

TRABAJO ESPECIAL DE GRADO

**PROPUESTA DE UN DISEÑO OPERATIVO PARA SERVICIO
DE VOZ SOBRE IP BASADO EN EL SOFTWARE LIBRE
ASTERISK EN SUPRA CARACAS**

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Ruiz G. Gregori Eduardo
para optar al Título de Ingeniero
Electricista.

Caracas, 2013

TRABAJO ESPECIAL DE GRADO

PROPUESTA DE UN DISEÑO OPERATIVO PARA SERVICIO DE VOZ SOBRE IP BASADO EN EL SOFTWARE LIBRE ASTERISK EN SUPRA CARACAS

PROFESOR GUÍA: PhD. Carlos Moreno
TUTOR INDUSTRIAL: M.S. Ricardo Santana

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Ruiz G. Gregori Eduardo
para optar al Título de Ingeniero
Electricista.

Caracas, 2013

CONSTANCIA DE APROBACIÓN

CONSTANCIA DE APROBACIÓN

Caracas, 07 de junio de 2013

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Gregory E. Ruiz G., titulado:

**“PROPUESTA DE UN DISEÑO OPERATIVO PARA SERVICIO DE VOZ
SOBRE IP BASADO EN EL SOFTWARE LIBRE ASTERISK EN SUPRA
CARACAS”**

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. Luis Fernández
Jurado

Prof. Zeldivar Bruzual
Jurado

Prof. Carlos Moreno
Prof. Guía

DEDICATORIA

Dedicado, principalmente, a mis dos grandes padres Doris Gómez y Gregori Ruiz, quienes me han ofrecido todo su esfuerzo, apoyo y amor incondicional, para que yo pueda lograr todas las metas que me he propuesto. Mejores padres no pude tener, ellos han sido mis ídolos, mis amigos y mis ejemplo a seguir. Por lo que les dedico todo este esfuerzo y especialmente, el presente trabajo de grado.

De igual manera, deseo dedicarle este trabajo a mi novia Rita Mariel Bueno, quien ha sido la persona que ha estado conmigo desde el inicio de esta meta y ha apaciguado mis temores con su amor. Gracias por todo, Te amo.

AGRADECIMIENTOS

A Dios por ser ese ente omnipotente que alimenta nuestra esperanza en los momentos más difíciles.

A mis padres, por ser una base fundamental, por apoyarme, y estar siempre ahí conmigo para que tuviera fuerza en la culminación de este estudio.

A mi hermana María Alejandra por ser un motivo en mí crecimiento personal, logrando así ser un buen ejemplo para ella.

Un especial agradecimiento a mi bella novia y amiga Rita Mariel Bueno, por ser el motor de mis sueños. Ya se cumplió uno, pero aún quedan más, Te amo.

Agradezco a la Universidad Central de Venezuela, por darme la oportunidad de evolucionar en mi vida como estudiante y profesional.

A mis profesores y compañeros de clase por todo el apoyo brindado.

A mis tutores, Carlos Moreno y Ricardo Santana por brindarme su apoyo y dedicación en la culminación de este proyecto.

A María Auxiliadora Rojas por ser un ejemplo de dedicación. Muchas gracias por cada duda que lograste solventar ¡Gracias!

A mis compañeros de Supra Caracas, en especial a Leonardo García y Antoni Marín por brindarme sus conocimientos y apoyo a la hora de realizar este proyecto.

En fin, ¡Gracias! a toda las personas que pusieron un granito de arena, directa o indirectamente, en la culminación de esta meta.

Ruiz G., Gregori E.

**PROPUESTA DE UN DISEÑO OPERATIVO PARA SERVICIO
DE VOZ SOBRE IP BASADO EN EL SOFTWARE LIBRE
ASTERISK EN SUPRA CARACAS**

Profesor Guía: Carlos Moreno. Tutor Industrial: Ing. Ricardo Santana. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución: Supra Caracas. 119h. + anexos

Palabras Claves: Servicio de voz sobre IP, Asterisk, Elastix, SIP

Resumen: El presente trabajo plantea una propuesta de un servicio de VoIP basado en Asterisk para la compañía Supra Caracas. En primer lugar, se recopiló información de las redes presentes en la compañía, para luego realizar un estudio de las aplicaciones, servicios y protocolos necesarios, a fin de definir las características de la configuración de la central telefónica. Dicha central fue configurada en la sede principal con el propósito de realizar pruebas que verifiquen la operatividad del diseño. Los resultados fueron analizados para validar la propuesta y su análisis demostró la factibilidad de la implementación del diseño, el cual actualmente se encuentra en etapa de implementación en la sede Supra Las Mayas.

ÍNDICE GENERAL

CONSTANCIA DE APROBACIÓN	iii
DEDICATORIA	iv
AGRADECIMIENTOS	v
RESUMEN	vii
ÍNDICE GENERAL	viii
LISTA DE TABLAS	xii
LISTA DE FIGURAS	xiii
ACRÓNIMOS	xv
INTRODUCCIÓN	17
CAPÍTULO I	19
DEFINICIÓN DEL PROBLEMA	19
1.1 Institución donde se llevó a cabo el siguiente trabajo especial de grado	19
1.2 Planteamiento del problema	20
1.3 Objetivos del proyecto	22
Objetivo general	22
Objetivos Específicos	22
1.4 Justificación del proyecto	23
CAPÍTULO II	25
MARCO TEÓRICO	25
2.1 Voz sobre IP	25
2.1.1 Definición de Voz sobre IP	25
2.1.2 Bases de la VoIP	26
2.1.2.1 Codificación de la voz	26

2.1.2.2 Codec	27
2.1.2.3 Protocolos de transporte.....	29
2.1.2.3.1 UDP	29
2.1.2.3.2 RTP	32
2.1.2.4 Protocolos de Señalización.....	35
2.1.2.4.1 SIP (Protocolo de Inicio de Sesiones).....	37
2.1.2.4.2 IAX2	38
2.1.2.5 Elementos que afectan la calidad de servicio de la voz sobre IP	39
2.1.2.5.1 Latencia	39
2.1.2.5.2 Pérdida de paquetes	42
2.1.2.5.3 Jitter	43
2.1.2.5.4 Eco	44
2.1.2.6 Softphones y Teléfonos IP	45
2.1.2.6.1 Softphones.....	45
2.1.2.6.2 Teléfono IP	47
2.2 Asterisk.....	48
2.2.1 Definición.....	48
2.2.2 Características.....	48
2.2.3 Distribuciones basadas en Asterisk	51
CAPÍTULO III	53
MARCO METODOLÓGICO	53
3.1 Propuesta de un diseño operativo de un servicio de VoIP	53
3.1.1 Requerimientos.....	53
3.1.2 Topología	55
3.1.3 Software	58
3.1.3.1 Servidor	58
3.1.3.2 Softphone	59
3.1.4 Codec	60
3.1.4.1 Determinación del ancho de banda.....	60
3.1.5 Protocolo de señalización.....	64
3.1.6 Usuarios.....	66

3.1.6.1 Perfiles	66
3.1.6.2 Extensiones.....	66
3.1.7 Hardware	67
CAPÍTULO IV	70
PRUEBAS Y RESULTADOS.....	70
4.1 Objetivo General	70
4.2 Escenarios de prueba	70
4.3 Listado de pruebas.....	73
4.3.1 Medición del retardo y pérdida de paquetes en la red	73
4.3.1.1 Procedimientos	73
4.3.1.2 Resultados	74
4.3.2 Verificación de la conectividad entre una PC y el Servidor Elastix.....	75
4.3.2.1 Procedimientos	76
4.3.2.2 Resultados	77
4.3.3 Registro de una extensión mediante Elastix.....	78
4.3.3.1 Procedimientos	78
4.3.3.2 Resultados	79
4.3.4 Comprobación del registro de un Softphone SIP	80
4.3.4.1 Procedimientos	80
4.3.4.2 Resultados	81
4.3.5 Establecimiento y finalización de una llamada utilizando SIP	83
4.3.5.1 Procedimientos	83
4.3.5.2 Resultados	85
4.3.6 Tasa de pérdidas de paquetes	86
4.3.6.1 Procedimientos	86
4.3.6.2 Resultados	88
4.3.7 Medición del Jitter	88
4.3.7.1 Procedimientos	89
4.3.7.2 Resultados	90
4.3.8 Medición de la tasa transferencia de bits en una llamada	93
4.3.8.1 Procedimientos	93
4.3.8.2 Resultados	95

4.3.9 Verificación de la interoperabilidad de las distintas plataformas.....	97
4.3.9.1 Procedimientos	97
4.3.9.2 Resultados	98
4.3.10 Pruebas a través de una VPN.....	98
4.3.10.1 Medición del retardo y pérdida de paquetes (VPN)	99
4.3.10.1.1 Procedimientos	99
4.3.10.1.2 Resultados	99
4.3.10.2 Medición de la tasa de Transferencia (VPN)	100
4.3.10.2.1 Procedimientos	100
4.3.10.2.2 Resultados	100
4.3.10.3 Establecimiento y finalización de una llamada (VPN)	101
4.3.10.3.1 Procedimientos	101
4.3.10.3.2 Resultados	102
4.3.10.4 Medición del retardo y pérdida de paquetes durante una llamada (VPN)	103
4.3.10.4.1 Procedimientos	103
4.3.10.4.2 Resultados	104
CAPÍTULO V	105
ANÁLISIS DE RESULTADOS.....	105
CONCLUSIONES	110
RECOMENDACIONES	112
REFERENCIAS BIBLIOGRÁFICA	113
BIBLIOGRAFÍA	116
ANEXOS	119

LISTA DE TABLAS

Tabla 1. Extensiones	67
Tabla 2. Pérdidas de paquetes	88
Tabla 3. Tasa de transferencia	96
Tabla 4. Verificación de llamadas entre distintos softphone.....	98

LISTA DE FIGURAS

Figura 1. Formato de la cabecera del protocolo UDP	30
Figura 2. Encabezado RTP	33
Figura 3. Efecto del retardo absoluto en la satisfacción del usuario.	40
Figura 4. Topología Física WAN	56
Figura 5. Topología lógica WAN	57
Figura 6. Trama de VoIP	61
Figura 7. Escenario 1	71
Figura 8. Escenario 2	72
Figura 9. Escenario 3	73
Figura 10. PING Test 9:00 Am	75
Figura 11. PING Test 12:00 Pm	75
Figura 12. PING Test 15:00 Pm	75
Figura 13. Verificación de conectividad desde la red 192.168.10.0/24.....	77
Figura 14. Verificación de conectividad desde la red 192.168.11.0/24.....	77
Figura 15. SIP show peers sin usuarios.....	79
Figura 16. SIP show peers con un usuario	79
Figura 17. Captura del flujo SIP en el registro de un Softphone	82
Figura 18. Captura de pantalla de la consola de Asterisk	82
Figura 19. Comunicación entre el terminal A y el servidor	85
Figura 20. Comunicación entre el servidor y el terminal B	86
Figura 21. Jitter: Desde el Terminal A hacia el servidor.	91
Figura 22. Jitter: Desde el servidor al terminal A.....	91
Figura 23. Jitter: Desde el Terminal B hacia el servidor.	92
Figura 24. Jitter: Desde el servidor al Terminal B.....	92
Figura 25. Tasa de transferencia.	95

Figura 26. Tasa de transferencia topología 2.	96
Figura 27. PING en el escenario de prueba 3.	99
Figura 28. Tasa de transferencia mediante una VPN.	101
Figura 29. PING en el escenario 3 durante una llamada.	104

ACRÓNIMOS

ADSL: Asymmetric Digital Subscriber Line (**Línea de abonado digital asimétrica**).

AGI: Asterisk Gateway Interface.

API: Application Programming Interface (**Interfaz de programación de aplicaciones**).

CANTV: Compañía Anónima Nacional Teléfonos de Venezuela.

CDR: Call Detail Recording (**Grabación de Llamadas en Detalle**).

DNS: Domain Name System (**Sistema de Nombre de Dominio**).

FCS: Frame check Sequence (**Verificador de secuencia trama**).

GPL: General Public License (**Licencia Pública General**).

GSM: Global System for Mobile Communications (**Sistema Global para las Comunicaciones Móviles**).

HTTPS: Hypertext Transfer Protocol Secure (**Protocolo seguro de transferencia de hipertexto**).

IAX: Inter-Asterisk eXchange protocol.

IETF: Internet Engineering Task Force (**Grupo Trabajo de Ingeniería de Internet**).

IP: Internet Protocol (**Protocolo de Internet**).

ISDN: Integrated Services Data Digital Network (**Red Digital de Servicios Integrados**).

ITU: International Telecommunication Union (**Unión Internacional de telecomunicaciones**).

IVR: Interactive Voice Response (**Respuesta de Voz Interactiva**).

LAN: Local Area Network (**Red de área Local**).

NGN: Next Generation Networking (**Red Próxima Generación**).

ODBC: Open DataBase Connectivity (**Conectividad a Bases de Datos Abiertas**).

OSI: Open System Interconnection (**Modelo de Interconexión de Sistemas Abiertos**).

PBX: Private Branch Exchange (**Ramal Privado de Conmutación**).

PCM: Pulse Code Modulation (**Modulación por Codificación de Pulsos**).

PPP: Point-to-point Protocol (**Protocolo punto a punto**).

PSTN: Public switched telephone network (**Red telefónica Conmutada**).

QoS: Quality of Service (**Calidad de Servicio**).

RFC: Request for Comments (**Petición de Comentarios**).

RTP: Real-time Transport Protocol (**Protocolo de Transporte de Tiempo real**).

SIP: Session Initiation Protocol (**Protocolo de Inicio de Sesiones**).

SNMP: Simple Network Management Protocol (**Protocolo Simple de Administración de Red**).

SRTP: Secure Real-time Transport Protocol (**Protocolo seguro de Transporte de Tiempo real**).

SUPRA: Servicio Urbano de Procesamiento, Recolección y Aseo.

TCP: Transmission Control Protocol (**Protocolo de control de transmisión**).

TFTP: Trivial file transfer Protocol (**Protocolo de transferencia de archivos trivial**).

TTS: Text to speech (**Conversor Texto - Voz**).

UDP: User Datagram Protocol (**Protocolo de datagrama de usuario**).

URL: Uniform Resource Locator (**Localizador de Recursos Uniforme**).

UTP: Unshielded Twisted Pair (**Par Trenzado con Protection**).

VoIP: Voice over IP (**Voz sobre IP**).

VPN: Virtual Private Network (**Red Privada Virtual**).

WAN: Wide Area Network (**Red de Área Amplia**).

INTRODUCCIÓN

Supra Caracas es una empresa encargada de prestar el servicio de aseo urbano, en las áreas públicas del Distrito Capital, fue fundada en Agosto del año 2011 y su principal misión es mejorar la calidad de vida en la capital, preservando el medio ambiente.

No obstante, por ser una empresa relativamente joven, no cuenta con una tecnología vanguardista en pro de sus objetivos, por lo que alienta a la inclusión de nuevas tecnologías, procedimientos y aplicaciones, con el fin de mantener el liderazgo en los servicios medio ambientales. En consecuencia, la Gerencia de las Tecnologías de la Comunicación busca promover el estudio, desarrollo e implementación de aplicaciones o tecnologías que fomenten una mejor comunicación dentro de la empresa.

Siguiendo con esta línea de pensamiento y debido a la carencia de un sistema de voz, el cual permita comunicar a los diferentes departamentos y sedes de la compañía, este proyecto propone un diseño de una central telefónica de voz IP mediante un software libre llamado Asterisk.

Para describir lo anteriormente señalado, este proyecto está conformado por cinco capítulos, en donde el primero abarca todo el planteamiento del problema, el segundo contiene las bases teóricas para la comprensión del estudio, el tercero describe la propuesta y todo tipo de información recolectada para la realización de

ésta, el cuarto presenta una recopilación de pruebas y resultados para avalar el diseño y por último, en el quinto se analizan los resultados del capítulo anterior.

La suma de todos los capítulos lleva a un estudio completo de las tecnologías de VoIP y software libre necesarias para el desarrollo y diseño del proyecto, con la finalidad de realizar un trabajo óptimo y eficiente, adecuándose a las necesidades de la empresa.

CAPÍTULO I

DEFINICIÓN DEL PROBLEMA

1.1 Institución donde se llevó a cabo el siguiente trabajo especial de grado

Sistema Urbano de Procesamiento Recolección y Aseo (Supra – caracas)

Es una empresa prestadora del servicio de aseo urbano, recolección de residuos sólidos, barrido, limpieza y lavado de áreas públicas del Distrito Capital, suministrándole de esta manera, soluciones integrales en materia medioambiental.

Supra - Caracas, es relativamente joven, fue fundada en Agosto del año 2011, por disposición del Presidente Hugo Rafael Chávez Frías, empresa que contribuye al desarrollo de la ciudad de Caracas. Ésta inició sus actividades dotada de unidades con tecnología innovadora en la recolección, transporte de basura y desechos sólidos garantizando un servicio de calidad y la satisfacción de las necesidades de todos los habitantes de Caracas.

La principal misión de la empresa Supra - Caracas, es preservar el medio ambiente para mejorar la calidad de vida de los caraqueños, así como mantener la

ciudad libre de residuos sólidos, con alta eficiencia y mejora continua de los procesos, en busca de la identificación de los trabajadores con la empresa para lograr eficazmente los objetivos organizacionales.

De igual manera, intenta mantenerse líder en los servicios medioambientales, enmarcada en los más altos principios de moral, ética profesional, con excelente clima organizacional, para satisfacer las necesidades de los caraqueños, en la recolección y saneamiento de todas las calles de la ciudad capital. Para conseguir el logro anterior, Supra - Caracas cuenta con un personal altamente calificado, leal, con una visión clara y estratégica, identificada y comprometida con una filosofía de trabajo orientada siempre a la participación activa del pueblo en el desarrollo de los proyectos, sin importar la envergadura de los mismos y al logro de todos los objetivos propuestos por la organización.

1.2 Planteamiento del problema

Para definir la situación que genera el estudio, es necesario comprender el estado de la empresa. Actualmente, Supra Caracas se encuentra dividida en cuatro sedes, las cuales a su vez conforman distintas Redes de áreas locales segmentadas mediante subredes. Estas sedes, se localizan separadas geográficamente y las podemos ubicar en las Mayas, las Artigas, la Yaguara y Zona rental.

A pesar de ser sedes de una misma empresa, éstas no poseen ninguna conexión entre sí, en lo que a telecomunicación se refiere, sin embargo, próximamente se llevará a cabo una interconexión mediante una red MetroEthernet

provista por CANTV, en donde se utilizará la tecnología Virtual Private Lan Service (VPLS); ésta permitiría a la red del proveedor emular el comportamiento de un conmutador o puente, creando una LAN compartida por todas las sedes con un único dominio de Broadcast.

Ya conociendo el momento por el cual transita la empresa y la puesta en marcha de la interconexión entre las sedes, surge la necesidad de aprovechar esta infraestructura, próximamente a ser llevada a cabo; no sólo para proporcionar una conexión entre diferentes redes, sino también para implementar un servicio de VoIP, el cual permita realizar llamadas de voz sobre IP entre usuarios de una misma red y diferentes sedes.

Todo esto representa un verdadero reto, ya que en principio, se hace necesario verificar las condiciones en cada una de las sedes; así como también, realizar una estimación del ancho de banda con el fin de determinar si el diseño planteado puede abarcar el servicio a todos los usuarios involucrados y coexistir con otros servicios presentes en la red. Por otra parte, es imperante analizar el entendimiento entre las diferentes redes para lograr una comunicación satisfactoria entre ellas, al igual que, lidiar con las diferentes aplicaciones y servicios que sean necesarios para el desarrollo del servicio de VoIP bajo una central telefónica basada en el software Asterisk.

En relación a lo antes planteado y buscando obtener información necesaria para el desarrollo del diseño operativo del nuevo servicio, se plantean las siguientes interrogantes: ¿Es posible diseñar una central telefónica de VoIP mediante el software libre Asterisk amoldándose a las exigencias de la empresa?, ¿Supra Caracas posee

una estructura necesaria para soportar un servicio de VoIP?, ¿Se puede lograr una comunicación exitosa entre distintas redes mediante la central telefónica Asterisk?.

1.3 Objetivos del proyecto

Objetivo general

"Realizar una propuesta de un diseño operativo para servicio de voz sobre IP basado en el software libre Asterisk en Supra Caracas"

Objetivos Específicos

- Recopilar información acerca de la estructura de las redes presentes en la compañía a fin de dimensionar la posibilidad de implementar el servicio en la empresa.
- Realizar un estudio de las aplicaciones, servicios y protocolos necesarios para la elaboración del diseño.
- Definir las características de la configuración de la central telefónica.

- Configurar la central telefónica basada en el software Asterisk en la sede principal de Supra Caracas.
- Realizar pruebas que verifiquen la operatividad del diseño.
- Analizar los resultados para la validación de la propuesta en las diferentes sedes de Supra Caracas.
- Evaluar la factibilidad de la implementación del diseño del servicio de VoIP dentro de la empresa.

1.4 Justificación del proyecto

Actualmente, el mundo se encuentra en una tendencia donde su propósito a nivel de telecomunicaciones, es converger los servicios de datos, voz y móviles hacia una red All-IP llamada Next Generation Networking (NGN), esto conlleva al creciente auge de tecnologías VoIP y aplicaciones como Asterisk, en lo que a voz se refiere.

Siguiendo con esta corriente, la empresa Supra Caracas, busca comprobar la factibilidad de implementar una central telefónica de VoIP mediante la aplicación

del software Asterisk. La cual, sí se llegara a implementar, conllevaría a mejoras importantes dentro de la compañía.

Entre los beneficios, podemos encontrar la optimización de la comunicación, no sólo en cada sede, sino a nivel general en la empresa. Mejorando así, la calidad de vida del trabajador y su eficiencia; por ejemplo, a la hora de comunicar una información a otro departamento no se necesitaría ir hacia esa dependencia, sino simplemente se podría llamar mediante el servicio de VoIP cómodamente desde su computadora o por medio de teléfonos de VoIP.

En referencia a la economía, se aprovecharía la interconexión existente y el servicio de internet de CANTV, para proporcionar una plataforma al servicio de VoIP, relativamente sin costo. Además, al poner en funcionamiento este servicio se reducirían las llamadas entre usuarios dentro de la empresa. Cabe destacar, que la mayoría de las llamadas se realizan mediante proveedores privados, las cuales generan un gasto innecesario por concepto de llamadas telefónicas, en consecuencia se podría ahorrar utilizando y fomentando el servicio de VoIP.

En fin, una propuesta de un diseño operativo de una central telefónica de IP, crearía las bases dentro de la empresa para una posible implementación de un servicio de VoIP, donde, no sólo mejora la calidad de la misma, sino que contribuye al desarrollo y crecimiento de ésta, manteniéndose así a la vanguardia de la tecnología y de las exigencias del mundo actual.

CAPÍTULO II

MARCO TEÓRICO

En esta sección se especificarán definiciones, conceptos y tecnologías necesarias para dar forma a la propuesta planteada, la cual, se fundamenta con bases teóricas, recomendaciones y normas, extraídas de textos, artículos y fuentes confiables.

2.1 Voz sobre IP

2.1.1 Definición de Voz sobre IP

Mejor conocida como Voice Over Internet Protocol o por su acrónimo VoIP es una tecnología que utiliza una serie de recursos como protocolos, aplicaciones, codecs, entre otros, que hacen posible la transmisión de señales de voz sobre redes de datos como por ejemplo la Internet.

Ésta se vale de los servicios del protocolo IP (Internet Protocol) para encapsular en paquetes, la voz previamente procesada, para luego ésta poder ser

transportada por la red de datos sin la necesidad de disponer de una infraestructura de telefonía convencional, como la PSTN. Logrando así, la convergencia entre la transmisión de voz y el envío de datos.

2.1.2 Bases de la VoIP

2.1.2.1 Codificación de la voz

Existen diferentes formas de codificar digitalmente el audio, pero el más común de los métodos (y el único utilizado en sistemas de telefonía) es el llamado “Pulse Code Modulation”. El cual, transforma una señal analógica en una secuencia de bits (señal digital).

Si se quiere entender la codificación de la voz es necesario comprender un poco modulación de codificación de pulsos. Ésta, tiene como principio que la amplitud de la forma de onda analógica sea muestreada a intervalos específicos, para que posteriormente se pueda volver a recrear. La cantidad de detalle que se captura depende tanto de la resolución de bits de cada muestra, como de la frecuencia con la que se extrae las muestras. Un bit de resolución mayor y una tasa de muestreo más alta, proporcionarán una mayor precisión, pero como consecuencia se necesitará un mayor ancho de banda para la transmisión de la información. [1]

2.1.2.2 Codec

Los codecs son, generalmente, los diferentes algoritmos matemáticos utilizados para digitalmente codificar y comprimir la información de audio analógico. Muchos de estos modelos tienen en cuenta la capacidad del cerebro humano para formar una impresión a partir de información incompleta.

Entre los principales codecs utilizados por la tecnología VoIP podemos encontrar:

- **G.711:** es una recomendación de codificación digital creada por la ITU-T con el objeto de representar señales de audio en frecuencias de la voz humana, mediante símbolos de 8 bits de resolución, con una tasa de muestreo de 8000 muestras por segundo, lo que proporciona un flujo de datos de 64 Kbit/s. Este codec tiene dos versiones conocidas como Alaw y Ulaw. El último corresponde con el estándar T1 usado tanto en los Estados Unidos como en Japón y A-law con el estándar E1 usado en el resto del mundo. Ambos métodos tienen una curva basada en perfiles logarítmicos, pero el A-law fue específicamente diseñado para ser implementado con facilidad por métodos digitales.
- **G.711.1:** ha sido aprobado por la ITU-T en marzo de 2008. Con la fin de permitir interoperar con la infraestructura G.711 existente, mejorando la calidad de la señal. Para esto se incorporó 2 nuevas capas al actual estándar

G.711. La primera capa mejora la calidad de G.711 en bajas frecuencias (banda de 50 a 300 Herzios) que habitualmente no se transmiten en la norma G.711. La segunda extensión, mejora la calidad de las altas frecuencias (banda de 4KHz a 7KHz). Por lo cual, éste nuevo codec permite añadir una o ambas capas incrementando el bit rate de 64 kbps hasta 80 o 96 kbps. [2]

- **G.726:** es el predecesor de lo que solía ser el G.721. G.726 puede funcionar a diferentes velocidades bits y los tipos más comunes son 16 Kbps, 24 Kbps y 32 Kbps. Además, ofrece una calidad casi idéntica a G.711, pero utiliza sólo la mitad del ancho de banda, esto es posible porque en lugar de enviar el resultado de la medición de cuantificación, se envía solamente la información necesaria para describir la diferencia entre la muestra actual y la anterior. [3]

- **G.729:** al igual que los anteriores se trata de una recomendación de la ITU, cuyas implementaciones han sido históricamente licenciadas, es decir no gratuitas. G.729 utiliza 8 kbit/s por cada canal, si se compara este valor con el de G.711, se notará que consume 8 veces menos ancho de banda, que representa un ahorro significativo de recursos. Por lo cual, la ventaja en la utilización de G.729 radica principalmente en su alta compresión y bajo consumo de ancho de banda, haciéndolo atractivo para comunicaciones vía Internet. Pese a su alta compresión no deteriora la calidad de voz significativamente y por esta razón ha sido ampliamente usado a través de los años por muchos fabricantes de productos de VoIP. [4]

- **GSM:** llamado oficialmente RPE-LTP (Regular Pulse Excitation–Long Term Prediction), se conoce mundialmente como GSM debido a que es el codec usado en el estándar GSM de comunicaciones móviles. Éste tiene una tasa de bits de 13 kbps con un MOS ideal de 3.6 y realiza la codificación generando coeficientes representativos de un intervalo de tiempo determinado. Este intervalo normalmente es de 20 milisegundos de voz. [5]

2.1.2.3 Protocolos de transporte

2.1.2.3.1 UDP

UDP (User Datagram Protocol) y TCP (Transmission Control Protocol) conforman los protocolos de la capa de transporte del modelo OSI, sin embargo este último casi nunca se utiliza para VoIP, porque si bien cuenta con mecanismos establecidos para asegurar la entrega, no es necesariamente rápido. Por esta razón, UDP aunque no es orientado a la conexión es el protocolo predilecto para la transmisión de la voz.

Cabe citar al RFC 768 (1980), el cual comenta que:

Este Protocolo de Datagramas de Usuario (UDP: User Datagram Protocol) se define con la intención de hacer disponible un tipo de datagramas para la comunicación por intercambio de paquetes entre ordenadores en el entorno de un conjunto interconectado de redes de computadoras. Este protocolo asume que el Protocolo de Internet (IP: InternetProtocol) se utiliza como protocolo subyacente.

Este protocolo aporta un procedimiento para que los programas de aplicación puedan enviar mensajes a otros programas con un mínimo de mecanismo de protocolo. El protocolo se orienta a transacciones, y tanto la entrega como la protección ante duplicados no se garantizan. Las aplicaciones que requieran de una entrega fiable y ordenada de secuencias de datos deberían utilizar el Protocolo de Control de Transmisión (TCP: Transmission Control Protocol).

Luego de citar al RFC 768, es necesario visualizar la estructura del encabezado UDP, a fin de reforzar el entendimiento del funcionamiento de este protocolo.

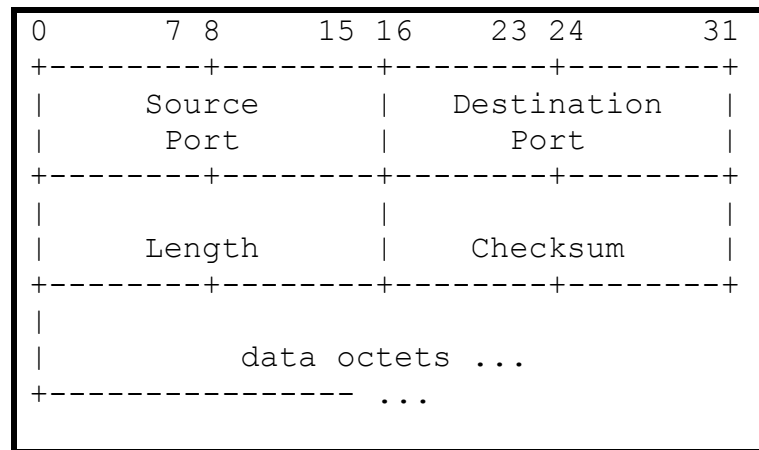


Figura 1. Formato de la cabecera del protocolo UDP

Fuente: (Postel, 1980)

Como se puede observar en la Figura 1, la cabecera del datagrama está conformada por 5 campos que serán definidos a continuación.

- **Source Port:** es opcional e indica el puerto del proceso emisor, por lo que en general se asume como el puerto de respuesta, al menos que se

especifique otro puerto. Su longitud es de 16 bits y si no se utiliza el valor que aparecerá será el cero.

- **Destination Port:** representa una dirección de destino, la cual posee una longitud de 16 bits
- **Length:** define la longitud en octetos del datagrama, por lo que su valor mínimo es de 8.
- **Checksum:** la suma de verificación tiene como propósito detectar cambios accidentales en una secuencia de datos para proteger la integridad de los datos, verificando que no haya discrepancias. Para su cálculo se utiliza una pseudo cabecera que también incluye las direcciones IP origen y destino. Para conocer estos datos, el protocolo UDP debe interactuar con el protocolo IP.
- **Data:** se conforma por todos los datos enviados por las capas superiores del modelo OSI.

Por último cabe mencionar aquellas aplicaciones que se basan en el protocolo UDP, se pueden encontrar servidores de archivos remotos, streaming multimedia, Sistema de Nombres de Dominio (DNS), Protocolo de Gestión Simple de Redes (SNMP), Protocolo de Transferencia de Ficheros Trivial (TFTP), telefonía sobre Internet, entre otros.

