1}{9} \sum_{i=1}^{10} (x_i - 135.1)^2}$$

$$\sigma = 54,7569377$$

Estas serían, la *media aritmética* (X) y la *desviación estándar* (σ) de la muestra extraída de toda la población. Las cuales podemos decir que son buenos *estimadores puntuales* de la *media aritmética poblacional* (μ) y de la *desviación estándar poblacional* (s).

Primero vamos a plantear nuestra hipótesis (H) en términos numéricos, y a la par planteamos una Hipótesis nula (H_0). Nuestra regla de decisión será “*Los tiempos de respuesta DUNDI entre servidores no ubicados continuamente deben ser menores a 100ms*”. Este es uno de los valores más altos que se presentaron en las pruebas, además DUNDI cancela toda consulta si no recibe una respuesta antes de los 1000ms y 100ms es apenas 1/10 del tiempo máximo permitido, esta aseveración sería suficiente para demostrar nuestra hipótesis.

¿Qué probable es esto, con un nivel de confianza del 99%?

$$H = 0ms > X \leq 100ms$$

$$H_0 = X > 100ms$$

Los grados de libertad que tendremos serán iguales a $n-1$ en este caso sería 9. Y si trabajamos con un nivel de confianza del 99% donde $\alpha = 0.01$ Pues el contraste es unilateral (de una cola), ya que no pueden existir tiempos menores a 0.

$$Z = \frac{\bar{X} - \mu}{\frac{\sigma}{\sqrt{n}}}$$

$$Z = \frac{135.1 - 100}{\frac{54.7569}{\sqrt{9}}}$$

$$Z = 1.92304531$$

Ahora vamos a buscar el valor de Z para un nivel de confianza del 99%.

Tabla V.XVI. Tabla Normalizada (Z).

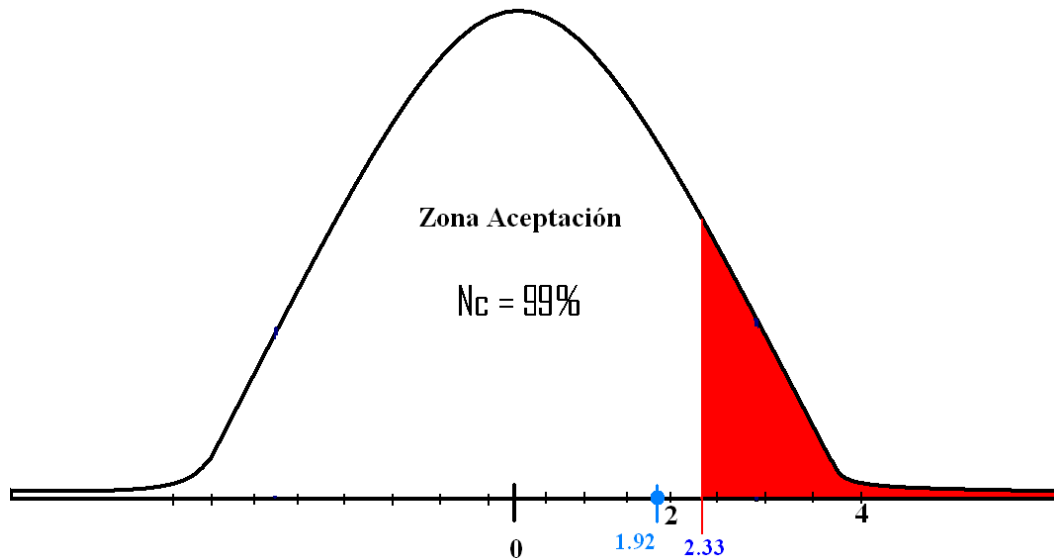
Z	0,00	0,01	0,02	0,03	0,04	0,05	0,06
0,0	0,5000	0,5040	0,5080	0,5120	0,5160	0,5199	0,5239
0,1	0,5398	0,5438	0,5478	0,5517	0,5557	0,5596	0,5636
0,2	0,5793	0,5832	0,5871	0,5910	0,5948	0,5987	0,6026
0,3	0,6179	0,6217	0,6255	0,6293	0,6331	0,6368	0,6406
0,4	0,6554	0,6591	0,6628	0,6664	0,6700	0,6736	0,6772
0,5	0,6915	0,6950	0,6985	0,7019	0,7054	0,7088	0,7123
0,6	0,7257	0,7291	0,7324	0,7357	0,7389	0,7422	0,7454
0,7	0,7580	0,7611	0,7642	0,7673	0,7704	0,7734	0,7764
0,8	0,7881	0,7910	0,7939	0,7967	0,7995	0,8023	0,8051
0,9	0,8159	0,8186	0,8212	0,8238	0,8264	0,8289	0,8315
1,0	0,8416	0,8438	0,8461	0,8485	0,8508	0,8531	0,8554
1,1	0,8643	0,8665	0,8686	0,8708	0,8729	0,8749	0,8770
1,2	0,8849	0,8869	0,8888	0,8907	0,8925	0,8944	0,8962
1,3	0,9032	0,9049	0,9066	0,9082	0,9099	0,9115	0,9131
1,4	0,9192	0,9207	0,9222	0,9236	0,9251	0,9265	0,9279
1,5	0,9332	0,9345	0,9357	0,9370	0,9382	0,9394	0,9406
1,6	0,9452	0,9463	0,9474	0,9484	0,9495	0,9505	0,9515
1,7	0,9554	0,9564	0,9573	0,9582	0,9591	0,9599	0,9608
1,8	0,9641	0,9649	0,9656	0,9664	0,9671	0,9678	0,9686
1,9	0,9713	0,9719	0,9726	0,9732	0,9738	0,9744	0,9750
2,0	0,97725	0,97778	0,97831	0,97882	0,97932	0,97982	0,98030
2,1	0,98214	0,98257	0,98300	0,98341	0,98382	0,98422	0,98461
2,2	0,98610	0,98645	0,98679	0,98713	0,98745	0,98778	0,98809
2,3	0,98928	0,98956	0,98983	0,99010	0,99036	0,99061	0,99086
2,4	0,99180	0,99202	0,99224	0,99245	0,99266	0,99286	0,99305

$$Z_{0,99} = 2.33$$

Ahora ubicamos los datos obtenidos dentro del gráfico de decisión.

