

UNIVERSIDAD AMAZÓNICA DE PANDO

ÁREA DE CIENCIAS Y TECNOLOGÍA

CARRERA DE INGENIERÍA DE SISTEMAS



PROYECTO DE GRADO

**“TELEFONÍA IP UTILIZANDO UNA RED PRIVADA VIRTUAL PARA LA
ZONA FRANCA COMERCIAL E INDUSTRIAL DE COBIJA”**

**PROYECTO DE GRADO PRESENTADO PARA OBTENER EL TITULO
ACADÉMICO DE LICENCIADO EN INGENIERÍA DE SISTEMAS.**

Postulante: Raúl Aguada Romero

Tutor: Lic. Humberto Fernández Calle

Asesor: Ing. José Balderrama Méndez

Cobija - Pando – Bolivia

2021

AGRADECIMIENTOS

Quiero agradecer en primer lugar a Dios, por guiarme en el camino y fortalecerme espiritualmente para empezar un camino lleno de éxito.

Agradecer a la base de todo, a mi familia, en especial a mis padres Edith y Raúl, esposa María Eliana e hijos Kevin Franz y Randy, a todos mis herman@s que quienes con sus consejos fueron el motor de arranque y mi constante motivación, muchas gracias por su paciencia y comprensión, y sobre todo por su amor.

Así, quiero mostrar mi gratitud a todas aquellas personas que estuvieron presentes en la realización de esta meta, de este sueño que es tan importante para mí, agradecer todas sus ayudas, sus palabras motivadoras, sus conocimientos, sus consejos y su dedicación.

Mis más sinceros agradecimientos a mi tutor de proyecto, quien con su conocimiento y su guía fue una pieza clave para que pudiera desarrollar una clave de hechos que fueron imprescindibles para cada etapa de desarrollo del trabajo.

A mis compañeros, quienes a través de tiempo fuimos fortaleciendo una amistad y creando una familia, muchas gracias por toda su colaboración, por convivir todo este tiempo conmigo, por compartir experiencias, alegrías, frustraciones, llantos, tristezas, peleas, celebraciones y múltiples factores que ayudaron a que hoy seamos como una familia, por aportarme confianza y por crecer juntos en este proyecto, muchas gracias.

¡Muchas gracias por todo!

DEDICATORIA

A mis padres que me han dado la existencia; y en ella la capacidad por superarme y desear lo mejor en cada paso por este camino difícil y arduo de la vida. Gracias por ser como son, porque con eso han ayudado a construir y forjar la persona que ahora soy.

A mis hermanos, esposa e hijos, quienes siempre me apoyaron con espíritu alentador, contribuyendo incondicionalmente a lograr las metas y objetivos propuestos.

A mis docentes y amigos; que en el andar de la vida nos hemos ido encontrando, porque cada uno de ustedes ha motivado mis sueños y esperanza de formarme como mejor persona.

RESUMEN.

El presente proyecto surge ante la necesidad de la Zona Franca Comercial e Industrial de Cobija de contar con mayor fluidez en la comunicación entre sus funcionarios, usuarios y población en general, tomando en cuenta la distancia que existe entre cada una de sus oficinas en el radio urbano de la ciudad de Cobija. El proyecto consistió en la Implementación de Telefonía IP utilizando software libre y la metodología Diseño de Redes CISCO (Top – Down Network Design), con la finalidad de aprovechar al máximo todos los beneficios de contar con una central telefónica Elastix en la institución. Con esto se pudo unir la transmisión de voz y de datos accediendo a VoIP, Fax, Mensajería Instantánea, Correo Electrónico, Colaboración y mucha otra información reutilizando todo el hardware y software con lo que ya contaba la institución en el funcionamiento de su red.

Con la implementación y puesta en marcha del servidor de telefonía IP Elastix se pone fin al precario sistema de comunicación que tenía ZOFRACOBIIJA gracias al relevamiento de información, reutilización de tecnologías y aplicación de la metodología. Alcanzando así los objetivos planteados inicialmente, sabiendo que la tecnología utilizada es económica, con escalabilidad a bajo costo y sencilla de configurar con relación a otro tipo de tecnologías.

PALABRAS CLAVES: Telefonía IP, Elastix, ZOFRACOBIIJA, VoIP.

ÍNDICE

| | | |
|--------|--------------------------------------------|----|
| 1. | MARCO INTRODUCTORIO..... | 12 |
| 1.1. | ANTECEDENTES..... | 13 |
| 1.2. | DESCRIPCIÓN DEL PROBLEMA..... | 14 |
| 1.2.1. | Planteamiento del problema..... | 15 |
| 1.3. | OBJETIVOS..... | 15 |
| 1.3.1. | Objetivo General..... | 15 |
| 1.3.2. | Objetivos Específicos..... | 15 |
| 1.4. | ALCANCES..... | 16 |
| 1.5. | METODOLOGÍA Y HERRAMIENTAS UTILIZADAS..... | 16 |
| 1.6. | APORTES..... | 17 |
| 1.9. | RESULTADOS OBTENIDOS..... | 17 |
| 1.10. | ORGANIZACIÓN DEL DOCUMENTO..... | 18 |
| 2. | MARCO TEÓRICO..... | 21 |
| 2.1. | MARCO INSTITUCIONAL..... | 22 |
| 2.1.1. | Descripción General..... | 22 |
| 2.1.2. | Logotipo..... | 23 |

| | |
|-----------------------------------------------------|----|
| 2.1.3. Misión. | 23 |
| 2.1.4. Visión. | 23 |
| 2.1.5. Organigrama Institucional..... | 23 |
| 2.2. MARCO LEGAL..... | 24 |
| 2.3. BASES TEÓRICAS..... | 26 |
| 2.3.1. Introducción a la Telefonía IP..... | 26 |
| 2.3.2. Voz sobre IP (VoIP)..... | 27 |
| 2.3.3. Análisis de VoIP. | 27 |
| 2.3.4. Voz Sobre IP (voip) y Telefonía IP..... | 29 |
| 2.3.5. Problemas en Una Red de VoIP..... | 32 |
| 2.3.6. Codificación de Voz..... | 40 |
| 2.3.7. Digitalización y Codificación. | 41 |
| 2.3.8. Protocolos De Transporte..... | 55 |
| 2.3.9. Protocolos para VoIP. | 58 |
| 2.3.10. Protocolos de Transporte..... | 64 |
| 2.3.11. Calidad De Servicio. | 66 |
| 2.3.12. Estándares De Comunicaciones De VoIP. | 72 |
| 2.3.12.4. PROTOCOLO DE INICIO DE SESION (SIP). | 81 |

| | | |
|-----------|-----------------------------------------------------|-----|
| 2.3.12.5. | Descripción de SDP. | 86 |
| 2.3.13. | Comparación entre SIP Y H.323..... | 87 |
| 2.3.14. | Redes Privadas Virtuales (VPN)..... | 88 |
| 2.3.15. | Asterisk. | 96 |
| 2.3.16. | Elastix..... | 99 |
| 2.4. | DESCRIPCIÓN DE LA METODOLOGÍA. | 101 |
| 2.4.1. | Fase 1: Analizar Requerimientos. | 101 |
| 2.4.2. | Fase 2: Desarrollar Diseño Lógico..... | 102 |
| 2.4.3. | Fase 3: Desarrollar Diseño Físico. | 103 |
| 2.4.4. | Fase 4: Probar, optimizar y documentar diseño. | 103 |
| 2.4.5. | Fase 5: Implementar y probar la red..... | 103 |
| 2.4.6. | Fase 6: Monitorear y Optimizar la Red..... | 104 |
| 3.1. | FASE I: ANALIZAR REQUERIMIENTOS..... | 106 |
| 4.1. | CONCLUSIONES. | 130 |
| 4.2. | RECOMENDACIONES..... | 131 |
| | Referencias Bibliográficas | 133 |

ÍNDICE DE FIGURAS.

| | |
|-------------------------|-----------|
| Figura 1. | 23 |
| Figura 2. | 24 |
| Figura 3. | 28 |
| Figura 4. | 31 |
| Figura 5. | 33 |
| Figura 6. | 34 |
| Figura 7. | 39 |
| Figura 8. | 42 |
| Figura 9. | 43 |
| Figura 10. | 44 |
| Figura 11. | 49 |
| Figura 12. | 51 |
| <i>Figura 13.</i> | <i>53</i> |
| <i>Figura 14.</i> | <i>56</i> |
| Figura 15. | 59 |
| Figura 16. | 61 |
| Figura 17. | 65 |

| | |
|-----------------|-----|
| Figura 18. | 69 |
| Figura 19. | 70 |
| Figura 20. | 78 |
| Figura 21. | 79 |
| Figura 22. | 89 |
| Figura 23. | 100 |
| Figura 24. | 108 |
| Figura 25. | 110 |
| Figura 26. | 119 |
| Figura 27. | 120 |
| Figura 28. | 120 |
| Figura 29. | 123 |
| Figura 30. | 124 |
| Figura 31. | 125 |
| Figura 32. | 126 |
| Figura 33. | 127 |
| Figura 34. | 128 |

INDICE DE TABLAS

| | |
|----------------------------------------|-----|
| Tabla 1..... | 36 |
| Tabla 2..... | 46 |
| Tabla 3..... | 47 |
| Tabla 4..... | 49 |
| Tabla 5..... | 51 |
| Tabla 6. Códec de banda completa. | 53 |
| Tabla 7..... | 61 |
| Tabla 8..... | 88 |
| Tabla 9..... | 108 |
| Tabla 10..... | 110 |
| Tabla 11..... | 111 |
| Tabla 12..... | 112 |
| Tabla 13..... | 112 |
| Tabla 14..... | 113 |
| Tabla 15..... | 114 |
| Tabla 16..... | 115 |
| Tabla 17..... | 116 |

| | |
|---------------|-----|
| Tabla 18..... | 116 |
| Tabla 19..... | 117 |
| Tabla 20..... | 121 |

CAPÍTULO I

1. MARCO INTRODUCTORIO.

1.1. ANTECEDENTES.

Desde hace algunos años, el mundo de las telecomunicaciones ha crecido a pasos agigantados, las diferentes sociedades hacen uso tanto de la telefonía, como de internet constantemente y esto es debido principalmente al gran número de beneficios y comodidades que se pueden obtener mediante el uso de estas redes. Por esta y otras razones, tanto pequeñas como grandes empresas e instituciones se han visto obligadas a realizar constantes cambios en cuanto a las tecnologías usadas en sus infraestructuras, para de esta manera poder brindar un servicio actualizado y de buena calidad a los clientes.

La Zona Franca Comercial e Industrial de Cobija es una entidad pública descentralizada, con personalidad jurídica, patrimonio propio y autonomía de gestión técnica, administrativa y financiera. Actualmente la institución cuenta con un limitado sistema de comunicación entre los funcionarios lo que dificulta el trabajo operativo y administrativo afectando así el desempeño de las actividades diarias de todos los profesionales y la prestación de un servicio de calidad hacia sus usuarios y población en general.

La realización del presente proyecto surge debido a la motivación que presenta ZOFRACOBIIJA por contar con un sistema que permita la comunicación permanente, ágil y continua entre sus funcionarios, usuarios y población en general.

Voz sobre IP o VoIP es una de las nuevas tecnologías orientadas a la conmutación de paquetes, la cual a través de un conjunto de protocolos logra la señalización necesaria

para que la voz pueda ser transportada en tiempo real y con una buena calidad. Actualmente en nuestro país las empresas e instituciones públicas y privadas vienen utilizando las nuevas tecnologías según lineamientos del gobierno central dispuesto en los Decretos Supremos 3251 y 1391.

1.2. DESCRIPCIÓN DEL PROBLEMA

La Zona Franca Comercial e Industrial de Cobija es una institución Pública descentralizada que presta servicios a la población en general. Con sus oficinas central ubicada en el km. 14 ½ carretera Cobija – Porvenir, de la misma manera cuenta con puestos de control ubicados en el Puente Internacional, Puente de la Amistad y Aeropuerto Internacional.

Por los servicios que presta ZOFRACOBIBA y el trabajo que se realiza en las diferentes oficinas ubicadas en el centro de la ciudad de Cobija, se tiene muchos inconvenientes con relación a la comunicación frecuente que debe haber entre los servidores públicos para prevenir y evitar ilícitos. De la misma manera la oficina central se encuentra a 14 ½ km. Del centro de la de la ciudad de Cobija lo que dificulta mucho la comunicación entre los usuarios y personas que quieren acceder a información y/o servicios de esta zona franca.

La solución propuesta del Proyecto de Grado es mejorar la comunicación que existe entre los servidores públicos de la Zona Franca Comercial e Industrial de Cobija y con la población en general, lo que repercutirá en la mejora de la recaudación de la institución por los servicios que presta a sus usuarios y población en general.

1.2.1. Planteamiento del problema

“Limitado sistema de comunicación entre los funcionarios lo que dificulta el trabajo operativo y administrativo de la Zona Franca Comercial e Industrial de Cobija”.

1.3. OBJETIVOS

1.3.1. Objetivo General

Implementar un sistema de comunicación de telefonía IP utilizando una Red Privada Virtual para la Zona Franca Comercial e Industrial de Cobija.

1.3.2. pro Específicos

- Analizar la situación actual de la comunicación en ZOFRACOBIIJA, a través de relevamiento de información.
- Diseñar la red necesaria para el óptimo funcionamiento de la Telefonía IP, en base a la información recolectada.
- Implementación de VPN, para utilizar las redes de forma privada mediante internet.
- Desarrollar políticas de seguridad en el área administrativa para llevar un control adecuado en el manejo de la información y grabación de llamadas.
- Implementar la telefonía IP utilizando software libre para el beneficio de los funcionarios y usuarios de ZOFRACOBIIJA.

1.4. ALCANCES.

La nueva era de la sociedad de la información pretende la convergencia total de los servicios informáticos y de telecomunicaciones, por ende la tecnología de telefonía IP, busca la intersección y/o unión de dos mundos históricamente separados, uno el de la transmisión de voz y el otro el de transmisión de datos.