2.1.2.3.2 RTP

El protocolo RTP (Real-time Transport Protocol) o por su nombre en español Protocolo de transporte en tiempo real surgió con la idea de crear un protocolo específico para la gran demanda de recursos en tiempo real por parte de los usuarios. Algunos de estos recursos son la música, videoconferencia, video, telefonía en Internet entre otras aplicaciones multimedia.

RTP fue conformado conjuntamente con el protocolo RTCP (RTP Control Protocol), es decir, Protocolo de Control RTP, cuya función principal es proporcionar mecanismos de realimentación para informar sobre la calidad en la distribución de los datos. El estándar de estos dos protocolos fue publicado por primera vez en 1996 por la IETF (Internet Engineering Task Force) como el RFC 1889, y actualizado posteriormente en 2003 en la RFC 3550. [6]

El protocolo RTP se ejecuta, por lo general, sobre UDP, ya que posee menor retardo que TCP. En consecuencia, con UDP se gana velocidad a cambio de sacrificar la confiabilidad que TCP ofrece. En síntesis, RTP no es capaz de garantizar la entrega de todos los paquetes, ni la llegada de éstos en el momento preciso.

El principal objetivo de RTP es multiplexar varios flujos de datos en tiempo real en un sólo flujo de paquetes UDP, pudiéndose enviar tanto unicast como multicast. Para esto los paquetes son numerados de la siguiente manera; se le asigna a cada paquete un número mayor que su antecesor. Lo cual, será útil para que la aplicación conozca si ha fallado o no, algún paquete en la transmisión.

Por otra parte, RTP ofrece una característica resaltante para las aplicaciones de contenido multimedia en tiempo real, como lo es el time-stamping, permitiendo a la fuente asociar una marca de tiempo con la primera muestra de cada paquete. Estas marcas corresponden al inicio del flujo, por esta razón, solo importa las diferencias entre dichas marcas de tiempo. Con este planteamiento, el destino es capaz de almacenar en un pequeño buffer e ir reproduciendo cada muestra el número exacto de milisegundos después del inicio del flujo, reduciendo los efectos de la fluctuación y sincronizando múltiples flujos entre sí. [7]

En el marco de las observaciones anteriores, para que el protocolo RTP pueda notificar el número de secuencia y las marcas de tiempo, es necesario la existencia de un encabezado, el cual se presentará en el Figura 2.

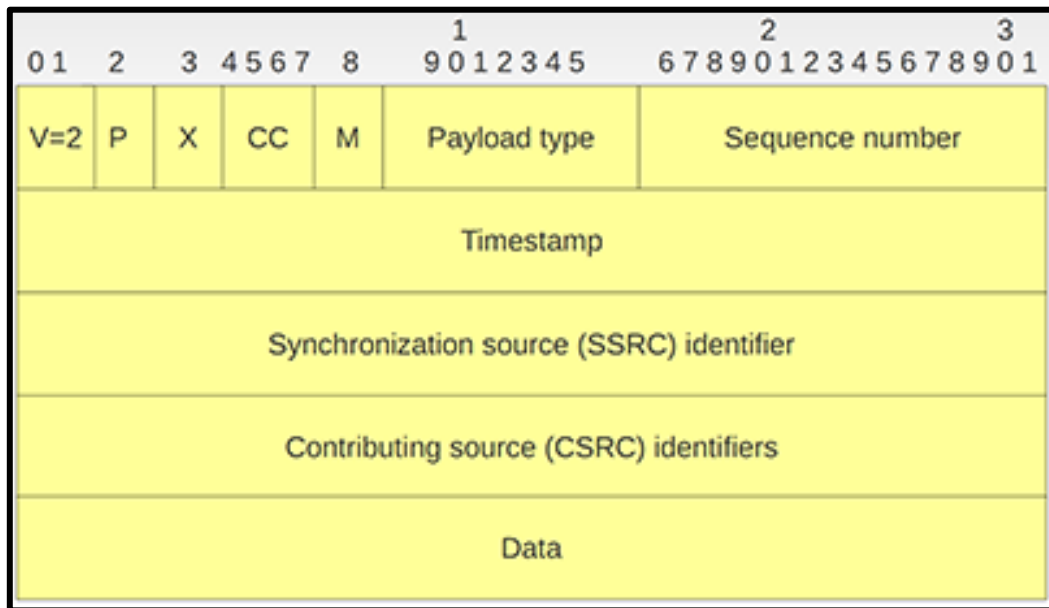


Figura 2. Encabezado RTP

Fuente: (Implementacion del protocolo RTSP)

- **V:** en este campo de longitud 2 bits se identifica la versión del protocolo
- **P:** Si campo posee un valor de 1, significa que el payload tiene un contenido relleno. Cabe destacar, que el último byte de la sección de relleno indica el número de octetos de relleno que se deben ignorar.
- **X:** está conformado por un único bit, el cual indica si hay un encabezado de extensión.
- **CC:** señala cuántos orígenes de contribución están presentes, de 0 a 15. Por lo que su longitud es de 4 bits.
- **M:** es un marcador específico de la aplicación, normalmente un marcador de inicio (1 bit).
- **Payload Type:** indica cuál es el algoritmo de codificación que se ha utilizado, se expresa en 7 bits.
- **Sequence number:** de longitud de 16 bits, es un contador que se incrementa en cada paquete RTP enviado.

- **Timestamp:** delimitado por 32 bits, indica cuándo se creó la primera muestra en el paquete.
- **SSRC:** Identifica la fuente del flujo RTP. Cada flujo de una sesión RTP debería tener un SSRC distinto. La idea es tener un identificador de fuente de flujo independiente de la dirección de red, para así poder identificar números de secuencia y marcas de tiempo provenientes de una misma fuente. Éste posee una longitud de 32 bits.
- **CSRC:** Compuesto por 32 bits, identifica las fuentes contribuyentes.
- **Data:** conformada por 32 bits, posee todos los datos enviados por las aplicaciones.

2.1.2.4 Protocolos de Señalización

Tradicionalmente, la señalización en voz sobre IP sigue los mismos principios que la señalización en la red telefónica conmutada (RTB), en otras palabras, la señalización y el flujo de voz están claramente separados y delimitados. Esta diferenciación se puede observar claramente en la VoIP, ya que la señalización se encuentra administrada por protocolos completamente distintos a los encargados del tráfico de voz.

Un protocolo de señalización es un lenguaje común hablado por los teléfonos y servidores de administración de llamadas, PSTN, PBX y sistemas heredados, por el cual se comunican para establecer, controlar y finalizar las llamadas. Actualmente, existen distintos protocolos de señalización tales como: SCCP, MGCP, MEGACO/H.248, H.323, IAX, SIP, entre otros. No obstante, los últimos dos son los que se estudiarán más a fondo. Aunque, es importante señalar que la mayoría de los protocolos de señalización mantienen las siguientes características en común. [8]

- Su propósito es indicar, registrar y facilitar eventos claves en una llamada: el comienzo, el final y cuando los usuarios intentan utilizar las funciones de telefonía como transferencias de llamadas o conferencias.
- A pesar de que las señales de llamada usualmente se envían utilizando UDP, no se consideran tráfico en tiempo real como los canales de medios de comunicación, que también utilizan UDP.
- Los patrones de tráfico generados en la red son cortos y por ráfagas, en oposición a los canales de medios, que tienden a ser consistentes y largo.
- La mayoría están disponibles en implementaciones libres como Asterisk, GnoPhone , OpenH323 , VOCAL y otros.

2.1.2.4.1 SIP (Protocolo de Inicio de Sesiones).

La Internet Engineering Task Force (IETF) define el Protocolo de Iniciación de Sesión (SIP), por primera vez, en su RFC 2543 en marzo de 1999, donde SIP se especifica cómo protocolo de señalización a nivel de aplicación que permite el establecimiento, la modificación y finalización de sesiones multimedia o llamadas a través de una red IP. Actualmente, el RFC 2543 se encuentra obsoleto y fue suplantado por el RFC 3261 aprobado en junio del 2002 con el status “Proposed standard”.

Entre las capacidades SIP se pueden encontrar las siguientes: [9]

- Determinar la ubicación de un punto final, que en la terminología SIP se refiere a cualquier cliente, servidor o gateway en una red de comunicación, en consecuencia SIP traduce el nombre del punto final en su dirección de red actual.
- Determinación de la disponibilidad de un punto final, si SIP descubre que un cliente no está disponible, éste devuelve un mensaje que indica si el cliente ya estaba conectado a una llamada o simplemente no respondió.
- El establecimiento de una sesión entre dos puntos finales y la gestión de llamadas mediante invitación, finalización, o la transferencia de los participantes.

- Negociación de las características de una llamada o videoconferencia cuando ésta se encuentra establecida, por ejemplo, ponerse de acuerdo sobre el tipo de codificación que los puntos terminales emplearan.
- El cambio de las características de una llamada o videoconferencia mientras se está conectado.

2.1.2.4.2 IAX2

Es la versión mejorada, actualizada y estandarizado de Inter-Asterisk-Exchange (IAX), el cual es un protocolo de señalización diseñado por el creador de Asterisk Mark Spencer, con el objetivo de solucionar algunos problemas existentes con otros protocolos. Actualmente, IAX es obsoleto, siendo así desplazado por IAX2, el cual se encuentra especificado y estandarizado en status “Informational” en el RFC 5456.

El principal objetivo de IAX2 ha sido minimizar el ancho de banda utilizado en la transmisión de voz y vídeo a través de la red IP, con particular atención al control y a las llamadas de voz y proveyendo un soporte nativo para ser transparente a NAT.

IAX2 utiliza un único puerto UDP 4569, y por lo tanto funciona bien en entornos con NAT (el obsoleto protocolo IAX1 usaba el puerto 5036). IAX2 utiliza

un único puerto UDP para el control y tráfico de datos, por lo que la señalización y el flujo de datos viajan conjuntamente, permitiendo así el paso por los router y firewalls de manera sencilla.

Cabe destacar, que IAX2 es un protocolo binario y está diseñado y organizado de manera que reduce la carga en flujos de datos de voz. A diferencia de SIP que como se señaló anteriormente, es un protocolo basado en texto. Esto es una ventaja desde el punto de vista de ancho de banda puesto que en binario se desperdiciarán menos bytes.

Adicionalmente, el protocolo permite la troncalización de varios canales de audio en el mismo flujo de datos. En otras palabras, en un mismo datagrama se pueden enviar varias sesiones al mismo tiempo, lo que significa una reutilización de datagramas y por consiguiente un ahorro de ancho de banda.

2.1.2.5 Elementos que afectan la calidad de servicio de la voz sobre IP

2.1.2.5.1 Latencia

Causada principalmente por enlaces de red lentos. La Latencia o retardo, en el caso de VoIP, es el tiempo que transcurre desde el instante en que los llamantes se expresan hasta el momento en que el receptor escucha esa expresión. La investigación ha demostrado que la latencia de ida y vuelta a menos de 150 ms no es inmediatamente perceptible, pero la latencia superior a 150 ms es notable, y el retardo

superior a 300 ms se considera inaceptable. A continuación se mostrará una figura, perteneciente a la recomendación G. 114, la cual señala el nivel de satisfacción de los usuarios respecto al retardo de la voz.

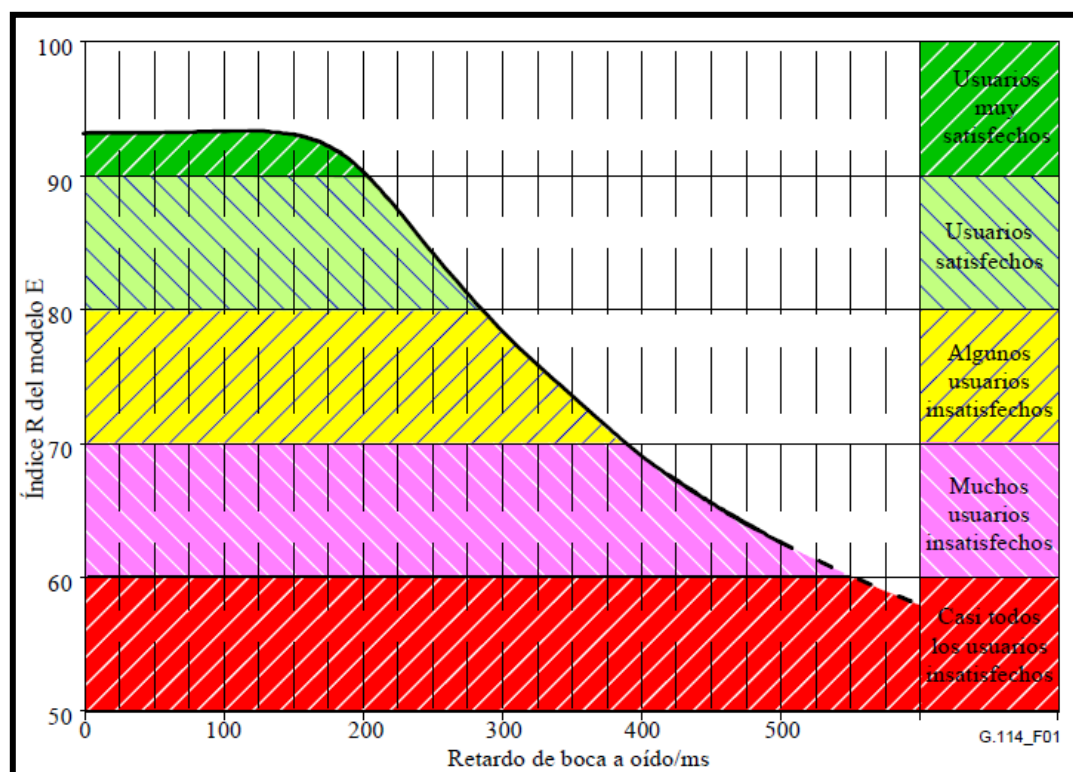


Figura 3. Efecto del retardo absoluto en la satisfacción del usuario.

Fuente: (Recomendación UIT-T G.114, 2003)

El retardo tiene los siguientes efectos en las aplicaciones de telefonía:

- Puede reducir la velocidad de la conversación humana.

- Puede causar que el transmisor y el receptor se interrumpan, sin querer, el uno al otro.
- Puede exacerbar otro problema de calidad de servicio como el eco.
- Puede causar retrasos en las aplicaciones de sincronización de llamadas de conferencia.

La mejor manera de vencer a la latencia es utilizar codecs de bajos intervalos de paquetización y mantener vínculos rápidos de la red, ya que los protocolos de QoS por sí solos no pueden mejorar directamente el impacto de la latencia. En otras palabras, no pueden acelerar la red.

La latencia es uno de los enemigos de la voz sobre IP, pero también hace posible algunas soluciones basadas en codecs, las cuales minimizan la pérdida de paquetes y jitter. Esto se debe a que esas soluciones como por ejemplo Jitter buffer y la ocultación de pérdida de paquetes (PLC) son dos fuentes de latencia. De hecho, algunos elementos que contribuyen al retardo son:

- Framing y paquetización
- Software de procesamiento y PLC

- Jitter buffer
- Enrutamiento y firewall transversal
- Transcodificación
- Medios de acceso y la interconexión de la red

En consecuencia, reducir al mínimo la latencia es una manera importante para maximizar la calidad percibida del servicio de VoIP. Las dos principales fuentes de latencia son Framing / paquetización, que puede agregar hasta 30 ms de latencia y el enrutamiento, que puede agregar 5-50 ms por salto.

2.1.2.5.2 Pérdida de paquetes

La pérdida de paquetes es perjudicial para las llamadas VoIP. Su principal causa es la congestión de la red. Por otra parte la solución para la pérdida de paquetes va ligada a la utilización de los codecs. Esto se debe, a que PLC es una característica de algunos codecs que permite un desglose de la calidad de la percepción para reducir el impacto de la pérdida de paquetes al mínimo a través de algoritmos de vectorización.

En marco de las observaciones anteriores, los codecs funcionan reemplazando el sonido que presumiblemente se habría producido por un paquete que se perdió, con el sonido que se predice en base a la secuencia de paquetes recibidos antes y después de él, esto se utiliza principalmente cuando se posee de un amplio buffer. Pero incluso con PLC en vigor, las tasas de pérdida de paquetes en una red de VoIP deben mantenerse por debajo de 1%. Si bien las medidas de calidad de servicio pueden mejorar el problema de la pérdida de paquetes, proporcionando ancho de banda reservado o prioridad para los paquetes de voz, sigue siendo importante conservar la capacidad de red disponible y mantener las tasas de pérdidas de paquetes por debajo del 1 %.

2.1.2.5.3 Jitter

Jitter es un problema más complejo que la latencia y las pérdidas de paquetes. Es la variación en el tiempo de retardo de un paquete al siguiente. Hace que los paquetes lleguen fuera de orden, dejando huecos en la secuencia de elaboración de la señal de voz. El Jitter se incrementa cuando el tráfico de voz debe viajar a través de varios routers. Mientras más saltos, peor es el jitter.

Para tratar de que el jitter tenga un menor impacto en la calidad de voz se emplea el siguiente principio. Si se espera un poco mas por los paquetes de voz en el destino (antes de reensamblar la señal de voz para enviarla al teléfono del destinatario) es posible que llegue una buena parte de los paquetes extraviados y la comunicación sufra menos las consecuencias. Sin embargo, el problema es que con esta acción se aumenta el retardo, que es un problema que interfiere con el servicio de

VoIP. No obstante, la idea es buena y por lo tanto es probable que lleguen una gran parte de los paquetes perdidos sin afectar significativamente el retardo.

En consecuencia, se define un *jitter buffer*, el cual es un pequeño registro donde se almacenan temporalmente todos los paquetes de voz durante un periodo de tiempo para esperar por posibles paquetes perdidos. El tiempo de espera se denomina “tamaño del buffer”.

2.1.2.5.4 Eco

Se está en presencia de eco cuando una persona escucha las palabras que acaba de mencionar, de nuevo, una fracción de segundo más tarde por teléfono. Es probable que, si el eco se produce en menos de 150 ms desde el momento que llegó a decir las palabras, entonces no se notará. El eco es causado por tres condiciones, y es peor cuando coexisten las tres:

- Conexión entre TDM y VoIP o terminales analógicos y puntos finales de VoIP. Mientras más puntos de interfaz tengan la red, mayor será el eco.

- Larga latencia de ida y vuelta entre la persona que llama y el receptor. Cuanto mayor sea la latencia, el eco será más molesto.

- Conexión de una ruta de llamada entre dos hilos analógicos y TDM o dispositivos analógicos de cuatro hilos. En este caso, el eco es causado por una incapacidad del circuito TDM o de cuatro hilos para cancelar la señal de tono local en el dispositivo de dos hilos.

2.1.2.6 Softphones y Teléfonos IP

2.1.2.6.1 Softphones

Un softphone es una aplicación de software que se ejecuta en un ordenador portátil o de escritorio. El audio debe pasar a través del sistema de sonido de la PC, por lo que normalmente necesitan un auricular que funcione bien con las aplicaciones de telefonía. Más recientemente, las aplicaciones de softphone se han diseñado para teléfonos inteligentes que le permiten conectarse a otras redes que no sean sólo la red celular. La interfaz del softphone suele parecerse a un teléfono físico, pero esto no es necesario. [10]

Los Softphones resuelven el problema de la portabilidad al ser instalados en un dispositivo que es probable que ya se mueve con usted, como su ordenador portátil o teléfono inteligente. Además, su costo es mínimo (por lo general libre, o en un rango de precio de \$ 30 por paquete). Asimismo, los softphones son sólo software, fáciles de instalar y actualizar, y suelen tener características que funcionan mediante periféricos, como una cámara web para video llamada.

Algunas de las desventajas de los softphones, es la necesidad de mantener los dispositivos encendidos, también la utilización de un auricular cada vez que se toma una llamada y el hecho de que muchos PCs de forma aleatoria, durante el día, deciden hacer algo distinto de lo que el usuario quiere que hagan, por lo que podrían provocar que el softphone dejase de trabajar mientras que algunos programas realizan tareas de fondo del CPU.

Entre los softphone más populares se pueden encontrar los siguientes:

- **X-lite:** Combina las funcionalidades de llamadas de voz y video con mensajería instantánea. Asimismo, puede ser usado tanto en Windows como en Linux. Está basado en el protocolo SIP y soporta distintos tipos de codec como: G .711, GSM, Speex, entre otros.
- **Zoiper:** Se puede conseguir gratuitamente y es compatible con la mayoría de sistemas operativos de Smartphone (iOS, Android, Windows Mobile); es fácil de usar y configurar.
- **Sjphone:** es un software libre disponible en Windows, Linux y Mac. Soporta tanto H.323 como SIP. Admite múltiples configuraciones y diferentes codecs tales como: G.711a, G.711u, GSM y iLBC.

- **Qutecom:** Anteriormente conocido como WengoPhone, QuteCom es un software libre, desarrollado inicialmente por Wengo. Es compatible con SIP y soporta una amplia gama de codecs de VoIP, incluyendo G.729, G.711, iLBC, G.722 y Speex.
- **3CX:** Disponible para Windows, Iphone y Android. Válido para protocolo SIP y para codecs G.711a, G.711u y GSM.

2.1.2.6.2 Teléfono IP

Es un dispositivo físico que se observa como un teléfono de oficina, tiene un auricular, botones numerados, pero además se conecta directamente a la red. Usualmente también es llamado teléfono VoIP , teléfono SIP o hardphone.

Los Hardphones tienen la ventaja de que los teléfonos tienen buenas propiedades acústicas para las comunicaciones de voz. Cualquier teléfono de buena calidad está diseñado para recoger las frecuencias de la voz humana, filtrar el ruido de fondo no deseado y normalizar la forma de onda resultante. Al mismo tiempo, un hardphone no requiere de un computador para estar funcionando todo el tiempo.

Pero, las desventajas de los teléfonos IP, es que son costosos y no portátiles, en relación a los distintos softphones de calidad que se encuentran hoy en el mercado, los cuales están disponibles de forma gratuita.

2.2 Asterisk

2.2.1 Definición

Es un software libre que emula el comportamiento y las funciones de una central telefónica o PBX. Asterisk es desarrollado por la empresa Digium, la cual invierte en el desarrollo del código fuente y en el hardware de telefonía de bajo costo, que opera en conjunto con Asterisk. Este software funciona en el ambiente Linux y permite conectividad en tiempo real entre la PSTN y redes VoIP. [11]

Asterisk es capaz de convertir una computadora en un servidor de comunicaciones, proveyéndolo de un sistema IP PBX, puertas de enlace VoIP, servidores de conferencias, entre otros. Es usado ampliamente por pequeñas y medianas empresas, multinacionales, call centers, compañías de telecomunicaciones, gobiernos alrededor del mundo y todo aquel aficionado que disponga de tiempo para experimentar con él. [12]

2.2.2 Características

- **IP PBX:** la principal característica de Asterisk es funcionar como IP PBX. Soporta interfaces para conectar a líneas internas y externas, tales como: PSTN, E1, T1, ISDN, etc. Además de todas las funcionalidades estándares de los PBXs, música y llamada en espera, direccionamiento de llamadas, entre otros.

- **Voice Over IP:** permite enviar voz a través de una red no orientada a la conexión utilizando el protocolo de Internet (IP).
- **Advanced Call Distribution:** puede recibir una llamada telefónica, identificar sus atributos y hacer decisiones de ruteo basándose en sus características. Una vez que se decide cómo rutear la llamada, se puede enviar a una extensión o a un grupo de ellas, grabar la llamada, enviar a un voicemail, entre otras.
- **Call Detail Records:** almacena los detalles de las llamadas, mediante archivos de texto plano o motores de base de datos. Con esta información es posible hacer una auditoria de quien realizó la llamada, cuánto tiempo duro, etc.
- **Call recording:** permite grabar las conversaciones que ocurren a través del IP PBX, por lo que se puede saber el contenido de las conversaciones.
- **Text to Speech:** es una tecnología que convierte un texto en sonidos de lenguaje natural, se puede utilizar junto con IVR.

- **Interactive Voice Response:** es un sistema que permite ofrecer servicios interactivos utilizando Asterisk, el cliente llama y encuentra archivos que reproducen instrucciones, también el sistema puede leer comandos o textos de entrada y en base a los comandos obtener información de una base de datos y reproducirlos utilizando TTS.
- **Voice Mail:** tiene incluido un sistema de correo de voz que permite que una persona deje un mensaje, adicionalmente soporta diferentes zonas de tiempo y notificación a los usuarios vía mail.
- **Call Queues:** permite administrar múltiples colas para atender llamadas.
- **Call Parking:** o llamada en espera es un tipo de servicio relacionado con las colas de llamadas; si hay una llamada en espera, el sistema permite al usuario administrar si quiere o no atender la llamada.
- **Conference Rooms:** soporta el uso de canales de conferencias. Éstos pueden ser públicos o privados, silenciados por un administrador y creados estática o dinámicamente.

- **Asterisk Gateway Interface:** AGI es un método estándar mediante el cual programas externos pueden interactuar con Asterisk. Hay interfaces para diferentes lenguajes de programación, entre ellos Python, Java, PHP, Perl, C#.

2.2.3 Distribuciones basadas en Asterisk

Instalar Asterisk es un proceso laborioso que requiere mucho cuidado y un buen manejo básico de GNU/Linux para compilarlo. Afortunadamente existen distribuciones pre compiladas de Asterisk, que contienen una interfaz web que facilita su instalación, configuración y administración. Algunas de las distribuciones existentes son:

AsteriskNOW permite instalar Asterisk y comenzar a crear aplicaciones telefónicas inmediatamente. Lo logra instalando una distribución GNU/Linux completa con CentOS, Asterisk, los drivers DAHDi y la FreePBX como interfaz administrativa si se desea. La complejidad de Asterisk y Linux es manejada por el instalador y la interfaz administrativa, lo que permite una mayor atención en crear las soluciones de telefonía.

Trixbbox Community Edition tiene sus inicios en el año 2004 cuando era conocido como Asterisk@Home. Desde entonces ha ido ganando terreno como una de las distribuciones más populares de Asterisk con un promedio de 65,000 descargas por mes. Trixbbox es conocido por su flexibilidad para satisfacer las necesidades de desarrollos personalizados del sistema.

FreeSWITCH es una plataforma de telefonía de código abierto, escalable y multiplataforma diseñada para enrutar e interconectar protocolos de comunicación usando audio, vídeo, texto o cualquier otro formato multimedia. Desde 2006 vino a competir contra opciones propietarias. También provee una plataforma estable de telefonía, en donde las aplicaciones telefónicas pueden ser desarrolladas bajo una amplia gama de herramientas libres.

Elastix es un software de código abierto para el establecimiento de comunicaciones unificadas. Pensando en este concepto el objetivo de Elastix es el de incorporar en una única solución todos los medios y alternativas de comunicación existentes en el ámbito empresarial. El proyecto Elastix se inició como una interfaz de reporte para llamadas de Asterisk y fue liberado en Marzo del 2006. Posteriormente el proyecto evolucionó hasta convertirse en una distribución basada en Asterisk.

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Propuesta de un diseño operativo de un servicio de VoIP

La propuesta de un servicio de VoIP se genera por la necesidad de la empresa Supra- Caracas de ofrecer a sus empleados una red con la capacidad de intercambiar datos y voz, con el objetivo de optimizar el desempeño de sus trabajadores.

Por lo tanto en la presente sección, se abarcarán los puntos necesarios para la estructuración y definición de la propuesta de servicio de voz sobre IP; enmarcados en la topología, los requerimientos, el software, entre otros.

3.1.1 Requerimientos

Luego de haber definido la estructura y el dimensionamiento de la empresa expuesta en los Anexos N° 2, es necesario comprender cada uno de los

requerimientos que presenta la compañía, a fin de realizar una propuesta acorde a las necesidades de la misma.

Para la determinación con claridad y exactitud de los requerimientos de la empresa se realizó una reunión con la Gerencia de Tecnologías de la Información, donde se establecieron cada uno de los puntos que se requieren, los cuales son presentados a continuación:

- Instalar un servidor de pruebas, donde se realicen tests para verificar el funcionamiento de un servicio de VoIP, sobre la red LAN de Supra Caracas las Mayas.
- Utilizar solamente software's libres o en su defecto gratis que sea compatible tanto con Linux como con Windows.
- Proveer de las configuraciones necesarias tanto al servidor como a la red, para una posible puesta en marcha del servicio de VoIP.

3.1.2 Topología

En esta sección se explicará cómo se encontrará distribuido el servicio de voz sobre IP en la red de Supra Caracas. En donde, se propone instalar un servidor de VoIP en el núcleo de los servicios de la red.

Cabe citar al Trabajo Especial de Grado de Bazán O. (2012), donde señala que:

El nodo central estará ubicado en la sede Las Mayas, desde el cual se pueda administrar toda la red. La elección de ésta sede como nodo central se debe a que la mayor cantidad del personal administrativo de la empresa opera en esta localidad, en consecuencia el grueso de los procesos se desarrollan en la misma: pagos, compras, despachos de camiones, control de operaciones, etc. Además, esta sede cuenta con el espacio físico para la instalación del centro de datos de la red.

En la orientación de lo antes expuesto, otras de las razones de proponer un solo servidor en la sede de las Mayas, es la cantidad de usuarios que se encuentra en cada una de las demás localidades. Tanto en las Artigas como en la Yaguara y Zona Rental la población de usuarios para el servicio de voz sobre IP no supera a los 20 clientes por sede y aunque se estima un crecimiento del 20% no se justifica el uso de un servidor local para cada área.

Por otra parte, tomando como base la propuesta de Bazán O. (2012), a continuación se describirá cómo ha de estar distribuido en la red WAN el servicio de VoIP.