Como podemos ver en el gráfico (*Fig V.26*), a través de los cálculos demostramos que los tiempos de consulta obtenidos son mucho menores al tiempo máximo permitido por DUNDI (1000ms), esto en las pruebas realizadas con un ancho de banda de 256Kbps, donde los tiempos resultantes fueron mayores a los obtenidos en el resto de escenarios con anchos de banda superiores, por lo cual esta afirmación también se comprueba para anchos de banda mayores a 256Kbps.

Figura V.23. Curva de Probabilidad



4.7. Disponibilidad de la red

Otro factor muy importante a tomar en cuenta sería la disponibilidad y tiempo de funcionamiento de nuestras centrales. Variable que se denotará al momento de tener una caída en el servidor o fallas no planificadas como cortes de energía eléctrica, daños a nivel de Hardware o un mal funcionamiento del Software. Es aquí donde aparece el concepto de “disponibilidad”, la cual se expresa con mayor frecuencia a través del índice de disponibilidad (un porcentaje) que se mide dividiendo el tiempo durante el cual el servicio está disponible por el tiempo total. Según José Ángel de Bustos Pérez nos dice que la disponibilidad se clasifica de acuerdo a la regla de los 9’s¹⁹. Ésta regla está detallada en la *Tabla IV.XXXVII*.

¹⁹<http://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-curso-salamanca-clustering/html/clustering-ha.html>

Tabla IV.XXXVII. Tabla porcentaje de disponibilidad.

DISPONIBILIDAD	
Servicio Up-Time	Tiempo de caída
0 %	24 horas
99 %	14.4 minutos
99.9 %	86.4 segundos
99.999 %	0.864 segundos
99.9999 %	0.0864 segundos

Tenemos un tiempo de operación total de 72800s, donde el tiempo en el que se mantuvo operativa la red fue de 72452s. Aplicando la relación que se describe en el párrafo anterior nuestra disponibilidad sería del 99.5219%.

Tabla IV.XXXVIII. Tiempos de disponibilidad de la red.

Tiempo hasta un corte	Uptime	Disponibilidad
15009 s	14979 s	99,80012%
18903 s	18660 s	98,71449%
11402 s	11373 s	99,74566%
8401 s	8359 s	99,50006%
19085 s	19081 s	99,97904%
72800	72452	99,52198%

4.8. Seguridad de la red

DUNDI utiliza el algoritmo de cifrado RSA y AES que es un sistema criptográfico en el que cada usuario posee dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada. RSA será seguro mientras no se conozcan formas rápidas de descomponer un número grande en producto de primos.

De esta manera se asegura un intercambio de mensajes DUNDI de manera confiable, pudiendo evitar problemas como clonación de identidades o nodos duplicados como medidas de ataque a nuestra red. Esto no implica que la red este totalmente segura, ya que DUNDI solo es el protocolo para comunicar los servidores, pero las llamadas se realizan a través de otros protocolos, por lo tanto la seguridad en la red, dependerá enteramente de su propietario, la persona que diseñe y la ponga en marcha y en mayor proporción de la necesidad de la empresa de dar seguridad al tráfico de voz dentro de su infraestructura y como es obvio, de la relación costo-beneficio.

4.9. Consumo de recursos

Gracias a Elastix y a su tablero de control podemos monitorear parámetros como los recursos del sistema. En la siguiente imagen se ven plasmados recursos del servidor como son CPU, RAM y SWAP o memoria virtual; y el porcentaje de consumo de dichos recursos con el protocolo DUNDI ya aplicado y corriendo.

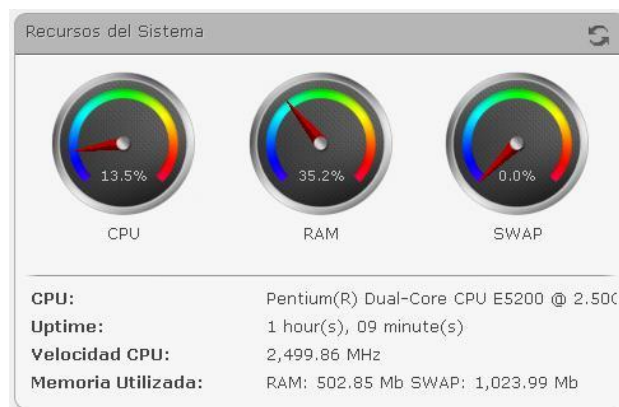


Figura IV.24. Recursos del Sistema consumidos.

Al hablar del disco duro, la capacidad necesaria para trabajar con Asterisk y el protocolo DUNDI es mínima, esta es otra de las múltiples ventajas de usar esta herramienta.

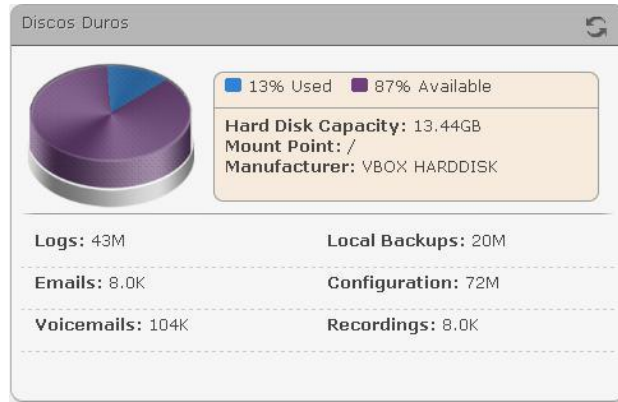


Figura IV.25. Consumo total del disco duro de la central telefónica.

Ahora veamos un gráfico que muestra el comportamiento de los Softphones frente al consumo de recursos que provocan en el sistema.

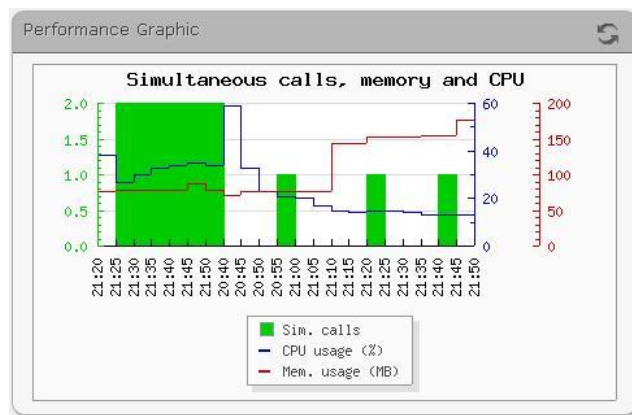


Figura IV.26. Consumo de recursos en llamadas simultaneas.