Dentro de los marcos incidentes y de gran impacto tecnológico, está el resurgimiento de la telefonía IP, ya que en el pasado este servicio carecía de parámetros de QoS (Quality of service) y de niveles de seguridad que no aportaban un elemento garantizado de confianza.

El sistema de telefonía IP implementado en administración de ZOFRACOBIA permite la comunicación permanente, ágil y continúa entre los servidores públicos, usuarios y población en general, mediante llamadas de voz, videoconferencias, mensajes instantáneos, transmisión de datos, entre otros que proporciona Elastix.

Por falta de presupuesto en la institución no se pudo realizar la adquisición de los teléfonos IP y su configuración, por tal motivo se procedió a realizar la conexión de los usuarios finales mediante software.

1.5. METODOLOGÍA Y HERRAMIENTAS UTILIZADAS

La metodología utilizada para el desarrollo del presente proyecto es el Diseño de Redes CISCO (TOP – DOWN NETWORK DESIGN) por ser completa para este tipo de trabajos. Esta metodología tiene seis fases: Analizar requerimientos, Desarrollar

diseño lógico, Desarrollar diseño físico, Probar – Optimizar y documentar diseño, Implementar y probar la red, Monitorear y optimizar la red. Con lo que primeramente se escucha al cliente para ver las metas del negocio, se obtiene una macro de la organización, se estructura todo el proceso de diseño, se implementa, prueba y optimiza la red.

1.6. APORTES.

Los principales aportes con la implementación de Telefonía IP sobre una VPN para la Zona Franca Comercial e industrial de Cobija, se detallan a continuación:

- Permitirá resolver el problema de la precaria comunicación que existía entre los funcionarios de ZOFRACOBIA.
- Mayor comunicación entre los funcionarios y las personas que acceden a los servicios de ZOFRACOBIA.
- Ampliación y fortalecimiento de la red local de ZOFRACOBIA.
- Posibilidad de mejora e integración con otros sistemas según los requerimientos de ZOFRACOBIA y acorde a los acelerados avances tecnológicos.

1.9. RESULTADOS OBTENIDOS.

1.9.1. Se analizó la situación actual de la institución con relación a la comunicación que se tiene entre los servidores públicos y la población en general, mediante técnicas de relevamiento de información, obteniendo de esta manera resultados que están siendo tomados en cuenta.

- 1.9.2. Se realizó el diseño de una nueva red de datos para el óptimo funcionamiento de la telefonía IP, utilizando una potente herramienta como es Cisco Packet Tracer.
- 1.9.3. Seguridad de la información transmitida por la VPN.
- 1.9.4. Administración inteligente de las llamadas.
- 1.9.5. Conferencias y videoconferencias entre más de dos usuarios.
- 1.9.6. Comunicación multimedia.
- 1.9.7. Comunicación desde cualquier lugar.

1.10. ORGANIZACIÓN DEL DOCUMENTO.

CAPITULO I

1.1. Antecedentes y motivación

1.2. Descripción del problema

1.3. Solución propuesta

1.4. Objetivos

1.4.1 Objetivo general

1.4.2 Objetivos específicos

1.5. Justificación

1.5.1. Justificación económica

1.5.2. Justificación social

1.5.3. Justificación técnica

1.5.4. Justificación Científica

1.6. Metodologías y herramientas utilizadas

1.7. Alcances

1.8. Aportes

1.9. Resultados obtenidos

1.9. Organización del documento

CAPITULO II. MARCO TEÓRICO.

2.1. Marco Institucional.

2.2. Marco Legal.

2.3. Marco Teórico.

2.3.1. Introducción.

CAPITULO III. MARCO APLICATIVO.

3.1. Marco Aplicativo.

CAPITULO IV. CONCLUSIONES Y RECOMENDACIONES.

4.1. Conclusiones.

4.2. Recomendaciones.

REFERENCIAS BIBLIOGRÁFICAS

ANEXOS

CAPITULO II

2. MARCO TEÓRICO.

2.1. MARCO INSTITUCIONAL.

Zona Franca Comercial e Industrial de Cobija es una entidad pública descentralizada, con personalidad jurídica de derecho público, patrimonio propio, autonomía de gestión administrativa, financiera, legal y técnica, bajo tuición del Ministerio de Producción y Microempresa, actual Ministerio de Desarrollo Productivo y Economía Plural. (ZOFRACOBIIJA, 2015).

2.1.1. Descripción General.

El Área de ZOFRACOBIIJA, comprende al radio urbano de la ciudad de Cobija del Departamento Pando. La Zona Franca Comercial e Industrial de Cobija debe contar con un área perfectamente delimitada (Instalaciones de ZOFRACOBIIJA), destinada a la realización de funciones administrativas, operativas y de depósito de mercancías, la cual estará ubicada en la principal vía de ingreso y salida de mercancías de la zona franca. Asimismo, ZOFRACOBIIJA debe contar con instalaciones adecuadas para la Administración Aduanera, así como instalaciones secundarias destinadas al ejercicio del control de ingreso de mercancías, en los aeropuertos, puertos y demás vías de acceso a la zona franca (ZOFRACOBIIJA, 2015).

2.1.2. Logotipo.

Figura 1.

Logotipo de ZOFRACOBIIJA.



Fuente: Página oficial de ZOFRACOBIIJA.

2.1.3. Misión.

Impulsar aceleradamente el desarrollo industrial y comercial en la Zona franca de Cobija, para contribuir al desarrollo social y económico del departamento Pando.

2.1.4. Visión.

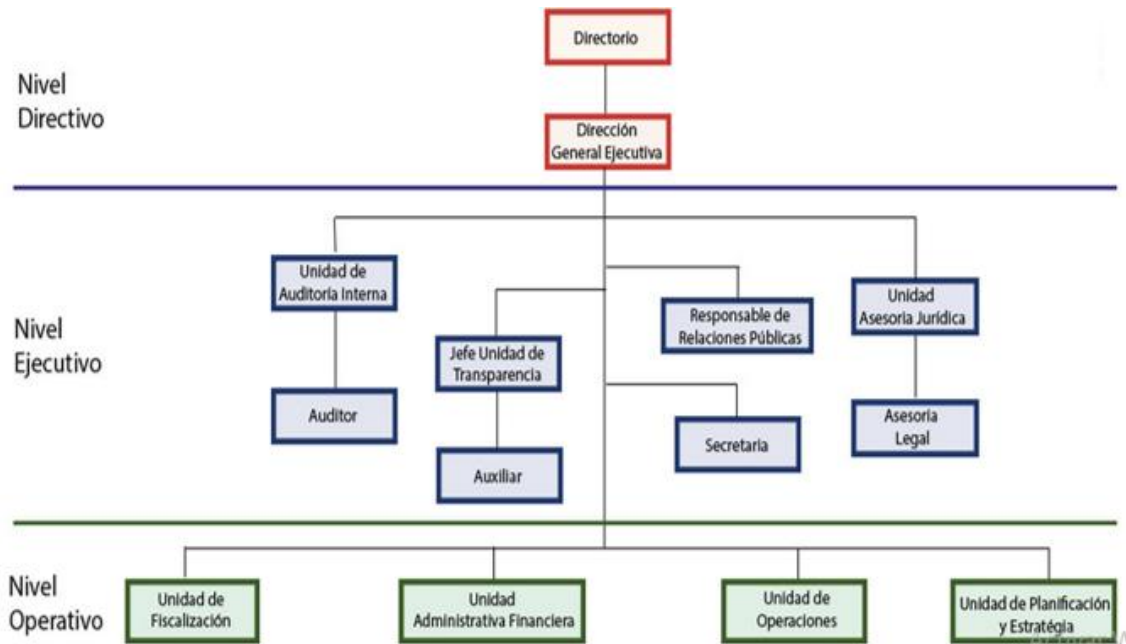
Ser una entidad modelo de apoyo al sector industrial y comercial a nivel nacional.

2.1.5. Organigrama Institucional.

La Zona Franca Comercial e Industrial de Cobija cuenta con un Organigrama Institucional, el cual se encuentra dividido en tres niveles: Nivel Directivo, Nivel Ejecutivo y Nivel Operativo. A continuación se muestra gráficamente el Organigrama Institucional de ZOFRACOBIIJA.

Figura 2.

Organigrama Institucional ZOFRACOBIIJA



Fuente: Página Oficial ZOFRACOBIIJA.

2.2. MARCO LEGAL.

La Zona Franca Comercial e Industrial de Cobija fue creada mediante Ley por un lapso de 20 años, con motivo de impulsa el desarrollo social y económico del departamento Pando. Se amplía su vigencia en dos ocasiones siendo la última en el año 2018 mediante la Ley N° 1048 estableciendo los mecanismos para promover el desarrollo productivo e industrial del departamento de Pando.

- Ley de 12 de octubre de 1983 se crea la Zona Franca Comercial e Industrial de la Ciudad de Cobija, por el plazo de veinte años, con el objeto de impulsar el desarrollo social y económico del Departamento Pando.

- Decreto Supremo N° 20287 de 8 de junio de 1984 aprueba el Reglamento de Funcionamiento de la Zona Franca Comercial e Industrial de la Ciudad de Cobija, con la finalidad de lograr su adecuado funcionamiento.
- Ley N° 1850 de 07 de abril de 1998 se amplía el plazo de vigencia de la Zona Franca Comercial e Industrial de Cobija, por veinte años, computables a partir de la fecha de la Ley.
- Ley N° 1990 de julio de 1999, regula el Régimen especial de Zonas Francas, en cuanto a su objeto, regímenes aduaneros aplicables y otras operaciones aduaneras.
- Decreto Supremo N° 25933 Reglamento de la Zona Franca Comercial e Industrial de Cobija, con la finalidad de cumplir los objetivos para el desarrollo económico y social del Departamento Pando se hace necesario implementar normas y mecanismos de orden tributario, operativo, organizativo y administrativo, necesarios para el funcionamiento eficiente de la.
- Que se hace necesario regular el tránsito en el resto del territorio aduanero nacional, de vehículos automotores legalmente internados en Zona Franca Comercial e Industrial de Cobija, aplicando El Régimen de Admisión Temporal para Reexportación en el mismo Estado, con la constitución de garantía prendaria del vehículo automotor, considerando los objetivos de ZOFRACOBIA previstos en la Ley de 12 de Octubre de 1983.
- Decreto Supremo N° 1871, tiene por objeto modificar el Decreto Supremo N° 25933, de 10 de octubre de 2000, modificado por Decreto Supremo N° 29744,

de 15 de octubre de 2008, para impulsar el desarrollo industrial en el Departamento de Pando.

- Ley N° 1048 del 07 de abril del 2018, que amplía el plazo de vigencia de la Zona Franca Comercial e Industrial de Cobija, así como establece mecanismos para promover el desarrollo productivo e industrial del Departamento de Pando

2.3. BASES TEÓRICAS.

2.3.1. Introducción a la Telefonía IP.

Según (Arias, 2015), la Telefonía IP es una tecnología que permite integrar en una misma red, basada en protocolo IP, las comunicaciones de voz y datos. Muchas veces se utiliza el término de redes convergentes o convergencia IP, aludiendo a un concepto un poco más amplio de integración en la misma red de todas las comunicaciones (voz, datos, video, etc.). Esta tecnología hace ya muchos años que está en el mercado (desde finales de los 90) pero no ha sido hasta hace poco que se ha generalizado gracias, principalmente a la mejora y estandarización de los sistemas de control de la calidad de la voz (QoS) y a la universalización del servicio Internet. Cuando hablamos de un sistema de telefonía IP estamos hablando de un conjunto de elementos que debidamente integrados permiten suministrar un servicio de telefonía (basado en VoIP) a la empresa. Los elementos básicos que forman este sistema son: La centralita IP, el Gateway IP y los diferentes teléfonos IP.

La realización del presente proyecto surge debido a la necesidad que tiene la Zona Franca Comercial e Industrial de Cobija de poder contar con Telefonía IP para la

comunicación remota segura. De esta manera la idea principal es Implementar una Red de Telefonía IP a través de VPN para la Zona Franca Comercial e Industrial de Cobija.

2.3.2. Voz sobre IP (VoIP).

Es una tecnología que permite comunicarse por voz a través de cualquier red que acepte el protocolo IP. El funcionamiento consiste en una emisión sonora la cual se digitaliza por medio de un códec de audio, para luego ser enviado hacia su destinatario en paquetes IP. Una vez realizado el recorrido, un códec de audio restituye y, en caso de estar comprimida, descomprime, la señal de voz de la mejor forma posible a su estado original (ANDERRUTHY, 2007).

En el momento de realizar una llamada, tanto el emisor como el receptor necesitan usar una serie de normas o reglas las cuales se van a encargar de diferentes temas como la señalización y detección de errores entre otros, los cuales son esenciales, para que tanto el envío como la recepción de datos se efectúe de manera eficiente, este conjunto de normas es lo que se conoce en el campo de las telecomunicaciones como protocolos. A continuación se presenta una explicación detallada del funcionamiento de cada uno de los protocolos que usa la tecnología VoIP para establecer una comunicación.

2.3.3. Análisis de VoIP.

De acuerdo a (Peláez, 2007), uno de los aspectos más importantes de esta tecnología es la conversión de las señales de voz estándar, en paquetes de datos comprimidos que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales. La

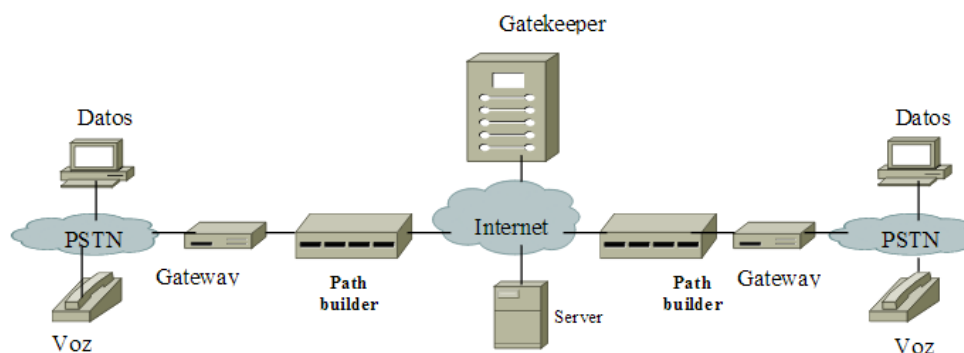
evolución de la transmisión conmutada por circuitos a la transmisión basada en paquetes toma el tráfico de la red telefónica pública y lo coloca en redes IP previamente acondicionadas.