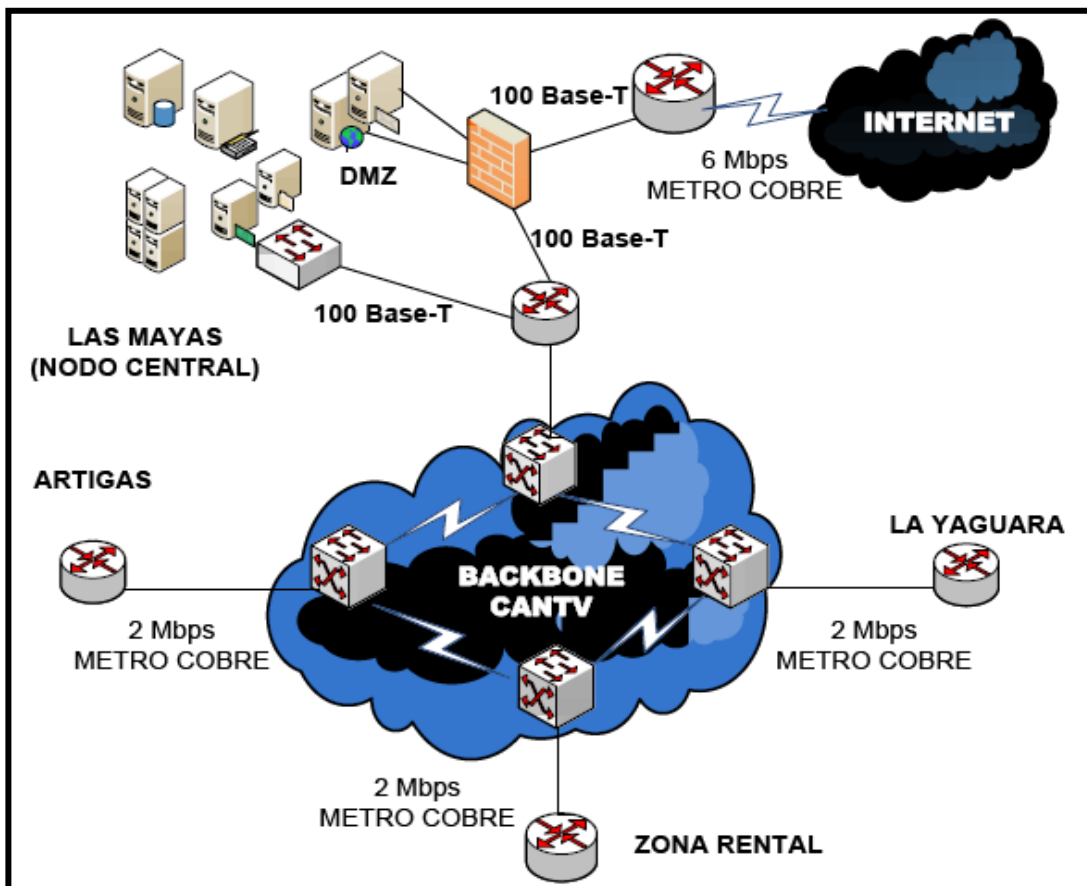


Figura 4. Topología Física WAN

Fuente: (Bazán, 2012, pág. 86)

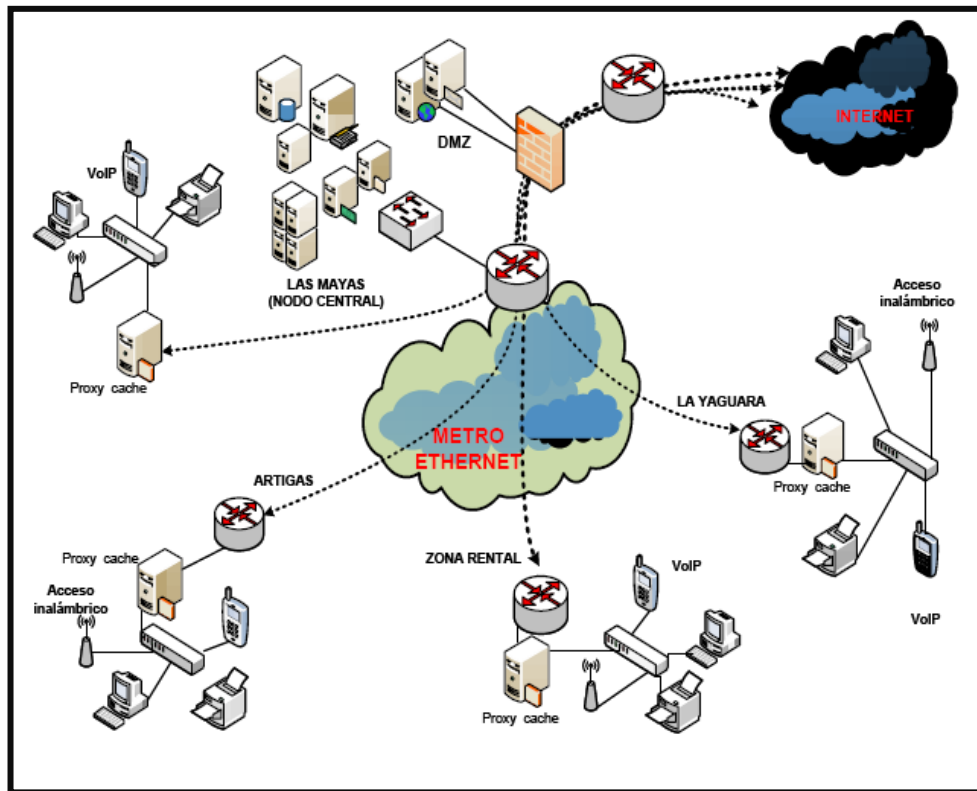


Figura 5. Topología lógica WAN

Fuente:(Bazán, 2012, pág. 85)

Luego de observar las topologías física y lógica de la red WAN perteneciente a la empresa, se propone colocar el servidor con el servicio de VoIP detrás del switch perteneciente al nodo central las Mayas, es el lugar ideal para que todas las sedes tengan acceso a él y además al ser este servicio solamente para las redes locales de la compañía y no para usuarios provenientes de otras redes, no existe la necesidad de colocarlo en la DMZ.

3.1.3 Software

Acatando lo dispuesto en la Gaceta oficial N° 38.095 de fecha 28/ 12/ 2004, la cual señala en su artículo primero lo siguiente:

Artículo 1. La Administración Pública Nacional empleará prioritariamente Software Libre desarrollado con Estándares Abiertos, en sus sistemas, proyectos y servicios informáticos. A tales fines, todos los órganos y entes de la Administración Pública Nacional iniciarán los procesos de migración gradual y progresiva de éstos hacia el Software Libre desarrollado con Estándares Abiertos.

Para esta propuesta se recurrirá, en su mayoría a distribuciones de software libre o en su defecto a software gratis que sean compatibles tanto con Linux como con Windows, ayudando así a la migración hacia los Software libres.

3.1.3.1 Servidor

Debido a la complejidad y necesidad de tener un amplio conocimiento del ambiente Linux para compilar Asterisk. Se propone utilizar un servidor basado en una distribución pre compilada de Asterisk llamada Elastix.

Elastix es una de las distribuciones más fáciles de usar y con mayor soporte en la red, asimismo su concepto de comunicaciones unificadas es simplemente atrayente, ya que puede abrir un abanico de opciones a más posibilidades de

comunicación y no solamente a voz sobre IP. Entre estas opciones, se pueden encontrar servidores de mensajería instantánea, de correo y de fax.

IP PBX como una función de Elastix introduce una interfaz gráfica web, la cual permite realizar todas las configuraciones de Asterisk por medio de ésta. Sin embargo, aun se puede acceder a la consola de Asterisk y configurar todo por medio de comandos.

3.1.3.2 Softphone

En este tópico se abarcan tres grandes grupos como lo son: usuarios en ambiente Linux, usuarios en ambiente Windows y por último usuarios a través de dispositivos móviles como celulares y tabletas.

En Supra Caracas, todos los dispositivos que se encuentran en ambiente Linux operan a través de la distribución Ubuntu 12.04.2. Para esta distribución se recomienda utilizar softphone tales como: SJphone, Qutecom y Zoiper. Este último posee la ventaja de ser uno de los pocos que puede funcionar con el protocolo IAX, lo cual es de gran ayuda a la hora de realizar pruebas con dicho protocolo.

Por otro parte, los usuarios del sistema operativo Windows, aunque sean pocos y se pretenda una migración total hacia Ubuntu, se les recomienda el uso de X-lite, Zoiper y 3CX. Cabe destacar que todos estos softphones son gratis, aunque poseen versiones no gratuitas, las cuales habilitan más opciones.

Por último, para los usuarios móviles existen softphones compatibles con Android, iOS, Windows phone tales como: Zoiper, 3CX, Nimbuzz, entre otros. Todas estas aplicaciones son compatibles con SIP, y en algunos casos no hacen falta ya que el mismo celular posee una opción para configuración de teléfonos SIP.

3.1.4 Codec

Este es un aspecto importante, ya que se verá reflejado tanto en la calidad de la voz, como en ancho de banda utilizado en la llamada. Para esta propuesta se decidió utilizar uno de los codecs más usado, el cual es llamado G. 711.

El principal motivo de esta elección, es que el codec G. 711 ofrece una excelente calidad de voz ya que prácticamente no la comprime, por otra parte éste ya viene habilitado en Asterisk y de igual manera en Elastix, por lo que no se necesita pagar por él, lo cual se traduce en un ahorro para la empresa. No obstante, G.711 posee una desventaja, ya que ocupa un ancho de banda considerable, lo que es poco recomendado para conexiones de ancho de banda.

3.1.4.1 Determinación del ancho de banda

Ya habiendo seleccionado el codec a utilizar, es preciso analizar cuanto será la tasa de transferencia por cada llamada. En consecuencia, se presentará la estructura básica de la trama de VoIP en una red LAN, que posee en general un

verificador de secuencia o FCS, la carga útil y 4 cabeceras que dependen de los protocolos o estándares que se utilicen.

Ethernet	IP	UDP	RTP	PAYLOAD	FCS
14 bytes	20 bytes	8 bytes	12 bytes	bytes depende del codec	2 bytes

Figura 6. Trama de VoIP

Fuente: “De elaboración propia”

Cabe destacar, que el encapsulado de la trama puede variar según sea su enlace, puede ocurrir que el enlace sea de una red WAN y en este caso se podría encapsular la trama con el protocolo PPP, cuya arquitectura está precisamente diseñada para la transmisión a través de enlaces WAN. Entendiendo que en el caso de Supra Caracas no se aplica

Para el cálculo del ancho de banda que es necesario para la comunicación en un solo sentido, se realiza utilizando la siguiente ecuación:

$$AB = AB_{codec} * \frac{\text{Longitud de encapsulacion} + \text{Longitud de carga útil}}{\text{Longitud de carga útil}} \quad (1)$$

Ecuación 1. Cálculo del ancho de banda para VoIP

A continuación, se describirán las variables de la ecuación donde:

- AB = Ancho de banda necesario para transmitir la voz.
- AB_{codec} = Ancho de banda del codec.
- $Longitud\ de\ carga\ útil$ = Longitud del payload.
- $Longitud\ de\ encapsulacion$ = Longitud de bits adicionales al payload debido a la encapsulación.

Por consiguiente, la longitud de la encapsulación de una trama LAN se obtiene de la siguiente manera:

- Cuatro Cabeceras Ethernet, IP, UDP y RTP: 14 bytes + 20 bytes + 8 bytes + 12 bytes = 54 bytes.
- FCS: 2 bytes.
- Para un total de 56 Bytes

Luego para el cálculo de la Longitud de carga útil es necesario, observar la Ecuación 2.

$$Longitud\ de\ carga\ útil = AB_{código} * Rt \quad (2)$$

Ecuación 2. Longitud de carga útil

La variable RT señalada en la Ecuación 2, es llamada retardo de encapsulamiento. Éste se encuentra definido en el RFC 1890, el cual especifica que el retardo de encapsulamiento por defecto debería ser de 20 ms.

Ya conociendo Rt y el codec a utilizar, se puede reemplazar los valores en la ecuación y obtendremos lo siguiente:

$$Longitud\ carga\ útil = 64000 \frac{bits}{seg} * 20 * 10^{-3} seg = 1280\ bits \quad (3)$$

$$Longitud\ carga\ útil = 1280\ bits * \frac{1\ byte}{8\ bits} = 160\ bytes \quad (4)$$

Luego se reemplaza los valores de longitud de carga, longitud de encapsulamiento y el ancho de banda en la Ecuación 1, para obtener el ancho de banda total.

$$AB = 64 \frac{kbits}{seg} * \frac{56\ bytes + 160\ bytes}{160\ bytes} = 86.4 \frac{kbits}{seg} \quad (5)$$

Es importante hacer notar, que éste ancho de banda es solamente para un flujo de voz en una red LAN utilizando el códec G.711, si se desea calcular el ancho de banda en otro tipo de red o con otro codec será necesario repetir los cálculos detallando las nuevas consideraciones.

3.1.5 Protocolo de señalización

Aunque en el Capítulo II se había comentado que IAX fue creado para solventar algunos problemas experimentados en SIP. Es momento de hacer una comparación para dirimir cual protocolo es mejor.

En lo que se refiere a ancho de banda, IAX utiliza un menor ancho de banda que SIP ya que los mensajes son codificados de forma binaria mientras que en SIP son mensajes de texto.

Por otra parte, en IAX la señalización y los datos viajan conjuntamente con lo cual se evitan los problemas de NAT que frecuentemente aparecen en SIP. En este último, la señalización y los datos viajan de manera separada y por eso aparecen problemas de NAT cuando el flujo voz debe superar los routers y firewalls.

En SIP el flujo RTP puede viajar de extremo a extremo sin la necesidad de pasar por el servidor de señalización de control. Por el contrario, en IAX debido a que la señalización y los datos viajan de forma conjunta, todo el tráfico de audio debe pasar obligatoriamente por el servidor IAX. Esto conlleva a un aumento en el uso del

ancho de banda que deben soportar los servidores, sobre todo cuando hay una gran cantidad de llamadas simultáneas.

Cabe destacar, que IAX2 es un protocolo pensado para la transmisión de video y voz sobre IP. Adicionalmente, presenta funcionalidades donde se destaca la posibilidad de enviar o recibir planes de marcado (dialplans) que resultan útiles al usarlo conjuntamente con servidores Asterisk. En cambio, SIP es un protocolo de propósito general y podría transmitir sin dificultad cualquier información y no sólo audio o video, esto lo hace más escalable que IAX, ya que éste se ve limitado sólo a transmisión de audio y video.

La decisión de asumir cuál de los dos protocolos se adecua más a las necesidades de la empresa, está basada en una de las características de SIP, la cual sostiene que este es un protocolo en estatus “Proposed Standard” por la IETF y debido a su aplicación en el tiempo, es ampliamente implementado por todos los fabricantes de equipos y software. Todo lo contrario de IAX2, el cual posee recientemente un estatus “informational”, expuesto en su RFC 5456. En consecuencia no se encuentra en una amplia gama de dispositivos existentes en el mercado.

Con la elección de SIP se busca tener un abanico más grande de opciones a la hora de elegir que softphone o Teléfono IP se desea proponer, además de contar con la seguridad de ser un protocolo en estatus “Proposed Standard”.

3.1.6 Usuarios

3.1.6.1 Perfiles

La creación de los perfiles, permite al administrador de la red la posibilidad de hacer un seguimiento a cada usuario, con el objetivo de obtener datos tales como número de llamadas y duración de las mismas, que servirán de base para la posible implementación de servidores de correo y Fax.

Estos perfiles comprenderán los datos como el nombre del usuario, login, contraseña, extensión y grupo al cual pertenece. Cabe destacar, que solamente pertenecerán al grupo de administradores los usuarios adscritos a la Gerencia de Tecnologías de la Información, los demás usuarios estarán catalogados en el grupo de extensiones, por lo cual no tendrán ningún permiso para modificar las características del servidor. Sin embargo, podrán acceder a opciones con el objeto de habilitar la llamada en espera, colocarse en estatus no disponible, entre otros.

3.1.6.2 Extensiones

Representan los números a los cuales se debe discar para comunicarse con otros usuarios. En la presente propuesta se plantea linkear los perfiles de usuarios con las extensiones, identificando a que departamento y sede pertenecen. A continuación se presentará una tabla, describiendo cómo deberá repartirse las extensiones conforme a las áreas señaladas.

Tabla 1. Extensiones

Fuente: “De elaboración propia”

Departamentos	Las Mayas	Las Artigas	La Yaguara	Zona Rental
Gerencia de Tecnologías de la Información	001 al 099			
Gerencia General	101 al 199			
Recursos Humanos	201 al 299			
Bienestar Social	301 al 399			
Compras	401 al 499			
Nómina	501 al 599		3001 al 3099	
Consultoría Jurídica	601 al 699			
Servicios Generales	701 al 799			
Seguridad	801 al 899		3101 al 3019	
Operaciones	901 al 999		3201 al 3299	
Registro y Control	1001 al 1099			
Auditoría y procesos	1101 al 1199			
Taller		2000 al 2099	3301 al 3399	
Almacén			3401 al 3499	
Ambiente		2100 al 2199		
Bio infecciosos		2201 al 2299		
Recaudación				4001 al 4099

3.1.7 Hardware

La elección de un hardware para implementar un servicio de VoIP, no es una ciencia exacta depende en gran medida de los requisitos y de las características con las que se desea ejecutar el servicio.

Como primer paso, se necesita cumplir con los requerimientos básicos del sistema operativo que funcionará en el servidor. Para esta propuesta, el sistema operativo a utilizar es una distribución de Linux llamada CentOS 5.9, ya que ésta viene integrada con Elastix.

Entre los requisitos mínimos de CentOS se identifican una memoria RAM de 64 MB, un espacio en disco duro de 1024 MB y un procesador de arquitectura i386 ó x86_64. Sin embargo estos requisitos hoy en día son ampliamente superados por cualquier ordenador, por lo cual para obtener una mejor idea de cuál es el hardware necesario se debe tener en cuenta las siguientes consideraciones:

- **Cantidad de extensiones y tipo:** como se expresa en los Anexos N° 2 (Tabla 2-1), se pretende tener un aproximado de 60 extensiones SIP, cabe destacar que debido a que solamente se propone tener un servicio que ofrezca realizar llamadas en la red de Supra Caracas y no uno que incluya usar líneas de teléfono convencionales (analógicas o digitales). No se necesitará tarjetas especiales o gateways ya que estos proporcionan conectividad hacia las redes de telefonías tradicionales (analógicas, BRI, PRI y GSM).
- **Número de llamadas simultáneas:** se pretende ofrecer un 50% del total posible en llamadas, lo que se traduce en 15 llamadas simultáneas.

- **Ratio de llamadas:** esta consideración se encuentra ligada a la anterior , por lo que se pretende un promedio de 5 llamadas por cada 20 usuarios

- **Codecs a utilizar:** como se propuso anteriormente solo se utilizará el codec G.711, esto es una ventaja para el rendimiento de un servidor de VoIP, ya que el codec G.711 casi no comprime el audio por lo cual no requiere tanta utilización de la memoria RAM. Por otra parte, al sólo utilizar un codec para toda la red no se necesitará aplicar transcoding. La práctica de este proceso merma en un 60% el número total de llamadas simultáneas en los servidores que utilicen Asterisk.

Luego de entender las variables que condicionan al servidor Elastix se propone un Server Quad Core o Dual Dual Core de 2GB a 4GB de memoria RAM. Además, de un disco duro no menor a 500 GB. Se podría pensar que estas especificaciones son un poco exageradas y más teniendo en cuenta que Asterisk ha logrado más de 350 llamadas simultáneas utilizando el codec G.711 y sin transcodificación con un procesador Pentium 4 y 1 GB de RAM. [13]

Sin embargo, pensando en que Elastix puede ofrecer mucho más que un servicio de VoIP y considerando que las computadoras promedio actuales poseen esas especificaciones, no cabe la menor duda que un servidor con tales características cumpliría con los requerimientos de la empresa.

CAPÍTULO IV

PRUEBAS Y RESULTADOS

4.1 Objetivo General

Comprobar la correcta operatividad de la propuesta de servicio de VoIP, así como también, verificar la compatibilidad y funcionamiento de los protocolos, programas y equipos que interactúen con el servidor y hagan posible la comunicación.

4.2 Escenarios de prueba

Para la realización de las siguientes pruebas, se optó por 3 topologías de ensayo distintas, que escenificarán tres posibles ambientes para un servicio de VoIP. La primera consiste en un ambiente controlado conformado por 2 terminales un router y el servidor Elastix, el esquema de este escenario se puede observar en la Figura 7.

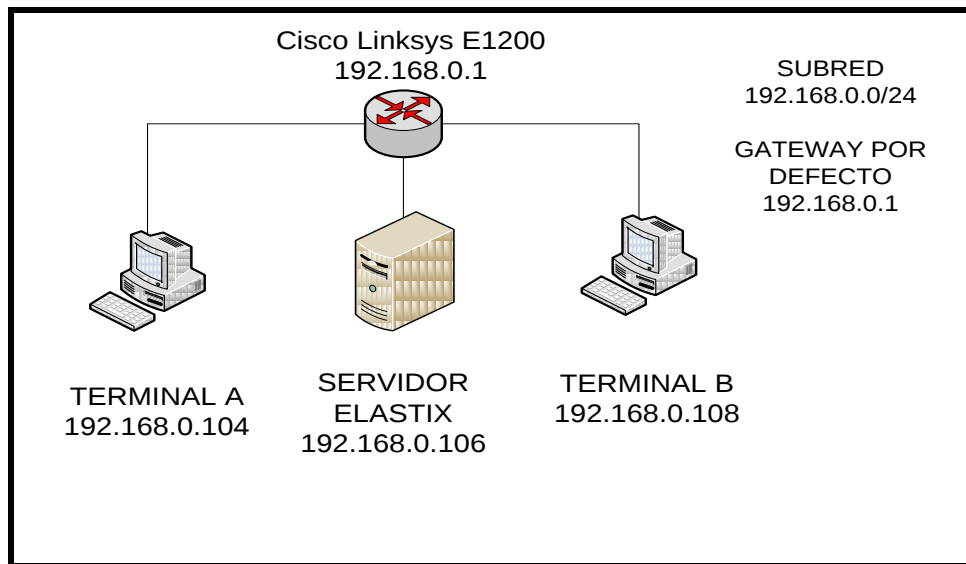


Figura 7. Escenario 1

Fuente: “De elaboración propia”

Por otro parte, la segunda topología se refiere la red de Supra las Mayas, en este escenario se estará en presencia del retardo y el tráfico producido por la red, por lo que dará una idea real de cómo sería el comportamiento de un servicio de voz sobre IP en la empresa. En la Figura 8 a continuación se describe este escenario

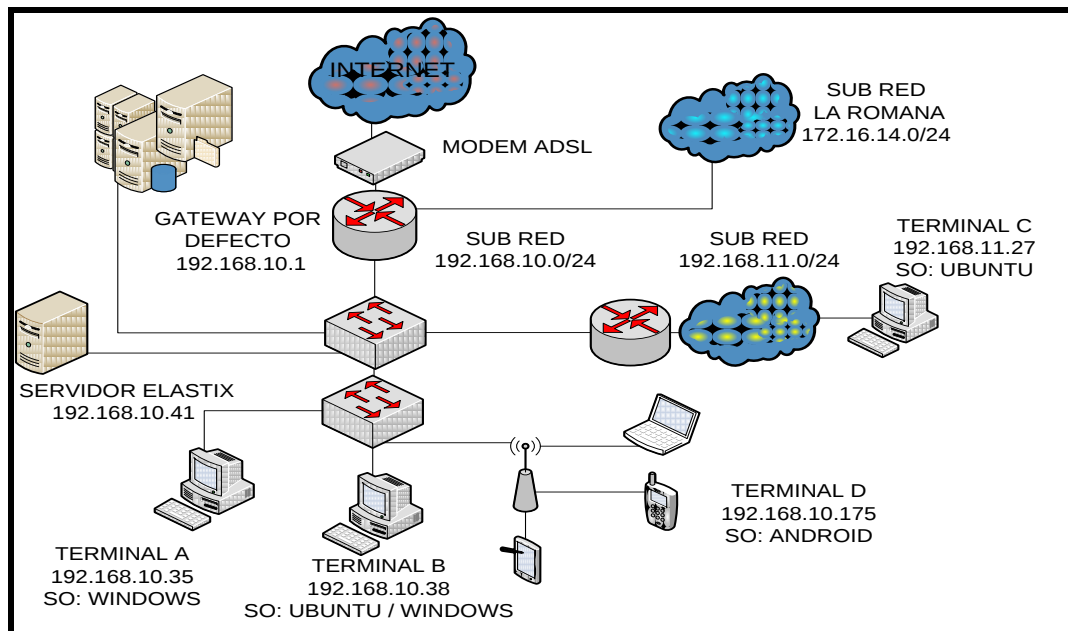


Figura 8. Escenario 2

Fuente: “De elaboración propia”

Por último, la tercera topología se puede observar en la Figura 9. Aquí se representa una comunicación por medio de una VPN que actualmente posee la compañía, en este sentido se decidió llevar a cabo unas pruebas con la finalidad de comprobar la factibilidad de realizar una llamada de voz sobre IP mediante la VPN

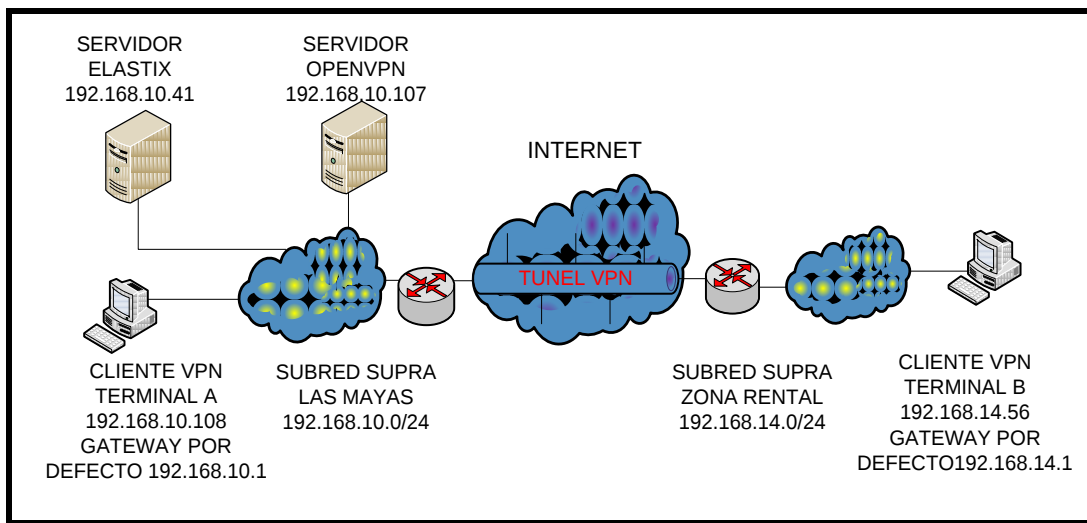


Figura 9. Escenario 3

Fuente: “De elaboración propia”

4.3 Listado de pruebas

4.3.1 Medición del retardo y pérdida de paquetes en la red

En este test, se utilizó el escenario número 2 para comprobar cuánto es el retardo y la pérdida de paquetes en la sub red de Supra Las Mayas.

4.3.1.1 Procedimientos

1. Se procedió a utilizar el terminal A descrito en la figura 8 perteneciente a la red 192.168.10.0/24 y con dirección IP 192.168.10.35.

2. Seguidamente, se ejecutó la Consola de Windows en el Terminal A.
3. Se escribió el siguiente comando “PING 192.168.10.1 -n 100”. Cabe destacar, que con este comando se está enviando 100 solicitudes de eco al Gateway por defecto de la Red Supra Las Mayas, cuya dirección es 192.168.10.1 y se encuentra en la red 192.168.10.0/24 señalada en la figura 8.
4. Luego, el resultado fue copiado en un block de notas para su posterior análisis.
5. Para finalizar, estos procedimientos se realizaron tres veces, en diferentes horas del día (9:00 AM ,12:00 PM y 15:00 PM). Con el fin de estar en presencia de distintos volúmenes de tráfico en la red.

4.3.1.2 Resultados

El resultado esperado para esta prueba, es de obtener un retardo en los paquetes menor a 150 ms y una pérdida de paquetes no mayor al 1% .A continuación se presentarán los resultados obtenidos mediante el comando PING para 3 distintas horas del día.

Estadísticas de ping para 192.168.10.1:
Paquetes: enviados = 100, recibidos = 100, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 1ms, Máximo = 45ms, Media = 3ms

Figura 10. PING Test 9:00 Am

Fuente: “De elaboración propia”

Estadísticas de ping para 192.168.10.1:
Paquetes: enviados = 100, recibidos = 99, perdidos = 1
(1% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 120ms, Media = 4ms

Figura 11. PING Test 12:00 Pm

Fuente: “De elaboración propia”

Estadísticas de ping para 192.168.10.1:
Paquetes: enviados = 100, recibidos = 100, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 1ms, Máximo = 193ms, Media = 7ms

Figura 12. PING Test 15:00 Pm

Fuente: “De elaboración propia”

4.3.2 Verificación de la conectividad entre una PC y el Servidor Elastix

Esta prueba se realizó con el objetivo de comprobar si los dispositivos de la subred Supra Las Mayas podían observar la presencia del Servidor Elastix en la red.

Por esta razón, el experimento se realizó en el escenario de pruebas 2 tipificado en la figura 8.

4.3.2.1 Procedimientos

1. Se anexó el servidor Elastix a la subred 192.168.10.0/24 de Supra Las Mayas, con una dirección IP 192.168.10.41 y un gateway por defecto de dirección 192.168.10.1, como se muestra en la figura 8.
2. Luego, se seleccionó el terminal B de dirección IP 192.168.10.38 perteneciente a la sub red 192.168.10.0/24, expuesta en la figura 8, y se accedió al terminal de Ubuntu.
3. Se procedió a ejecutar el siguiente comando “PING 192.168.10.41 -c20”.Con el propósito de hacer una solicitud de eco al servidor Elastix previamente instalado en la subred 192.168.10.0/24.
4. Se capturaron los resultados para posterior análisis.
5. Adicionalmente, se seleccionó el terminal C de dirección IP 192.168.11.27 correspondiente a la subred 192.168.11.0/24, como se señala en la figura 8, y se accedió al terminal de Ubuntu.
6. Posteriormente, se ejecutó el siguiente comando “PING 192.168.10.41 -c20”.Con la intención de comprobar, si se puede establecer una conexión al servidor Elastix desde otra subred perteneciente a la red de Supra Las Mayas.

7. Por último, se recolectaron los datos obtenidos.

4.3.2.2 Resultados

```
administrador@A000279426supra:~$ ping 192.168.10.41 -c20
PING 192.168.10.41 (192.168.10.41) 56(84) bytes of data.
64 bytes from 192.168.10.41: icmp_req=1 ttl=64 time=1.48 ms
64 bytes from 192.168.10.41: icmp_req=2 ttl=64 time=2.39 ms
64 bytes from 192.168.10.41: icmp_req=3 ttl=64 time=1.50 ms
.
.
64 bytes from 192.168.10.41: icmp_req=18 ttl=64 time=1.46 ms
64 bytes from 192.168.10.41: icmp_req=19 ttl=64 time=3.94 ms
64 bytes from 192.168.10.41: icmp_req=20 ttl=64 time=1.73 ms
--- 192.168.10.41 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19029ms
rtt min/avg/max/mdev = 1.400/2.018/5.383/0.969 ms
```

Figura 13. Verificación de conectividad desde la red 192.168.10.0/24

Fuente: “De elaboración propia”

```
administrador@A000275826supra:~$ ping 192.168.10.41 -c20
PING 192.168.10.41 (192.168.10.41) 56(84) bytes of data.
64 bytes from 192.168.10.41: icmp_req=1 ttl=64 time=1.50 ms
64 bytes from 192.168.10.41: icmp_req=2 ttl=64 time=1.44 ms
64 bytes from 192.168.10.41: icmp_req=3 ttl=64 time=1.48 ms
.
.
64 bytes from 192.168.10.41: icmp_req=18 ttl=64 time=2.35 ms
64 bytes from 192.168.10.41: icmp_req=19 ttl=64 time=1.47 ms
64 bytes from 192.168.10.41: icmp_req=20 ttl=64 time=1.49 ms
--- 192.168.10.41 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19030ms
rtt min/avg/max/mdev = 1.437/2.127/7.724/1.386 ms
```

Figura 14. Verificación de conectividad desde la red 192.168.11.0/24

Fuente: “De elaboración propia”

4.3.3 Registro de una extensión mediante Elastix

En esta prueba, se pudo comprobar si la creación de una extensión mediante la interfaz gráfica de Elastix, se traduce en algún cambio en la consola de Asterisk, por lo cual se estaría verificando si el servidor Elastix funciona correctamente. Cabe señalar, que para esta prueba se utilizó el escenario número 1, reseñado en la figura 7.

4.3.3.1 Procedimientos

1. Primeramente, se accedió al servidor Elastix de dirección IP 192.168.0.106 y dirección de subred 192.168.0.0/24, con la finalidad de ingresar a la consola de Asterisk mediante el comando “Asterisk-r”.
2. Después, se ejecutó el comando “SIP show peers”.
3. Se tomó un screenshot de la consola de Asterisk.
4. Luego, se creó una extensión SIP como se muestra en el apartado de Anexos N°3 (3.1.2) .Cabe destacar que la extensión se registró con el nombre “1001”
5. Para terminar, se repitió el paso número 3.