Al analizar la *Figura IV.25*. podemos ver el impacto causado por el sistema al momento de realizar llamadas simultáneas desde o hacia un mismo dominio. Aquí tenemos varias llamadas entrantes y salientes, como resultado obtenemos un uso del CPU que en su punto máximo llego a ser del 60%, mientras que la memoria usada tuvo un pico de 180MB. Demostrando así que el consumo de recursos es mínimo.

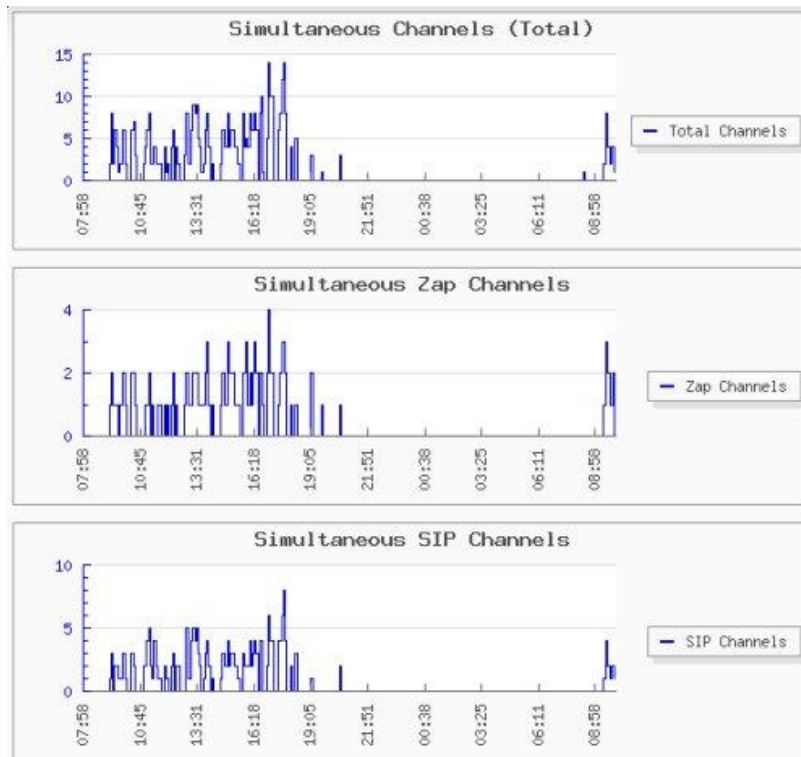


Figura IV.27. Uso de los canales mostrados cronológicamente.

En base a las *Figuras IV.24., IV.25., y IV.26.* es fácil percibir que el consumo que provoca DUNDI en todos los entes relacionados a la red es mínimo, aún siendo las características de la máquina de prueba bastantes sencillas. Pudiendo mejorarse el desempeño del protocolo y de sus servicios, aumentando la capacidad de los equipos con los que se trabaje, ya sea aumentando la capacidad de procesamiento, o el nivel de memoria RAM, y de esta manera disminuir los tiempos de respuesta que entrega el protocolo y aumentar así su eficiencia. Reduciendo también los costos de la implementación y manteniendo un buen desempeño.

Otra manera de mejorar el funcionamiento del protocolo es usarlo dentro de una máquina real y no virtualizada, en el caso de que la VoIP tenga un impacto fuerte en la empresa y sea necesario darle la importancia y se cuente con los recursos para ello.

CONCLUSIONES

- DUNDI nos brinda mejores resultados dentro de una red convergente, en la que exista redundancia, teniendo como principal problema para esto el costo de implementación. Donde el número de servidores, el tipo de enlace físico y el ancho de banda utilizado para los enlaces, son las principales variables que afectan su funcionamiento. Se demostró que el protocolo puede trabajar sin ningún problema con enlaces iguales o mayores a 512Mbps. Y logrando trabajar al límite de su capacidad, en un enlace de 256Kbps sin presentar problemas mayores. Ya que el consumo de ancho de banda de los paquetes DUNDI no tiene mayores impactos en la red. Existiendo problemas únicamente si el ancho de banda es menor, es entonces cuando se producen cortes en la red y pérdida de comunicación.
- Al ser DUNDI un sistema no centralizado, es decir que, la información que cada uno de los equipos aprende la comparte con el resto, mejora su respuesta ante fallas de un equipo, entregándonos un porcentaje de disponibilidad de 99,52198%. Siendo poco probable que el sistema colapse.
- El nivel de consumo de recursos con el protocolo puesto en marcha es de: 13.5% CPU (Dual-Core 2.5GHz), 32.5% RAM (3.23Gb), y apenas el 13% de Disco Duro (14Gb), del total de Recursos Disponibles de la máquina de prueba.
- El tiempo que toma agregar un nuevo punto a la red es menor a 1/3 del necesario que al aplicar otro protocolo (con tres servidores), relación que disminuye conforme aumenta el número de servidores configurados. Siendo la red totalmente escalable. Dado que el tiempo de configuración es mínimo, resulta necesario solamente duplicar cualquiera de los servidores ya instalados y realizar ligeros cambios dentro de la estructura de los archivos relacionados con DUNDI. Además los resultados demuestran que al incluir un nuevo nodo previamente configurado, en la red, el tiempo que le toma reconocerlo tienen un promedio de 10s.