Las señales de voz se encapsulan en paquetes IP que se pueden transportar como IP nativo o como IP Ethernet, Frame Relay o ATM. Hoy en día las arquitecturas inter operables de Voz sobre IP se basan en la especificación H.323 versión 2, que define Gateway (interfaces de telefonía con la red) y gatekeepers (componentes de conmutación interoficina), y sugiere la forma de implementar, en rutar y finalizar llamadas telefónicas a través de Internet, actualmente se están realizando propuestas de otras especificaciones en los consorcios industriales tales como SIP, SGCP e IPDC, las cuales ofrecen ampliaciones en lo tocante a al control de llamadas y señalización dentro de arquitecturas de voz sobre IP.

A continuación se muestra en la Figura 3 una red de telefonía IP, con los componentes que se requiere para poder tener conectividad de voz y datos en la red.

Figura 3.

Red de Telefonía sobre IP.



Fuente: Tecnología de comunicación Voz sobre IP (Monografía de Pregrado)

2.3.4. Voz Sobre IP (voip) y Telefonía IP.

Los términos de VoIP y Telefonía IP se utilizan comúnmente como sinónimos, pero entre ambos existen diferencias claras. La principal diferencia es que VoIP se refiere al transporte de voz encapsulada dentro de paquetes de datos, utilizando el protocolo de Internet (IP) sobre redes públicas o privadas. En cambio Telefonía IP, es un sistema avanzado de comunicaciones que utiliza el protocolo de Internet como medio de transporte para crear un sistema telefónico con todas las funciones de la telefonía tradicional, pero que además agrega nuevas posibilidades (Sierra A. , 2008; Peláez, 2007).

En otras palabras VoIP, del inglés Voice over Internet Protocol, es la tecnología en la que se digitaliza, comprime la voz y se encapsula sobre el protocolo IP. La Telefonía IP es la infraestructura que nos permite hacer llamadas a cualquier teléfono de la red telefónica.

La Telefonía IP es aquella que reúne la transmisión de voz y datos a través de redes IP (Internet Protocol) en forma de paquetes de datos (de ahí deriva la denominación Voz sobre IP o VoIP). Estas redes transportan la información basadas en el Protocolo de Internet (IP). El ejemplo más común de esta red es Internet y las redes LAN (Local Área Network o redes de área local), es decir redes que se componen de un número pequeño de equipos y con una extensión no muy amplia (local).

Esta telefonía es una tecnología que está basada en el sistema de “conmutación de paquetes”, a diferencia de la Telefonía Tradicional que se basa en la “conmutación de

circuitos”. La conmutación de paquetes es aquella donde la información antes de ser enviada es empaquetada. En las redes IP, cada paquete es transmitido individualmente y éste puede seguir diferentes rutas hacia su destino. Una vez que los paquetes llegan a su destino, estos son otra vez re-ensamblados.

La Telefonía IP surge como alternativa a la Telefonía Tradicional, brindando nuevos servicios al cliente y una serie de beneficios económicos. Esto debido a que la Telefonía IP reúne dos mundos históricamente separados: la transmisión de voz y la de datos, entre dos puntos distantes. Esto permite utilizar las redes de datos para efectuar las llamadas telefónicas, es decir, una única red se encarga de cursar todo tipo de comunicación, ya sea de voz, datos, vídeo o cualquier otro tipo de información.

En la Figura 2 se logra apreciar que en la situación actual existe la red de la telefonía analógica o tradicional (A) que es la que permite realizar solo llamadas entre teléfonos análogos por medio de las centrales telefónicas análogas que se comunican con la red de Telefonía Tradicional o PSTN para así llegar al destino deseado.

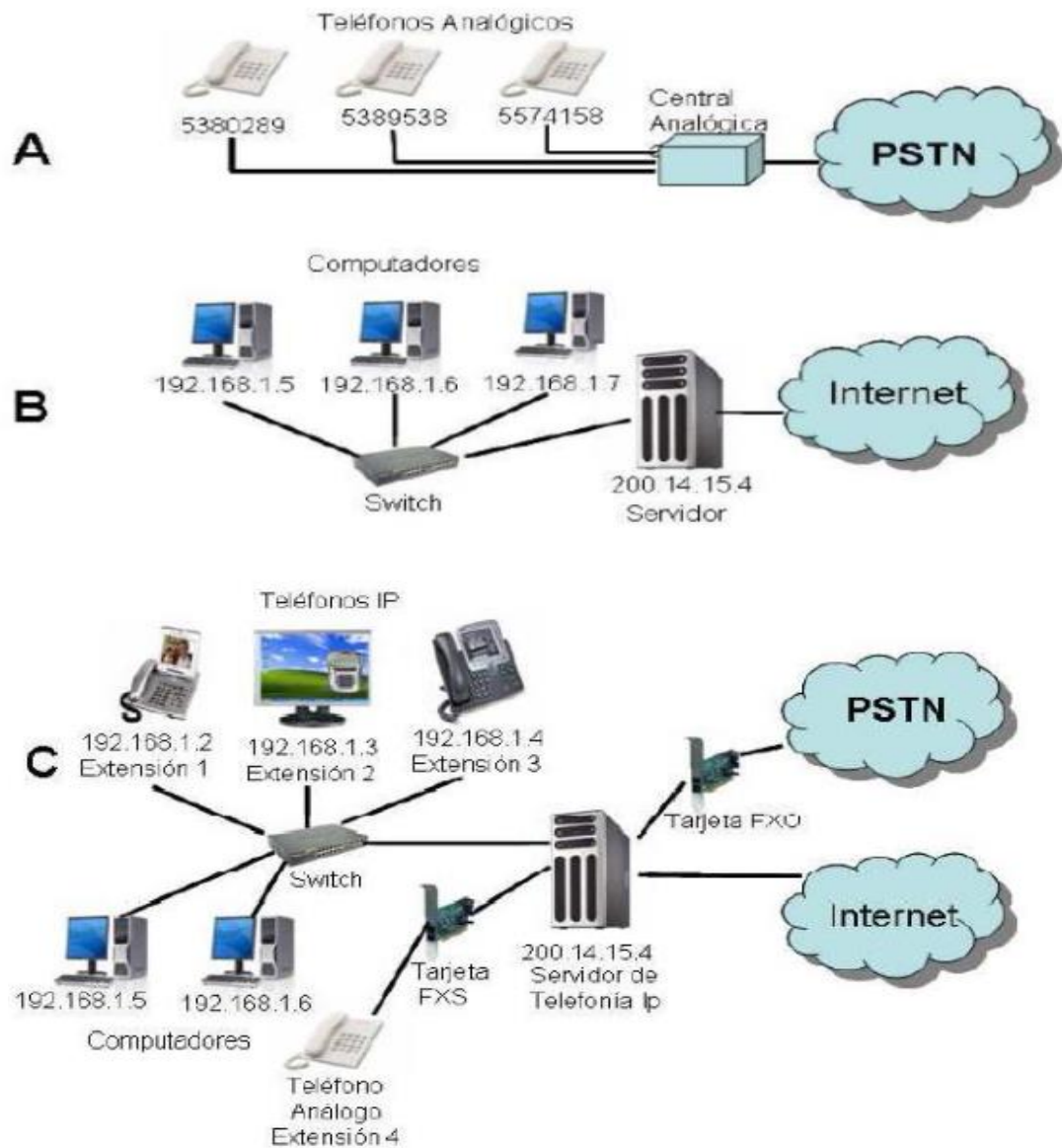
En esta situación también se encuentra la red de datos (B) que es aquella que permite conectar computadores entre si bajo una red LAN y a su vez permitir que estos salgan a Internet a través de un servidor o un router, logrando una comunicación con otras LAN's que se encuentren distantes.

La Telefonía IP por su parte, permite realizar ambas funciones (A y B) bajo un mismo esquema de red, es decir, bajo la red de datos se pueden realizar llamadas tanto hacia la Telefonía Tradicional como internamente y también permitir la conexión de

computadores entre sí con salida a Internet. Para esto es necesario la utilización de Teléfonos Tradicionales, Teléfonos IP o Softphones, un servidor de telefonía IP, y tarjetas o adaptadores de interfaz FXO y FXS que serán explicadas más adelante.

Figura 4.

Diferencia entre Red de Telefonía Tradicional y Telefonía IP



Fuente: Tecnología de comunicación Voz sobre IP (Monografía de Pregrado)

2.3.5. Problemas en Una Red de VoIP.

Para implementar la ToIP en una red LAN, es importante considerar básicamente tres (3) variables, de acuerdo a las recomendaciones del RFC 3246, donde se especifica que son principalmente:

- Retardo.
- Variación del Retardo (“Jitter”, de aquí en adelante).
- Pérdida de Paquetes.

2.3.5.1. Retardo.

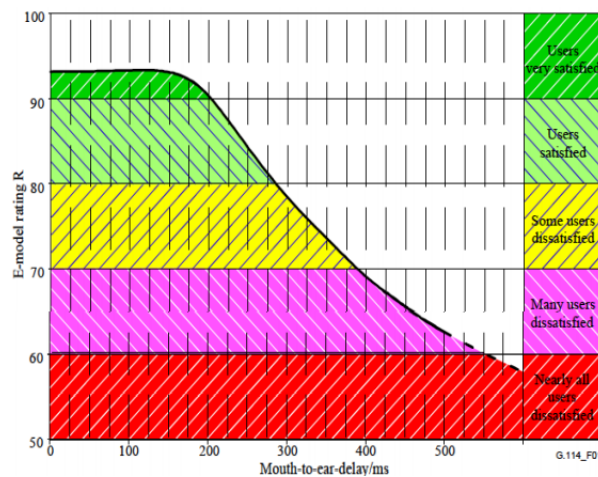
El retardo es la variable que considera el tiempo que se tarda la comunicación en establecerse de un punto a otro. La ITU-T recomienda la utilización del G.114 y G.131, como medidas de referencia para indicar si la red se encuentra dentro de los parámetros aceptables para ejecutar las acciones inherentes a una conversación a través de un medio digital como es el hablar y el escuchar, y así poder entablar la comunicación sin ninguna distorsión (Cortés & Fabián L., 2012).

El Estándar G.114 indica que para tener una conversación telefónica a través de una red IP, el retardo aceptable debe estar por debajo de los 150 milisegundos, y no de superar los 400 milisegundo de ser así la calidad en el retardo se considera inaceptable. Si se diera el caso de que el retardo esta por fuera del rango permitido, entonces la calidad de la conversación se degradaría, ocasionando inconvenientes en la acción de escuchar y hablar.

Finalmente con el G.114, los resultados llevaron a establecer la relación entre el retardo y la calidad de las conversaciones, lo cual es posible ver con la figura 3.

Figura 5.

Determinación del efecto del Retardo absoluto por el E-Model.



Fuente: Metodología para la implementación de Proyectos de Telefonía IP en las Instituciones miembro de la RUAV, Proyecto de Postgrado.

Con el E-model lanzado en la recomendación ITU-T Rec. G.107, se busca analizar el comportamiento de los retardos en el proceso de llamada en las redes IP, finalmente es allí donde se propone el modelo como base de un estudio subjetivo para la VoIP. La estructura de análisis del E-Model contempló principalmente tres (3) elementos que aportan a los retardos:

- El retardo absoluto (T_a): Total en la transmisión en un solo sentido, de origen a destino. Permite establecer el deterioro de una conversación como consecuencia del largo trayecto que debe recorrer.

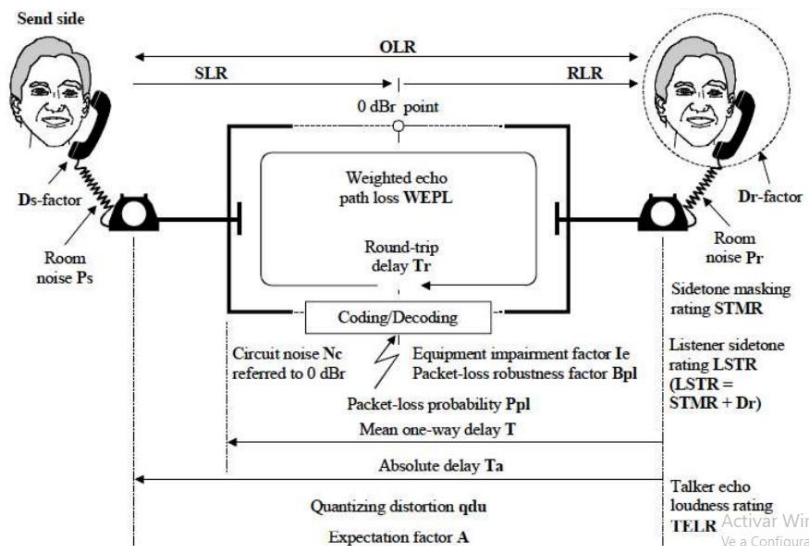
- El retardo medio (T): El retardo que hay durante la conversación desde el punto de recepción hasta el punto desde es establecida la comunicación del lado del transmisor.

- Retardo Total (Tr): Es el retardo en el bucle que corresponde a los 4 hilos de cobre que son utilizados en la llamada.

Los elementos que describen el retardo pueden verse en la figura 4.

Figura 6.

Referencia en la conexión del E-Model.



Fuente: Fuente: Metodología para la implementación de Proyectos de Telefonía IP en las Instituciones miembro de la RUAV, Proyecto de Postgrado.

Se tiene entonces, que de acuerdo al medio de transmisión de datos por donde viaje la voz, existen unos valores de retardos que deben ser contemplados, para determinar si las comunicaciones de origen a destino tienen las condiciones suficientes que aseguran que la calidad de la transmisión de voz será la adecuada. Por ejemplo, una fibra óptica submarina aporta al retardo 5 microsegundos por cada kilómetro de distancia; para el caso de una

transmisión satelital el aporte al retardo varía acorde a la órbita en la cual se encuentre el satélite, es decir que una comunicación que utilice un satélite ubicado en la órbita geoestacionaria (a 36000 Kilómetros de altura) genera un retardo de 260 ms desde la estación terrena hacia el satélite.