4.3.3.2 Resultados

Se espera que el comando “SIP show peers” muestre cómo se agregan los usuarios y su estado en la IPBX de Asterisk. Por tanto, a continuación se observa el resultado a través de la consola de Asterisk

```
[root@localhost ~]# asterisk -r
Verbosity is at least 3
localhost*CLI> sip show peers
Name/username      Host                               Dyn Forcerpor
t ACL Port        Status
0 sip peers [Monitored: 0 online, 0 offline Unmonitored: 0 online, 0 offline]
localhost*CLI> _
```

Figura 15. SIP show peers sin usuarios

Fuente: “De elaboración propia”

```
[root@localhost ~]# asterisk -r
Verbosity is at least 3
localhost*CLI> sip show peers
Name/username      Host                               Dyn Forcerpor
t ACL Port        Status
1001              (Unspecified)                   D    N
A 0              UNKNOWN
1 sip peers [Monitored: 0 online, 1 offline Unmonitored: 0 online, 0 offline]
-- Remote UNIX connection
-- Remote UNIX connection disconnected
localhost*CLI> _
```

Figura 16. SIP show peers con un usuario

Fuente: “De elaboración propia”

4.3.4 Comprobación del registro de un Softphone SIP

En este Test se utilizó el sniffer Wireshark y el softphone X-lite, para observar si se realiza el registro de los Softphone en el servidor Elastix, por medio de la consola de Asterisk y la interfaz Wireshark. Es importante señalar, que la prueba se llevó a cabo en el escenario 1, descrito en la figura número 7.

4.3.4.1 Procedimientos

1. Se creó una extensión para un Softphone SIP, como se especifica en el apartado Anexos N°3 (3.1.2). Esta extensión se identificó con el número “1000”
2. Seguidamente, se accedió al servidor Elastix expuesto en la figura 7, el cual posee una dirección IP 192.168.0.106 perteneciente a la subred 192.168.0.0/24. Para luego ingresar a la consola de Asterisk mediante el comando “Asterisk-r”.
3. Luego, se inició el sniffer en el terminal A señalado en la figura 7, se seleccionó la interfaz Ethernet de dirección IP 192.168.0.104 correspondiente a la subred 192.168.0.0/24 mediante la siguiente secuencia de configuraciones: Capture → Interface → Ethernet:192.168.0.104.
4. Se ejecutó la captura de paquetes mediante el comando Start y se filtró el tráfico SIP, gracias a la opción de Wireshark “Filter: SIP”.

5. Posteriormente, se configuró el softphone X-lite con una extensión previamente registrada, como se describe en la sección Anexos N° 3 (Figura 3-23).

6. Para finalizar, inmediatamente se observó el flujo de tráfico SIP mediante la siguiente línea pasos de opciones de Wireshark: statistics → Flow-Graph → Displayed packets - General Flow - Standard source / destination addresses → Ok. Se tomó un screenshot al resultado emitido por Wireshark y la consola de Asterisk.

4.3.4.2 Resultados

Se espera obtener un resultado, que describa un flujo de tráfico SIP referente al registro del Softphone, así como también un cambio en la consola de Asterisk que señale el registro por medio del Softphone

Time	192.168.0.104	192.168.0.106	Comment
7.579194000	(26994) Request: REGISTER s	(5060)	SIP: Request: REGISTER sip:192.168.0.106 (fetch bindings)
7.579608000	(26994) Status: 401 Unautho	(5060)	SIP: Status: 401 Unauthorized (0 bindings)
7.584751000	(26994) Request: REGISTER s	(5060)	SIP: Request: REGISTER sip:192.168.0.106 (fetch bindings)
7.585516000	(26994) Request: OPTIONS si	(5060)	SIP: Request: OPTIONS sip:1000@192.168.0.104:26994;rinstance
7.585665000	(26994) Status: 200 OK (	(5060)	SIP: Status: 200 OK (0 bindings)
7.591700000	(26994) Status: 200 OK	(5060)	SIP: Status: 200 OK
7.597792000	(26994) Request: SUBSCRIBE	(5060)	SIP: Request: SUBSCRIBE sip:1000@192.168.0.106
7.598227000	(26994) Status: 401 Unautho	(5060)	SIP: Status: 401 Unauthorized
7.606124000	(26994) Request: SUBSCRIBE	(5060)	SIP: Request: SUBSCRIBE sip:1000@192.168.0.106
7.606605000	(26994) Status: 200 OK	(5060)	SIP: Status: 200 OK
7.606791000	(26994) Request: NOTIFY sip	(5060)	SIP: Request: NOTIFY sip:1000@192.168.0.104:26994
7.632502000	(26994) Status: 200 OK	(5060)	SIP: Status: 200 OK

Figura 17. Captura del flujo SIP en el registro de un Softphone

Fuente: “De elaboración propia”

```
-- Registered SIP '1000' at 192.168.0.104:26994
localhost*CLI> sip show peers
Name/username      Host                               Dyn Forcerpor
t ACL Port      Status                               D  N
1000/1000          192.168.0.104                     D  N
  A 26994      OK (6 ms)
1 sip peers [Monitored: 1 online, 0 offline Unmonitored: 0 online, 0 offline]
```

Figura 18. Captura de pantalla de la consola de Asterisk

Fuente: “De elaboración propia”

4.3.5 Establecimiento y finalización de una llamada utilizando SIP

Esta prueba consiste en realizar una llamada entre 2 softphones ubicados en los terminales A y B, concernientes a la figura 8, y capturar el tráfico generado por los protocolos RTP y SIP. Se debe señalar, que esta prueba se llevó a cabo en el escenario 2, por lo que se tuvo que filtrar el flujo para, solamente, observar el establecimiento y finalización de la llamada.

4.3.5.1 Procedimientos

1. Se ejecutó el programa Wireshark en el terminal A de dirección IP 192.168.10.35 y en el terminal B de dirección IP 192.168.10.38, ambos pertenecientes a la subred 192.168.10.0/24 escenificada en la figura 8
2. Luego, se procedió a capturar el tráfico filtrando, solamente, los protocolos SIP y RTP. Esto se llevó a cabo mediante las siguientes secuencias de comandos en la pantalla principal de Wireshark.

Para capturar el tráfico en el Terminal A:

Capture → Interface → Ethernet: 192.168.10.35 → Start

Filtrado:

Filter: "SIP OR RTP"

Para capturar el tráfico en el Terminal B:

Capture → Interface → Ethernet: 192.168.10.38 → Start

Filtrado:

Filter: "SIP OR RTP"

3. Seguidamente, se utilizó 2 extensiones SIP previamente creadas ("1001" y "1003"), en el servidor Elastix identificado en la figura 8, y registradas mediante el softphone X.-lite. Para luego realizar una llamada entre el terminal A y B, durante 1 min.

Cabe destacar, que en esta prueba la extensión "1003" pertenece al terminal A y la nombrada "1001" concierne al terminal B. La llamada se realizó discando la extensión 1001 desde el software X- Lite del terminal A y se recibió la llamada en el Terminal B

4. Por último, se examinó el flujo del tráfico capturado, por medio de la siguiente sucesión de opciones en la interfaz principal de Wireshark:

Terminal A: Telephony → VoIP Calls → Initial speaker 192.168.10.35 ("1003" < sip:1003@192.168.10.41 < sip:1001@192.168.10.41) → Flow

Terminal B: Telephony → VoIP Calls → Initial speaker 192.168.10.41 ("Gregory Pasante" < sip:1003@192.168.10.41 < sip:1001@192.168.10.38:5060) → Flow

4.3.5.2 Resultados

El resultado deseado es obtener una llamada satisfactoria, donde el proceso de establecimiento y finalización sea similar al especificado en la sección SIP del capítulo II. A continuación se mostrará el resultado obtenido.

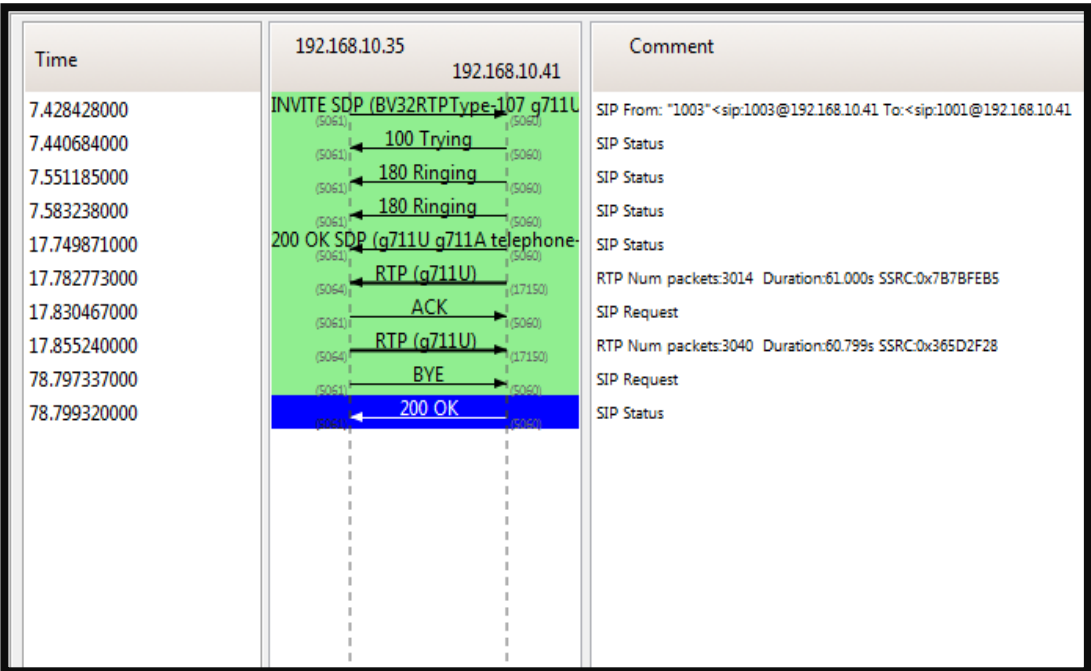


Figura 19. Comunicación entre el terminal A y el servidor

Fuente: “De elaboración propia”

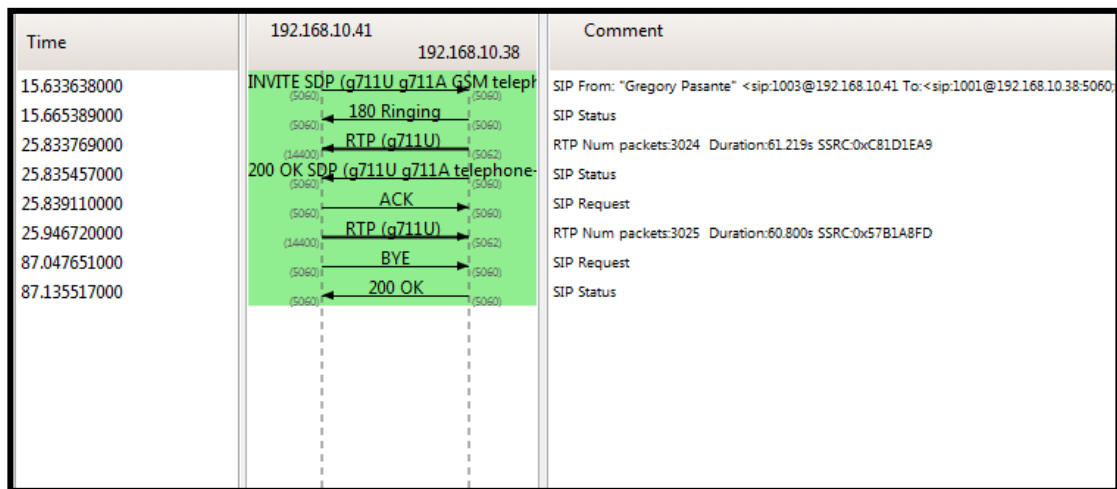


Figura 20. Comunicación entre el servidor y el terminal B

Fuente: “De elaboración propia”

4.3.6 Tasa de pérdidas de paquetes

Esta prueba se efectuó con la finalidad de simular una llamada en ambiente real, se realizó en el escenario de pruebas número 2 tipificado en la figura 8, en donde se buscó capturar los paquetes RTP para medir si se perdían o no durante la llamada

4.3.6.1 Procedimientos

1. Se inició el programa Wireshark en el terminal A de dirección IP 192.168.10.35 y en el terminal B de dirección IP 192.168.10.38, ambos pertenecientes a la subred 192.168.10.0/24 señalada en la figura 8.

2. Luego, se procedió a capturar el tráfico filtrando solamente el protocolo RTP. Seleccionando la siguiente serie de ítem de Wireshark que se muestran a continuación:

Para capturar el tráfico en el Terminal A:

Capture → Interface → Ethernet: 192.168.10.35 → Start

Filtrado:

Filter: “ RTP”

Para capturar el tráfico en el Terminal B:

Capture → Interface → Ethernet: 192.168.10.38 → start

Filtrado:

Filter: “RTP”

3. Seguidamente, se realizó una llamada desde el terminal A (extensión 1003) hacia el terminal B (extensión 1001), identificados en la figura 8.

4. Por último, se recolectó los datos arrojados por Wireshark en ambos terminales, por medio de la secuencia de opciones expuestas a continuación:

Para Terminal A y B: Telephony → RTP → show all stream

4.3.6.2 Resultados

El resultado esperado para esta prueba es que la tasa de pérdida de paquetes no supere el 1% total de paquetes enviados y recibidos. Es importante señalar, que la IP PBX de Asterisk funciona como intermediario del flujo RTP, en consecuencia todo tráfico RTP que se transmita entre dos terminales debe dirigirse primero al servidor Asterisk. Por esta razón, el resultado obtenido se presentará en 2 tramos .El primero comprenderá el flujo presente entre el terminal A y el servidor, y el segundo representa el tráfico existente entre el servidor y el terminal B

Tabla 2. Pérdidas de paquetes

Fuente: “De elaboración propia”

Tramo A: TERMINAL A (192.168.10.35) ↔ SERVIDOR (192.168.10.41)				
Sentido	Src IP addr	Dst IP addr	Packets	Lost
Forward	192.168.10..35	192.168.10.41	3040	0(0,0%)
Reverse	192.168.10.41	192.168.10..35	3014	0(0,0%)
Tramo B: SERVIDOR (192.168.10.41) ↔ TERMINAL B (192.168.10.35)				
Forward	192.168.10. 38	192.168.10.41	3024	0(0,0%)
Reverse	192.168.10.41	192.168.10.38	3025	7(0,2%)

4.3.7 Medición del Jitter

Al igual que la anterior prueba, se utilizó la topología 2 , señalada en la figura 8, y se capturó las estadísticas del tráfico RTP.

4.3.7.1 Procedimientos

1. Se inició el programa Wireshark en el terminal A de dirección IP 192.168.10.35 y en el terminal B de dirección IP 192.168.10.38, ambos pertenecientes a la subred 192.168.10.0/24 correspondiente a la figura 8.
2. Seguidamente, se procedió a capturar el tráfico de paquetes filtrando solamente el protocolo RTP. Ejecutando las siguientes opciones en el programa Wireshark como se muestra a continuación.

Para capturar el tráfico en el Terminal A:

Capture → Interface → Ethernet: 192.168.10.35 → Start

Filtrado:

Filter: “RTP”

Para capturar el tráfico en el Terminal B:

Capture → Interface → Ethernet: 192.168.10.38 → start

Filtrado:

Filter: “RTP”

3. Se ejecutó una llamada desde el terminal A (extensión 1003) hacia el terminal B (extensión 1001), identificados en la figura 8, durante un minuto.
4. Para finalizar, se observó y se recogió las gráficas emitidas por Wireshark relacionadas al tráfico RTP. Cabe destacar, que la secuencia de opciones a continuación fueron necesarias para obtener el resultado.

Terminal A:

Telephony → RTP → show all stream → Forward 192.168.10.35:5064 to 192.168.10.41:17150 → Analyze → Graph → Graph1

Telephony → RTP → show all stream → Forward 192.168.10.41:17150 to 192.168.10.35:5064 → Analyze → Graph → Graph1

Terminal B:

Telephony → RTP → show all stream → Forward 192.168.10.38:5062 to 192.168.10.41:14400 → Analyze → Graph → Graph1

Telephony → RTP → show all stream → Forward 192.168.10.41:14400 to 192.168.10.35:5062 → Analyze → Graph → Graph1

4.3.7.2 Resultados

Se espera que el jitter entre el punto inicial y final de la comunicación sea menor a 100 ms. Los resultados obtenidos podrán ser observados a continuación.

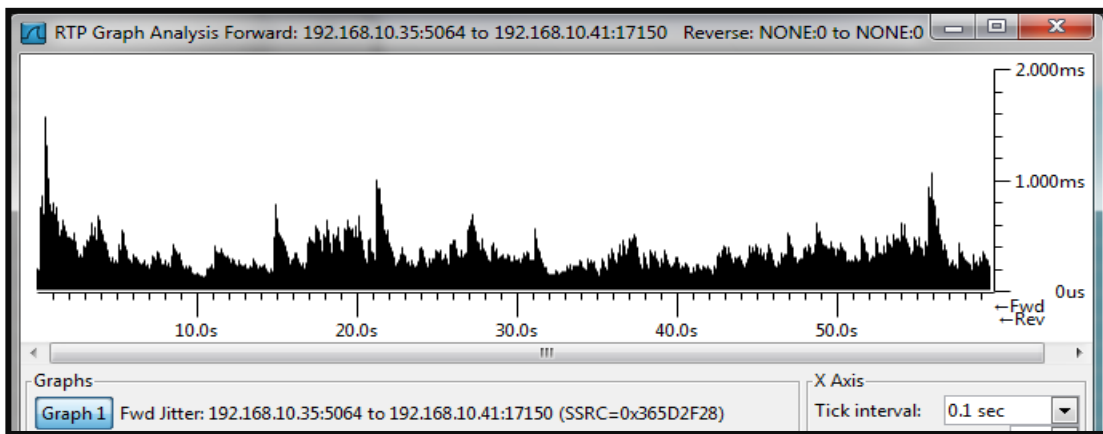


Figura 21. Jitter: Desde el Terminal A hacia el servidor.

Fuente: “De elaboración propia”

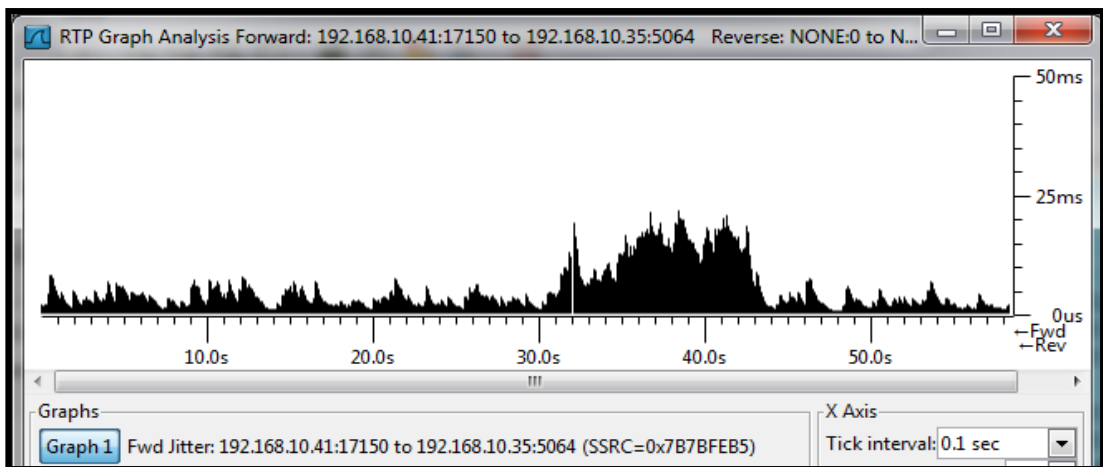


Figura 22. Jitter: Desde el servidor al terminal A

Fuente: “De elaboración propia”

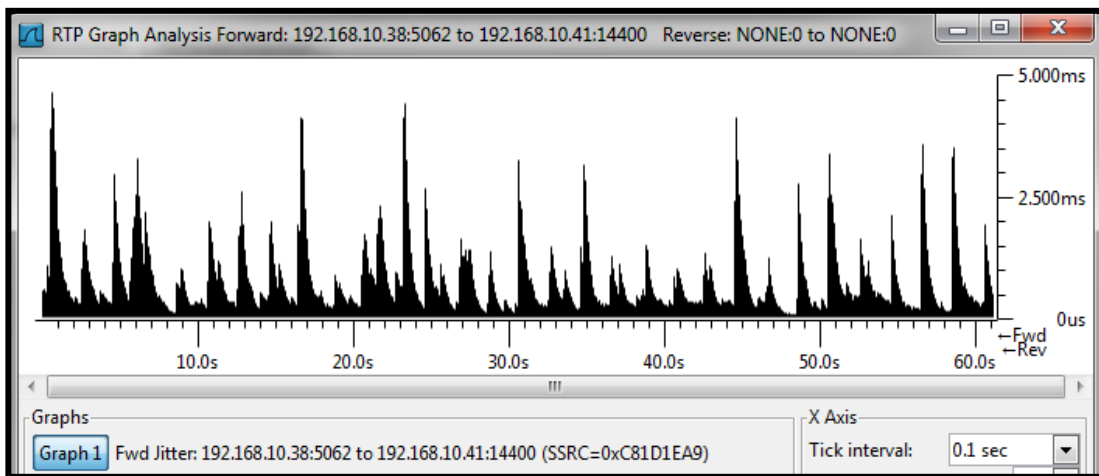


Figura 23. Jitter: Desde el Terminal B hacia el servidor.

Fuente: “De elaboración propia”

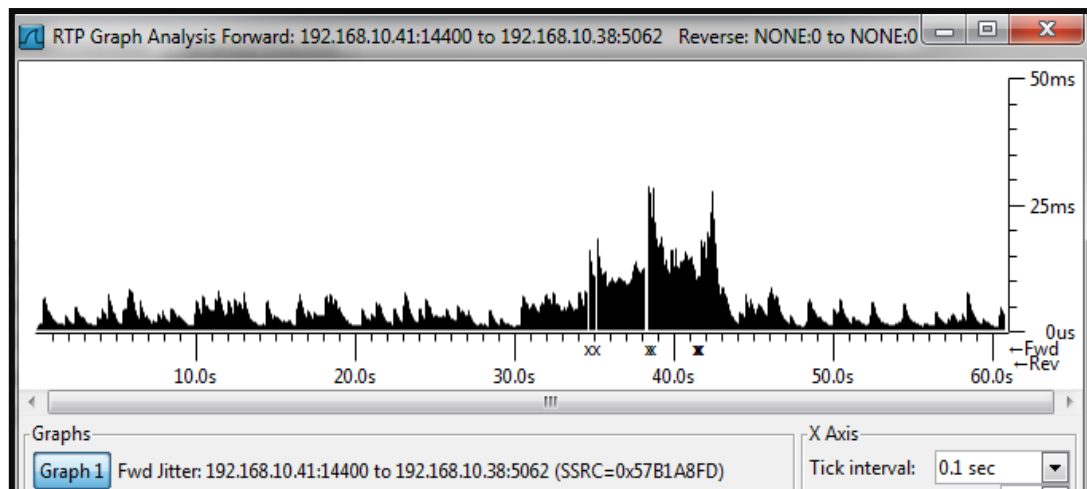


Figura 24. Jitter: Desde el servidor al Terminal B.

Fuente: “De elaboración propia”

4.3.8 Medición de la tasa transferencia de bits en una llamada

Para medir la tasa de transferencia en una llamada se realizaron dos pruebas. La primera, utilizó la topología de pruebas número 1 señalada en la figura 7, filtrando de esta manera todo tráfico proveniente de internet y de aplicaciones que interactúen con los servidores de la red, logrando así una mayor exactitud en la medición. La segunda prueba, se realizó en el escenario número 2, descrito en la figura 8, donde se incluyó un tráfico de descarga y carga, desde y hacia el internet, simulando el peor escenario en la red.

Es importante señalar, que para este Test se utilizó una aplicación gratuita llamada Networx, esta herramienta sirve para recoger datos sobre el uso de ancho de banda y medir la velocidad de Internet o cualquier otra conexión de red. Se encuentra disponible para su descarga en la siguiente dirección URL <http://www.softperfect.com/products/networx/>

4.3.8.1 Procedimientos

Prueba 1: Topología 1, Figura 7

1. Se activó la aplicación Networx para medir la tasa de transferencia, en el terminal A descrito en la figura número 7.
2. Seguidamente, se realizó una llamada entre el terminal A de dirección IP 192.168.0.104 y el terminal B de dirección IP 192.168.0.108, ambos

pertenecientes a la subred 192.168.0.0/24 expuesta en la figura 7, por un plazo de 1 min.

3. Al finalizar la llamada, se accedió a la barra de tareas del sistema operativo Windows, se procedió hacer click en el icono de Network e inmediatamente se seleccionó la opción “mostrar gráfico”. Para luego, hacer un screenshot y capturar los datos obtenidos por la aplicación. Adicionalmente, se escogió el ítem “velocímetro”, en la herramienta, para obtener una interpretación numérica del gráfico capturado.

Prueba 2: Topología 2, Figura 8

1. Se ejecutó la herramienta Networx con el fin de medir la tasa de transferencia, en el terminal A descrito en la figura número 8.

2. Luego, se procedió a realizar un proceso de descarga y carga de archivos, desde y hacia el internet, utilizando todo el ancho de banda disponible para navegación por internet.

3. A continuación, se realizó una llamada entre el terminal A de dirección IP 192.168.10.35 y el terminal B de dirección IP 192.168.0.38, ambos pertenecientes a la subred 192.168.10.0/24 señalada en la figura 8, por un periodo de 1 min.

4. Por último, se escogió la característica “mostrar gráfico” en la aplicación Networx, con el propósito de ejecutar un screenshot y capturar los datos obtenidos por la herramienta.

4.3.8.2 Resultados

Se desea comprobar si los Bits/s enviados y recibidos en una llamada corresponden a la tasa de transferencia del codec utilizado, que en este caso es el llamado G .711. Por esta razón, se espera una tasa de transferencia de 86.4kbits/s tanto en el canal de subida como en el de bajada.



Figura 25. Tasa de transferencia.

Fuente: “De elaboración propia”

Tabla 3. Tasa de transferencia

Fuente: “De elaboración propia”

Datos	Donwload	Upload
Tasa de transferencia promedio	88,1 kbit/s	88,2 kbit/s
Tasa de transferencia máxima	93,4 kbit/s	93,4 kbit/s
Datos recibidos	645 KB	
Datos enviados	646 KB	
Total de datos transferidos	1,26 MB	
Desde 19/02/2013 09:49:55 a.m		
Tiempo transcurrido: 00-01-00		

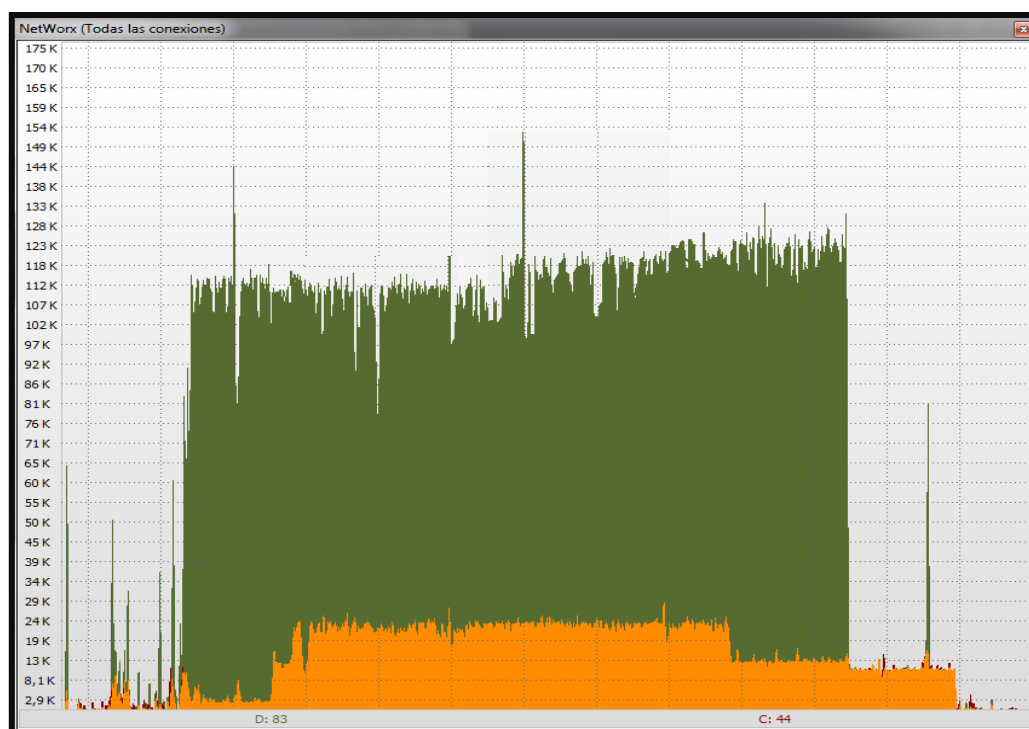


Figura 26. Tasa de transferencia topología 2.

Fuente: “De elaboración propia”

4.3.9 Verificación de la interoperabilidad de las distintas plataformas.

Con este experimento se busca comprobar si se pueden obtener llamadas exitosas mediante distintos tipos de softphone en diferentes sistemas operativos. Se llevará a cabo en la topología de pruebas 2 escenificado en la figura 8. Es de señalar, que se prestará mayor atención a la plataforma móvil, en busca de integrarla al servicio de VoIP

4.3.9.1 Procedimientos

1. Se procedió a registrar extensiones ya previamente creadas. Para el sistema operativo Windows, se utilizó el softphone X-lite, el cual fue instalado en el terminal A ,por otra parte para la distribución Ubuntu se empleó el software Qutecom en el terminal B y para el ambiente Android el terminal D manejó el softphone Zoiper. Cabe recalcar que todos estos terminales están descritos en la figura 8.
2. Luego, se realizaron llamadas entre cada una de las plataformas.
3. Por último, se verificó si la llamada fue exitosa

4.3.9.2 Resultados

El resultado esperado es conseguir que todos los intentos de llamadas sean exitosos, sin importar el sistema operativo o el softphone que se esté utilizando. A continuación se presentará los resultados obtenidos.

Tabla 4. Verificación de llamadas entre distintos softphone.

Fuente: “De elaboración propia”

Softphone	X-lite(Windows)	Qutecom(Ubuntu)	Zoiper(Android)
X-lite(Windows)	✓	✓	✓
Qutecom(Ubuntu)	✓	✓	✓
Zoiper(Android)	✓	✓	✓

4.3.10 Pruebas a través de una VPN

Todas las pruebas a continuación se hicieron en el escenario de 3, identificado por la figura 9, buscando comprobar la posibilidad de tener un servicio de VoIP por medio de la VPN de Supra Caracas.

4.3.10.1 Medición del retardo y pérdida de paquetes (VPN)

4.3.10.1.1 Procedimientos

1. Se procedió a conectar el terminal B de dirección IP 192.168.14.56 perteneciente a la sede de Supra Zona Rental con el terminal A de dirección IP 192.168.10.108 y de dirección subred 192.168.10.0/24 ubicado en Supra las Mayas, por medio del Cliente OPENVPN.
2. Seguidamente, se ejecutó la consola de Windows en el terminal B y se escribió comando “PING 192.168.10.108 -n 100” para realizar un envío de paquetes ICMP al terminal A de la figura 9.
3. Luego, el resultado fue copiado en un block de notas para su análisis.

4.3.10.1.2 Resultados

Estadísticas de ping para 192.168.10.108: Paquetes: enviados = 100, recibidos = 99, perdidos = 2 (2% perdidos), Tiempos aproximados de ida y vuelta en milisegundos: Mínimo =322ms, Máximo = 679ms, Media =426ms
--

Figura 27. PING en el escenario de prueba 3.