RECOMENDACIONES

- Es recomendable tener un modelo de red redundante, para asegurar la disponibilidad de la red. Y tener un mínimo tiempo de respuesta ante fallas. Esto dependerá de la importancia que tenga la VoIP dentro de la empresa en la que se lo aplique, dado el costo de implementación de este tipo de redes, donde se debe contar con al menos un enlace principal y un enlace secundario para evitar la caída del servicio.
- Es muy importante el diseño de la red, debemos priorizar el orden y la identidad única de cada punto, ya sea este un servidor o un Softphone, es decir; no existan IPs repetidas y/o extensiones configuradas bajo el mismo alias en diferentes servidores.
- En cuanto al ancho de banda se recomienda tener una división de tráfico y configurar un canal exclusivo para el paso de VoIP dentro de las líneas de comunicación, este ancho de banda deber ser por lo menos del 14% del total disponible, y no debe ser mínimo a 256Mbps para tener un correcto funcionamiento. Es aconsejable contar con un enlace de 512Mbps dedicados para que el desempeño sea totalmente idóneo. Siempre y cuando la empresa así lo requiera, y cuente con los recursos necesarios para lograr estas metas.
- Es importante seleccionar el códec adecuado para el sistema de telefonía IP, con el fin de garantizar una calidad de voz a un ancho de banda adecuado y poder estimar el tráfico cursado en el canal de comunicación. Pues se comprobó que el ancho de banda usado por DUNDI es mínimo, el análisis de consumo de ancho de banda se debe redirigir hacia los demás protocolos involucrados en VoIP para lograr un desempeño aún mejor.
- Se debe tener muy en cuenta datos de configuración como son el tiempo de cache, en caso de que la red gestionada sea robusta por ejemplo, es necesario que este tiempo sea lo suficientemente alto para que cada servidor guarde la información por un tiempo pertinente, logrando evitar broadcast de actualización de la información

innecesarios, los mismos que crearan tráfico en la red, y la saturaran. Otro dato muy importante es el TTL, el cual debe ser igual o menor al número de saltos existentes entre los dos nodos más distantes en la red. Para evitar bucles que inunden la red y creen problemas.

- Existen diversos enfoques en la evaluación de los sistemas de telefonía IP, por lo cual se recomienda un adecuado análisis de los recursos a utilizar dentro de los sistemas, los cuales nos garantizarán un mejor desempeño y una adecuada robustez en el trabajo realizado por nuestro protocolo DUNDI.
- La importancia que han tomado los sistemas de telecomunicaciones a nivel empresarial, obliga a la implantación de tecnologías que reduzcan costos de implementación y mantenimiento por lo que la utilización de sistemas de telefonía IP basados en software de código abierto es una buena opción para la pequeña y mediana industria (PYME's) frente a sistemas de telefonía tradicional.

RESUMEN

En la ciudad de Riobamba, en el domicilio del autor, se monta una red de prueba para realizar el análisis del protocolo DUNDI en sistemas distribuidos de redes de VoIP.

Con el objetivo de determinar cuánto puede facilitar este protocolo el proceso de propagación de los planes de marcado de cada servidor a otros servidores ubicados remotamente a través de la red, reduciendo tiempo y recursos necesarios.

Para lo cual se utilizara un método científico deductivo basado en la observación del funcionamiento de este protocolo.

Se configuran tres servidores dentro de una misma red física, creando interfaces lógicas solo entre dos pares de ellos. Estas interfaces tienen el nombre de par DUNDI. Creamos un plan de marcado distinto en cada servidor, luego configuramos y registramos varios softphones en cada uno. Y finalmente se configuran los archivos necesarios para poner en marcha el protocolo DUNDI.

Como resultado tenemos un nivel de disponibilidad del 99,52198%, pues al ser un sistema no centralizado, mejora su respuesta ante fallas de un equipo y es poco probable que el sistema colapse, con una probabilidad de 0.47802% de que suceda.

Se concluye que DUNDI brinda cierto nivel de inteligencia para seleccionar entre todas las rutas conocidas la mejor, o la que menor peso tenga; tiene una buena respuesta ante fallas, y el consumo de recursos es mínimo, pudiendo catalogar el protocolo como eficiente.

Es recomendable tener una red redundante, para disminuir los puntos de fallo. Un control periódico de los recursos del sistema y actualizaciones tanto de Software como de Hardware para tener la red operativa.

SUMMARY

In Riobamba city, in the author's home address, install a prove network to do the analysis of DUNDI protocol into the distributed system on VoIP networks.

With the objectives to determinate how can facilitate this protocol, the propagation of the dial plans each server to the other servers through network, reducing time and required resources.

For that realize the observation and data collection, like response times, delay times, efficiency in the network, and responsiveness to failures. Three servers are configured within the same physical network, creating logical interfaces only between two pairs of them. These interfaces have the name of pair DUNDI. Create a different dial plan in each server, then configure and registered three softphones in each one, being able to broaden this up 100. Finally configure the files of DUNDI protocol.

As a result we have a level of availability of 99,52198%, as being a no centralized system, improve its response to failures of equipment and is very unlikely that the system collapse, with a 0.47802% probability happens.

It is conclude that DUNDI gives a certain level of intelligence to select between all the known routes the best, or witch has the lower weight; it has a good response to failures, and the minimum resource consumption, cataloging as efficient protocol.

It is recommended to have a redundant network, to decrease the points of failure. A recurring control of the resources of the system and update both software and hardware to keep the network operational.

GLOSARIO

Dialplan

Un plan de marcado establece el número esperado y el patrón de dígitos de un número de teléfono. Esto incluye los códigos de país, códigos de acceso, códigos de área y todas las combinaciones de dígitos marcados.

Canal

Vía o medio utilizado para comunicar un mensaje.

CentOS

Es una distribución libre y disponible de Linux que se basa en Linux Red Hat Enterprise Linux RHEL.

Clustering

Es la facultad que tienen varias máquinas para realizar una tarea como si se tratase de una sola máquina, siendo esto transparente para las máquinas clientes.

DHCP (Dynamic Host Configuration Protocol)

Protocolo utilizado para la configuración dinámica y está encargado de asignar, de forma automática, direcciones IP a los hosts de una red de computadoras.

DNS (Domain Name Server)

Servidor de Nombres de Dominio, se encarga de convertir nombres de dominio en direcciones IP.

Ethernet

Es un estándar de transmisión de datos para redes de área local para computadoras, que define el acceso al medio.

Gateway

Es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

GPL (General Public License)

Licencia Pública General, fue creada por la Free Software Foundation para proteger la libre

distribución, modificación y uso de Software Libre.

HTTP (HyperText Transfer Protocol)

Protocolo de Transferencia de Hipertexto, es el protocolo estándar para la transmisión de páginas Web.