Por otra parte los retardos de una PSTN orientada a la conmutación de circuitos son controlados y constantes, sin embargo cuando se trata de una red IP, están en función del proceso de encolamiento, conmutación o enrutamiento de los paquetes de datos, que viajan a través de los dispositivos de conectividad. De Igual forma, los retardos asociados al proceso de transmisión de la información:

- **Retardo en la captura del paquete:** Tiempo transcurrido entre la llegada de la cabecera del paquete y su completa recepción.
- **El re-envío del paquete:** Esto lo define el proceso de conmutación, ya sea por el método de Cut-Through o Store-and-Forward por sus siglas en inglés.
- **La longitud del paquete:** determinar el tamaño de los paquetes es fundamental en el tiempo que transcurre en procesarlos, sin embargo es importante no ir a los extremos en la definición de esta variables, porque la circulación de paquetes pequeños en la red mejora la velocidad pero reduce el desempeño, más aun cuando se está utilizando enlaces en modo trunk, por donde circula muchas redes. Por otro lado, paquetes muy grandes, pueden mejorar el desempeño en la red, pero los retardos pueden incrementarse debido al tamaño de la información para poder ser procesada en su totalidad, por el respectivo equipo de conectividad.

Debido a que los retardos son analizados utilizando el E-model, es importante tener presente que asociado a este modelo, se utiliza otra herramienta que consiste en el factor MOS “Mean Opinión Score”, el cual se encarga de determinar la calidad de la voz en un transmisión de IP con un número ubicado dentro del rango entre 1 y 5. Sin embargo, el Factor MOS no debe ser considerado como una métrica absoluta para garantizar o establecer la calidad de la voz a través de una comunicación en ToIP, por ende se sugiere la utilización en conjunto con las otras variables complementarias al retardo como el Jitter y la Pérdida de paquetes.

En la Tabla 1 se especifica los niveles y evaluación de la calidad de la voz en ToIP utilizando el factor MOS junto con la comparación de la escala que utiliza el Factor R que se extrae del E-Model:

Tabla 1.

Definición de las categorías de Calidad de la voz de transmisión.

| R-Value Range | Speech Transmission Quality Category | User Satisfaction |
|-------------------|--------------------------------------|-------------------------------|
| $90 \leq R < 100$ | Best | Very Satisfied |
| $80 \leq R < 90$ | High | Satisfied |
| $70 \leq R < 80$ | Medium | Some Users Dissatisfied |
| $60 \leq R < 70$ | Low | Many Users Dissatisfied |
| $50 \leq R < 60$ | Poor | Nearly all Users Dissatisfied |

NOTE 1 – Connections with R-Values below 50 are not recommended

NOTE 2 – Although the trend in transmisión planning is to use R-

Values into other metrics e.g. MOS, %GoB, %PoW, can be found in Annex

B/G.107.

Nota: Se especifica los niveles y evaluación de la calidad de la voz en ToIP utilizando el factor MOS junto con la comparación de la escala que utiliza el Factor R que se extrae del E-Model JITTER.

Fuente: Metodología para la implementación de Proyectos de Telefonía IP en las Instituciones miembro de la RUAV, Proyecto de Postgrado.

En las redes orientadas a conmutación de paquetes existe un retardo asociado a los medios de transmisión de datos y componentes activos de la red, en la trayectoria que sigue cada paquete que conforma la información. Ese retardo es el tiempo que hay entre la llegada de un paquete y otro, producto de los caminos que son seguidos y que puede perjudicar la calidad en la transmisión de paquetes de voz. El Jitter, como es conocida esta variable, empeora cuando los enlaces son entre grandes distancias y en redes lentas o congestionadas.

Para el caso de un proyecto de ToIP, los valores recomendados del Jitter no deben superar los 10 ms, en caso que esta cifra no pueda lograrse, se debe recurrir a elementos que compensen ese tipo de variabilidad en la llegada. Una alternativa son los tamaños del Buffer de Jitter que tiene una relación inversamente proporcional con la pérdida de paquete y directa con el retardo, es decir que entre más grande se haya configurado el Buffer, menos pérdidas o descartes de paquetes habrán, pero el retardo se incrementará significativamente. Este tipo de configuración puede ser establecida en los equipos terminales de telefonía IP.

2.3.5.2. Pérdida de Paquetes.

La pérdida de paquetes es una variable, cuyo valor se genera como consecuencia de factores asociados con los elementos en la transmisión de una red, como los buffer en los switches o router que pueden alcanzar en un momento su capacidad máxima y deben iniciar un proceso de descarte de paquetes, ocasionando que la información llegue incompleta. Otra manera de percibir este fenómeno es mediante el retardo de paquetes, que se demoran en poder llegar al destino y complican el proceso de reconstrucción de la información que puede hacer ilegible (Cortés & Fabián L., 2012).

Para evitar que este tipo de fenómenos se presenten en una red que transporte voz, es recomendable utilizar medidas tales como una asignación de canal dedicado exclusivamente al transporte de voz, otra alternativa consiste en la segmentación de la red con fines de dedicar una de ellas exclusivamente para la parte de ToIP, sin que implique que por allí circularán datos que consuman ancho de banda atípico al esperado, establecer políticas de Calidad de Servicio, basado en sistemas de encolamiento como el WFQ o basado en etiquetas para el caso de MPLS, de tal manera que puedan diferenciar el tipo de tráfico que circula por la red.

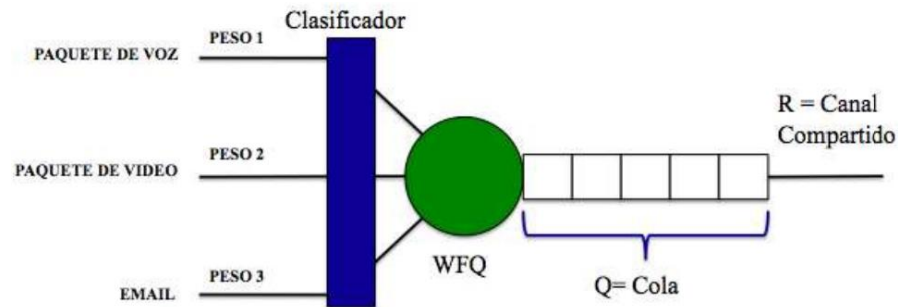
Dentro de los diferentes métodos de encolamiento que existen, se descarta el FIFO, porque directamente no permite diferenciar el tráfico de voz de los demás tipos de flujos. El FIFO es orientado al orden de llegada y no a la prioridad del flujo.

El método más adecuado consiste en el “Weighted Fair Queuing” (WFQ), que permite la diferenciación del flujo de forma interactiva antes de entrar al encolamiento, reduciendo el tiempo de respuesta y finalmente, permite asignar la capacidad de canal restante entre

flujos que demanden mucho del mismo. En la Figura 5, se muestra la forma que WFQ funciona, diferenciando el flujo de tráfico y finalmente brindándole prioridad sobre el mismo canal.

Figura 7.

Esquema lógico de encolamiento con WFQ.



Fuente: Metodología para la implementación de Proyectos de Telefonía IP en las Instituciones miembro de la RUA V, Proyecto de Postgrado.

El esquema lógico para WFQ, permite que los paquetes en el momento de ser encolados ya estén previamente clasificados, disminuyendo el nivel de retardo generado por esta operación. Esto se ve directamente afectado por las tareas del clasificador y del programador, para finalmente asignar el flujo a la cola y enviarla a través canal compartido. De igual forma garantiza una tasa constante de asignación de canal sobre el flujo de datos.

No es obligatorio el utilizar métodos de encolamiento para garantizar una tasa de pérdidas mínima. Sin embargo, los retardos de una red no deben superar los 90 ms en redes cableadas ni debe superar el 99% de pérdida de paquetes, pero en la práctica hay fronteras de retardo de 150 ms, pero con compensaciones de echo de entre 20 ms y 30 ms. Para el caso de las redes LAN se habla de retardos máximos de 10 ms y preferible de 1 ms como línea de base, con un máxima de 1% de pérdida de paquetes.

2.3.6. Codificación de Voz.

Las redes de datos, como es el caso de la red IP sobre la que se soporta este tipo de telefonía, son redes digitales. Esto significa que el caso de transportar señales vocales, originalmente analógicas, requiere que en algún punto de la red se realice la digitalización de la señal de audio. De esta forma, una señal continua en el tiempo y que toma infinidad de valores es convertida y cuantificada a una secuencia de números discretos. Esta tarea suele realizarse, generalmente, en los propios terminales y el elemento vital involucrado de forma directa es el códec.

Inicialmente, los códec se basaron en codificar de la manera más eficiente posible la forma de onda de la señal de entrada, haciendo uso de características de la voz y el oído humano (por ejemplo, ha sido comprobado que el oído es más sensible a ruidos y distorsiones en señales de baja amplitud que en aquellas de mayor amplitud). Con el paso del tiempo, con el objetivo de reducir el ancho de banda consumido en la transmisión, se comenzaron a utilizar técnicas predictivas. Estas técnicas consisten en predecir los valores de las muestras en función de la extrapolación obtenidas de las muestras previas, y codificar exclusivamente la diferencia entre el valor predicho y el valor real de la muestra. Posteriormente, se añade una nueva idea en la codificación de la voz. Se trata de generar voz sintética la cual emula la producción de voz en el aparato fonador humano. En este tema se han diseñado modelos válidos basados en un generador de impulsos y un filtro lineal ambos variables con el tiempo.

La voz humana puede incluir tonos que alcancen hasta los 20 KHz, que está directamente relacionado con el límite de frecuencias que es capaz de percibir el oído. Sin

embargo, la mayor parte de la energía se concentra en las frecuencias más bajas, por debajo de los 4 KHz. Es por ello que la mayor parte de los códec utilizados, considerados de banda estrecha, se centran en el tratamiento de la voz en ese intervalo. No obstante, se han desarrollado códec que cubren un espectro más amplio a cambio de ocupar un mayor ancho de banda en la transmisión de los datos a través de la red.

2.3.7. Digitalización y Codificación.

La digitalización es el primer paso en el proceso de la transmisión de voz a través de la red de paquetes. Esta tarea consiste en la conversión de una señal de naturaleza analógica en una señal que toma valores discretos. Para conseguir tal efecto se divide este proceso en dos etapas: muestreo y cuantificación.

La tarea de codificación es la pieza clave donde toma relevancia el códec de voz. Se basa en la traducción de los valores discretos a numéricos para su transmisión.

2.3.7.1. Muestreo.

La finalidad del muestreo consiste en tomar muestras de la señal vocal de manera periódica. La periodicidad de las muestras debe satisfacer el Teorema de Nyquist. Teorema fundamental de la teoría de la información que establece que la mínima frecuencia a la que puede ser muestreada una señal para que pueda ser reconstruida sin perder información debe duplicar la frecuencia máxima de la señal.

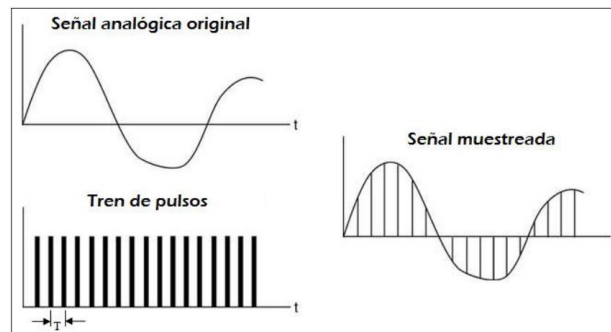
Debido a lo expuesto anteriormente, es plausible filtrar la voz humana a 3,4 KHz sin dejar de ser entendible por el receptor. De tal manera, y basándose en el mencionado teorema,

para que sea posible reconstruir esta señal a partir de sus muestras, la tasa de muestreo debe ser, como mínimo, de 6,8 KHz. Teniendo en cuenta que los filtros reales no pueden implementar cortes abruptos tal cual los teóricos, se ha establecido de manera extendida en la telefonía una frecuencia de muestreo de 8 KHz, lo que equivale a tomar una muestra de voz cada 125 microsegundos.

En la siguiente ilustración se representa una porción de una señal analógica que posee una frecuencia máxima, que al ser combinada con un tren de pulsos de una periodicidad $T=1/f_s=1/2*f_{\max}$ donde f_s Designa la frecuencia de muestreo, se consigue una señal muestreada válida para su posterior reconstrucción en el extremo receptor de la comunicación. A continuación se muestra ejemplo del muestreo de una señal analógica:

Figura 8.

Muestreo de una señal Analógica.



Fuente: Diseño e implementación de un sistema de Voz sobre IP basado en la plataforma Elastix para la empresa Quórum Teleco (Proyecto de Pregrado).

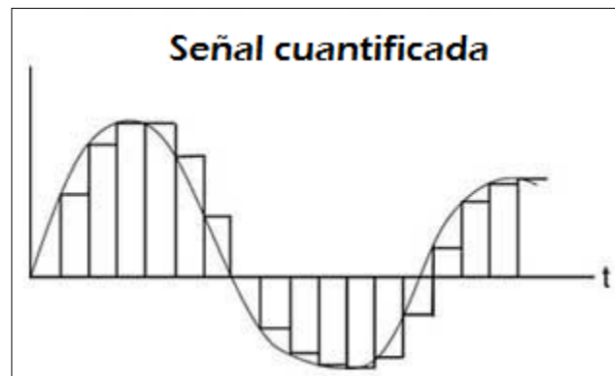
2.3.7.2. Cuantificación.

Una vez se ha obtenido las muestras a partir de la señal original, el siguiente paso consiste en la cuantificación. Este proceso consiste en convertir las muestras analógicas en

muestras que tomen un conjunto de valores discretos. Así, se completa el proceso de la digitalización. En la siguiente figura se muestra un sencillo ejemplo del resultado de este proceso.

Figura 9.

Cuantificación de una señal Muestreada.