Fuente: “De elaboración propia”

4.3.10.2 Medición de la tasa de Transferencia (VPN)

4.3.10.2.1 Procedimientos

1. Se utilizó 2 extensiones previamente creadas y configuradas en los softphones pertenecientes a los terminales A y B. Cabe destacar, que los terminales se encuentran identificados en la figura número 9.
2. Se inició el establecimiento del cliente OPENVPN en los dos ordenadores
3. Luego, se activó la aplicación Networx en el terminal B.
4. Seguidamente, se realizó una llamada entre los terminales.
5. Se registraron los resultados mostrados por Networx, mediante la opción gráfica de esta aplicación.

4.3.10.2.2 Resultados

Se espera obtener una tasa de transferencia superior a la evaluada en la red LAN de Supra las Mayas .A continuación se presenta el resultado recolectado.

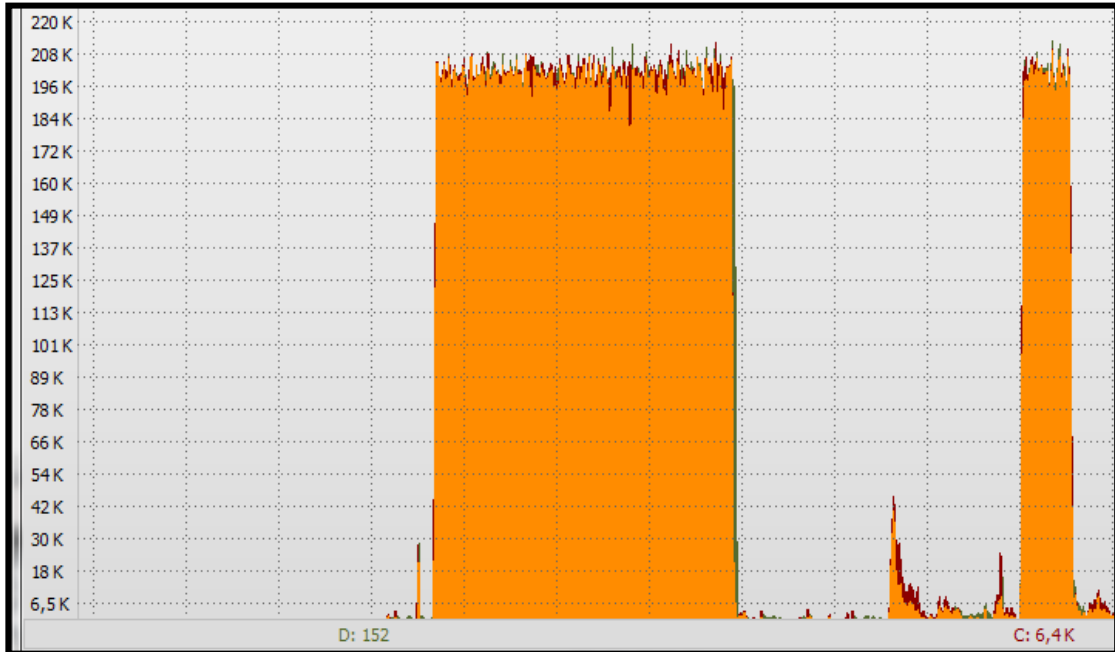


Figura 28. Tasa de transferencia mediante una VPN.

Fuente: “De elaboración propia”

4.3.10.3 Establecimiento y finalización de una llamada (VPN)

4.3.10.3.1 Procedimientos

1. Se procedió a establecer una conexión mediante la VPN entre el terminal A y B descritos en la figura 9.
2. Se ejecutó el programa Wireshark en los 2 terminales anteriores.

3. Luego, se procedió a capturar el tráfico de la llamada, filtrando solamente los protocolos SIP y RTP, siguiendo la secuencia de opciones descritas a continuación.

Para capturar el tráfico en el Terminal A:

Capture → Interface → Ethernet: 192.168.10.108 → Start

Filtrado:

Filter: "RTP"

Para capturar el tráfico en el Terminal B:

Capture → Interface → Ethernet: 192.168.14.56 → start

Filtrado:

Filter: "RTP"

4. Seguidamente, se realizó una llamada entre los 2 terminales durante 1 min.
5. Por último, se finalizó la captura de tráfico y se recogieron los datos.

4.3.10.3.2 Resultados

A pesar, que se pudo realizar el establecimiento y finalización de una llamada no se pudo capturar tráfico RTP y SIP para el análisis, simplemente se obtuvieron paquetes UDP. Adicionalmente, se apreció un retardo considerable en el audio.

4.3.10.4 Medición del retardo y pérdida de paquetes durante una llamada (VPN)

Debido, a que en la prueba anterior no se pudo capturar los paquetes RTP y SIP, no se logró analizar variantes como la pérdida de paquetes, el jitter, entre otros. En consecuencia se planteó utilizar el comando PING durante una llamada para obtener un valor de cuánto sería el retardo y la pérdida de paquetes en una llamada en curso.

4.3.10.4.1 Procedimientos

1. Se procedió a conectar el Terminal B a la red de Supra Las Mayas por medio del Cliente OPENVPN, señalado en la figura 9.
2. Luego, se realizó una llamada entre los Terminales A y B
3. Seguidamente y durante la llamada, se escribió el siguiente comando “PING 192.168.10.108 -n 100” en la consola de Windows del terminal B. Para enviar solicitudes de eco al terminal A
4. Se esperó a que se terminara de ejecutar el comando PING.
5. Luego, se finalizó la llamada.

6. Por último, se recolectaron los datos arrojados por el comando PING.

4.3.10.4.2 Resultados

Se espera que los resultados no varíen en comparación a la prueba de “Medición del retardo y pérdida de paquetes a través de un túnel VPN”. El resultado obtenido se mostrará a continuación.

Estadísticas de ping para 192.168.10.108: Paquetes: enviados = 100, recibidos = 75, perdidos = 25 (25% perdidos), Tiempos aproximados de ida y vuelta en milisegundos: Mínimo =2135ms, Máximo = 2603ms, Media =2371ms

Figura 29. PING en el escenario 3 durante una llamada.

Fuente: “De elaboración propia”

CAPÍTULO V

ANÁLISIS DE RESULTADOS

A raíz de las pruebas realizadas en el capítulo anterior, a continuación se describirán los análisis obtenidos gracias a los resultados que arrojaron los distintos tests.

Luego de revisar los resultados arrojados por la prueba “Medición del retardo y pérdida de paquetes en la red” se puede asegurar que la red de Supra las Mayas se encuentra apta para la habilitación de un servicio de Voz sobre IP, esto se debe a que no presenta una pérdida significativa en el tráfico de paquetes, además también se puede observar como el retardo de los paquetes no supera los 150 ms recomendados por la ITU en su documento G.114.

Por otra parte, se detalla cómo el retardo de los paquetes aumenta mientras éste tenga que pasar por mas dispositivos intermedios, este hecho se demuestra al analizar los resultados emitidos por la prueba “Verificación de la conectividad entre una PC y el Servidor Elastix”, la cual además de corroborar el buen funcionamiento y configuración de la interfaz de red del servidor, demuestra de que manera aumenta el retardo si el terminal se encuentra en otra sub red distinta a la del servidor.

Conjuntamente con la prueba anterior, existen otras que arrojaron resultados que avalan el buen funcionamiento del servidor, ejemplo la nombrada “Registro de una extensión mediante Elastix”. Como ya se ha señalado el software propuesto ofrece una interfaz gráfica, la cual ayuda a la configuración del sistema. Sin embargo es necesario comprobar que aquellos cambios que se realicen en la interfaz sean reseñados en los archivos de configuración. Esto se pudo comprobar mediante los resultados arrojados, ya que al consultar la consola Asterisk se observó una nueva extensión agregada.

Otra prueba importante es la llamada “Comprobación del registro de un Softphone SIP”. Cabe destacar, que si los softphones no logran registrarse en el servidor no podrán ofrecer ninguna comunicación y mucho menos ser capaces de realizar una llamada. Al analizar los resultados recolectados en esta prueba, se puede observar cómo en el proceso de registro entre un softphone y un servidor, estos intercambian paquetes SIP. El softphone envía mensajes de solicitud como **REGISTER** utilizado para registrar un cliente SIP y **SUBSCRIBE** el cual establece un diálogo SIP para recibir estadísticas. De igual manera, el servidor envía mensajes como **NOTIFY** usado por el servidor de la central telefónica para comunicar estadísticas y **OPTIONS** que funciona para consultar a otro cliente SIP sobre sus capacidades, tipos de contenidos, extensiones, codecs, entre otros. Por otra parte, al finalizar el proceso de registro se observó de qué forma en la consola de Asterisk se ve reflejado un nuevo usuario SIP online, que en este caso sería el softphone que se acaba de registrar, lo cual es una prueba fehaciente de un exitoso registro SIP.

Ya verificado el registro de un softphone sólo queda, analizar el proceso más importante, el cual es el establecimiento y finalización de una llamada. De éste, se puede obtener datos significativos como el jitter, las pérdidas de paquetes, la tasa de transferencia, entre otros.

La prueba de “Establecimiento y finalización de un llamada utilizando SIP”, demuestra que el proceso de establecimiento y finalización se asemeja al descrito en la teoría de SIP. El cliente que desea comunicarse con otro envía toda la señalización al servidor Elastix, para luego ser éste un intermediario en la señalización entre los dos terminales. No obstante, estos resultados tienen una peculiaridad, demuestran el funcionamiento del protocolo SIP y la efectiva realización de una llamada, y adicionalmente dan a entender que para una comunicación entre 2 terminales en un ambiente Asterisk, el flujo de RTP debe pasar por el servidor Elastix antes de llegar al otro terminal. Esto se debe a las características que ofrece Asterisk, como por ejemplo grabación de llamadas.

Para verificar la calidad del servicio, es necesario calcular valores como la pérdida de paquetes RTP, lo cual se realizó en la prueba “Tasa de pérdidas de paquetes”. Los resultados arrojaron una pérdida insignificante de los paquetes, la cual no superaba el 0.2%, demostrando así un excelente comportamiento del sistema.

Además de medir las pérdidas de paquetes, se logró determinar el jitter. Como se pudo observar, los resultados muestran valores aceptables, éstos no superan los 100 ms, lo cual es ideal en la comunicación mediante VoIP. Sin embargo, se pudo notar un incremento del jitter en el paso del flujo por el servidor, lo cual es totalmente previsible, ya que a medida que el tráfico de voz pase por un router, switch o cualquier otro dispositivo intermedio, el jitter se incrementará.

En la prueba “Medición de la tasa de transferencia de bits en una llamada” los datos arrojaron una tasa de transferencia un poco superior a la calculada anteriormente con el codec G.711. Cabe destacar, que a pesar de realizarse en un ambiente controlado no se pudo evitar la recepción de los paquetes ARP enviados

por el router, siendo ésta la causa de la diferencia entre el resultado teórico y el práctico. Por otro parte, se pudo observar cómo se mantiene estable el tráfico de la llamada, en presencia del tráfico producido por la descarga y carga, desde y hacia internet, aunque era de esperarse ya que el flujo de la llamada solamente pertenece a la red de área local.

La prueba “Verificación de la interoperabilidad de las distintas plataformas”, demostró la coexistencia entre distintos sistemas operativos en un mismo servicio de VoIP y la posibilidad de ingresar los dispositivos móviles como teléfonos inteligentes y tabletas a la tecnología de VoIP, para así darle un mayor grado de movilidad al servicio.

Adicionalmente para finalizar, se analizaron todos los resultados provenientes de las “Pruebas a través de una VPN”. La medición del retardo y la pérdida de paquetes a través del túnel VPN, mostró un incremento considerable en la latencia en comparación a la presentada en la LAN de Supra las Mayas. Un Promedio de un retardo de 426 ms para un servicio de VoIP no es recomendable, sin embargo se decidió realizar más pruebas para estudiar el verdadero comportamiento de una llamada por medio de una VPN. En consecuencia, se ejecutó una prueba para medir la tasa de transferencia de una llamada, en la cual los datos indicaron un incremento de esta tasa, cabe señalar que dicho resultado se debe al cifrado proveniente por el OPENVPN y a los encabezados que se agregan.

Luego de analizar la prueba anterior, se observaron los datos recolectados de la prueba “Establecimiento y finalización de una llamada (VPN)”. Éstos muestran solamente tráfico UDP y en consecuencia no se pudo diferenciar entre el tráfico RTP y SIP. Todo lo anterior, se debe que al llegar el tráfico a la interfaz virtual

creada por OPENVPN, éste se encapsula nuevamente en un datagrama UDP, para ser enviado a la interfaz real de la PC como un stream UDP. El resultado recolectado, imposibilitó la medición de la pérdida de paquetes y del jitter.

Al experimentar que existía un flujo de audio, aunque con cierto retraso, en la prueba de establecimiento y finalización de una llamada, se decidió realizar la prueba “Medición del retardo y pérdida de paquetes durante una llamada (VPN)”, pero de una forma distinta. Aunque el comando PING no envíe paquetes RTP, con su resultado se puede obtener una idea de cómo está el tráfico en la red. Al observar los resultados de esta prueba, se nota un incremento considerable del retardo y de la pérdida de paquetes. El 25% de los paquetes enviados durante la llamada se perdieron y el retardo promedio fue de 2371 ms. Es importante señalar, que el incremento de estos valores se debe a la tasa de subida que tiene una conexión ABA, ya que se registró un máximo de 17 KB/s y con el incremento del doble de la tasa de transferencia de una llamada mediante VPN la tasa de transferencia necesaria sería aproximadamente de 23.75 KB/s. Al superar la tasa de transferencia a la tasa disponible se crea una saturación en la red produciendo retardo y pérdida en los paquetes.

CONCLUSIONES

La tecnología VoIP representa un nuevo avance en lo que a comunicación de voz se refiere, además es una clara alternativa para todas las empresas que desean sacar el máximo provecho a su red de datos. Ésta utiliza una plataforma ya existente ahorrando así una inversión extra en la instalación de una red dedicada a la telefonía.

Por otra parte, el funcionamiento de una servicio de VoIP basado en el software libre Asterisk cumple con los requisitos impuesto por la política de software libre aplicada en las instituciones públicas, al permitir el control absoluto tanto de la configuración como del mantenimiento de dicho servicio , descartando así la necesidad de contratar y solicitar soporte de alguna compañía.

De acuerdo a las pruebas realizadas se concluye que no se puede prestar un servicio de VoIP mediante la VPN, que actualmente posee la empresa. Sin embargo, se demuestra la factibilidad de la propuesta de un diseño operativo para servicio de voz sobre IP basado en el software libre Asterisk en Supra Caracas, por lo que se dejan los cimientos para una posible implementación en la empresa.

Es importante señalar, que actualmente la compañía Supra Caracas se encuentra en un proceso de implementación de esta propuesta en su sede principal Supra Las Mayas, ya que con ésta se solucionará el problema de comunicación entre departamentos, debido a lo extenso del complejo. Además, se dejan las bases para la

posible implementación de otros servicios que ofrece Elastix como por ejemplo: un servidor de correo, de Fax y de mensajería instantánea, que incrementaría el abanico de opciones de comunicación en la empresa.

RECOMENDACIONES

A medida que crezca la empresa y exista un número considerable de usuarios en las sedes ubicadas en Artigas, Yaguara y Zona Rental, es recomendable agregar un servidor Elastix en cada una de las sedes. Estos servidores, deberán seguir el esquema propuesto de extensiones, ya que en el momento de querer conectar las sedes y prestar el servicio de VoIP en toda la empresa, se hará necesario que los servidores se configuren en modo troncal, por lo cual, la utilización de ese esquema facilitaría las configuraciones.

Por otro parte, se recomienda implementar el servicio de VoIP, sólo en la sede principal, ya que para poder ofrecer esta tecnología de manera satisfactoria es necesario una conectividad capa 2 entre las sedes. Asimismo, se aconseja luego de analizar las pruebas a través de la VPN, no utilizar este medio para implementar un servicio de VoIP entre las diferentes localidades de la empresa.

Ya existiendo las bases para la implementación de la propuesta, se aconseja realizar estudios acerca de otros servicios ofrecidos por Elastix; las aplicaciones de servicios como mensajería instantánea y correo institucional fortalecerían la plataforma comunicacional de la empresa.

Por último, se recomienda realizar un estudio acerca de una posible interconexión entre el servicio de VoIP y la red PSTN de CANTV.

REFERENCIAS BIBLIOGRÁFICA

- [1] Madsen, L. J. (2011). *Asterisk: The Defenitive Guide* (Tercera ed.). Estados Unidos: O'Reilly.App A, p.601
- [2] VoIP Foro. (s.f.). Recuperado el 2013, de VoIP Foro Codec G.711.1 - G729.1 - G722.1 - G722.2: <http://www.voipforo.com/codec/nuevos-codecs-g7111-g7291.php>
- [3] Madsen, L. J. (2011). *Asterisk: The Defenitive Guide* (Tercera ed.). Estados Unidos: O'Reilly.App B, p.627
- [4] Landivar, E. (2008). *Comunicaciones Unificadas con Elastix* (Primera ed., Vol.I).Cap 2, p. 44
- [5] Cruz, D. Q. (2007). *Diseño e implementacion de una red de telefonía IP con software libre en la RAAP*. Tesis, Pontificia Universidad Católica del Perú, Lima.Cap 2,p. 28
- [6] Gil Cabezas, J. (2008/2009). Recuperado el 2013, de <http://www.uco.es/~i62gicaj/RTP.pdf>
- [7] Dean, T. (2010). *Network+ Guide to Networks* (Quinta ed.). Boston, Estados Unidos: Course Technology.Cap 11,p. 554.
- [8] Wallingford, T. (2005). *Switching to VoIP*. Estados Unidos: O'REILLY.Cap 7,p. 134.

- [9] Dean, T. (2010). *Network+ Guide to Networks* (Quinta ed.). Boston, Estados Unidos: Course Technology. Cap 11, p. 550.
- [10] Madsen, L. J. (2011). *Asterisk: The Defenitive Guide* (Tercera ed.). Estados Unidos: O'Reilly. Cap 5, p. 86-87
- [11] Goncalvez, F. E. (2006). *ASTERISK PBX Guía de configuración* (Primera ed.). (O. O. Alvarez, Trad.). Cap 1, p. 18
- [12] Certad, C. C. (9 de marzo de 2012). *6 distribuciones de Asterisk*. Recuperado el 2013, de <http://fraterneo.blogspot.com/2012/03/6-distribuciones-de-asterisk-pbx.html>
- [13] *Asterisk dimensioning*. (s.f.). Recuperado el 2013, de <http://www.voip-info.org/wiki/index.php?page=Asterisk+dimensioning>
- [14] Rouse, M. (March de 2011). *What is SRTP?* Recuperado el 2013, de <http://whatis.techtarget.com/definition/SRTP-Secure-Real-Time-Transport-Protocol-or-Secure-RTP>.
- [15] *Cisco Systems, Inc.* (s.f.). Recuperado el 2013, de <http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/telepresence.html#wp42119>
- [16] Alfonso Martín, I. V. (2013). *Servicios Audiovisuales SIP (Session Initiation Protocol)*. Obtenido de www.it.uc3m.es.

- [17] Horak, R. (2007). *Telecommunications and Data Communications Handbook*. New Jersey, Estados Unidos: Wiley-Interscience. Cap 12, p. 616
- [18] Madsen, L. J. (2011). *Asterisk: The Defenitive Guide* (Tercera ed.). Estados Unidos: O'Reilly. Cap 2, p. 46

BIBLIOGRAFÍA

- Alfonso Martín, I. V. (2013). *Servicios Audiovisuales SiP (Session Initiation Protocol)*. Obtenido de www.it.uc3m.es
- Asterisk dimensioning*. (s.f.). Recuperado el 2013, de <http://www.voip-info.org/wiki/index.php?page=Asterisk+dimensioning>
- Bates, R. J. (s.f.). *Broadband Telecommunications Handbook* (Segunda ed.). Estados Unidos: McGraw-Hill TELECOM.
- Bazán, O. A. (2012). *Diseño de la red metropolitana y la red local en nodo central para la compañía Supra Caracas*. Trabajo Especial de Grado, Universidad Central de Venezuela, Caracas.
- Certad, C. C. (9 de marzo de 2012). *6 distribuciones de Asterisk*. Recuperado el 2013, de <http://fraterneo.blogspot.com/2012/03/6-distribuciones-de-asterisk-pbx.html>
- Cisco Systems, Inc. (s.f.). Recuperado el 2013, de <http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/telepresence.html#wp42119>
- Cruz, D. Q. (2007). *Diseño e implementacion de una red de telefonía IP con software libre en la RAAP*. Tesis, Pontificia Universidad Católica del Perú, Lima.
- Dean, T. (2010). *Network+ Guide to Networks* (Quinta ed.). Boston, Estados Unidos: Course Technology.
- Escuela de Ingeniería Eléctrica de la Universidad Central de Venezuela*. (s.f.). Recuperado el 2012, de <ftp://neutron.ing.ucv.ve/pub/Practica%20VoIP/>
- Freeman, R. I. (2005). *Fundamentals of Telecommunications* (Segunda ed.). New Jersey, Estados Unidos: Willey-Interscience.
- García, R. (2008). *Integracion de PBX analógica/digital (NEC) con PBX IP por software (Asterisk) del Ministerio del Poder Popular para la cultura e*

- interconexión con la red PSTN de CANTV*. Trabajo Especial de Grado, Universidad Central de Venezuela, Caracas.
- Gil Cabezas, J. (2008/2009). Recuperado el 2013, de <http://www.uco.es/~i62gicaj/RTP.pdf>
- Goncalvez, F. E. (2006). *ASTERISK PBX Guía de configuración* (Primera ed.). (O. O. Alvarez, Trad.)
- Grant, I. A. (2010). *Digital Communications* (Tercera ed.). Inglaterra: Pearson.
- Group, N. W. (June de 2002). *RFC 3261*. Recuperado el 2013, de IETF.ORG: <http://www.ietf.org/rfc/rfc3261.txt>
- Horak, R. (2007). *Telecommunications and Data Communications Handbook*. New Jersey, Estados Unidos: Wiley-Interscience.
- Implementacion del protocolo RTSP*. (s.f.). Obtenido de <http://profesores.elo.utfsm.cl/~agv/elo323/2s10/projects/ApablazaBustamante/req.html>
- Landivar, E. (2008). *Comunicaciones Unificadas con Elastix* (Primera ed., Vol. I).
- Landivar, E. (2008-2009). *Comunicaciones Unificadas con Elastix* (Segunda ed., Vol. II).
- Madsen, L. J. (2011). *Asterisk: The Defenitive Guide* (Tercera ed.). Estados Unidos: O'Reilly.
- Meggelen, J. V. (2005). *Asterisk: The Future of Telephony*. Estados Unidos: O'Reilly.
- Moreno, D. R. (2006). *Propuesta para solucionar el problema de comunicación telefónica en la Facultad de Ciencias de la UCV utilizando un servidor PBx de Software*. Trabajo Especial de Grado, Universidad Central de Venezuela, Caracas.
- Muñoz, A. (2009-2010). *Elastix A Ritmo de Merengue*. Santo Domingo, República Dominicana.
- Naranjo, I. L. (2009). *Telefonía de Código Abierto Asterisk: caso práctico de la implatación de un sistema de telefonía VoIP en una empresa*. Tesis, Escuela Técnica Superior de Ingeniería Informatica, Sevilla.

- Postel, J. (1980). *RFC 789*. Recuperado el 2013, de IETF.ORG:
<http://www.ietf.org/rfc/rfc768.txt>
- Román, B. F. (2012). *Estudio y diseño de una red de datos y VoIP en la empresa Rinteco CIA. LTDA. Usando Open Source y construccion de IVRS de Asterisk para mejoramiento en calidad de atención al cliente*. Proyecto previo a la obtencion del Titulo de Ingeniero en Electrónica y Telecomunicaciones, Escuela Politécnica Nacional, Quito.
- Ross, J. F. (2009). *Computer Networking*. Addison-Wesley.
- Rouse, M. (March de 2011). *What is SRTP?* Recuperado el 2013, de
<http://whatis.techtarget.com/definition/SRTP-Secure-Real-Time-Transport-Protocol-or-Secure-RTP>
- Toscano, G. N. (2012). *Análisis y diseño de una red de alta disponibilidad para centrales Asterisk basada en la tecnología DUNDI*. Tesis, Escuela Superior Politécnica de Chimborazo, Riobamba.
- UIT: Unión Internacional de Telecomunicaciones. (Mayo de 2003). Recuperado el 2013, de <http://www.itu.int/rec/T-REC-G.114-200305-I/es>
- VoIP Foro. (s.f.). Recuperado el 2013, de <http://www.voipforo.com/>
- VoIP-Info.org. (s.f.). Recuperado el 2013, de <http://www.voip-info.org/>
- Wallingford, T. (2005). *Switching to VoIP*. Estados Unidos: O'REILLY.

ANEXOS

[ANEXO N° 1]

[FUNDAMENTACIÓN TEÓRICA]

1.1 Protocolos de transporte

1.1.1 SRTP

Secure Real-Time Transport Protocol (SRTP) es una extensión de RTP con la intención de proporcionar cifrado, autenticación del mensaje y protección contra reenvíos a los datos RTP en aplicaciones unicast y multicast. Éste fue concebido y desarrollado por expertos en comunicaciones de Cisco y Ericsson publicándose oficialmente en marzo de 2004 por la IETF en el RFC 3711. **[14]**

En la Figura 1-1 se puede observar la estructura de la cabecera del protocolo SRTP, muchos de los campos son iguales a los del encabezado del protocolo RTP y por ende a continuación solo se señalaran los nuevos campos.

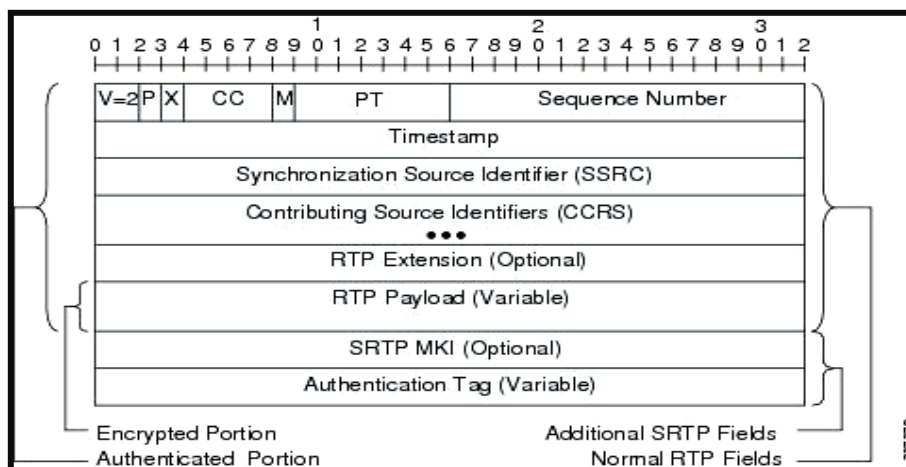


Figura 1-1. Encabezado SRTP

Fuente:(Cisco Systems, Inc)

- **RTP Extension (opcional):** es un campo de longitud variable que contiene un identificador de perfil específico de 16-bit y un identificador de longitud de 16-bits, seguido de los datos de extensión de longitud variable.
- **RTP Payload:** campo de extensión variable que contiene los datos de las aplicaciones en tiempo real (voz, video, etc).
- **SRTP MKI:** también llamado “Identificador de Llave Maestra”, el cual es un campo opcional de longitud configurable, que se utiliza para indicar la llave maestra, a partir de que las claves de sesión individuales que se obtuvieron para el cifrado y / o autenticación, dentro de un contexto de cifrado dado.

- **Authetication Tag:** campo de longitud configurable, usado para contener los datos de autenticación de mensaje para la cabecera RTP y la carga útil del paquete particular.

Con SRTP, el cifrado se aplica sólo a la carga útil del paquete RTP. La autenticación de mensajes, sin embargo, se aplica tanto a la cabecera RTP, así como la carga útil de RTP. Puesto que la autenticación de mensajes se aplica al número de secuencia dentro de la cabecera RTP, SRTP indirectamente proporciona una protección contra los ataques de repetición. [15]

1.1.2 RCTP y SRCTP

Como se había mencionado anteriormente, RTP viene con un protocolo complementario llamado Real Time Control Protocol (RTCP), de la misma forma que SRTP viene acompañado del llamado Secure Real Time Control Protocol (SRTCP).

RTCP le brinda al Real Time Protocol un mecanismo de control, el cual se basa en la transmisión periódica de paquetes de control a todos los participantes en sesión ofreciéndole información sobre la calidad de los datos distribuidos por la fuente. El protocolo subyacente debe proveer de la multiplexación de los datos y de los paquetes del control. Por tanto, la función primordial de RTCP es la de proveer una realimentación de la calidad de servicio recogiendo estadísticas de la conexión, además de información como por ejemplo cantidad de paquetes enviados, paquetes perdidos o jitter, entre otros. Es decir, una aplicación puede usar esta información

para incrementar la calidad de servicio, ya sea limitando el flujo o usando un codec de compresión más bajo.

Por otra parte, al igual que RTP no contiene ninguna característica de autenticación o cifrado, por lo que necesita de SRTP, de igual manera, el protocolo RCTP no posee ninguna de estas y allí es donde interviene SRCTP. Lo que significa que éste simplemente aporta a RCTP las mismas opciones que le ofrece SRTP a RTP.

1.2 Protocolos de señalización

1.2.1 SIP (Protocolo de Inicio de Sesiones)

1.2.1.1 Componentes

- **User Agent (UA):** es cualquier nodo que inicia o responde a las solicitudes SIP.
- **User Agent Client (UAC):** se trata de dispositivos de usuario final, que pueden incluir estaciones de trabajo, PDAs, teléfonos móviles, o teléfonos IP. El User Agent Client inicia una conexión SIP.

- **User Agent Server (UAS):** es un tipo de servidor que responde a las peticiones de los User Agent Client para el inicio y finalización de una sesión. Prácticamente hablando, un dispositivo tal como un teléfono IP puede actuar como User Agent Client y como un User Agent Server, lo cual permite ponerse en contacto directamente y establecer sesiones con otros clientes de una manera peer-to-peer. Cabe destacar, que los User Agent Client y los User Agent Server pueden considerarse como User Agent.

- **Servidor de Registro:** este servidor mantiene una base de datos que contiene información acerca de las ubicaciones (direcciones de red) de cada User Agent dentro de su dominio. Cuando un User Agent se une a una red SIP, transmite su información de ubicación al servidor de registro SIP.

- **Servidor proxy:** acepta peticiones de información de ubicación de los User Agent, luego, consulta al servidor de registro más cercano en nombre de los agentes de usuario. Si el User Agent receptor está en el dominio del servidor proxy SIP, entonces ese servidor también actuará como un intermediario para el establecimiento y finalización de llamadas entre el agente de usuario que solicita y el agente de usuario receptor. Si el agente de usuario destinatario se encuentra en el dominio del servidor proxy SIP, el servidor proxy pasará información de sesión a un servidor SIP de redirección. Cabe destacar, que los servidores proxy son opcionales en una red SIP.

- **Servidor de Redirección:** acepta y responde a las peticiones de los agentes de usuario y servidores proxy SIP que solicitan información acerca de la ubicación de los beneficiarios que pertenezcan a dominios externos. Un servidor de redirección no se involucra en el establecimiento o el mantenimiento de sesiones. De igual forma que los Servidores Proxy, un Servidor de Redirecciones es opcional en una red SIP.