IP (Dirección)

Número que identifica de manera lógica a un computador dentro de una red de computadoras, que utiliza el protocolo IP.

LAN (Local Area Network)

Red de Área Local, es una red de computadoras de tamaño medio, disperso dentro de un edificio o hasta dentro de una ciudad.

Linux

Es un Sistema operativo, también conocido como GNU/Linux, basado en UNIX, distribuido bajo la licencia GPL, siendo este Software Libre.

MAC (Media Access Control)

Dirección de Control de Acceso al Medio, es un identificador de 48 bits que identifica, de manera única, a una tarjeta de red.

Macro

Es una serie de instrucciones que se almacenan para que se puedan ejecutar de forma secuencial mediante una sola llamada u orden de ejecución.

MySQL

Sistema Gestor de Bases de Datos.

Switch

Es un dispositivo de interconexión de redes de computadoras, que interconecta dos o más segmentos de red.

Open Source

Código abierto (en inglés open source) es el término con el que se conoce al software distribuido y desarrollado libremente. El código abierto tiene un punto de vista más orientado a los beneficios prácticos de compartir el código que a las cuestiones morales y/o filosóficas las cuales destacan en el llamado software libre.

PBX

Un PBX es cualquier central telefónica conectada directamente a la red pública de teléfono por medio de líneas troncales para gestionar, además de las llamadas internas, las entrantes y/o salientes con autonomía sobre cualquier otra central telefónica.

Softphone

Un Softphone (en inglés combinación de Software y de Telephone) es un software que hace una simulación de teléfono convencional por computadora.

Telefonía

Sistema telefónico en el que la conexión entre el aparato portátil y la central se realiza mediante ondas hercianas.

Troncal

En lenguaje técnico de telefonía, una línea troncal es un enlace que interconecta las llamadas externas de una central telefónica, concentrando y unificando varias comunicaciones simultáneas en una sola señal para un transporte y transmisión a distancia más eficiente (generalmente digital) y poder establecer comunicaciones con otra central o una red entera de ellas.

UNIX

Sistema operativo portable, multitarea y multiusuario.

URL (Uniform Resource Locator)

Localizador Uniforme de Recursos, es una secuencia de caracteres que se usa para nombrar recursos de Internet para su localización, de acuerdo a un formato estándar para los diversos protocolos utilizados en Internet como HTTP, FTP, etc.

ANEXOS

ANEXO 1

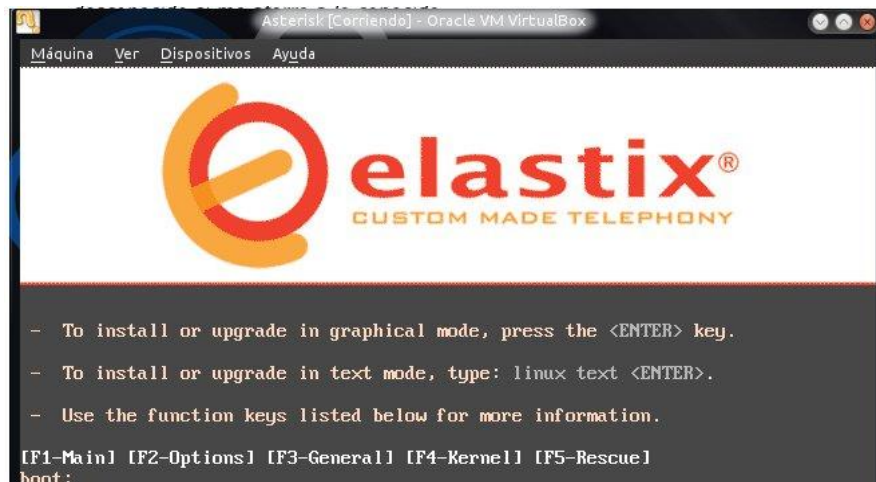
INSTALACIÓN Y CONFIGURACIÓN DE ELASTIX

4.9.1. Instalando Elastix

Descargamos la versión más reciente de esta aplicación desde su página oficial <http://elastix.org/index.php/es/descargas/distro-principal.html>



Elegimos el archivo de instalación acorde a las características de nuestro sistema; es decir: plataforma, lenguaje, sistema operativo, etc. Iniciamos la instalación.



Iniciamos con configuraciones básicas como: elección el idioma para el proceso de instalación, idioma del teclado, etc.



Siguiente paso es crear las particiones del disco, aquí se nos dan varias alternativas, se elige la configuración por defecto del SO.



Configuramos la IP del sistema, esto se lo puede realizar este momento o una vez concluida la instalación de los servidores



Se asignan los nombres a cada servidor acorde a la planificación preestablecida.



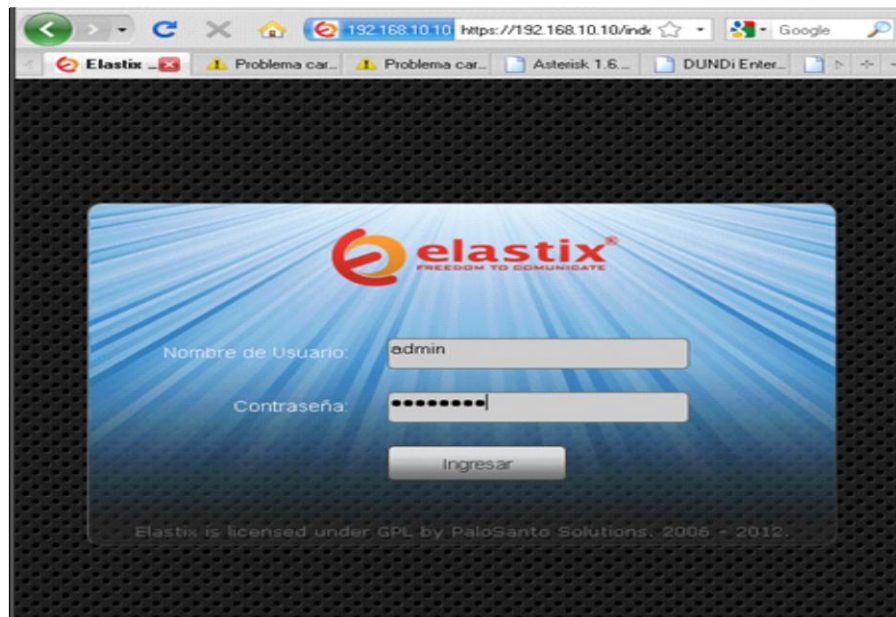
Ingresamos claves para el administrador, para el acceso y seguridad de nuestro servidor, una clave para el acceso a la base de datos, que en este caso, es una base montada bajo MySQL, y por ultimo una clave para el administrador del complemento de la central telefónica Asterisk.