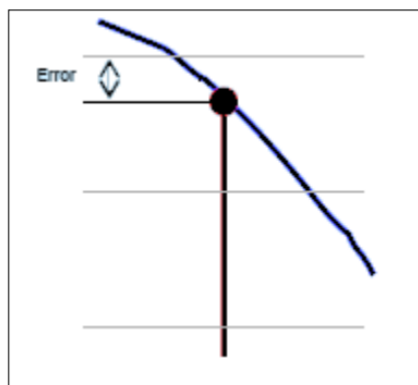
Fuente: Diseño e implementación de un sistema de Voz sobre IP basado en la plataforma Elastix para la empresa Quórum Teleco (Proyecto de Pregrado).

Como es de esperar, al transformar los infinitos valores que puede tomar una señal analógica a un conjunto discreto, se produce una distorsión conocida como ruido de cuantificación. A pesar de su nombre, esta distorsión no es propiamente un ruido, pues no proviene de factores externos, sino que es intrínseco a esta tarea. Existe una relación directa entre la cantidad de valores discretos, la distorsión asociada y el ancho de banda necesario. Esta relación se basa en que cuanto más valores discretos se usen en el proceso de la cuantificación, menor será la distorsión pero mayor la cantidad de información que es necesaria transmitir.

A modo de ejemplo, se representa en la siguiente ilustración el error cometido en la cuantificación de una muestra. De modo que se puede observar la diferencia existente entre el valor tomado por la señal analógica y el nivel de cuantificación correspondiente para su muestra.

Figura 10.

Error de cuantificación.



Fuente: Diseño e implementación de un sistema de Voz sobre IP basado en la plataforma Elastix para la empresa Quórum Teleco (Proyecto de Pregrado).

2.3.7.3. Codificación.

A pesar de ya disponer de una señal digital es necesario codificar los valores discretos, es decir, asignarles valores numéricos, para que sea posible su empaquetamiento y posterior transmisión. Para llevar a cabo esta operación y su inversa se utilizan los códecs (codificadores / decodificadores).

2.3.7.4. Codecs.

Los códecs pueden ser clasificados en base a distintos factores que los caracterizan, como pueden ser su tasa de bits, la calidad del audio codificado, su complejidad, el tipo de tecnología que usan o el retardo que introducen.

Originariamente, los códecs fueron diseñados para ser usados en el rango de frecuencias donde se concentra la mayor parte de energía, entre los 300 Hz y los 3,4 KHz. Estos códecs se conocen como de banda estrecha (NB, NarrowBand). Con posterioridad, se han incluido códecs capaces de trabajar en rangos más amplios, entre 50 Hz y 7 KHz, considerados de banda ancha (WB, WideBand). Actualmente, la ITU-T ha estandarizado códecs de banda “superancha” (SWB, SuperWideBand), para el rango comprendido entre 50 Hz y 14 KHz, y de banda completa (FB, FullBand), para el intervalo de frecuencias de 50 Hz a 20 KHz.

Un conjunto de códecs de banda estrecha se detallan con mayor profundidad en los siguientes epígrafes, pues son los que se utilizan en la codificación de los ficheros de audio usados en este proyecto. Este tipo de códecs son los más usados hoy en día en la telefonía móvil y fija.

En cuanto a los de banda ancha se presentan los códecs más representativos en el ámbito de la transmisión de audio. La mayor parte deriva de los códecs de banda estrecha, aunque se presentan nuevas alternativas en función de su utilización. Se están haciendo más presentes debido al hecho de que los operadores móviles están desarrollando nuevos servicios en sus redes como el denominado “voz en alta definición”. Los códecs de banda superancha

no son muy numerosos debido a su reciente inclusión en la transmisión de audio de alta calidad. En general, son extensiones incluidas en los anexos de códecs de banda ancha estandarizados por la ITU-T, a excepción de SILK desarrollado por Skype. Por último se han desarrollado los códecs de banda completa. Estos presentan una nueva experiencia en la transmisión del audio que no sólo busca proporcionar una alta calidad en la voz humana sino que pretende captar el sonido ambiental. Los dos más recientes son las extensiones de G.711.1 y G.722.

En la tabla 2 se recoge una comparativa de la calidad de audio esperada para los distintos tipos de códec, atendiendo a la banda de frecuencias de funcionamiento. Estas conclusiones junto con las gráficas comparativas presentadas a continuación han sido extraídas por el equipo de investigación de Nokia.

Tabla 2.

Calidad esperada según tipo de Códec

| Tipo de códec | Banda de frecuencias (Hz) | Calidad Esperada |
|----------------------|----------------------------------|-------------------------|
| NB | 300 – 3400 | Teléfono |
| WB | 50 – 7000 | Radio AM |
| SWB | 50 – 14000 | Radio FM |
| FB | 20 - 20000 | CB |

Nota: Comparativa de la calidad de audio esperada para los distintos tipos de códec, atendiendo a la banda de frecuencias de funcionamiento.

Fuente: Diseño e implementación de un sistema de Voz sobre IP basado en la plataforma Elastix para la empresa Quórum Teleco (Proyecto de Pregrado).

El siguiente conjunto de tablas muestran los códecs de voz más representativos pertenecientes a cada tipo de códec, según la clasificación establecida. En ellas se recoge las tasas de bit y el retraso generado en la codificación, y su aplicación básica en las comunicaciones.

Tabla 3.

Códec de banda estrecha.

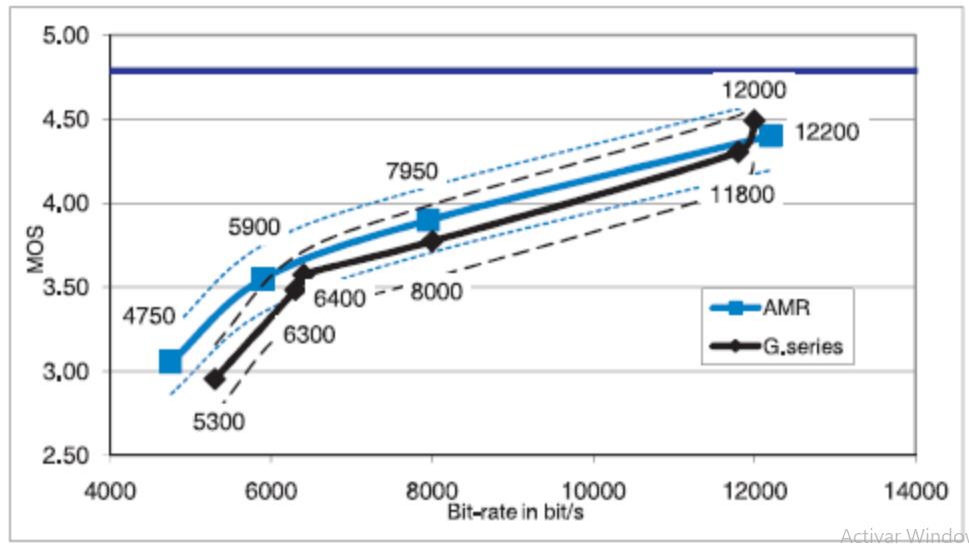
| Códec | Nombre | Tasa de bit (Kbps) | Retardo (ms) | Comentarios |
|--------------|-------------------------------------------------------------------------------|-------------------------------|-------------------------|---------------------------------------------------------------------------------------------|
| G.711 | PCM: Pulse Code Modulation | 64 / 56 | 0,125 | Utiliza dos posibles leyes de compresión: μ -law y A-law |
| G.723.1 | Hybrid MPC-MLQ and ACELP | 6,3 / 5,3 | 37,5 | Desarrollado inicialmente para videoconferencias en la PSTN. Se utiliza actualmente en VoIP |
| G.728 | LD-CELP: LowDelay Code Excited Linear Prediction | 40 / 16 / 12,8 / 9,6 | 1,25 | Diseñado para aplicaciones DCME (Digital Circuit Multiplex Encoding) |
| G.729 | CS-ACELP: Conjugate Structure Algebraic Codebook Excited Linear Prediction | 11,8 / 8 / 6,4 | 15 | Ampliamente utilizado en aplicaciones de VoIP, a 8 KHz |

| | | | | |
|------|-------------------------------|--------------|---------|------------------------------------------------------------------|
| AMR | Adaptative Multi Rate | 12,2 a 4,75 | 20 | Utilizado en redes celulares GSM |
| iLBC | internet Low Bitrate Códec | 15,2 / 13,33 | 20 / 30 | Utilizado en VoIP por su robustez ante pérdida de paquetes |

Fuente: Diseño e implementación de un sistema de Voz sobre IP basado en la plataforma Elastix para la empresa Quórum Teleco (Proyecto de Pregrado).

Figura 11.

Comparación entre AMR y Códex de la Serie G de la ITU-T.



Fuente: Diseño e implementación de un sistema de Voz sobre IP basado en la plataforma Elastix para la empresa Quórum Teleco (Proyecto de Pregrado).

La comparación entre AMR y la serie G de la ITU-T (figura 9), revela que el primero de ellos es ligeramente mejor, en cuanto a calidad del sonido, para tasa de bits similares.

Tabla 4.

Códex de banda ancha.

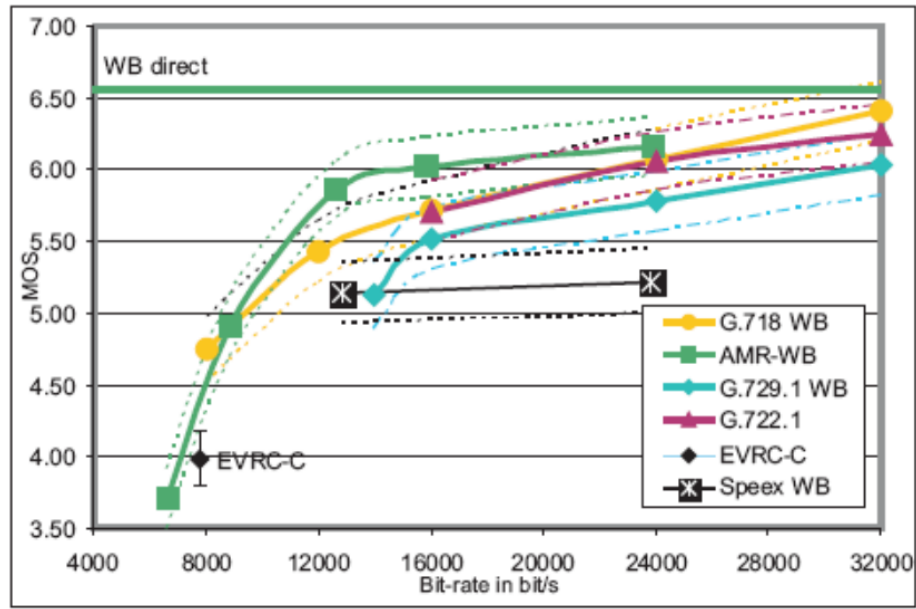
| Códec | Nombre | Tasa de bit (Kbps) | Retardo (ms) | Comentarios |
|-------|------------------|--------------------|--------------|-----------------------------------------------------------------------------------------------------------------------------|
| G.722 | Sub – band ADPCM | 64 / 56 / 48 | 3 | Originalmente creado para audio y videoconferencias. Actualmente utilizado en servicios de telefonía de banda ancha en VoIP |

| | | | | |
|---------|-----------------|--------------|---------|--------------------------------------------------------------------------------------------------|
| G.722.1 | TRansform Coder | 32 / 24 | 40 | Usado en audio y videoconferencias |
| G.711.1 | WideBand G.711 | 96 / 80 / 64 | 11,875 | Amplía el ancho de banda del códec G.711, optimizando su uso para VoIP |
| G.729.1 | WideBand G.729 | 8 a 32 | 49 | Amplía el ancho de banda del códec G.729, optimizando su uso para VoIP con audio de alta calidad |
| G.722.2 | AMR – WB | 23,85 a 6,6 | 25,9375 | Estándar en común con 3GPP |

Fuente: Diseño e implementación de un sistema de Voz sobre IP basado en la plataforma Elastix para la empresa Quórum Teleco (Proyecto de Pregrado).

Figura 12.

Comparativa entre Códecs de Banda Ancha.



Fuente: Diseño e implementación de un sistema de Voz sobre IP basado en la plataforma Elastix para la empresa Quórum Teleco (Proyecto de Pregrado).

De nuevo, puede apreciarse que, en la mayor parte de los casos, el códec AMR de banda ancha sigue proporcionando mejor calidad de audio que el resto de los códecs analizados.

Tabla 5.

Códecs de banda Superancho.

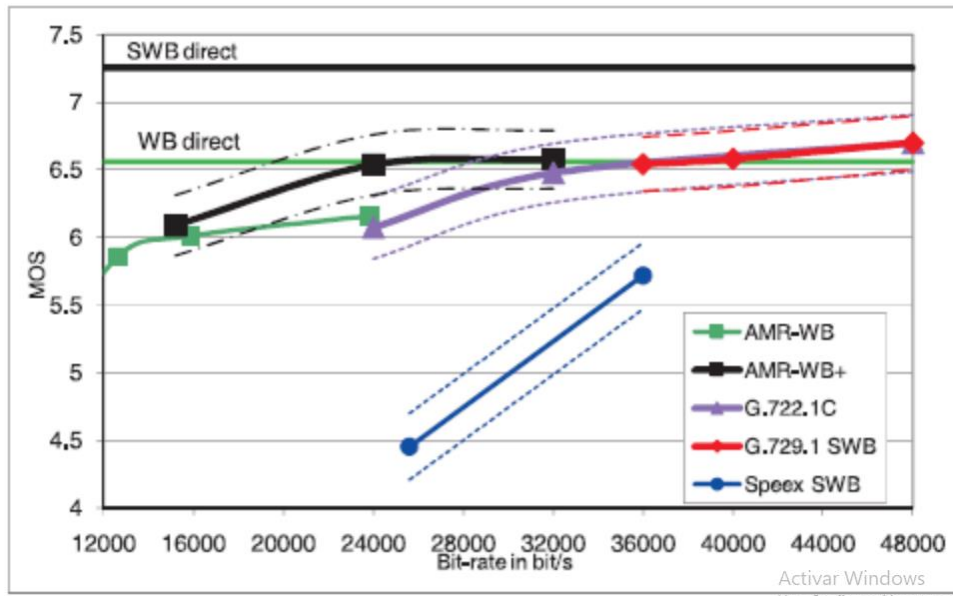
| Códec | Nombre | Tasa de bit (Kbps) | Retardo (ms) | Comentarios |
|-------|--------|--------------------|--------------|-------------|
| | | | | |

| | | | | |
|-------------|--------------------------|--------------|---------|-------------------------------------------|
| G.711.1 SWB | G.711.1 Superwideband | 128 a 96 | 12,8125 | Extensión interoperable con G711 y G711.1 |
| G.722 SWB | G.722 Superwideband | 96 / 80 / 64 | 12,3125 | Extensión interoperable con G.722 |
| G.722.1C | Anexo C de G.722.1 | 48 / 32 / 24 | 40 | Optimizado para su uso en tiempo real |
| SILK | SILK | 8 a 24 | 25 | Utilizado por Skype |

Fuente: Diseño e implementación de un sistema de Voz sobre IP basado en la plataforma Elastix para la empresa Quórum Teleco (Proyecto de Pregrado).