1.2.1.2 Mensajes SIP

SIP es un protocolo basado en texto usando el conjunto de caracteres UTF-8 (8-bit Unicode Transformation Format) definidos en el RFC 2279. Por lo cual, gran parte de los mensajes SIP y la sintaxis de los campos de encabezado son análogos a HTTP/1.1.

Un mensaje SIP es una solicitud de un cliente a un servidor o una respuesta de un servidor a un cliente. Ambos mensajes, solicitud o respuesta, utilizan el formato básico de la norma RFC 2822, sin embargo éstos son distintos. Todos los tipos de mensaje SIP consisten en una línea inicial (startline), uno o más campos de encabezado, una línea en blanco indicando el final del encabezado y opcionalmente el contenido del mensaje.

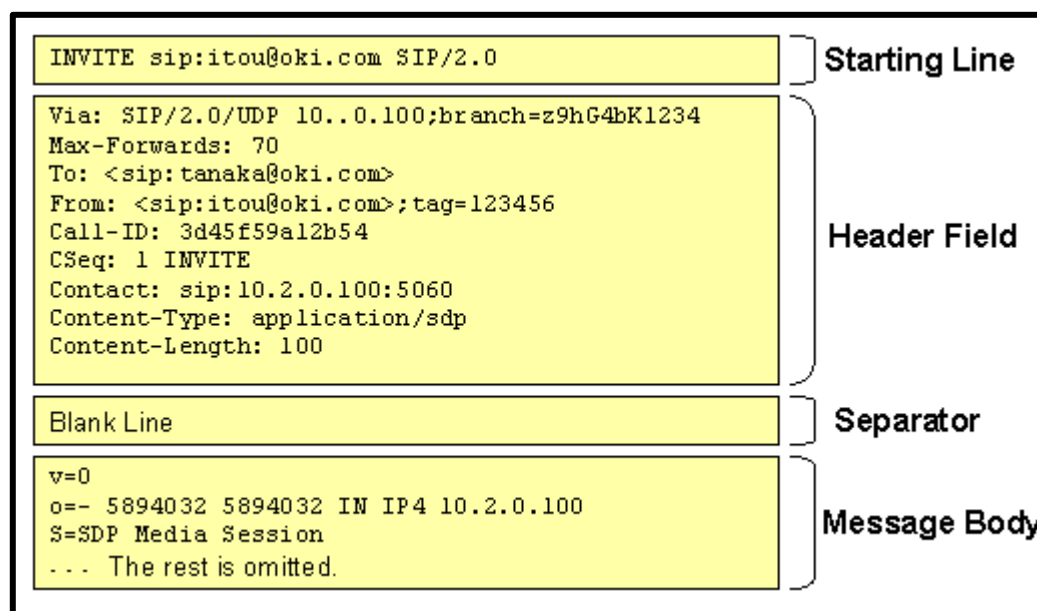


Figura 1-2. Estructura de un mensaje SIP

Fuente:(http://docs.oracle.com/cd/E12529_01/wlss31/programming/wwimages/message-blocks.gif)

Cabe destacar, que la línea vacía debe estar presente incluso si no existe el cuerpo de mensaje. Por otra parte, la línea de inicio puede ser una línea de solicitud o una línea de estado dependiendo si el mensaje es una solicitud o una respuesta, respectivamente.

1.2.1.2.1 Solicitudes

Se caracterizan por tener una Línea-de-Solicitud en la línea de inicio. Una Línea-de-Solicitud contiene un nombre de método, un URI-de-solicitud, y la versión del protocolo separados por un espacio simple

El Método indica el propósito de la solicitud. La especificación RFC 3261 define seis métodos: [17]

- **INVITE:** se utiliza para solicitar a un usuario el establecimiento de una sesión.
- **ACK:** confirma el establecimiento de una sesión.
- **CANCEL:** utilizado por los clientes para cancelar sesiones que aún estén pendientes por establecerse (el servidor aún no ha enviado una respuesta final); la recepción de un CANCEL por parte de un servidor aborta el intento de establecimiento de la sesión, pero no impide que se lleve a cabo el three-way handshake (el servidor envía un 487 Transaction Cancelled).
- **BYE:** utilizado por los usuarios para abandonar una sesión en curso; si la sesión estaba integrada por dos usuarios, utilizar BYE equivale a terminar la sesión.
- **REGISTER:** utilizado por los UAs para informar a un servidor de registro la localización actual del usuario.

- **OPTIONS:** utilizado para solicitar las capacidades de un servidor: methods, protocolos y codecs soportados, etc.

Ya señalado los métodos solamente queda definir los dos últimos parámetros; el URI de la solicitud y la versión SIP. La primera indica el usuario o servicio al cual la solicitud está siendo dirigida y la segunda señala la versión del protocolo SIP que está en uso. Por último, para poder observar la estructura de los mensajes de solicitud observemos los siguientes ejemplos.

- INVITE sip:Alice.Smith@domain.com SIP/2.0
- ACK sip:alice@192.0.0.1 SIP/2.0

1.2.1.2.2 Respuesta

Las respuestas SIP se distinguen de las solicitudes por contener una línea-Estado como línea inicial. Una línea-Estado consiste en la versión del protocolo seguida por un código numérico de estado y su texto asociado separados por espacio simple.

Status-Line = SIP-Version Status-Code Reason-Phrase

El parámetro SIP-Version, al igual que las solicitudes, representa la versión del protocolo SIP, por lo que haciendo referencia al RFC 3261, se debe incluir “SIP/2.0” al inicio de la Status-Line.

Status-Code es un código entero de tres dígitos que indica el resultado de la acción solicitada. El motivo (Reason-Phrase) es un texto breve describiendo el estado. El código está dirigido a ser interpretado por una máquina y el motivo por un usuario.

El primer dígito del Status-Code define la clase de respuesta. Los últimos dos dígitos no tienen un rol específico. Por esta razón, cualquier respuesta con un código entre 100 y 199 se identifican como "1xx response". Los seis valores que permite SIP/2.0 se pueden describir de la siguiente manera.

- **1xx: Provisional:** solicitud recibida, procesando la solicitud.
- **2xx: Success:** la acción fue recibida correctamente, entendida y aceptada.
- **3xx: Redirection:** otra acción es necesaria para completar la solicitud.
- **4xx: Client Error:** la solicitud contiene un error sintáctico o no puede ser ejecutada en este servidor.
- **5xx: Server Error:** el servidor ha fracasado en atender una solicitud aparentemente válida.
- **6xx: Global Failure:** la solicitud no puede ser atendida en ningún servidor.

En la siguiente tabla se muestran algunas respuestas SIP con sus códigos y descripciones correspondientes.

Tabla 1-1. Respuestas SIP

Fuente: (<ftp://neutron.ing.ucv.ve/pub/Practica%20VoIP/>)

Clase	Código	Descripción
1xx (Provisional)	100	Intentando
	180	Repicando
2xx (Satisfactorio)	200	Satisfactorio (OK)
3xx (Redirección)	301	Movido permanentemente
	302	Movido temporalmente
4xx (Error del cliente)	400	Mala solicitud
	401	Desautorizado
	404	No encontrado
	405	Método no permitido
	407	Autenticación requerida por el servidor proxy
	483	Demasiados saltos
	486	Ocupado aquí
5xx (Error del servidor)	500	Error interno del servidor
	501	No implementado
	505	Versión no soportada
6xx (Falla global)	600	Ocupado en todas partes
	604	No existe en ninguna parte

1.2.1.3 Establecimiento y finalización de una llamada

En la siguiente figura se muestra los procesos de establecimiento y finalización de una llamada en SIP. Se trata de un caso típico que consiste en una llamada entre dos usuarios del mismo dominio a través de un servidor proxy que

presta servicio en ese dominio. Las flechas azules indican solicitudes mientras que las rojas indican respuestas.

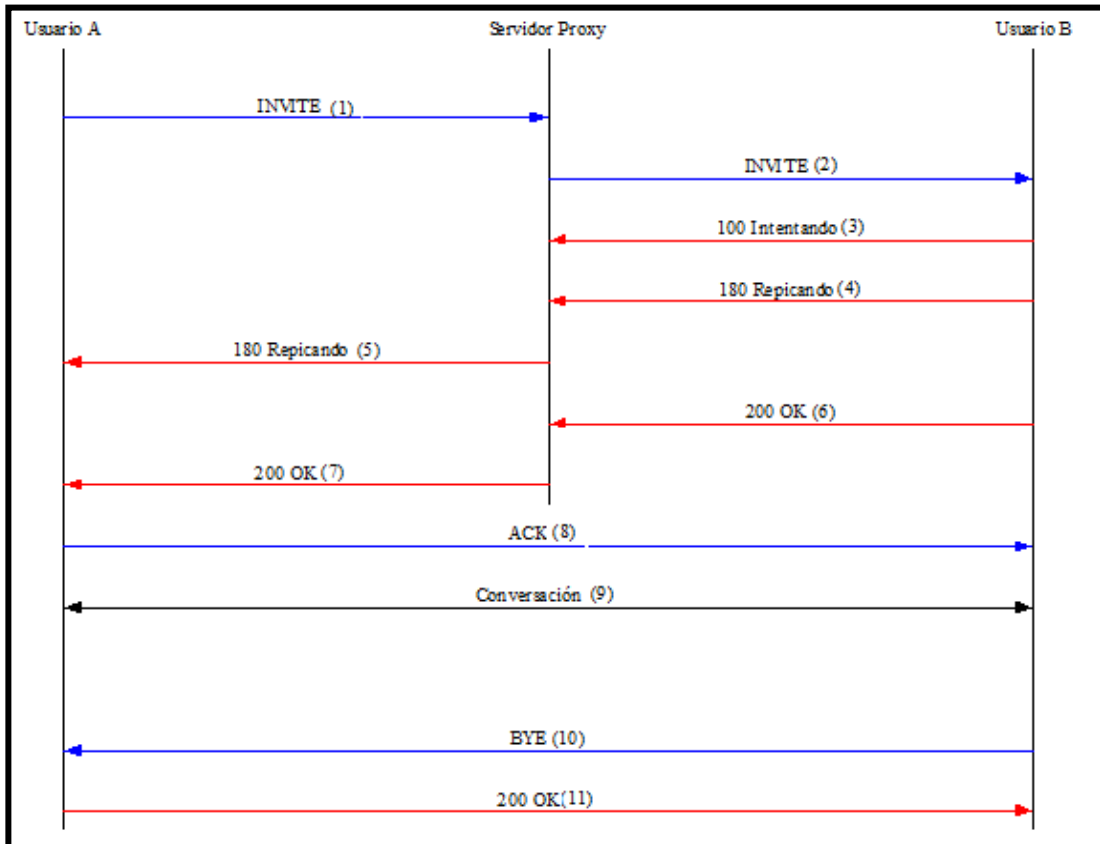


Figura 1-3. Establecimiento y finalización de una llamada SIP

Fuente: “ De elaboración propia”

Como se puede observar en la Figura 1-3, el mensaje que comienza el establecimiento de una llamada SIP es la solicitud “INVITE” (1). Es importante señalar, ésta es la única solicitud especificada en el RFC 3261, que puede originar la

creación de un diálogo. Sin embargo, puesto que no se ha establecido uno, ésta es una solicitud fuera de diálogo.

El servidor proxy recibe esta solicitud “INVITE” y la encamina hacia el usuario B (2). El usuario B responde con el mensaje 100 (Intentando) (3) para indicar al servidor proxy que se están tomando acciones para establecer la sesión. Esta respuesta se diferencia de otras respuestas provisionales en que nunca es reenviada por un servidor proxy. Luego el usuario B envía una respuesta 180 (Replicando) (4) para indicar al usuario A que se está alertando al usuario B. Esta respuesta es encaminada por el servidor proxy (5).

Una vez que el usuario B decide aceptar la sesión, envía una respuesta 200 (“OK”) (6) al usuario A y este mensaje es encaminado por el servidor proxy hacia el usuario A (7). Al llegar esta respuesta al usuario A, el diálogo queda completamente establecido. Por consiguiente, cualquier solicitud que se envíe a partir de este momento es una solicitud dentro de diálogo. Esto incluye a la solicitud “ACK” (8), la cual es enviada para indicar que se reconoce la respuesta 200. Después que se envía esta solicitud se establece la sesión (9). Cabe destacar, que en este momento comienza el flujo de voz a través de los dos participantes, sin pasar por el servidor proxy y transportado por el protocolo RTP.

Para finalizar la sesión y el diálogo, se envía una solicitud BYE. En este caso, el usuario B es el que finaliza la sesión mandando la solicitud “BYE” (10), la cual es respondida por el usuario A con un mensaje “OK” (11), concluyendo así la sesión.

1.2.2 IAX2

1.2.2.1 Tramas IAX2

Para intercambiar el audio y la señalización entre los participantes de la llamada se utilizan dos tipos de *frames* llamados Full y Mini. También se les suelen llamar F y M.

1.2.2.1.1 Full Frames

Los Full Frames pueden enviar los datos de señalización o el tráfico de voz. Generalmente, se utilizan para controlar el inicio, la configuración y la finalización de una llamada IAX, sin embargo, también pueden ser utilizados para transportar un stream de datos, aunque esto no suele ser óptimo.

Las tramas completas se envían de forma confiable, por lo que todos los Full Frames requieren una confirmación inmediata luego de su recepción. Este reconocimiento puede ser explícito a través de un mensaje 'ACK' o implícito basado en la recepción de una respuesta adecuada a los Full Frames emitidos.

La longitud del encabezado de un Full Frames es de 12 octetos. En la siguiente figura se podrá apreciar los campos y su longitud, que componen un Full Frame.

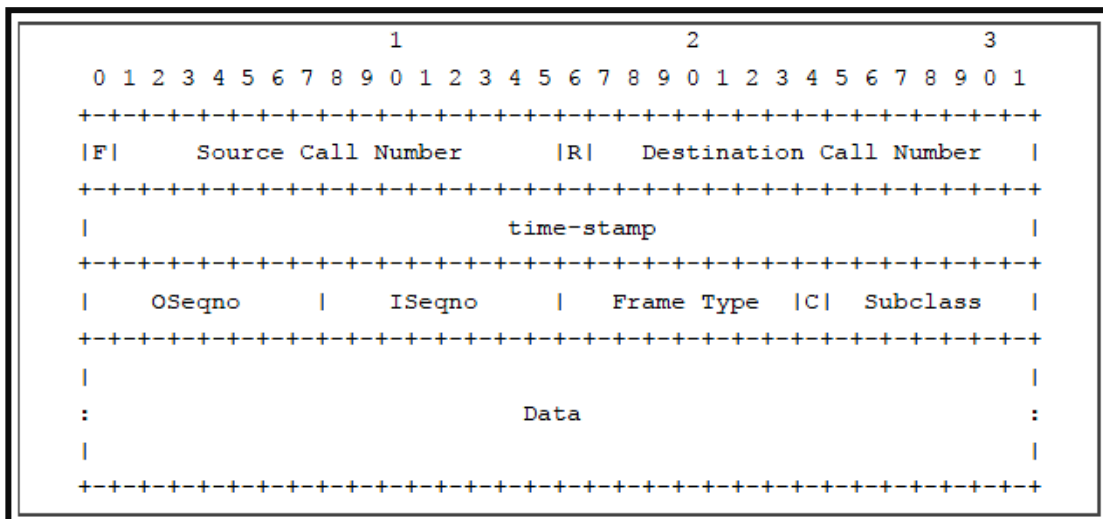


Figura 1-4. Full Frame

Fuente:(Landivar, 2008, pág. 216)

El significado de cada uno de los campos es el siguiente:

- **F:** es un bit que indica si la trama es F (full frame) o no. Para que sea F o full frame debe contener un 1.
- **Source Call Number:** 15 bits que identifican la conversación de origen ya que puede haber varias comunicaciones multiplexadas por la misma línea.
- **R:** bit de retransmisión. Adquiere un valor de “1” cuando la trama es retransmitida.

- **Destination Call Number:** identifica el destino
- **Timestamp:** registra el tiempo en cada paquete enviado.
- **OSeqno:** número de secuencia de salida con 8 bits. Comienza en 0 y se incrementa cada mensaje.
- **ISeqno:** similar a OSeqno pero representa el número de secuencia para la entrada.
- **Frame Type:** indica de qué clase de trama se trata.
- **C:** un 0 indica que el campo subclase debe tomarse como 7 bits (un solo mensaje). Un valor de 1 indica que el campo subclase se obtiene con 14 bits (dos mensajes consecutivos).
- **Subclass:** Subclase del mensaje.
- **Data:** datos que se envían en formato binario.

1.2.2.1.2 Mini Frames

Mini Frames se llaman así debido a que su cabecera es conformada por tan solo 4 octetos. Las Tramas Mini no llevan ningún control o señalización de datos, su único propósito es llevar a un flujo de medios en una llamada ya establecida IAX2. A diferencia de los Full Frames, éste no está orientado a la conexión, por lo que la transmisión es poco confiable. Esta decisión fue tomada debido a que las llamadas en VoIP típicamente pueden perder varios frames sin obtener una degradación significativa en la calidad de llamada, mientras que la sobrecarga producida para garantizar la fiabilidad aumenta los requisitos de ancho de banda y disminuye el rendimiento.

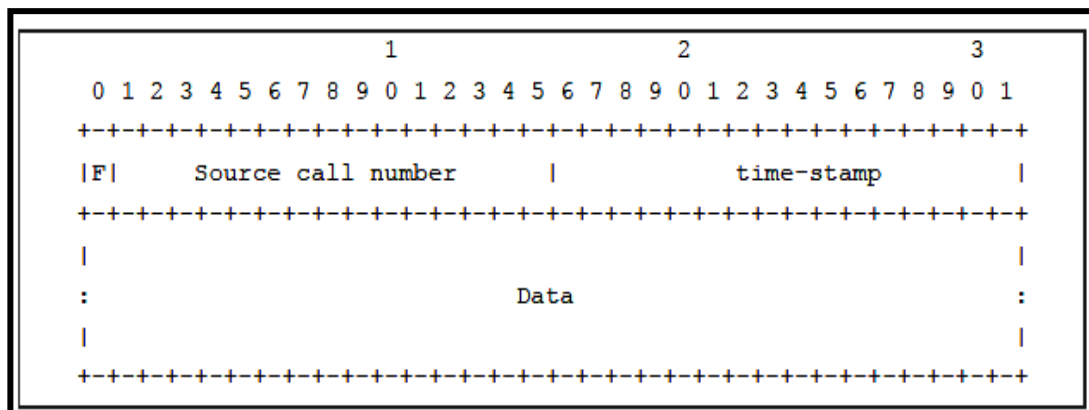


Figura 1-5. Mini Frame

Fuente:(Landivar, 2008, pág. 216)

1.2.2.2 Establecimiento y finalización de una llamada IAX

En este estándar el establecimiento y finalización de una llamada se suele separar en 3 procesos llamados establecimiento, flujo y finalización de la llama. Estos procesos se pueden observar mejor en la siguiente figura.

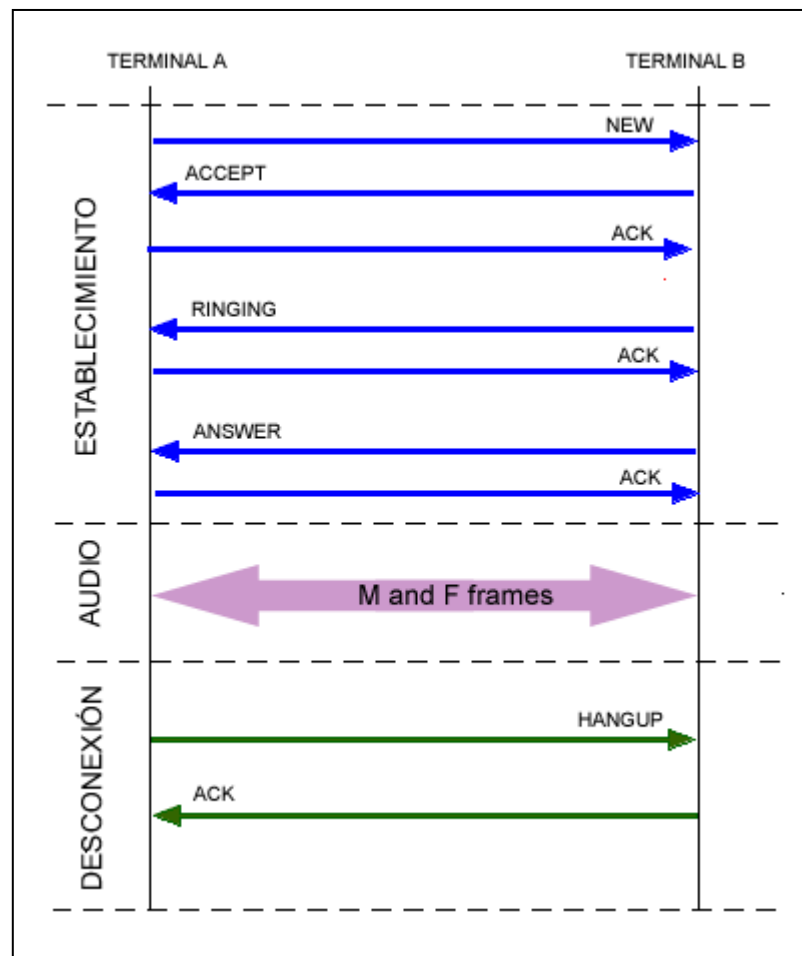


Figura 1-6. Establecimiento y finalización de una llamada IAX

Fuente: (VoIP Foro)

Como se puede observar en la Figura 1-6 el establecimiento de la llamada empieza cuando el terminal A envía el mensaje “new” hacia el terminal B, si el terminal B acepta la llamada se envía un mensaje al terminal A un “Accept” y cuando esté es recibido, el terminal A responde con un mensaje “Ack”, que simplemente representa un acuse de recibo .Luego el Terminal B envía al terminal A un mensaje “ringing”, significando que el terminal B esta repicando .Seguidamente el terminal A responde con un “Ack” en donde reafirma la llegada del mensaje, al final el terminal B acepta y responde el mensaje con “Answer”, para luego ser respondido por el terminal A con “Ack”, finalizando así el proceso de establecimiento de la llamada.

Después empieza el intercambio de datos o voz, esto se realiza de manera bidireccional entre los terminales, entre éstos se envían los Frames M y F.

Para finalizar, cuando alguno de los dos terminales desee liberar la llamada, simplemente se envía un mensaje de tipo “hangup” y el terminal al cual confirma la recepción del mensaje con un “Ack”.

1.2.3 H.323

Es una recomendación del UIT-T que describe una arquitectura y un grupo de protocolos para establecer y gestionar sesiones de multimedia en una red de conmutación de paquetes. Ésta describe los elementos de un sistema H.323, lo que incluye terminales, Gateways, Gatekeepers, controladores multipunto, procesadores

multipunto y unidades de control multipunto. Cabe destacar, que también describe los mensajes y procedimientos de control para comunicar estos componentes.

1.2.3.1 Elementos

1.2.3.1.1 Terminales

Los terminales son el cliente de puntos finales que proporcionan en tiempo real una o dos vías de comunicación. Todos los terminales deben soportar las comunicaciones de voz; video y datos son opcionales. H.323 especifica los modos de operaciones necesarios para que los terminales puedan trabajar con audio, video y datos al mismo tiempo.

Es importante señalar, que todos los terminales H.323 también deben ser compatibles con H.245, que se utiliza para negociar las capacidades y el uso del canal. Además, de tres componentes adicionales como son: una versión a escala reducida de Q.931 para señalización y configuración de llamadas; Inscripción / Admisión / Status (RAS), que es un protocolo utilizado para comunicarse con un Gatekeeper y por último RTP / RTCP para la secuenciación de audio y los paquetes de vídeo.

1.2.3.1.2 Gateways

Son elementos opcionales dentro del entorno H.323, los cuales son utilizados para diversos niveles de conversión de protocolos. Una puerta de enlace o Gateway, comprende una Media Gateway (MG) y un Media Gateway Controller (MGC), que comúnmente son dispositivos físicamente distintos. El MG sirve como un convertidor de protocolo entre las redes y los dispositivos que tienen capacidad nativa H.323 y los que no. La puerta de enlace, también puede traducir entre audio, vídeo y formatos de datos. Finalmente, el Gateway puede realizar conversiones entre los sistemas de señalización de protocolo de paquetes H.225 y protocolos externos tales como el Sistema de Señalización 7 (SS7) y Q.931. Cabe mencionar, que alternativamente, las conversiones de señalización se pueden realizar por los Gatekeepers, procesadores de llamada, o Session Border Controllers. [17]

1.2.3.1.3 Gatekeepers

Actúan como los puntos centrales en zonas H.323 (es decir, zonas de control). Los puntos finales pueden comunicarse directamente, ya sea en un ambiente unicast o multicast, si no está presente el gatekeeper. Si éste está presente, todos los puntos finales en su zona deben registrarse en él. El gatekeeper realiza la función de control de admisión, además determina si los dispositivos están autorizados a conectarse y si hay suficiente ancho de banda para soportar la llamada.

Por otra parte, los Gatekeepers sirven para traducir las direcciones IP de LAN en direcciones de Internetwork Packet Exchange (IPX), tal como se definen en la especificación RAS. También puede actuar para enrutar llamadas H.323 a través de

Gateways, si es necesario, y supervisar la capacidad de tasa de bits de la red, con la habilidad de negar el acceso a una sesión si los umbrales programables de ancho de banda se han alcanzado o superado. Por último, también pueden llevar a cabo determinadas funciones administrativas, tales como la contabilidad, la facturación, el directorio y la recopilación de datos de uso de red. Es importante señalar, que los guardianes pueden ser elementos distintos de la red, o se puede incorporar sus funciones en los MCUs

1.2.3.1.4 MCU, MC y MP

Multipoint Control Units (MCU) es el apoyo en conferencia entre tres o más participantes terminales. El MCU dispone de un controlador multipunto (MC) y opcional procesadores multipunto (MP). El MC es el responsable de la negociación en el control de llamadas para alcanzar niveles comunes de comunicación. El MP puede procesar ya sea un solo flujo de medios o múltiples flujos de medios, dependiendo de la naturaleza de la conferencia.

1.2.3.2 Stack de Protocolos

H.323 no puede considerarse como un protocolo dependiente de sí mismo, sino más bien se trata de una recomendación que especifica el modo de interactuar de varios protocolos entre sí. En la Figura 1-7 se muestra el stack de protocolos más importantes de la recomendación H.323.

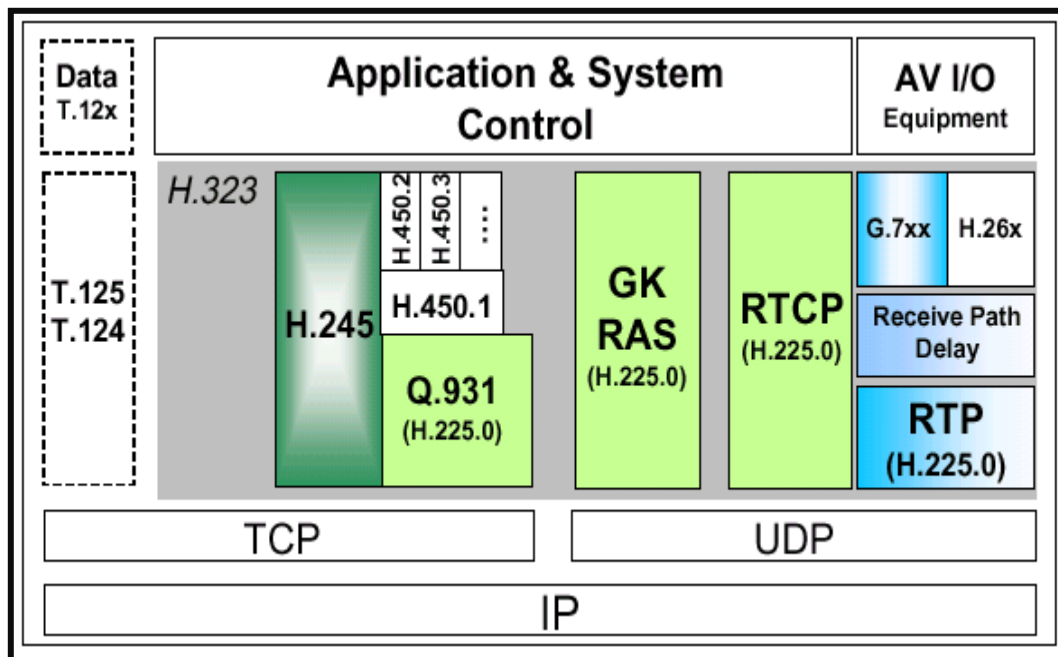


Figura 1-7. Stack de protocolos

Fuente:(Escuela de Ingeniería Eléctrica de la Universidad Central de Venezuela)

A continuación se describirán brevemente algunos de los protocolos que conforman la recomendación H.323.

- **H.225:** Es un protocolo de señalización de llamada y empaquetamiento de trenes de medios para sistemas de comunicación multimedios por paquetes. Entre sus funciones esta la conocida como Registration, Admission and Status (RAS), la cual es utilizada entre un terminal H.323 y un Gatekeeper para proporcionar la resolución de direcciones y servicios de control de admisión. De igual modo, otra de sus atribuciones es la de señalización de llamadas, que hace vida entre dos entidades H.323 con el fin de establecer la comunicación. Por último, hace la función de

empaquetamiento, la cual consiste en formatear los trenes de vídeo, audio, datos y control transmitidos en mensajes de salida hacia la interfaz de la red y recupera los trenes de vídeo, audio, datos y control recibidos de los mensajes que han sido introducidos desde la interfaz de la red.

- **H.245:** Protocolo de control para comunicaciones multimedia, que describe los mensajes y los procedimientos utilizados para el intercambio de capacidad, apertura y cierre de canales lógicos para audio, vídeo y datos, control e indicaciones.

- **Real-time Transport Protocol (RTP):** como se había comentado, se utiliza para enviar o recibir información multimedia (voz, vídeo o texto) entre dos entidades.

- **H.235:** protocolo que describe la seguridad dentro de H.323, incluida la seguridad para la señalización y para los medios de comunicación.

- **H.239:** define el uso de doble secuencia en videoconferencia, normalmente uno para video en vivo y el otro para las imágenes fijas.

- **H.450:** serie que describe diversos servicios complementarios.

- **T.120:** ésta recomendación define un conjunto de protocolos para conferencia de datos

1.2.3.3 Establecimiento y finalización de una llamada

Como el objetivo principal de la tecnología VoIP es poder establecer una llamada mediante una red de datos, es importante señalar cómo los protocolos de señalización, en este caso H.323, llevan a cabo el establecimiento y la finalización de una llamada. A continuación se explicará este proceso.

La figura 1-8 muestra, cómo el canal de señalización RAS se abre antes de que se establezca cualquier otro canal. A través de este canal, el terminal A debe solicitar acceso a la red de paquetes por el gatekeeper. Esto se hace por medio de un mensaje de petición de admisión (ARQ, Admission Request) (1). El guardián de puerta concede la petición con un mensaje de confirmación de admisión (ACF, Admission Confirm) (2). Luego, el guardián de puerta indica en el mensaje ACF (2) si la señalización de llamada se envía directamente al otro punto extremo o si se encamina a través del gatekeeper. En este caso, la señalización se encaminará a través del guardián de puerta. En el mensaje ACF el gatekeeper también indica una dirección de transporte para la señalización de la llamada.