Una vez configurados todos los parámetros necesarios, el proceso de instalación y copia de archivos en el disco se llevan a cabo.



Finalmente tenemos la pantalla de bienvenida, al ingresar la IP configurada desde un navegador. Aquí ingresamos con el usuario y contraseña configurados en los pasos anteriores.



ANEXO 2

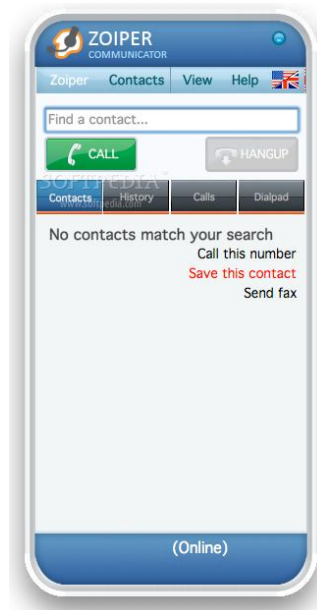
INSTALACIÓN Y CONFIGURACIÓN DE LOS SOFTHONES

Instalamos y Configuramos los Softphones

Por motivos prácticos vamos a trabajar con softphones, que es software para simulación de teléfonos convencionales por computadora, Al configurar un teléfono softphone lo que lograremos es tener una PC conectada que cumpla con las mismas funciones de un teléfono convencional, para esto es necesario instalar un software que haga las veces de teléfono. Además se necesita disponer de audífonos y micrófono. Existen varias alternativas para softphones, entre ellos podemos citar los siguientes:

- *Zoiper*: Este software nos permite trabajar con extensiones de tipo SIP e IAX, además es multiplataforma: <http://www.asteriskguru.com>
- *XtenLite*: Este software trabaja con extensiones SIP únicamente, también es multiplataforma: <http://www.xten.com/index.php?menu=download>
- *3CX Phone*: <http://www.3cx.com/VOIP/voip-phone.html>

Simplemente ahora vamos a las pagina de descarga de estos teléfonos o aquel de nuestra elección y procedemos a instalarlos.



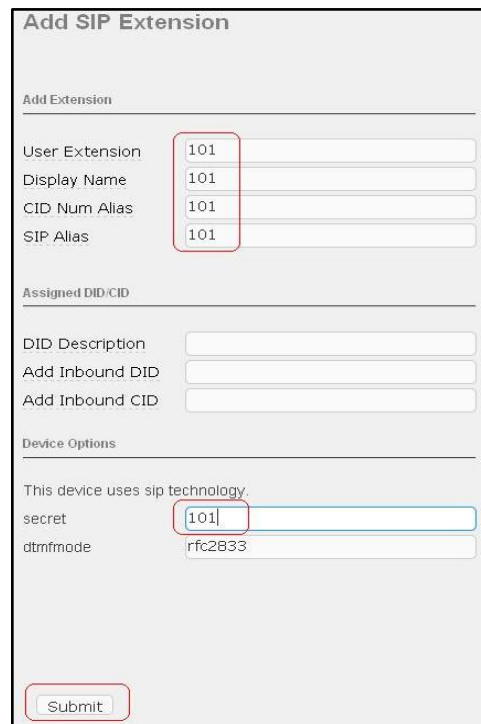
Ahora configuraremos en la central una extensión.

Ingresamos en el servidor mediante web. Luego elegimos los menús

PBX > PBX Configuration > AddanExtension



The screenshot shows the Elastix web interface. At the top, there is a navigation bar with tabs for 'Sistema', 'Agenda', 'Email', 'Fax', and 'PBX'. Below this is a secondary navigation bar with 'PBX Configuration' selected, along with other options like 'Operator Panel', 'Voicemail', 'Monitoring', 'Endpoint Configurator', and 'Conference'. The main content area is titled 'PBX Configuration' and has a sidebar menu with 'Extensioes' highlighted. The main form is titled 'Add an Extension' and contains a 'Device' dropdown menu with 'Generic SIP Device' selected. A 'Submit' button is visible below the dropdown.



The screenshot shows the 'Add SIP Extension' form. It has several sections: 'Add Extension' with fields for 'User Extension', 'Display Name', 'CID Num Alias', and 'SIP Alias', all containing the value '101'; 'Assigned DID:CID' with fields for 'DID Description', 'Add Inbound DID', and 'Add Inbound CID'; and 'Device Options' with a note 'This device uses sip technology.' and fields for 'secret' (containing '101') and 'dtmfmode' (containing 'rfc2833'). A 'Submit' button is at the bottom.

- **Extensión del Usuario:** Debe ser único. Éste es el número que se puede marcar de cualquier otra extensión. Puede ser cualquier longitud, pero convencionalmente se utiliza una extensión de tres o cuatro cifras.
- **DisplayName:** Es el nombre del Caller ID, para llamadas de este usuario serán