Figura 13.

Comparativa de Códecs de Banda Superancha.



Fuente: Diseño e implementación de un sistema de Voz sobre IP basado en la plataforma Elastix para la empresa Quórum Teleco (Proyecto de Pregrado).

En la anterior gráfica se comprueba que AMR de banda ancha extendido, AMR-WB, continúa siendo el códec que aporta mayor calidad a la comunicación. No obstante, no se ha incluido en la tabla 5 como una opción válida pues presenta un alto retardo para la telefonía en tiempo real.

Tabla 6. Códec de banda completa.

| Códec | Nombre | Tasa de bit (Kbps) | Retardo (ms) | Comentarios |
|-------|--------|--------------------|--------------|-------------|
| | | | | |

| | | | | | |
|-------|---------------------------|---|----------|----|---------------------------------------------------|
| G.719 | Low Complexity, full band | – | 32 a 128 | 40 | Primer Códec fullband estandarizado por la ITU-T. |
|-------|---------------------------|---|----------|----|---------------------------------------------------|

Fuente: Diseño e implementación de un sistema de Voz sobre IP basado en la plataforma Elastix para la empresa Quórum Teleco (Proyecto de Pregrado).

Los Códecs más utilizados en la actualidad son mencionados a continuación:

- **Códecs De Audio.**

- **GSM** – 13 Kbps (full rate), tamaño de marco de 20ms
- **iLBC** – 15Kbps, tamaño de fram 20ms: 13.3 Kbps, tamaño de frame 30ms
- **ITU G.711** – 64 Kbps, basado en muestras. También conocido como alaw/ulaw
- **ITU G719** – 32/48/64/128 Kbps, tamaño de frame 28ms
- **ITU G.722** – 48/56/64 Kbps
- **ITU G.723.1** – 5.3/6.3 Kbps, tamaño de frame 30ms
- **ITU G.726** – 16/24/32/40 Kbps
- **ITU G.728** – 16 Kbps
- **ITU G.729** – 8 Kbps, tamaño de frame 10ms
- **Speex** – 2.15 to 44.2 Kbps
- **LPC10** – 2.5 Kbps
- **DoD CELP** – 4.8 Kbps

- **Códecs De Video.**

- **VP8** es un códec utilizado para codificar y decodificar video de alta definición ya sea un archivo una transmisión. El códec VP8 es en contraste con el H.264 codec – libre de usar.
- **H.264/MPEG-4 Part 10 o AVC (Advanced Video Coding)** es actualmente unos de los formatos más utilizados para grabación, compresión y reproducción de video en alta definición. En contraste con VP8, H.264 no es libre.

2.3.8. Protocolos De Transporte.

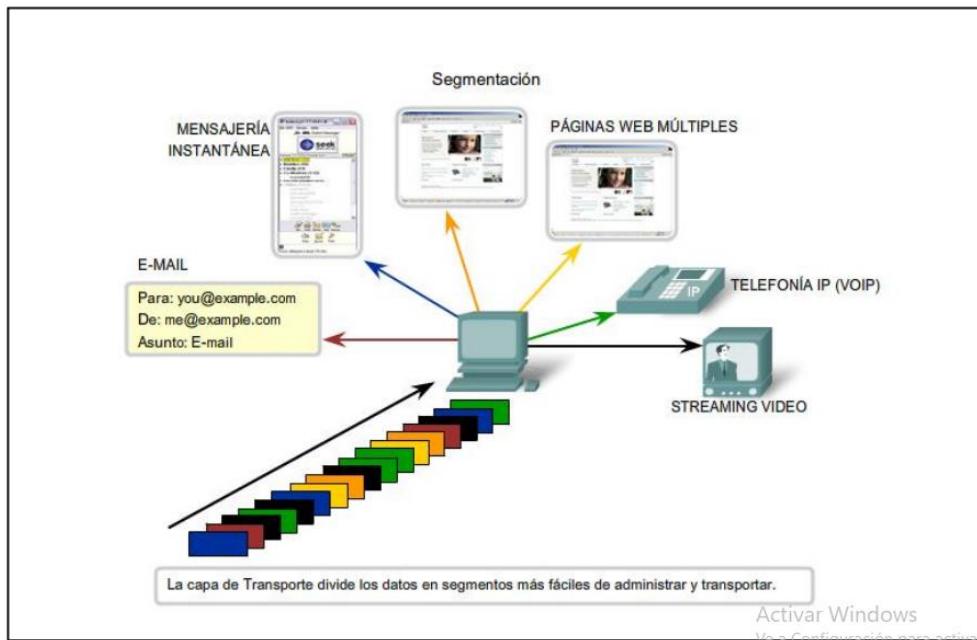
La capa de Transporte permite la segmentación de datos y brinda el control necesario para re ensamblar las partes dentro de los distintos streams de comunicación. Las responsabilidades principales que debe cumplir son:

- Seguimiento de la comunicación individual entre aplicaciones en los hosts origen y destino.
- Segmentación de datos y gestión de cada porción.
- Reensamble de segmentos en flujos de datos de aplicación.
- Identificación de las diferentes aplicaciones.

Hay dos tipos de servicio o protocolos utilizados en la capa transporte, orientado a la conexión (TCP) y no orientado a la conexión (UDP). En el servicio orientado a la conexión consta de tres partes: establecimiento, transferencia de datos, y liberación. En el servicio no orientado a la conexión se tratan los paquetes de forma individual.

Figura 14.

Multiplexación de diferentes en la capa de transporte.



Fuente: Tecnología de comunicación Voz sobre IP (Monografía de Pregrado).

2.3.8.1. Protocolo TCP.

TCP es un protocolo de transporte que se transmite sobre IP, descrito en la RFC 793. TCP ayuda controlando que los datos transmitidos se encuentren libre de errores y sean recibidos por las aplicaciones en el mismo orden en que fueron enviados. Si se pierden datos en el camino introduce mecanismos para que estos datos sean reenviados por el emisor.

Esto causa una carga extra de información en el flujo de datos, ya que hay que enviar información de control adicional. Es por esto que TCP es un buen protocolo para control de sesiones pero no tan bueno para transmisión de datos en tiempo real. Por esta razón la voz en

sí no se envía usando este protocolo, sin embargo TCP juega un rol muy importante en muchos protocolos relacionados con un servidor Elastix.

Aplicaciones que utilizan TCP:

- Servicio de Correo electrónico (SMTP, POP3).
- Transferencia de Archivos (SMB, FTP).
- Exploradores Web (HTTP, HTTPS).

El concepto de “puerto” se maneja mucho en este tema ya que es una abstracción para poder relacionar los flujos de datos con servicios de comunicaciones por red específicos. Un ejemplo común es el puerto 80 que se asocia con el servicio de web o el protocolo http, otro es el puerto 23 que se asocia al servicio de conexión remota o protocolo telnet.

2.3.8.2. Protocolo UDP.

(Marín & Luis, 2013) Es un protocolo simple, sin conexión descrito en la RFC 768. Se diferencia con TCP en que a este protocolo no comprueba si los datos llegan con errores o no y tampoco si llegan en secuencia. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos.

Aplicaciones que utilizan UDP:

- Sistemas de Nombres de dominio (DNS).
- Streaming de Video.
- Voz sobre Ip (VOIP).

El protocolo UDP al no incluir información de control, reduce la cantidad de información extra en los paquetes por lo que es un protocolo más rápido que TCP y adecuado para transmisión de paquetes de información en tiempo real como lo es la voz.

2.3.9. Protocolos para VoIP.

2.3.9.1. Protocolos De Señalización.

(Gómez & Francisco, 2014) La realización de una llamada entre dos teléfonos cualesquiera implica la utilización de diversos equipos electrónicos, los cuales deben comunicarse entre sí. Para poder garantizar que la comunicación entre los equipos se realiza adecuadamente, son necesarias diversas reglas y/o normas. Estas reglas y/o normas de las que se habla es lo que se conoce como protocolo de señalización.

Por señalización se entiende el conjunto de informaciones intercambiadas entre los dos extremos de la comunicación que permiten efectuar operaciones de:

- Supervisión (detección de condición o cambio de estado).
- Direccionamiento (negociación y establecimiento de llamada).
- Explotación (gestión y mantenimiento de la red).

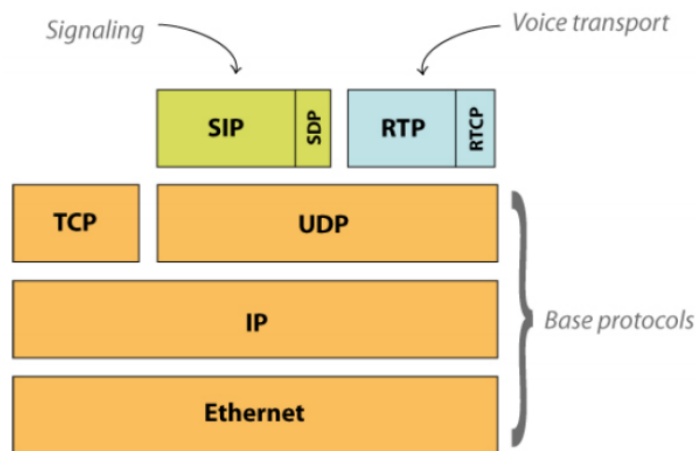
Actualmente existen muchos protocolos para la señalización de la VOIP, diseñados por diferentes fabricantes u organismos como la ITU-T o el IETF, y que son implementados en Asterisk, tales como: SIP, H323, IAX2, MGCP

2.3.9.2. Protocolo SIP (Session Initiation Protocol).

(Gómez & Francisco, 2014) El protocolo SIP es principalmente un protocolo de señalización de capa de aplicación para iniciación, modificación y terminación de sesiones de comunicación multimedia entre usuarios siendo de manera interactiva. Aquello que implique multimedia se refiere a las aplicaciones de mensajería instantánea, aplicaciones de video, de audio, de conferencias y aplicaciones similares (Alcayde García, y otros, 2008). Los clientes SIP usan el puerto 5060 en TCP (Transmisión Control Protocol) y UDP (User Datagram Protocol) para conectar con los servidores SIP. Todas las comunicaciones de voz/video van sobre RTP (Real-time transport Protocol).

Figura 15.

Ubicación de Protocolo SIP en el modelo TCP/IP.



Fuente: VoIP y Asterisk: Redescubriendo la Telefonía

Funcionamiento. El protocolo SIP, protocolo de inicio de sesión, permite establecer el procedimiento inicial de conexión para que dos UAs se conecten. User Agents (UAs) se

llaman así a los terminales SIP que pueden ser Teléfonos SIP, Softphone, Gateways FXS/IP, Routers SIP, Teléfonos USB, etc.

Existen 2 tipos de User Agents (UA's) para la comunicación SIP los cuales son:

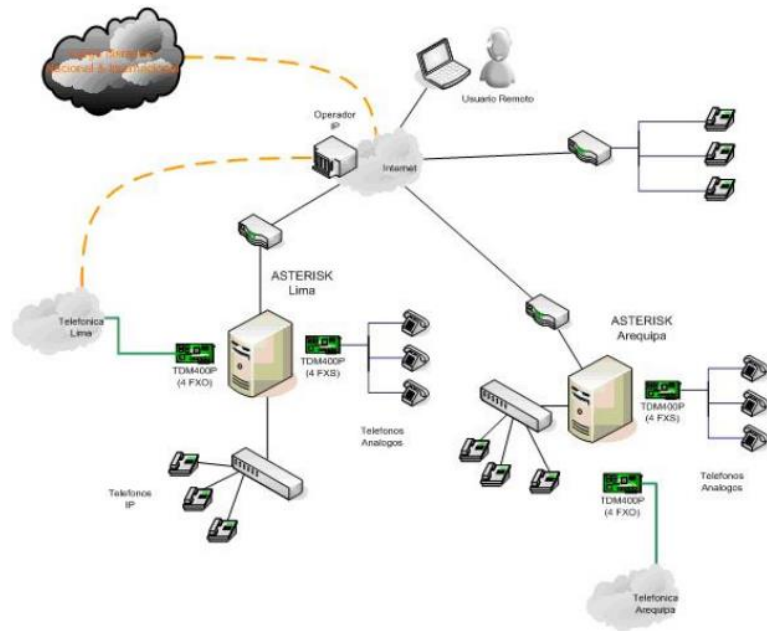
- **User Agent Client (UAC):** Origina las solicitudes SIP.
- **User Agent Server (UAS):** Responde a la solicitud de UAC.

Los UAC Y UAS son capaces, sin los servidores de red, de soportar una comunicación básica. Existen otros Componentes involucrados en la comunicación: Servidor Proxy SIP: Realiza las funciones de intermediador entre el UAC y el UAS. Una vez le llega una petición de inicio de llamada de UAC decide a que servidor debería ser enviada y entonces retransmite la petición, que en algunos casos puede llegar a atravesar varios proxys SIP antes de llegar a su destino.

Servidor de Redirección: Es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor. Servidor de Registro: es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla. Servidor de Localización: Facilita información al Proxy o Redirect sobre la ubicación del destinatario de una llamada.