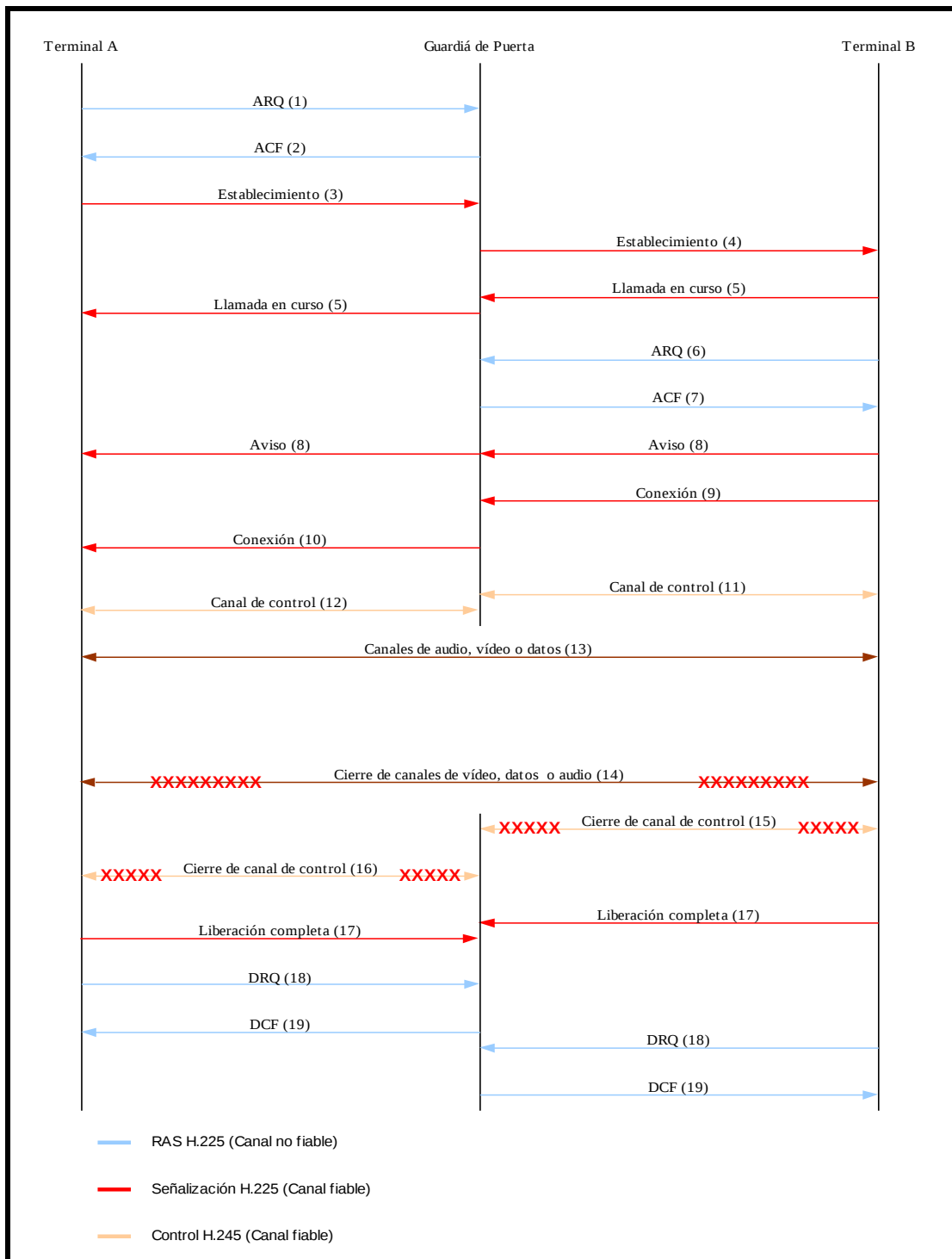


Figura 1-8. Establecimiento y finalización de una llamada H.323

Fuente:(Escuela de Ingeniería Eléctrica de la Universidad Central de Venezuela)

Seguidamente, el terminal A comienza el envío de mensajes de señalización utilizando la dirección de transporte indicada por el mensaje ACF. El terminal A envía un mensaje “Establecimiento” (3) para indicar su deseo de establecer una conexión hacia el terminal B. Luego el guardián de puerta reenvía este mensaje hacia el terminal B (4), el cual responde con un mensaje “Llamada en curso” (5) para indicar al guardián de puerta que se ha iniciado el establecimiento de la llamada solicitado y que no se aceptará más ninguna información de establecimiento de llamada. De la misma forma, el guardián de puerta envía un mensaje “Llamada en curso” (5) al terminal A. El terminal B debe responder a este mensaje al terminal A y por consiguiente, solicita el acceso al guardián de puerta por medio de un mensaje ARQ (6). Esta solicitud es confirmada con un mensaje ACF (7). A partir de este momento el terminal B puede enviar mensajes de señalización hacia el terminal A por medio del gatekeeper. Posteriormente, el mensaje “Aviso” (8) es enviado por el terminal B y encaminado por el guardián de puerta hacia el terminal A, para indicar que se ha iniciado el aviso al usuario B, en términos de hoy día, "el teléfono está repicando". Finalmente, una vez que el usuario B responde la llamada, el terminal B envía al gatekeeper el mensaje “Conexión” (9) para indicar aceptación de la llamada. Este mensaje contiene una dirección de transporte del terminal B para su utilización en el canal de control H.245 entre el guardián de puerta y el terminal B. El gatekeeper reenvía al terminal A, el mensaje “Conexión” (10), pero con una dirección de transporte de él para su utilización en el canal de control H.245 entre el terminal A y el guardián de puerta.

Una vez que ambos lados han intercambiado los mensajes de establecimiento de llamada de la fase A, los puntos extremos, si proyectan emplear H.245, establecerán el canal de control H.245 (11 y 12). Se utilizan los procedimientos de la REC. UIT-T H.245 en el canal de control H.245 para el intercambio de capacidad y la apertura de canales de medios. Después del intercambio de capacidades y la determinación de principal-subordinado, se utilizarán

los procedimientos de la recomendación H.245 para abrir canales lógicos para los diversos trenes de información (13). Los trenes de audio y vídeo, que se transmiten por los canales lógicos establecidos en H.245, utilizarán un protocolo no fiable. Las comunicaciones de datos, que se transmiten por los canales lógicos establecidos en H.245, se transportan utilizando un protocolo fiable.

Al finalizar la llamada, lo primero que se debe hacer es interrumpir las transmisiones de vídeo, datos y audio (14). Luego se deben cerrar los canales de control H.245 (15 y 16). En la figura 8 se supone que el terminal B es quien finaliza la llamada y por consiguiente, es quien cierra primero el canal de control. Después se enviarán mensajes “Liberación completa” (17) y se cerrarán los canales de señalización. Finalmente, cada punto extremo transmitirá en el canal RAS un mensaje de petición de desligamiento (DRQ, Disengage Request) al guardián de puerta (18). El guardián de puerta responderá con un mensaje de confirmación de desligamiento (DCF, Disengage Confirm) (19).

1.3 Asterisk

1.3.1 Arquitectura

Asterisk, no tiene un concepto interno de troncales o estaciones parecido a la PBX tradicional. En éste, todo lo que entra o sale del sistema pasa a través de un canal de algún tipo. Hay muchos tipos diferentes de canales, sin embargo, el dialplan de Asterisk maneja todos los canales de una manera similar, lo que significa que, por ejemplo, un usuario interno puede existir en el extremo de una troncal externa (por

ejemplo, un teléfono móvil) y ser tratado por el Dialplan exactamente de la misma manera que el usuario sería si estuviera en una extensión interna.

Un canal, es el equivalente a una línea telefónica en un circuito de voz digital, generalmente consiste en una señal analógica de un sistema de telefonía convencional o en alguna combinación de Codecs y protocolos de señalización.

Asterisk es muy modular. La distribución oficial de Digium incluye varios módulos agrupados por categorías según su funcionalidad. Desde codecs, formatos, canales, aplicaciones, etc.

1.3.1.1 Módulos

Un módulo es un componente cargable que proporciona una funcionalidad específica, tal como un controlador de canal (por ejemplo, `chan_sip.so`), o un recurso que permite la conexión a una tecnología externa (tal como `func_odbc.so`). Los módulos se cargan basados en el “archivo `/etc/asterisk/modules.conf`”. En realidad, es posible iniciar Asterisk sin módulos en absoluto, a pesar de que en este estado no será capaz de realizar la mayoría de las tareas. Sin embargo, a continuación se describirán brevemente sus módulos para comprender la naturaleza modular de Asterisk con el fin de apreciar su arquitectura.

Los módulos que conforman a Asterisk son: **[18]**

- **Applications:** se utilizan en “extensions.conf” para definir las distintas acciones que pueden ser aplicadas a una llamada. La aplicación “Dial ()”, por ejemplo, es responsable de realizar las conexiones salientes a los recursos externos y es posiblemente la aplicación del Dialplan más importante.
- **Bridging modules:** aparecen a partir de la versión 1.8 de asterisk. Realizan el actual puente de canales en las nuevas API de puente. Cada uno ofrece diferentes características, que se utilizan en diferentes situaciones en función de lo que el puente necesite. Actualmente sólo se utiliza “app_confbridge”.
- **Call Detail Recording Modules:** los módulos de CDR, están diseñadas para facilitar métodos de almacenamiento de los registros detallados de llamadas
- **Channel Event Logging Module:** canal registro de eventos proporciona un control mucho más robusto sobre la información de las actividades de llamadas.
- **Channel Drivers:** sin este módulo, Asterisk no tendría manera de hacer llamadas; cada controlador de canal es específico para cada tipo de

protocolo o canal que soporta (SIP, RDSI, etc.). El modulo de canales actúa como una puerta de entrada al núcleo de Asterisk.

- **Codec translator:** los traductores codec permiten convertir formatos de audio stream entre llamadas.

- **Format Interpreters:** realizan la función de traductores de codecs, pero hacen su trabajo en archivos en lugar de canales. Si se tiene una grabación en un menú que ha sido almacenado como GSM, necesitará de un formato intérprete para reproducir la grabación a cualquier canal que no utilice el codec GSM.

- **Dialplan Functions:** Complementan las aplicaciones de Dialplan. Ofrecen mejoras como manejo de cadenas tiempo y disputas de fechas.

- **The PBX modules:** son módulos periféricos que proporcionan un control mejorado y los mecanismos de configuración. Por ejemplo, “pbx_config” es el módulo que carga en Asterisk el tradicional Dialplan.

- **Resource modules:** integran a Asterisk con recursos externos. Por ejemplo, “res_odbc” permite interoperar con conexiones de base de datos ODBC.

- **Addon modules:** se desarrollan en la comunidad con el uso de diferentes módulos o derechos de distribución del código fuente principal. Se guardan en un directorio aparte y no se compila; se instala de forma predeterminada.

- **Test modules:** son utilizados por el equipo de desarrollo de Asterisk para validar el nuevo código, no son útiles a menos que usted sea un desarrollador del software Asterisk

[ANEXO N° 2]

[LEVANTAMIENTO DE INFORMACIÓN]

En esta etapa del proyecto se visitó todas las sedes que conforman la empresa Supra Caracas, con el fin de obtener los datos necesarios de cada LAN para formular y dimensionar una propuesta de un servicio de voz sobre IP. Se tomó en cuenta para el levantamiento de información: cantidad equipos y usuarios, acceso inalámbrico, servicios, entre otros.

A continuación se presentará, detalladamente, los datos recolectados de las diferentes sedes de Supra Caracas.

2.1 Artigas

Está conformada por un taller y un edificio administrativo de dos pisos, en los cuales se utilizan un total de 12 computadoras de escritorio y 2 impresoras, además de un enrutador con acceso inalámbrico y un switch de 8 puertos, que son los encargados de la administración de los servicios en la red.

Los usuarios en esta sede se encuentran distribuidos de la siguiente manera:

- **Primer Piso:** está conformado por seis estaciones de trabajo, las cuales tres están conectadas a la red inalámbricamente mediante el router inalámbrico y las demás se encuentran cableadas directamente hacia el switch. Los equipos de esta planta, que se conectan inalámbricamente a veces tienen problemas para establecer conexión con la red, esto se debe a que el router se encuentra en el piso superior y hay obstáculos como pisos, paredes, etc., ocasionando así una atenuación de la señal inalámbrica.

- **Segundo piso:** compuesto por seis computadoras, de las cuales tres se encuentran cableadas y las otras dos poseen acceso mediante el enrutador inalámbrico.

- **Taller:** esta localidad se encuentra ubicada a unos 50 metros de distancia del switch, la cual se encuentra cableada por UTP y solamente posee una estación de trabajo.

Para finalizar, el servicio de internet se obtiene a través de una conexión ADSL de CANTV con una velocidad de 2048 Kbps. Además, la dirección de red de la sede es 192.168.12.0/24.

2.2 La Yaguara

Esta sede conjunto con las Artigas conforman las sucursales más pequeñas de la empresa a nivel de usuarios, debido a que es una sede en constante ampliación y por los momentos se encuentran cableadas solo dos edificaciones, las cuales integran un total de veinte computadores y dos impresoras, un switch de 24 puertos y un enrutador inalámbrico.

Los dos inmuebles principales se encuentran a una distancia de 65 metros y están conectados por unos cables UTP, cabe señalar que todos los usuarios de esta sede se encuentran conectados a puntos de red.

Es importante mencionar, que por los momentos no se posee acceso a internet, sin embargo solo se espera por la instalación por parte de CANTV de una conexión ADSL con una velocidad de 2048 Kbps. Por otra parte, la dirección de la LAN es 192.168.10.13/24

2.3 Zona Rental

Cuenta con una red de 31 usuarios, de los cuales 25 son ordenadores y los 6 restantes son laptops con acceso inalámbrico, además cuenta con dos impresoras y dos servidores uno encargado del servicio de recaudación y otro funcionando como repositorio. Todos estos equipos se encuentran distribuidos mediante oficinas en la edificación de la sede.

La administración de LAN se hace a través de un enrutador con acceso inalámbrico y un switch no administrable de 24 puertos que se encuentran en la oficina principal, el switch se comunica a través de una conexión UTP con otro de 16 puertos ubicado en otra oficina que reparte el servicio a 12 ordenadores.

Como se comentó, el edificio está dividido en oficinas, en donde los usuarios se encuentran repartidos de la siguiente forma: en la principal operan 13 computadoras que están cableadas hasta el switch de 24 puertos, además 3 laptops que acceden a la red inalámbricamente. En la segunda hay 12 puestos de trabajo y todas las máquinas están conectadas físicamente mediante un cable UTP a un switch de 16 puertos, además posee 3 laptops conectadas inalámbricamente.

Por último, esta LAN posee la dirección de red 192.168.14.0 con una máscara de sub red 255.255.255.0. Además, es necesario señalar que esta sede al igual que las anteriores posee un servicio de internet mediante la empresa CANTV, la cual ofrece una conexión ADSL con una velocidad de 2048 Kbps.

2.4 Las Mayas

Es la sede más grande e importante de la empresa Supra Caracas en ella coexisten más de 300 empleados y posee 7 edificaciones que conforman un gran complejo ubicado al Sur de Caracas en el sector las Mayas. Cuenta con un servicio de internet que proporciona CANTV ABA de 2048 Kbps.

Debido a la importancia que tiene esta sede para la empresa, además de ser el lugar donde se realizaron la mayoría de las investigaciones, pruebas y ensayos para este proyecto. Se recolectaron los datos acerca de las redes con una mayor precisión y detalle, los cuales serán presentados a continuación.

2.4.1 Cableado troncal, backbone o vertical

Es la columna vertebral del cableado de esta sede, el cual tiene como objetivo proporcionar interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones. Como se podrá observar en la siguiente figura el backbone se encuentra dividido por 4 tramos, los cuales posee características y estructuras distintas.

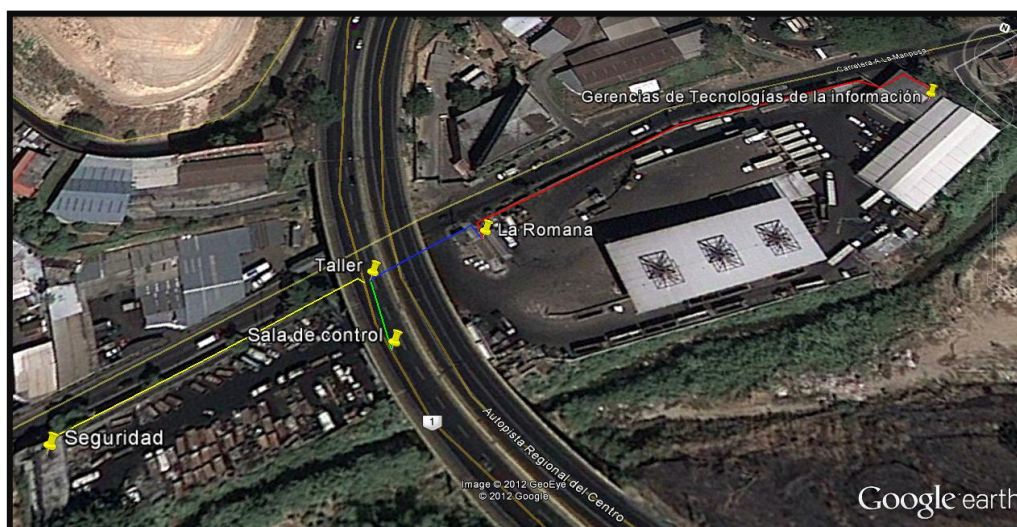


Figura 2-1. Backbone Sede las Mayas

Fuente: “De elaboración propia”

- **Gerencia - La Romana:** este es el tramo de mayor importancia, ya que en la Gerencia de Tecnologías de la información, se encuentra el cuarto de telecomunicaciones, que es el núcleo de toda la red de Supra Caracas Las mayas. Además, provee el acceso a la red de La romana, el cual es el punto de control de la entrada de desechos sólidos. Este trayecto es de aproximadamente 250 metros, en la que se utilizan una serie de switches, que funcionan como repetidoras, para que la señal no se atenúe.

- **Romana - Taller:** cuenta con una longitud cincuenta y cinco metros de largo (55 m), en donde la mayoría del trayecto se hace aéreo, sin protección de cableado, debido a las condiciones del terreno. Al igual que el trayecto anterior este utiliza cable UTP categoría 5e.

- **Taller - Sala de control:** es un trayecto de 30 m de largo, que se encuentra interconectado por cable UTP categoría.

- **Taller – seguridad:** es un segmento de aproximadamente 150 m de largo, en donde no se usa ningún switch intermedio y su conexión es por medio de cable UTP. A pesar que supera por 50 metros a las recomendaciones asociadas al cable UTP categoría 5e, las pruebas de comunicación siempre han resultado satisfactorias.

- **Gerencia de tecnologías de la información - Planta baja:** éste es el tramo más pequeño de todos , comienza en un switch de 24 puertos, en el Cuarto de telecomunicaciones ubicado en el segundo piso del edificio sede, pasando por otro switch, ubicado en almacén, hasta llegar a planta baja a un switch de 24 puertos. Todo este trayecto no pasa de los 20 metros y está compuesto en su totalidad por cable UTP categoría 5e.

2.4.2 Representación lógica y física de la Red

Para poder hacer una representación de la red, se utilizará la Figura 2-2, en donde se puede observar como diferentes sub redes se encuentran en una misma Vlan, pero donde se encuentra una estructura completamente jerárquica.

Se puede detallar, el círculo amarillo que representa el núcleo donde se encuentran todos los servicios de la red, además de contener la puerta de enlace hacia el Internet, es fácil notar que se encuentra en lo más alto de la jerarquía. Si falla este nodo, todo los demás nodos sentirán el efecto de dicha falla tanto en los servicios como en la conexión.

También se observa, nodos de distribución como el almacén y la romana, que son prácticamente puntos de interconexión entre otros sub nodos que prestarán servicios de acceso en diferentes estaciones como por ejemplo: sala de control, seguridad, taller entre otros.

Además de esta diferenciación jerárquica, existe otra clasificación lógica, como es la de las sub redes. La cual será clarificada en los apartados siguientes, pero se puede adelantar que los círculos naranja, cian, verde rojo, morado y amarillo pertenecen a la sub red 192.168.10.0/24, el negro representa a la red 172.16.14.0/24 y por último al azul, le corresponde la sub red 192.168.11.0/24.

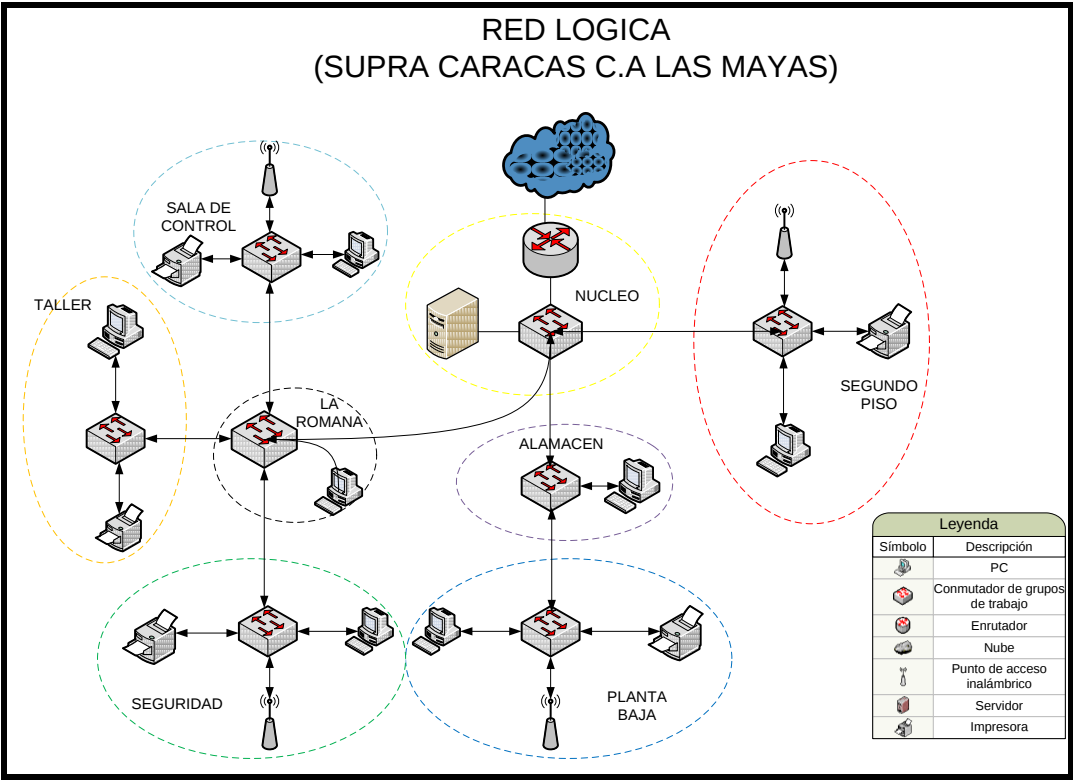


Figura 2-2. Topología Lógica

Fuente: “De elaboración propia”

Por otra parte, para visualizar la representación física de la red, se puede observar la Figura 2-3, en donde se nota, que en la sede de Supra Caracas Las Mayas, se optó por estructurar que todos los nodos secundarios fuesen switches, esto supone una gran ventaja en comparación con los hubs, ya que se segmentan los dominios de colisión y los switches dedican todo el ancho de banda a cada uno de sus puertos por igual.

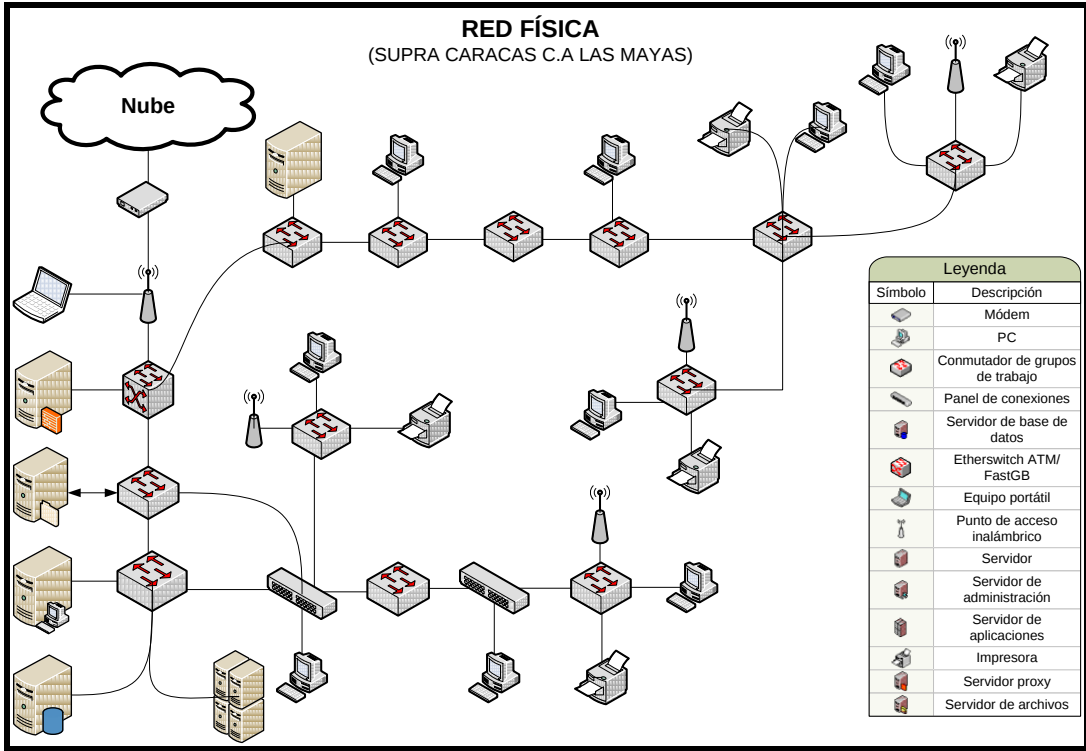


Figura 2-3. Topología Física

Fuente: “De elaboración propia”

2.4.3 Segmentos de red

En Supra Caracas las Mayas, la red se encuentra segmentada en tres subredes, que permiten un mejor desempeño y control de los servicios implementados en las mismas.

2.4.3.1 Sub red las Mayas 192.168.10.0/24

Es la red principal de Supra Caracas las mayas, se encuentra la mayoría de los servicios presentes en toda la red, así como también la puerta de enlace hacia la red pública de Cantv. Se puede señalar, que en este segmento de red se encuentra el núcleo de distribución de toda la red de Supra Caracas las Mayas.

Esta red está compuesta, por 3 Switch de 24 puertos, 5 enrutadores inalámbricos, 6 servidores, 5 impresoras y 50 equipos finales distribuidos entre laptops y ordenadores

Por último, entre los departamentos se encuentran: la Gerencia de las Tecnologías de la Información, Recursos Humanos, Bienestar Social, Compras, Nomina, Gerencia General, Consultoría Jurídica, Servicios Generales, Seguridad, Control y Operaciones.

2.4.3.2 Sub red las mayas 172.16.14.0/24

Esta sub red, fue creada con el propósito de separar el sistema de la romana, de cualquier otra red, para así establecer una red dedicada, solo para este sistema, incrementando así su seguridad. Asimismo, se especifica que el sistema de la romana es el encargado de monitorear y controlar el acceso de desechos sólidos a la planta.

La red cuenta solamente, con 2 swtichs, un servidor y 3 computadoras, que son necesarias y suficientes para administrar el sistema completo de la romana. Donde se encuentra, la coordinación de operaciones, la cual es la única que maneja el sistema de la romana, no obstante la Gerencia de Tecnología de la información es la que posee el servidor que contiene el servicio de la romana.

2.4.3.3 Sub red las mayas 192.168.11.0/24

Esta es una subred, donde su área de captación es todo el piso de planta baja del edificio sede de Supra Caracas C.A las Mayas. En esta red, no se encuentra ningún sistema o servicio importante solamente es utilizada para darle acceso a internet e interconectar localmente a los host que encuentran en la planta baja de la sede.

Otro aspecto de esta red es que no cuenta con host directamente cableados, si no que la mayoría, por no decir todos, utilizan el acceso inalámbrico para poder acceder a la a red. Está integrada, por un router inalámbrico, una impresora y 15 usuarios que fluctúan en el uso de PC y laptops.

Finalmente, se encuentran los departamentos de Nómina, Auditoria y Proceso, Registro y Control, Gerencia de Operaciones y por último Gerencia de Tecnologías de la Información

2.4.4 Población estimada de usuarios para el servicio de Voz sobre IP

Aunque la población de la red de Supra Carcas se ubica en más de 120 usuarios, una buena parte de ellos no podrá acceder al servicio por seguridad y política de la empresa, por lo cual en principio se estima que un 40% de los usuarios sean los que utilicen el servicio de VoIP

Es importante señalar, que respecto al crecimiento de la empresa en los últimos 7 meses no ha habido nuevos ingresos, dando a pensar que el crecimiento esperado será bajo y no superará al 10% en los próximos meses. Debido a esto, solo se estimará un 10% más de lo esperado para la definición de los usuarios para el servicio de voz sobre IP. A continuación se mostrará una tabla con el total de usuarios y los estimados.

Tabla 2-1. Población estimada de usuarios para el servicio de voz sobre IP

Fuente: “De elaboración propia”.

Sede	Total de usuarios en la sedes	Usuarios estimados VoIP
Las Artigas	12	5
La Yaguara	20	8
Zona Rental	31	13
Las Mayas	69	30
Total	132	56

[ANEXO N° 3]

[CONFIGURACIONES]

En esta sección, se presentará las configuraciones básicas necesarias para poder ejecutar un servidor Elastix, que pueda realizar tareas como registro de usuarios y ejecución de llamadas. Cabe destacar, que el software Elastix permite llevar a cabo diferentes tareas, sin embargo el propósito de estas configuraciones es dejar las bases para un servicio de Voz sobre IP.

3.1 Servidor Elastix

3.1.1 Instalación de Elastix

El siguiente procedimiento de instalación borrará todos los datos de su disco duro, donde se recomienda hacer esta instalación en un disco que no tenga ninguna información importante.

Se verifica que el computador tenga la orden de arranque el CD-ROM o DVD-ROM en el BIOS. Luego, se introduce el CD y comienza la instalación. Lo primero que debe observarse en la pantalla será el logo de Elastix con varias opciones para escoger, sin embargo en este caso sólo se le dará a ENTER.

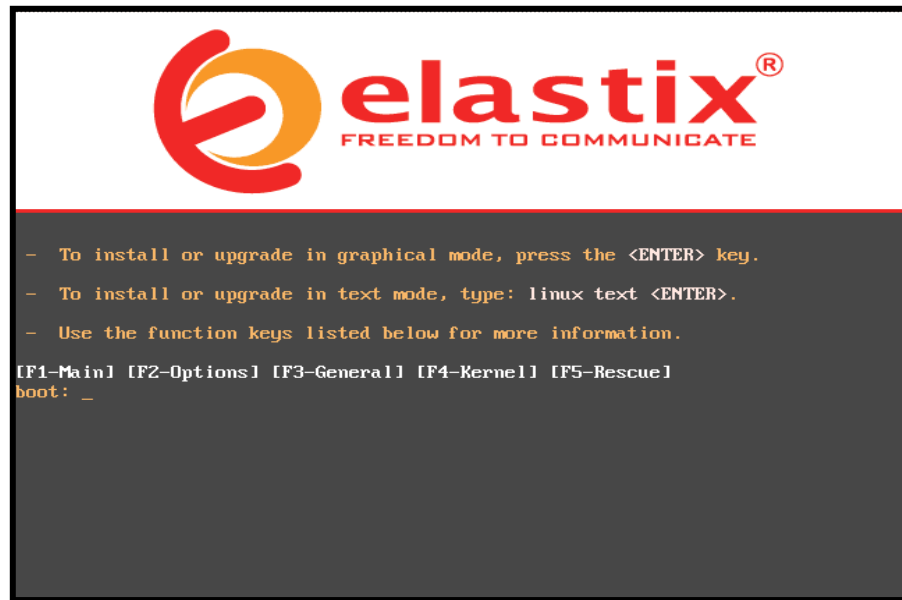


Figura 3-1. Cuadro de instalación de Elastix

Fuente: “De elaboración propia”

Luego de esto, el sistema irá mostrando una serie de datos y parámetros hasta llegar a una pantalla donde pide seleccionar el lenguaje de la instalación. Se selecciona español como se muestra en la siguiente figura.