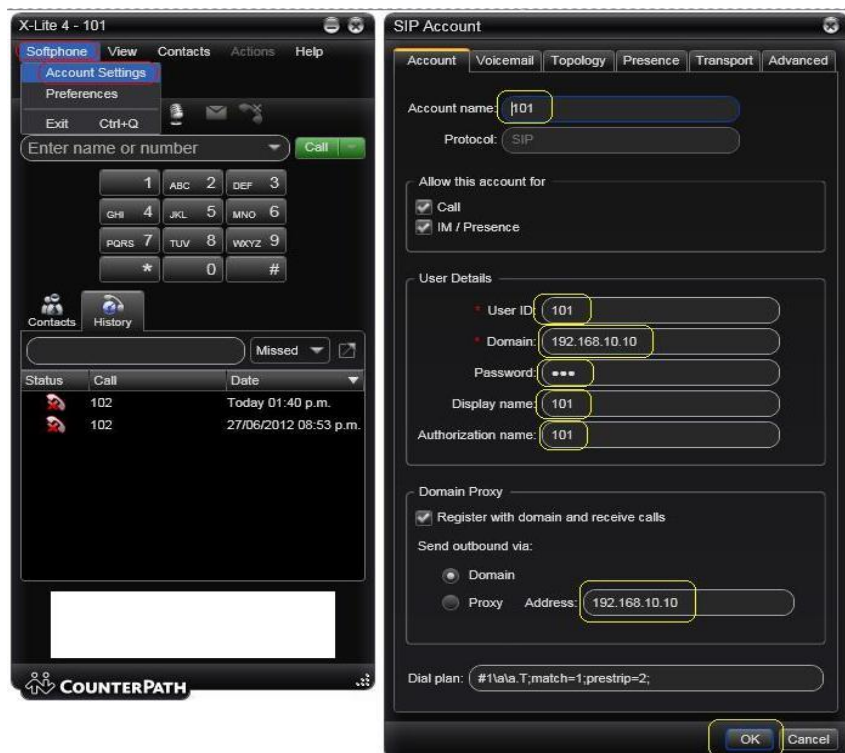
fijadas con su nombre. Sólo debe ingresar el nombre no la extensión.

- **Secret:** Esta es la contraseña usada por el dispositivo de la telefonía para autenticar al servidor de Asterisk.

Procedemos de la misma manera para crear las extensiones 102 y 109. E igualmente en los otros dos servidores para crear las extensiones en cada uno (201 – 209, 301- 309).

Configurando Softphones.

Una vez que tenemos configuradas las extensiones, los softphones y estos se registren en la central. Debemos tener en cuenta que los datos configurados en los teléfonos deben ser exactamente los mismos con los que creamos las extensiones.



Primero elegimos el menú *Softphones* como en este caso, o directamente al menú *Settings* para configurar los parámetros con los cuales debe registrarse.

Softphone>AccountSettings>AddAccount

Ahora vamos a configurar una cuenta completando las siguientes variables:

- **Displayname:** el nombre con que queremos que se nos identifique cuando realicemos una llamada desde nuestro softphone hacia otros.
- **Username:** el nombre del usuario según se ha cargado en el servidor de VoIP.
- **Password:** contraseña particular del usuario, para registrarse en el servidor.
- **Authorization user name:** esta variable debe estar cargada con el mismo valor que el Username.
- **Domain:** dirección IP o nombre de dominio correspondiente al servidor de VoIP.

El resto de los campos se dejan como vienen por defecto. Hacemos clic en Aplicar, luego en Aceptar. A continuación se mostrará una ventana indicando que la cuenta se ha creado en el X-Lite:

Seleccionamos Close. El softphone buscará registrarse con la nueva cuenta en el servidor VoIP. Si la cuenta se ha configurado correctamente, luego de unos segundos la interfaz del X-Lite debería verse de la siguiente manera:

La información de usuario que se ve en el display del teléfono nos indica que éste ha sido configurado correctamente y está listo para ser usado

ANEXO 3

ARCHIVOS DE CONFIGURACIÓN DE DUNDI

Archivos de Configuración DUNDI.

Servidor 1: PBX_A

iax_custom.conf

```
« Regresar Archivo: iax_custom.conf
[vozcom]
type=user
dbsecret=dundi/secret
context=vozcom-local
qualify=yes
disallow=all
allow=ulaw
allow=alaw
;
[vozorg]
type=user
qualify=yes
dbsecret=dundi/secret
context=vozorg-local
disallow=all
allow=ulaw
allow=alaw
```

extensions_custom.conf

```
« Regresar Archivo: extensions_custom.conf  Guardar  Recargar Asterisk
; This file contains the contexts the agents login for the module call center.
; and contains the context conferences for module conferences of elastix 1.0.

[vozcom-local]
exten => _0057.,1,Dial(SIP/justvoip/${EXTEN})
exten => _10X,1,Dial(SIP/${EXTEN},15)
exten => _10X,n,GotoIf("${DIALSTATUS}" = "BUSY")?busy:unavail)
exten => _10X,n(busy),Voicemail(${EXTEN}@default,b)
exten => _10X,n,Hangup
exten => _10X,n(unavail),Voicemail(${EXTEN}@default,u)
exten => _10X,n,Hangup

[dundi-remoto]
switch => DUNDi/vozorg

[from-internal-custom]
exten => 1234,1,Playback(demo-congrats) ; extensions can dial 1234
exten => 1234,2,Hangup()
exten => h,1,Hangup()
include => agentlogin
include => conferences
include => calendar-event
include => weather-wakeup

[agentlogin]
exten => _*8888.,1,Set(AGENTNUMBER=${EXTEN:5})
```

dundi.conf

```
« Regresar Archivo: dundi.conf  Guardar  Recargar Asterisk

[general]
department=ServidorA
organization=ESPOCH
locality=Riobamba
stateprov=Chimborazo
country=Ecuador
email=admin@servidorA.com
phone=+57XXXXXXXXXX
bindaddr=0.0.0.0
port=4520
entityid=08:00:27:B4:CB:0B
cachetime=3600
ttl=32
autokill=yes
secretpath=dundi
storehistory=yes
[mappings]
vozcom => vozcom-local,0,IAx2,vozcom:${SECRET}@192.168.10.10/${NUMBER}
vozorg => vozorg-local,0,IAx2,vozorg:${SECRET}@192.168.10.10/${NUMBER}
;
[08:00:27:33:73:B8]; Servidor B
model = symmetric
host = 192.168.10.20
inkey = vozorg
outkey = vozcom
include = all
permit = vozcom
qualify = yes
;
[08:00:27:C6:84:6E] ; Servidor C
model = symmetric
host = 192.168.10.30
inkey = vozcom
outkey = vozorg
include = all
permit = all
qualify = yes
;
:[*]
```