Figura 16.

Infraestructura SIP.



Fuente: VoIP y Asterisk: Redescubriendo la Telefonía

Tabla 7.

Tabla de mensaje SIP.

| Mensaje | Explicación |
|-----------------|------------------------------------------------------------------------------------------------------------------|
| INVITE | Permite invitar un usuario para participar en una sesión o para modificar parámetros en una sesión ya existente. |
| ACK | Confirma el establecimiento de una sesión. |
| OPTION | Solicita información sobre las capacidades de un servidor. |
| BYE | Indica la terminación de una sesión. |
| CANCEL | Cancela una petición pendiente de llamada. |
| REGISTER | Registrar al User Agent. |

Respuesta SIP: Las peticiones SIP llevan asociada una respuesta enumerada con un código que la identifica. Estos códigos van desde el identificador 100 hasta el identificador 699, siendo además agrupadas en diferentes grupos de respuestas tales como: 1xx, 2xx, 3xx, 4xx, 5xx, 6xx.

2.3.9.3. Protocolo IAX (Inter - Asterisk eXchange protocol)

Este protocolo es utilizado para manejar conexiones VoIP ya sea entre servidores Asterisk, o entre servidores y clientes. El protocolo IAX ahora se refiere generalmente al IAX2, la segunda versión del protocolo IAX2 (Sierra A. , 2008).

IAX2 fue creado y estandarizado en Enero de 2004 por Mark Spencer y su empresa Digium, la creadora de Asterisk, y es creado para y por Asterisk. Y surge también, para corregir algunos de los problemas principales del protocolo SIP, estos objetivos son:

- Minimizar el ancho de banda usado en las transmisiones de control y multimedia.
- Cambiar de protocolo de texto a protocolo binario. Pequeñas cabeceras y bajo consumo de ancho de banda.
- Evitar problemas de NAT (Network Address Translation). IAX2 usa UDP sobre un único puerto, el 4569, donde viajan la información de señalización y datos.
- Soporte para transmitir planes de marcación (dialplans).

IAX2 soporta la autenticación de estilo PKI (Public Key Infrastructure) y trunking.

IAX2 realiza autenticación en llamadas entrantes y salientes. En cuanto a seguridad, éste permite la autenticación, y en ciertas situaciones cifrado entre terminales.

Al hacer trunking con IAX2 solamente el ancho de banda usado se asigna siempre. Otros protocolos usados para el trunking asignan siempre cierta cantidad de ancho de banda para mantener todos los canales abiertos. El trunking de IAX2 permite que los streams múltiples de voz compartan un solo “trunk” a otro servidor, reduciendo así las sobrecargas creadas por los paquetes de IP. El trunking requiere que ambos lados se conozcan, es decir, si un lado tiene trunk=yes y el otro no, se conseguirá solo audio unidireccional.

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

IAX2 soporta Trunking, donde un simple enlace permite enviar datos y señalización por múltiples canales. Cuando se realiza Trunking, los datos de múltiples llamadas son manejados en un único conjunto de paquetes, lo que significa que un datagrama IP puede entregar información para más llamadas sin crear latencia adicional. Esto es una gran ventaja para los usuarios de VoIP, donde las cabeceras IP son un gran porcentaje del ancho de banda utilizado, además de que permite reducir la latencia y el jitter.

IAX2 soporta los siguientes tipos de mensajes, optimizados para cada uno de los tipos de comunicaciones que puede establecer.

- DTMF Media Message: Datos del protocolo DTMF.
- Voice Media Message: Transporte de Voz.

- Video Media Message: Transporte de Vídeo.
- Text Media Message: Transporta Texto.
- Image Media Message: Transporta Imágenes.
- HTML Media Message: Transporta HTML.
- Confort Noise Media Message: Transporta información de calidad del enlace.

2.3.10. Protocolos de Transporte.

2.3.10.1. Protocolo UDP (User Datagram Protocol).

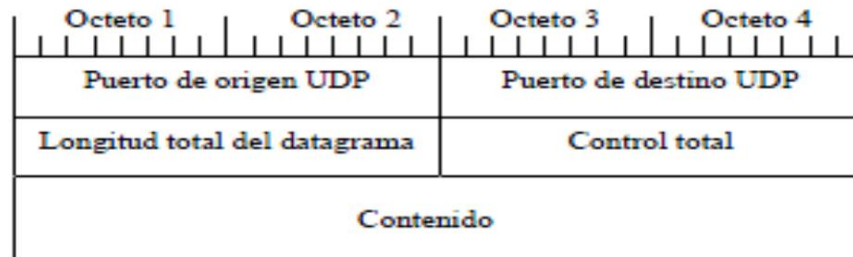
El protocolo UDP tiene la característica de funcionar en un modo sin conexión, es decir, envía datagramas procesados independientemente por la red, los cuales pueden tomar rutas diferentes y ser recibidos en un orden diferente (Alberto & Raúl, 2013).

Se diferencia con TCP en que a este protocolo no le importa si los datos llegan con errores o no y tampoco le importa si llegan en secuencia. UDP divide la información en paquetes, también llamados datagramas, para ser transportados dentro de los paquetes IP a su destino. Como no es necesario incluir mucha información de control, el protocolo UDP reduce la cantidad de información extra en los paquetes por lo que es un protocolo más rápido que TCP y adecuado para transmisión de información que debe ser transmitida en tiempo real como la voz.

En la siguiente imagen se puede observar como es el formato de encabezamiento de un datagrama UDP.

Figura 17.

Datagrama UDP.



Fuente: Fuente: Diseño e implementación de un sistema de Voz sobre IP basado en la plataforma Elastix para la empresa Quórum Teleco (Proyecto de Pregrado).

2.3.10.2. Protocolo RTP (Real Time Protocol).

RTP (Real-time Transport Protocol – Protocolo de Transporte en Tiempo Real) es un protocolo de transporte y control, adaptado a las aplicaciones que requieren que la información sea enviada en tiempo real. El protocolo RTP es independiente del protocolo de transmisión subyacente y de las redes involucradas. Generalmente se emplea por encima del protocolo UDP. RTP funciona de extremo a extremo y no reserva ningún recurso en la red, pues no se efectúa ninguna acción en los routers (el control de calidad de servicio no se realiza con dicho protocolo). (Grupo de expertos sobre telefonía IP de la UIT-D, 2005). La función principal de RTP es multiplexar varios flujos de datos en tiempo real en un solo flujo de paquetes UDP, pudiéndose enviar tanto a un solo destino (Unicast) o múltiples destinos (Multicast). Los paquetes son numerados de la siguiente manera: se le asigna a cada paquete un número inmediatamente mayor que su antecesor. Esto será útil para que la aplicación conozca si ha fallado algún paquete o no en la transmisión. Si ha fallado, al no tener un control de flujo de errores, de confirmaciones de recepción ni de solicitud de transmisión, la

mejor opción es la interpolación de los datos, la cual se da en el receptor, en caso de que se trate de una aplicación que posea esta facultad. El protocolo que transporta la voz propiamente dicha o lo que comúnmente se denomina carga útil se llama RTP (Real-time Transport Protocol) y su función es simple: transportar la voz con el menor retraso posible (Alberto & Raúl, 2013).

2.3.11. Calidad De Servicio.

2.3.11.1. Concepto De Calidad De Servicio (QoS).

Todas las características de un servicio de Telecomunicaciones, las cuales van a determinar su capacidad para satisfacer las necesidades, tanto explícitas como implícitas del usuario que va a usar el servicio es lo que se conoce como calidad de servicio (Alberto & Raúl, 2013).

La calidad de servicios se puede definir como la capacidad de una red para generar un tratamiento diferente a los diversos tipos de tráfico, mejorando de esta manera el servicio prestado. Para ofrecer calidad en las conversaciones de una red de voz sobre IP, el ancho de banda requerido por los dos flujos de tráfico (voz y datos) se debe garantizar con independencia del estado del resto de las conexiones, basándose para esto en criterios como:

- Control de las Fluctuaciones de la red.
- Priorización de los paquetes que requieran menor latencia.
- Supresión de Silencios.

2.3.11.2. Arquitectura en QoS.

La calidad de servicio es un factor importante en la construcción y diseño de redes de telecomunicaciones, debido al crecimiento desmesurado de los servicios sobre el protocolo IP, el desarrollo de aplicaciones y su convergencia. Para esto existen modelos de arquitectura que se encargan de realizar la gestión del tráfico de los paquetes sobre la red (Alberto & Raúl, 2013).

2.3.11.2.1. Servicio De Mejor Esfuerzo.

Se conoce como servicio al mejor esfuerzo a aquel en donde la red hace todo lo necesario para asegurar que el paquete llegue a su destino, es el servicio que prestan actualmente protocolos como ftp y http2. En este las aplicaciones envían datos en cualquier cantidad sin preguntar a la red. Por lo cual no lo hace adecuado para las aplicaciones sensibles al retardo o en aplicaciones en donde halla grandes variaciones en el ancho de banda. Por excelencia la red que opera de esta forma es Internet.

2.3.11.2.2. Servicios Integrados o IntServ.

El tipo de arquitectura IntServ, es un modelo de servicios múltiples que permiten configurar variedad de políticas de QoS, en este las aplicaciones piden a la red un tipo específico de servicio antes de comenzar con la transmisión. Este requerimiento se realiza con señalización explícita, la aplicación informa a la red el perfil de su tráfico, y pide a esta un tipo particular de servicio que concuerde con sus requerimientos de retardo y ancho de banda. En esta arquitectura se espera que la aplicación comience la transmisión solo luego

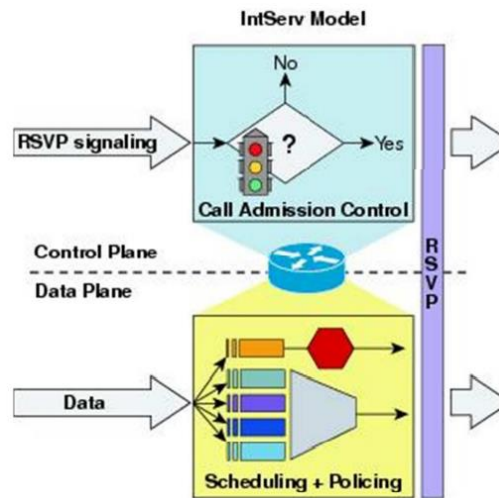
de obtener una autorización de la red y este tráfico debe cumplir con el perfil que se haya descrito.

IntServ clasifica el flujo del tráfico sirviéndose de las cabeceras de los datagramas IP. Clasificándolos en 3 tipos con el fin de especificar el tratamiento que se le debe realizar a cada uno de ellos, estos tipos son servicios garantizados, entre estos se encuentran los servicios de datos en tiempo real, servicios de carga controlada, para tráfico en tiempo real menos crítico como el VoD (video on demand), y el best effort service descrito en la anterior sección.

Para realizar su despliegue, IntServ utiliza el protocolo de reserva de recursos RSVP el cual se encarga de las necesidades de calidad de servicio para el tráfico de las aplicaciones a lo largo de toda la infraestructura de la red. Asegurando que cada dispositivo de red sea capaz de reservar el ancho de banda necesario para que pueda comenzar la transmisión.

Figura 18.

Arquitectura de Servicios Integrados IntServ.



Fuente: Tecnología de comunicación Voz sobre IP (Monografía de Pregrado).

2.3.11.3. Servicios Diferenciados o DiffServ.

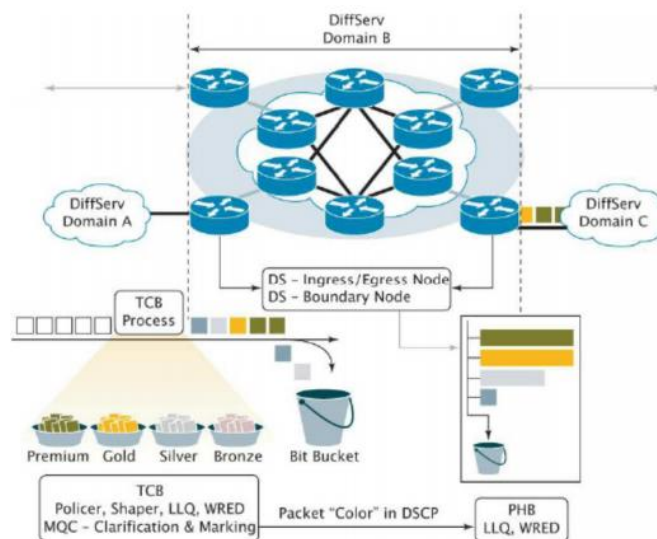
El protocolo de servicios diferenciados, nace debido a la necesidad clara de tener un método sencillo y amplio para la prestación de diferentes clases de servicio para el tráfico IP, con el fin de tener soportar diversos tipos de aplicación y el requerimiento de ciertos modelos de negocio. Diffserv se enfoca en proporcionar calidad de servicio a redes que emplean un conjunto bien definido de bloques de construcción en los cuales se pueden configurar más de un tipo de comportamiento en los paquetes de datos de cada servicio. Esta configuración es realizada en un pequeño segmento de la cabecera IP, para la versión 4 este es conocido como el octeto DSCP y, clase de servicio para IPv6. Este es usado para marcar los paquetes para que reciban un tratamiento preferencial en cada nodo de la red. Se requiere que se llegue a

un acuerdo en el comportamiento de este campo entre los servicios inter-dominio, la interoperabilidad entre proveedores y consistencia en el comportamiento esperado de los servicios agregados a la red. Por lo tanto se ha estandarizado un esquema para el uso final de DiffServ llamado el campo DS. Los cuales son definidos en la RFC 24753.

Para proveer calidad de servicio de extremo a extremo DiffServ usa dos componentes principales para el marcado de paquetes, usando el segmento ToS o configurando comportamientos por salto.

Figura 19.

Arquitectura de Servicios Diferenciados DiffServ.



Fuente: Tecnología de comunicación Voz sobre IP (Monografía de Pregrado).

2.3.11.4. Protocolo de Reserva de Recursos (RSVP).

RSVP es el primer protocolo estándar significativo de la industria, para configurar dinámicamente QoS punto a punto.