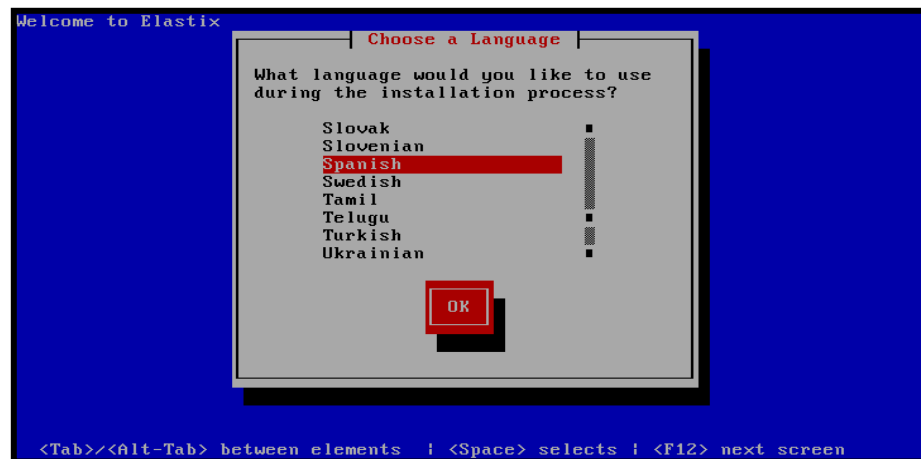


Figura 3-2. Elección del lenguaje

Fuente: “De elaboración propia”

Seguidamente, el sistema pedirá la configuración del teclado a utilizar y se selecciona en este caso el español.

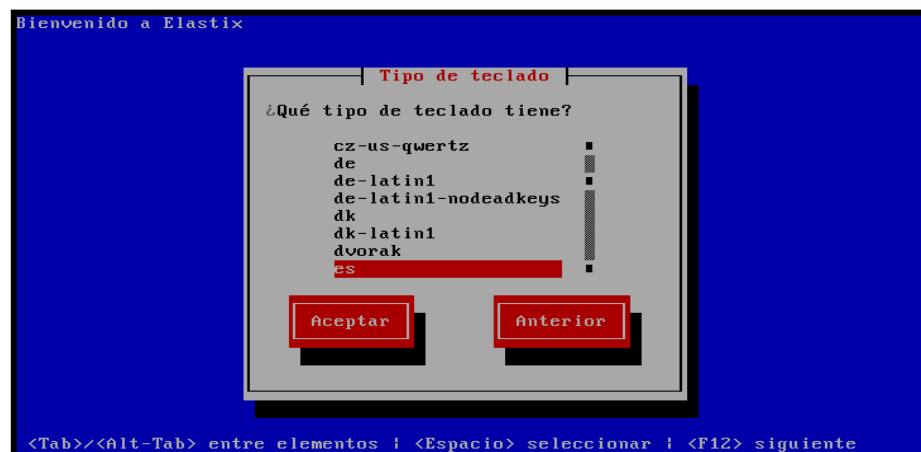


Figura 3-3. Elección del tipo de teclado

Fuente: “De elaboración propia”

Posteriormente, se entra a una pantalla de recibimiento, donde se da la bienvenida a Elastix; se le da click en “aceptar” y luego el sistema se dirige a una opción donde se debe seleccionar el tipo de partición del disco duro y cómo se quiere distribuir dichas particiones

Lo recomendable, es dejar que el sistema haga sus particiones automáticamente ya que viene optimizado para ello. Se debe seleccionar la primera opción “mis particiones en dispositivos seleccionados y crear diseño predeterminado”.



Figura 3-4. Selección del tipo de partición

Fuente: “De elaboración propia”

Cuando se selecciona "Aceptar y se presiona "ENTER", saldrá un cuadro de aviso el cual advierte sobre si se está seguro de borrar toda la información de disco, a lo que se le responde que sí.



Figura 3-5. Borrando disco

Fuente: "De elaboración propia"

Finalizado esto, saldrá un mensaje preguntando si se quiere revisar cómo han quedado las particiones y se responde que no. Se continúa con la siguiente pantalla en donde el sistema pedirá el gestor de arranque. Por defecto aparece en la primera opción GRUB, la cual se selecciona y se le da "Aceptar"

En la siguiente pantalla a continuación, se debe seleccionar "SI", ya que con esto se estará accediendo a la configuración de la interfaz Ethernet del servidor.



Figura 3-6. Elección de la configuración de interfaz de red

Fuente: “De elaboración propia”

A continuación saldrá una pantalla en la cual se debe seleccionar “activar el soporte IPv4”, para luego darle “Aceptar” y continuar con la configuración.

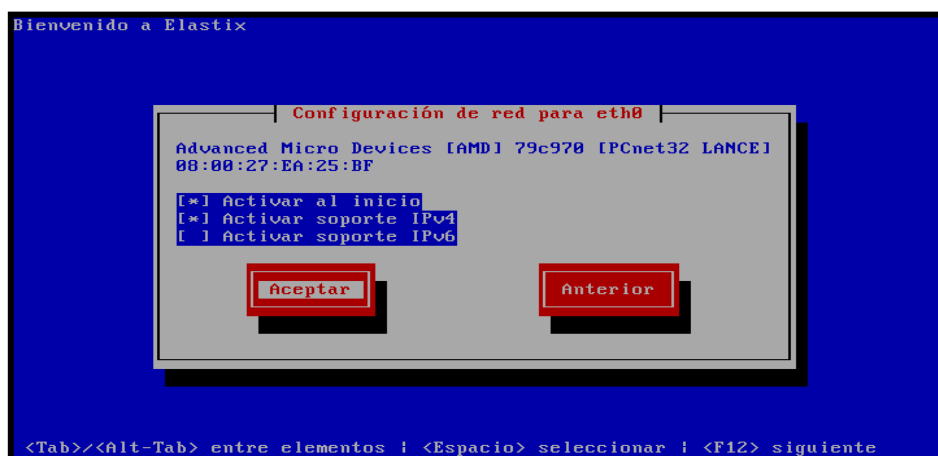


Figura 3-7. Activación del soporte IPV4

Fuente: “De elaboración propia”

Seguidamente, lo primero que se debe hacer es desplazarse hasta la opción q "Configuración de IP dinámica", donde aparecerá entre paréntesis un símbolo de asterisco (*). Esto quiere decir que la opción de obtener una dirección IP desde un servidor DHCP está habilitada (es la que viene siempre seleccionada por defecto en las instalaciones de Elastix). Una vez sobre la opción antes mencionada, se presiona la barra espaciadora para deseleccionar el símbolo de (*) y proceder a la siguiente línea donde se puede introducir de forma manual la dirección IP, la máscara de red como se muestra a continuación.

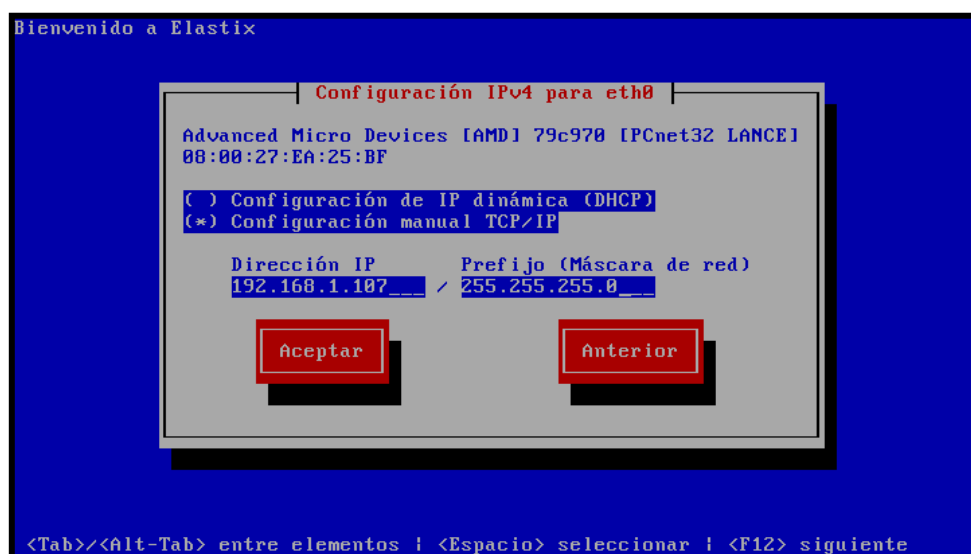


Figura 3-8. Configuración manual TCP/ IP

Fuente: "De elaboración propia"

Luego de seleccionar "Aceptar" aparece otra pantalla, en la cual se debe ingresar manualmente la puerta de enlace y los DNS primario y secundario, para después darle "Aceptar". Como en el ejemplo de la siguiente figura,

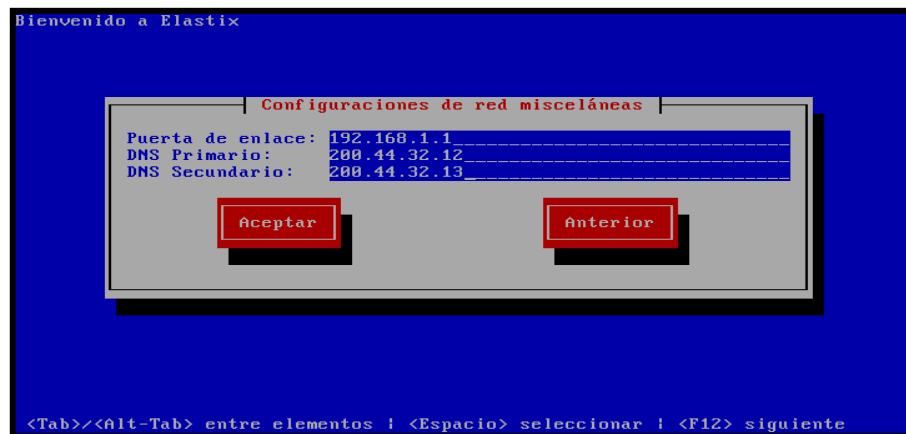


Figura 3-9. Configuración d la Puerta de enlace y DNS

Fuente: "De elaboración propia"

Para finalizar con las configuraciones de la red, saldrá una última pantalla donde el sistema pedirá ingresar el nombre del host, donde se selecciona manualmente y se ingresa el nombre del host como en la Figura 3-10.



Figura 3-10. Nombre del Host

Fuente: "De elaboración propia"

Cuando se termine de configurar la pantalla anterior, saldrá la opción “selección del huso horario”, en este caso se selecciona "América/Caracas" y se prosigue con la instalación.

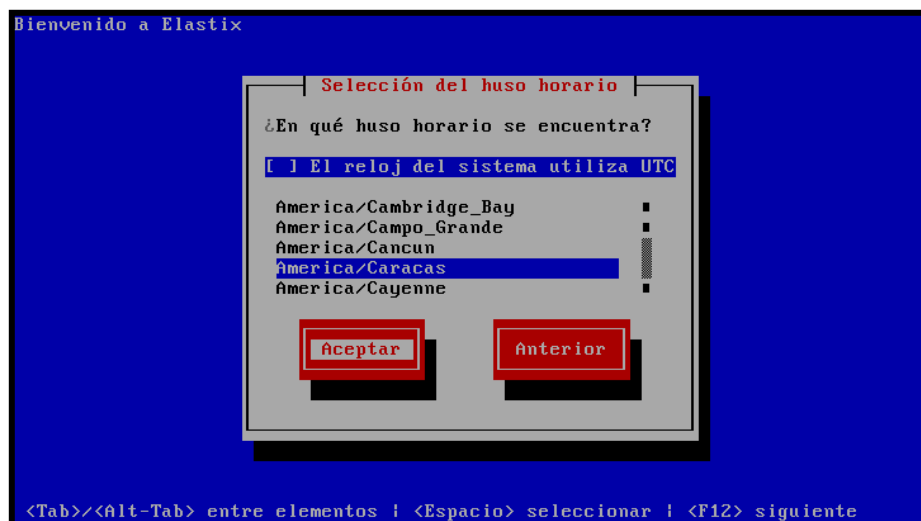


Figura 3-11. Selección del huso Horario

Fuente: “De elaboración propia”

Después, saldrá un cuadro, en el cual se solicita asignar una contraseña al usuario root, que es el administrador del sistema. Es muy importante no perder esta contraseña ya que podría terminar con una reinstalación de todo el sistema si esto ocurre.



Figura 3-12. Configuración de la contraseña de root

Fuente: "De elaboración propia"

Finalizado el cuadro anterior, se llegara a otro en el cual el sistema solicita seleccionar cuales paquetes se desean instalar; este cuadro se deja intacto y solamente se selecciona "Aceptar".



Figura 3-13. Selección del grupo de paquetes

Fuente: "De elaboración propia"

Seguidamente, el sistema comenzará a hacer unas rutinas de preparación, verificando dependencias, paquetes, etc. Cuando esto finalice se dirigirá a una ventana donde se mostraran todas las actividades del proceso de instalación.

Luego comenzará con el formateo de las particiones ya creadas y los sistemas de archivos. Al término de esto, se podrá observar una pantalla en la cual se mostrarán las instalaciones de cada uno de los paquetes que componen a Elastix.



Figura 3-14. Instalación del paquete

Fuente: “De elaboración propia”

Cuando la barra de progresión de la parte de abajo llegue al 100%, entonces ya se obtendrá el sistema instalado completamente. Éste se reiniciará y cuando vuelva a iniciar mostrará una pantalla similar a la pantalla inicial que se observó cuando se introdujo el CD de instalación. Con esto, se da por finalizado el proceso

de instalación y lo único que se mostrará en el arranque son dos opciones. De la cual, siempre se debe seleccionar la opción por defecto que es la "Elastix-base".

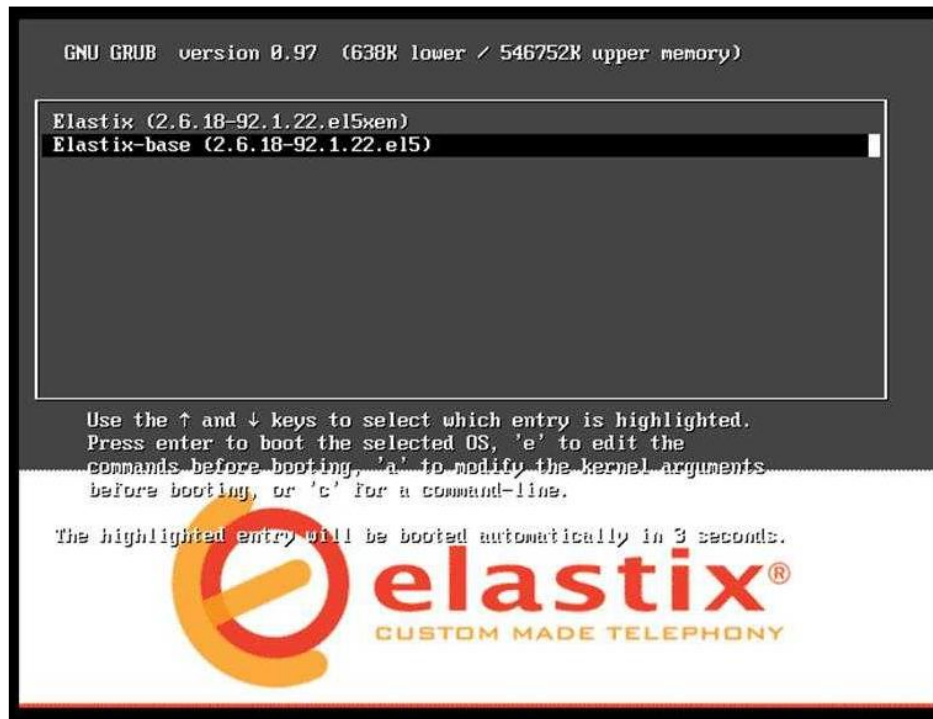


Figura 3-15. Arranque del servidor Elastix

Fuente: "De elaboración propia"

3.1.2 Creación de extensiones

Es importante saber que a la hora de configurar la IP PBX existen dos métodos que llevan al mismo resultado, uno es mediante la interfaz gráfica y la otra es ejecutando la consola de Asterisk. No obstante, en esta sección solamente se explicará cómo configurar la IP PBX utilizando la interfaz gráfica.

Como primer paso para ingresar a la interfaz gráfica, es necesario acceder a la consola del servidor Elastix con el usuario “root” y la contraseña previamente establecida, luego aparecerá el URL que se debe digitar en el navegador para ingresar a la consola Web, asegúrese que la dirección IP corresponda a la asignada durante la instalación. Seguidamente, se debe ejecutar cualquier navegador e ingresar la dirección IP como se muestra en las siguientes figuras.

```
CentOS release 5.9 (Final)
Kernel 2.6.18-348.1.1.el5 on an i686

localhost login: root
Password:
Last login: Thu Apr 25 04:22:29 on tty1

Welcome to Elastix
-----

Elastix is a product meant to be configured through a web browser.
Any changes made from within the command line may corrupt the system
configuration and produce unexpected behavior; in addition, changes
made to system files through here may be lost when doing an update.

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://192.168.0.106

[root@localhost ~]#
```

Figura 3-16. Consola del servidor Elastix

Fuente: “De elaboración propia”

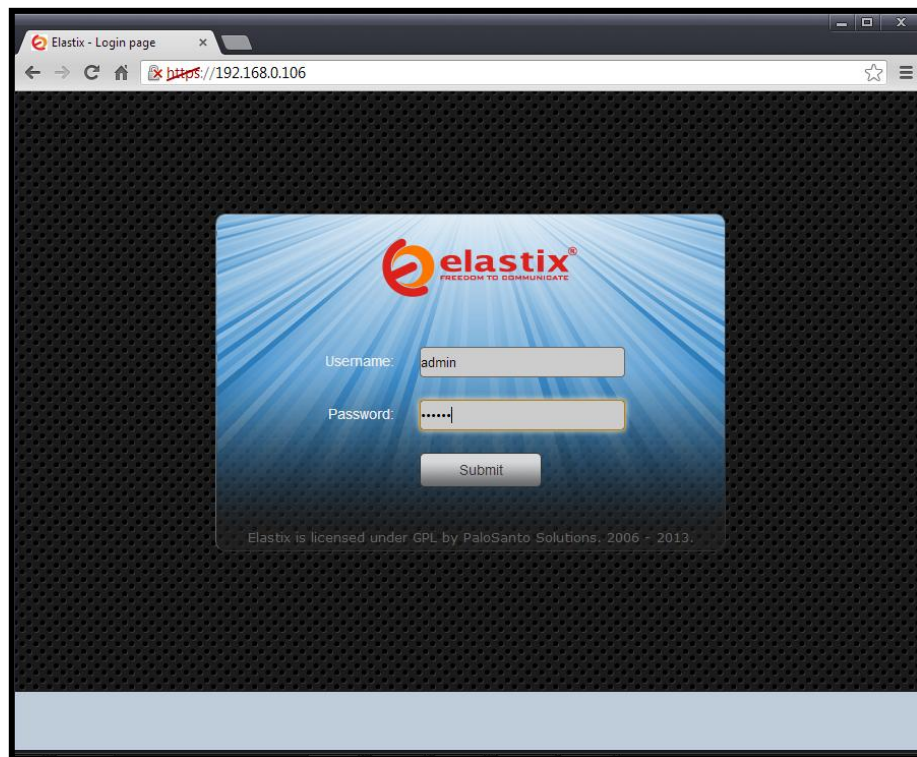


Figura 3-17. Accediendo a la interfaz Web

Fuente: “De elaboración propia”

Cuando se ingresa por primera vez, el navegador web solicitará la confirmación de los certificados de seguridad, ya que automáticamente se establece una conexión segura HTTPS. Al confirmar, los certificados de seguridad en el navegador, inmediatamente pedirá que se ingrese el usuario y la clave. Por defecto, el usuario es “admin” y la clave es la que se asignó durante la instalación.

Luego de introducir el usuario y la clave correcta, se ingresa a la consola de administración Web, desde donde se realizará la gestión de servidor Elastix, por

defecto la primera pantalla que aparece es la de información del sistema (Dashboard). La cual se puede observar a continuación.

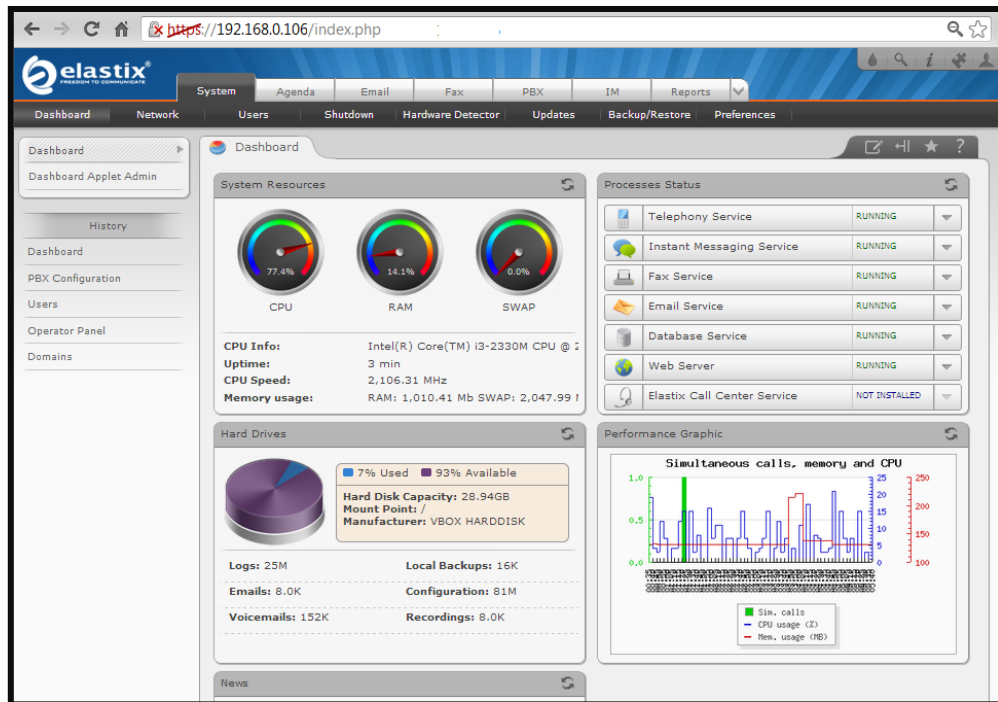


Figura 3-18. Dashboard de Elastix

Fuente: “De elaboración propia”

3.1.2.1 Procedimiento para crear Extensiones en Elastix

Una vez que se tenga acceso a la interfaz Web, se procederá a la creación de las extensiones. Para configurar una extensión se deben ingresar 4 parámetros básicos de configuración:

- El tipo de extensión SIP o IAX2
- El número de la extensión
- El nombre de la extensión
- La clave de la extensión

Cada una de las extensiones debe tener un número único, cuando se dispone de un enlace E1 con una serie de DID asignados por el proveedor, se utiliza como parámetro de asignación los últimos dígitos del plan numérico, esto facilita la marcación directa desde la PSTN hacia nuestra PBX-IP Elastix.

Para crear una extensión se siguen los pasos como se muestra en la siguiente figura.



Figura 3-19. Selección del tipo de extensión

Fuente: “De elaboración propia”

Como se puede observar, luego de desplegar el menú “Device” aparecerán distintos tipos de extensiones, pero para este proyecto solamente se utilizará “Generic SIP Device”.

Luego de hacer clic en “Submit”, se procede a crear cada una de las extensiones, asignando los 4 parámetros básicos, para este ejemplo se creará la siguiente extensión:

1.- Tipo de Extensión: **SIP**

2.- Número de extensión: **1000**

3.- Nombre de extensión: **Gregori**

4.- Clave de la extensión: **Prueba01**

En la siguiente figura se puede observar renglones resaltados en rojos, los cuales se deben editar; los demás se encuentran seleccionados por defectos y no hace falta modificarlos.

Add Extension

User Extension: 1000

Display Name: Gregori

CID Num Alias:

SIP Alias:

Extension Options

Outbound CID:

Ring Time: Default

Call Waiting: Disable

Call Screening: Disable

Pinless Dialing: Disable

Emergency CID:

Assigned DID/CID

DID Description:

Add Inbound DID:

Add Inbound CID:

Device Options

This device uses sip technology.

secret: prueba01

dtmfmode: rfc2833

Dictation Services

Dictation Service: Disabled

Dictation Format: Ogg Vorbis

Email Address:

Language

Language Code:

Recording Options

Record Incoming: On Demand

Record Outgoing: On Demand

Voicemail & Directory

Status: Disabled

Voicemail Password:

Email Address:

Pager Email Address:

Email Attachment: ☐ yes ☒ no

Play CID: ☐ yes ☒ no

Play Envelope: ☐ yes ☒ no

Delete Voicemail: ☐ yes ☒ no

IMAP Username:

IMAP Password:

VM Options:

VM Context: default

VMX Locator

VMX Locator: Disabled

Use When: ☐ unavailable ☐ busy

Voicemail Instructions: ☒ Standard voicemail prompts.

Press 0: ☒ Go To Operator

Press 1:

Press 2:

Submit

Figura 3-20. Menú de extensiones SIP

Fuente: “De elaboración propia”

Por último, después de haber rellenado los campos se debe hacer clic en “Submit” e inmediatamente aparecerá otro ítem llamado “apply configuration changes here”, en el cual es necesario hacer clic para guardar los cambios realizados.

3.1.3 Creación de Perfiles de Usuario

Luego de finalizar la creación de las extensiones, es necesario linkear esas extensiones con los usuarios de la red. Para esto se debe acceder a la pestaña “System”, luego a “User” y por último a “Create New User” como se muestra en la figura.

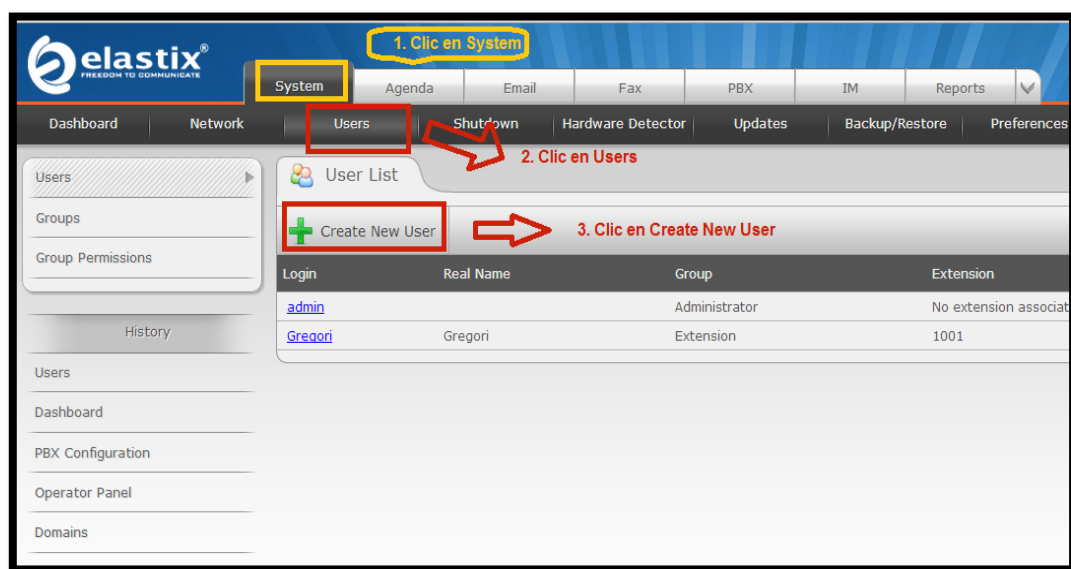


Figura 3-21. Creación de un nuevo usuario

Fuente: “De elaboración propia”

Seguidamente aparecerá una pantalla, donde se piden algunos datos como nombre de usuario, login, contraseña, grupo a que pertenece y la extensión a la cual se asociará ese perfil.

Utilizando la extensión creada en la sección anterior se procederá a rellenar los campos y a salvar los cambios como se muestra en la siguiente imagen.



Figura 3-22. Nuevo usuario

Fuente: “De elaboración propia”

Como se observa en la figura anterior, existe un campo llamado “Mail Profile”, que no fue rellenado. Esto se debe, a que ese apartado proporciona una cuenta de correo ligada al servidor Elastix, pero en esta propuesta no incluye ese servicio.

Por otra parte, es necesario aclarar que en el ítem “Group” se eligió “Extension”, esto se debe a que la mayoría de los usuarios pertenecerán a ese grupo y solo los encargados del sistema podrán acceder como administradores. El perfil “Extension” no tendrá privilegios sobre la IP PBX y aunque podrán acceder con su perfil por medio de la interfaz gráfica, no serán capaces modificar ninguna característica. Sin embargo, aquellas personas que pertenezcan al perfil “Extension” podrán visualizar su correo o agenda, si estos servicios se encuentran activados.

3.2 Softphone

A pesar de que existe una gran variedad de softphone y cada con una manera distinta de configurar, en general todos requieren de los siguientes parámetros.

- Used Id: es el número de la extensión a la cual se está asociado
- Domain: comúnmente es la IP del servidor Elastix.
- Password: es la contraseña asociada a la extensión.
- Display name: nombre que será visto por los demás usuarios.

Una vez obtenido conocimiento de los campos necesarios para configurar un Softphone, el proceso es tan sencillo como rellenar las casillas y darle aceptar. A continuación se presentará unos ejemplos con los Softphone X-lite, Qutecom utilizando de ejemplo la extensión creada anteriormente.

SIP Account

Account Voicemail Topology Presence Transport Advanced

Account name: Account 1

Protocol: SIP

Allow this account for

- ☒ Call
- ☒ IM / Presence

User Details

* User ID: 1000

* Domain: 192.168.0.106

Password:

Display name: Gregori

Authorization name: 1000

Domain Proxy

☒ Register with domain and receive calls

Send outbound via:

☒ Domain

☐ Proxy Address:

Dial plan: #1\!a.T;match=1;prestrip=2

OK Cancel

Figura 3-23. Configurando X-lite

Fuente: “De elaboración propia”

The screenshot shows a window titled "QuteCom - Login". Inside, there's a header section with a user icon and the text "Configurar el perfil de SIP" followed by "Por favor complete la información que permitirá que su programa de telefonía se conecte a su cuenta SIP". Below this are several input fields: "Nombre de la cuenta:" with the value "Gregori", "Ingreso / Nombre de usuario:" with "1000", "Contraseña:" with "*****", "Dominio SIP:" with "192.168.1.106", and "Nombre a mostrar:" with "Gregori". There is an expandable section "Avanzado" with a right-pointing arrow. At the bottom left is a "Need help?" link with a question mark icon. At the bottom right are three buttons: "Back", "Connect", and "Cancelar".

Nombre de la cuenta:	Gregori
Ingreso / Nombre de usuario:	1000
Contraseña:	*****
Dominio SIP:	192.168.1.106
Nombre a mostrar:	Gregori

► Avanzado

[Need help?](#) Back Connect Cancelar

Figura 3-24. Configurando Qutecom

Fuente: "De elaboración propia"

Como se puede ver en las figuras anteriores, con esas configuraciones ya el softphone puede registrarse al servidor Elastix, las demás configuraciones vienen por defecto y no son necesario cambiarlas, sin embargo otro de los puntos importantes es que softphone admita el codec a utilizar, en este caso el G.711 ya viene incluido en la mayoría de los softphone.