Servidor 1: PBX_B

iax_custom.conf

```
« Back File: iax_custom.conf

[vozorg]
type=user
qualify=yes
dbsecret=dundi/secret
context=vozorg-local
disallow=all
allow=ulaw
allow=alaw
;
[vozcom]
type=user
dbsecret=dundi/secret
context=vozcom-local
qualify=yes
disallow=all
allow=ulaw
allow=alaw
```


extensions_custom.conf

```
« Back File: extensions_custom.conf Save Reload Asterisk
; This file contains the contexts the agents login for the module call center.
; and contains the context conferences for module conferences of elastix 1.0.

[vozorg-local]
exten => _20X,1,Dial(SIP/${EXTEN})

[dundi-remoto]
switch => DUNDI/vozcom
```

dundi.conf

```
« Back File: dundi.conf Save Reload Asterisk
[general]
department=Servidor2
organization=ESPOCH
locality=Riobamba
stateprov=Chimborazo
country=Ecuador
email=admin@servidorB.com
phone=+57XXXXXXXXX
bindaddr=0.0.0.0
port=4520
entityid=08:00:27:33:73:B8
cachetime=3600
ttl=3
autokill=yes
secretpath=dundi
storehistory=yes
;
[mappings]
vozorg => vozorg-local,0,IAX2,vozorg:${SECRET}@192.168.10.20/${NUMBER}
vozcom => vozcom-local,0,IAX2,vozcom:${SECRET}@192.168.10.20/${NUMBER}
;
[08:00:27:B4:CB:0B] ; Servidor A
model = symmetric
host = 192.168.10.10
inkey = vozcom
outkey = vozorg
include = all
permit = vozorg
qualify = yes

[08:00:27:C6:84:6E] ; Servidor C
model = symmetric
host = 192.168.10.30
inkey = vozcom
outkey = vozorg
include = all
permit = all
qualify = yes
;
;[*]
```

Servidor 1: PBX_C

iax_custom.conf

```
« Regresar Archivo: iax_custom.conf

[vozcom]
type=user
dbsecret=dundi/secret
context=vozcom-local
qualify=yes
disallow=all
allow=ulaw
allow=alaw
;
[vozorg]
type=user
qualify=yes
dbsecret=dundi/secret
context=vozorg-local
disallow=all
allow=ulaw
allow=alaw
```

extensions_custom.conf

```
« Back File: extensions_custom.conf Save Reload Asterisk

; This file contains the contexts the agents login for the module call center.
; and contains the context conferences for module conferences of elastix 1.0.

[vozcom-local]
exten => _0057.,1,Dial(SIP/justvoip/${EXTEN})
exten => _30X,1,Dial(SIP/${EXTEN},15)
exten => _30X,n,GotoIf("${DIALSTATUS}" = "BUSY"?busy:unavail)
exten => _30X,n(busy),Voicemail(${EXTEN}@default,b)
exten => _30X,n,Hangup
exten => _30X,n(unavail),Voicemail(${EXTEN}@default,u)
exten => _30X,n,Hangup

[dundi-remoto]
switch => DUNDI/vozorg
switch => DUNDI/vozcom
```

dundi.conf

<< Back File: dundi.conf

Save

Reload Asterisk

```
[general]
department=ServidorC
organization=ESPOCH
locality=Riobamba
stateprov=Chimborazo
country=Ecuador
email=admin@servidorC.com
phone=+57XXXXXXXXXX
bindaddr=0.0.0.0
port=4520
entityid=08:00:27:C6:84:6E
cachetime=3600
ttl=32
autokill=yes
secretpath=dundi
storehistory=yes
;
[mappings]
vozcom => vozcom-local,0,IAX2,vozcom:${SECRET}@192.168.10.30/${NUMBER}
vozorg => vozorg-local,0,IAX2,vozorg:${SECRET}@192.168.10.30/${NUMBER}
;
[08:00:27:33:73:B8] ; Servidor B
model = symmetric
host = 192.168.10.20
inkey = vozorg
outkey = vozcom
include = all
permit = vozcom
qualify = yes
;
[08:00:27:B4:CB:0B] ; Servidor A
model = symmetric
host = 192.168.10.10
inkey = vozorg
outkey = vozcom
include = all
permit = all
qualify = yes
;
;[*]
```

BIBLIOGRAFIA

- 1.- CABEZAS, J.,** Protocolo de transporte en tiempo real., Córdoba-Argentina., Universidad de Córdoba., 2009., Pp 5-10.

- 2.- KAPOR, V.,** Asterisk basics, and load balancing via DUNDi., California - EEUU, s.ed., 2010., Pp 7-21.

- 3.- LANDIVAR, E.,** Comunicaciones unificadas con Elastix., México DC – México., s.ed.; 2008., 208 p.

- 4.- LANDIVAR, E.,** Comunicaciones unificadas con Elastix., 2da ed., México DC – México., s.ed., 2009., Pp 119-130.

- 5.- MULLINIX, J.,** DUNDi configuration., Cohutta – EEUU., Cohutta.com Inc., s.ed.; 2009., Pp 2-9.

- 6.- RICHARDSON, JR.,** DUNDi, so easy a caveman could do it!.,

Arisona – EstadosUnidos.,Astricon.,2007., Pp 1-12.

7.-SPENCER, M.,Distributed Universal Number Discovery and the
General Peering agreement., California - EstadosUnidos.,Digium
Inc.,2004., Pp 5-8.

8.-ROSENBERGJ., “SIP : Session Initiation Protocol ”., RFC 3261.,
2002.,Pp 100-105.

BIBLIOGRAFIA DE INTERNET

9.- ASTERISK 1.6. Y EL PROTOCOLO DUNDI

<http://www.voztovoice.org/?q=node/239>

[2012/05/20]

10.- CONFIGURACIÓN DUNDI

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

[02/07/2004]

11.- CONFIGURAR ELASTIX

<http://www.elastix.org/index.php/es/component/kunena/11-ayuda/27762-ayuda.html>

[2012/04/21]

11.- CONFIGURAR DUNDI EN ELASTIX

<http://www.elastix.org/index.php/es/component/kunena/11-ayuda/27762-ayuda.html>

[2012/05/01]

12.-DUNDI ENTERPRISE CONFIGURATION SIP

<http://www.voip-info.org/wiki/view/DUNDi+Enterprise+Configuration+SIP+with+no+passwords>

[2012/05/12]

13.- USANDO DUNDI

<http://www.julianmenendez.es/usando-dundi-asterisk/>

[2012/06/27]