RSVP, el cual corre sobre IP, le permite a una aplicación reservar dinámicamente el ancho de banda de la red. RSVP es el único protocolo estándar de señalización, diseñado para garantizar el ancho de banda punto a punto, para redes IP.

RSVP es una importante característica de QoS, pero no resuelve todos los problemas e impone algunas restricciones, tal como el tiempo requerido para configurar una reservación punto a punto.

El protocolo RSVP es utilizado por el host para solicitar una QoS al router para una aplicación particular y es usado por el router para establecer un ancho de banda en todos los nodos intermedios del trayecto.

RSVP opera sobre IPv4 como sobre IPv6; no es un protocolo de enrutamiento y solo se utiliza para reservar ancho de banda y buffer. En el modelo de capas el protocolo RSVP ocupa la función de la capa 3 sobre IP, en la misma forma que los protocolos routing (OSPF y BGP), de multicast (IGMP), de gestión (ICMP) y de transporte (TCP y UDP). Una sesión manejada por el protocolo RSVP está definida mediante 3 direcciones: La dirección IP de destino (Receptor), el identificador de protocolo y el puerto UDP.

2.3.12. Estándares De Comunicaciones De VoIP.

2.3.12.1. Protocolo H.323.

Se trata de una recomendación la cual fue definida originalmente por la Comisión de Estudio 16 del UIT-T, como una variante de la norma de la Recomendación H.320 relativa a la videotelefonía por la Red Digital de Servicios Integrados (RDSI), adaptada en este caso a las redes de datos locales del tipo Ethernet, Fast Ethernet y Token Ring. Esta Recomendación se trata del control de llamadas, la gestión de multimedios y la gestión del ancho de banda para conferencias punto a punto y multipunto. También habla sobre la gestión de interfaces entre la red LAN (Local Area Network – Red de Área Local) y otras redes. Está concebida para la codificación y compresión de señales de voz e imágenes para su transporte a través de redes IP. Las normas que contiene esta Recomendación pueden aplicarse con independencia del medio físico de la red IP: ATM (Asynchronous Transfer Mode – Modo de Transferencia Asíncrona), FDDI (Fiber Distributed Data Interface – Interfaz de Datos Distribuida a través de Fibra), etc. En modo no conectado y sin garantía de la calidad de servicio (sin corrección de errores). El protocolo H.323 está actualmente considerado como la norma insoslayable de telefonía por Internet. En lo sucesivo, esta norma se aplica a todas las redes por paquetes y no solamente a las redes locales.

Características importantes del Protocolo H.323.

- Soporte para multiconferencias: A pesar de que H.323 permite mantener multiconferencias sin el uso de unidades especializadas, las MCUs (Multipoint

Control Units), proporcionan una arquitectura más robusta y flexible para el mantenimiento de multiconferencias.

- Gestión del ancho de banda: El tráfico de audio y de vídeo resulta costoso en cuanto a recursos de ancho de banda, y podría colapsar la red. H.323 permite la gestión del ancho de banda, pudiendo limitar el número de conexiones H.323 simultáneas, así como especificarles el ancho de banda disponible a aplicaciones y terminales H.323.
- Establecimiento de llamada rápida (Fast Call – Llamada Rápida). H.323 también establece mecanismos para que la llamada quede establecida con un mínimo de dos paquetes.
- Capacidades para la redundancia de la red. Mediante servidores de direccionamiento alternativos (Alternate Gatekeepers) la red podrá soportar la caída de estos equipos críticos, sin pérdida de comunicación.

2.3.12.2. Elementos De H.323.

El protocolo H.323 define cuatro elementos fundamentales en la arquitectura de red.

1. TERMINALES.

Dispositivo final de comunicación, el cual puede ser un teléfono IP o un equipo de videoconferencia de alta definición. Allí están determinado los tipos de protocolos de la estructura de H.323 que pueden ser utilizados, con el fin de brindar una variedad de servicios. A continuación se presenta una explicación detallada de los equipos terminales más comunes (Cortés & Fabián L., 2012).

a) Adaptador para Teléfonos Analógicos (ATA).

Son dispositivos que sirven para el aprovechamiento tanto de los teléfonos analógicos, como de las máquinas de fax usados en la red PSTN, el adaptador se encarga de interconectar el teléfono analógico con la computadora o con una red LAN, a través de una conexión tipo Ethernet. La señal analógica es convertida en los diferentes protocolos y estándares de Voz sobre IP, tal cual lo hace un teléfono IP (Marín & Luis, 2013).

Estos adaptadores se caracterizan por tener uno o más conectores RJ-11 para conectar los teléfonos analógicos y un conector RJ-45 para la conexión con la red LAN.

b) Teléfonos IP.

Un teléfono IP es un equipo con las mismas características físicas de un teléfono normal, con la única diferencia que en vez de conectarse con la red telefónica se conecta con una red de datos o de telefonía IP. La mayoría de estos teléfonos son basados en hardware, tienen un switch incorporado que les sirve para compartir la conexión de red con el computador y también adquieren una dirección IP propia mediante la cual se les puede acceder y configurar (Sierra A. , 2008).

c) Softphones.

Los softphones son aplicaciones para equipos digitales como computadores, tabletas, teléfonos inteligentes (smartphones), que permiten a los usuarios acceder a una red telefónica de Voz sobre IP. Los softphones requieren de una conexión de VoIP o una puerta de enlace (gateway) VoIP conectada al equipo donde se está ejecutando la aplicación. Cuando se está

usando la aplicación del softphone, la computadora o el equipo donde se está ejecutando requiere un ancho de banda suficiente para la conexión a Internet, y una cuenta con un proveedor de servicios de telefonía por Internet en caso de que la conexión vaya a ser remota, esta conexión normalmente usa un formato SIP (Sierra A. , 2008).

d) Gateway.

En una red de comunicaciones un gateway es un nodo de la red cuya función principal es hacer de interfaz con otra red que use diferentes tipos de protocolos. Pueden existir gateways a nivel de hardware los cuales contienen traductores de protocolos, dispositivos de adaptación de impedancias, conversores de ratio entre otros y a nivel de software que sirven para interconectar redes que tengan diferentes protocolos de red encargándose de realizar la conversión de protocolos requerida (Marín & Luis, 2013).

Un Gateway en VoIP es un dispositivo el cual sirve para convertir todo el tráfico de la telefonía tradicional en tráfico IP, y posteriormente transmitirlo en una red de datos. Básicamente sirve para conectar la red pública telefónica con la red IP. Estos gateways permiten que las llamadas salientes generadas por la central tradicional se conviertan a IP y salgan por la red de internet o viceversa.

Existen unidades analógicas y unidades digitales de Gateway. Las analógicas sirven para conectar las líneas telefónicas regulares al gateway, están disponibles entre 2 y 4 líneas, mientras que las unidades digitales permiten conectar líneas digitales, una o más líneas E1, o una o más líneas T1.

2. Gatekeeper.

Su función es registrar y re direccionar de las peticiones de sesiones entre terminales, ya sea que realice una función de señalización en modo directo, donde los terminales a través de RAS establecen la direcciones IP de otros terminales y entablen comunicación directa, siendo el método más eficiente en la configuración, porque evita tener que pasar por el Gatekeeper y disminuye su procesamiento. El otro modo es Gatekeeper en modo de enrutamiento, donde hace un papel activo y se encarga de enrutar las sesiones entre dos terminales, lo cual hace que su nivel de procesamiento sea aún mayor (Cortés & Fabián L., 2012).

3. UNIDAD DE CONTROL MULTIPUNTO (MCU).

Responsable por las conferencias multipunto y de suministrar servicios avanzados de conferencia acorde al fabricante del dispositivo. La MCU actúa como un puente entre las terminales que van a participar de una conferencia y brinda la posibilidad de permitir sesiones colaborativas (Cortés & Fabián L., 2012).

4. SERVIDOR PROXY.

Se encarga de encaminar peticiones/respuestas hacia el destino final. El encaminamiento se realiza salto a salto de un servidor a otro hasta alcanzar el destino final. Un servidor proxy es una entidad intermediaria en una red SIP que es responsable de reenviar peticiones SIP a un UAS (User Agent Server) de destino o a otro servidor proxy en nombre de otro UAC (User Agent Client). El servidor proxy también interpreta y si es necesario,

reescribe partes de los mensajes de petición antes de reenviarlos. También se asegura de poner en funcionamiento las políticas en la red, tales como autenticar a un usuario antes de darle servicio (Sierra A. , 2008).

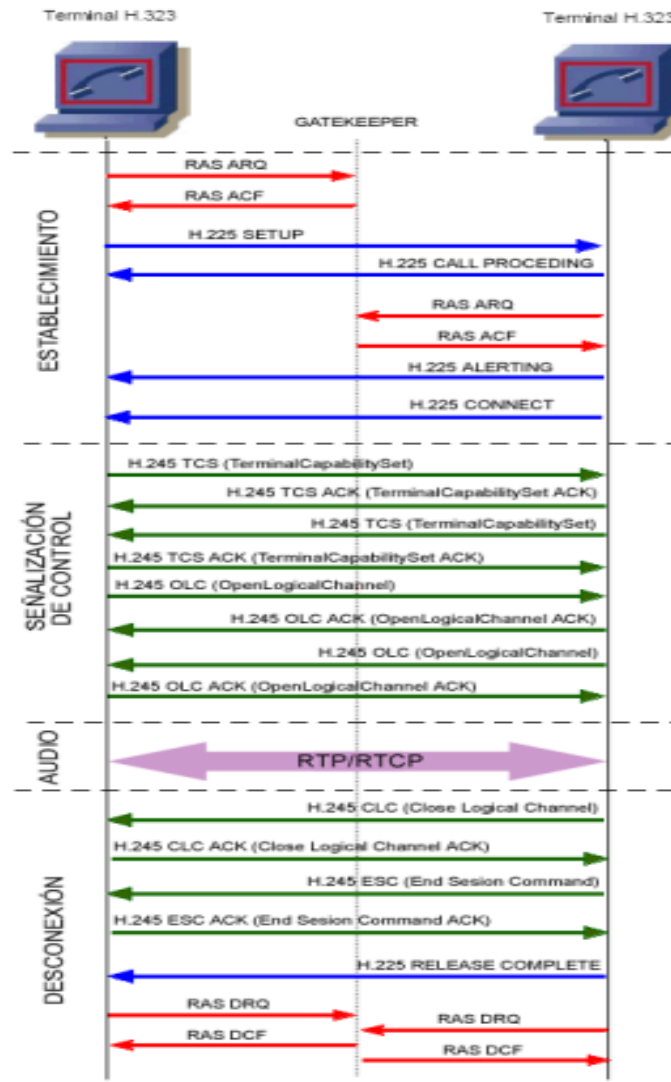
2.3.12.3. Conjunto de Protocolos H.323.

Dentro de H.323 se incluyen todo un conjunto de protocolos perfectamente integrados (en la Figura 2 se ilustra la pila de protocolos H.323) que toman parte en el establecimiento y mantenimiento de conferencias multimedia: Q.931 para el establecimiento de llamada, H.225 para la señalización, H.245 para la negociación de capacidades y el establecimiento de canales, H.450.x para la definición de servicios suplementarios (Call Park, Call Pickup, Call Hold, Call Transfer, Call Diversion, MWI, ...), RAS para el registro de terminales y el control de admisión, RTP/RTCP para el transporte y secuenciación de los flujos multimedia, G.711/G.712 para la especificación de los codecs, T.120 para colaboración y "dataconferencia".

Ejemplo de una llamada H.323:

Figura 21.

Ejemplo de una llamada H.323.



Fuente: Diseño de un Sistema de Telefonía de voz y video sobre IP para la ONG CREAB (Proyecto de Pregrado).

Una llamada H.323 se caracteriza por las siguientes fases:

1. Establecimiento.

- Uno de los terminales se registra en el guardián utilizando el protocolo RAS (mensajes ARQ y ACF).
- Mediante el protocolo H.225 se manda un mensaje de inicio de llamada (SETUP) con los datos (IP y puerto) de llamante y llamado.
- El terminal llamado contesta con CALL PROCEEDING.
- El segundo terminal tiene que registrarse con el guardián de manera similar al primer terminal.
- ALERTING indica el inicio de generación de tono.
- CONNECT indica el comienzo de la conexión.

2. SEÑALIZACIÓN DE CONTROL.

- Se abre una negociación mediante el protocolo H.245, para establecer quién será maestro y quién esclavo, las capacidades de los participantes y los códecs de audio y vídeo a utilizar. Como punto final de esta negociación se abre el canal de comunicación (direcciones IP, puerto).

3. AUDIO (+ DATOS y/o VÍDEO).

- Los terminales inician la comunicación y el intercambio de audio (+ datos y/o vídeo) mediante RTP/RTCP.

4. DESCONEXIÓN.

- Cualquiera de los participantes activos puede iniciar el proceso de finalización de llamada mediante mensajes CloseLogicalChannel y EndSessionComand de H.245.
- Posteriormente utilizando H.225 se cierra la conexión con el mensaje RELEASE COMPLETE
- Por último se liberan los registros con el guardián utilizando mensajes del protocolo RAS.

2.3.12.4. PROTOCOLO DE INICIO DE SESION (SIP).

(Sierra A. , 2008) El protocolo de inicio de sesión (Session Initiation Protocol – Protocolo de Inicio de Sesión), es un protocolo de señalización y control de la capa de aplicaciones, utilizado para establecer, mantener y terminar sesiones multimedia, estas sesiones incluyen telefonía por internet, conferencias y aplicaciones similares, las cuales sirven para generar medios como datos, audio y video. Es posible usar las invitaciones SIP para establecer las sesiones, este protocolo soporta sesiones de tipo Unicast y Multicast es decir tanto de un emisor a un solo receptor o de un emisor a múltiples receptores.

2.3.12.4.1. Componentes SIP.

Es muy importante saber que en un sistema SIP existen dos componentes claves los cuales son el User Agent y el Server, tanto el teléfono que llama como el que recibe la llamada son identificados por direcciones SIP, a continuación se explicara de forma más detallada cada uno de estos componentes.

- **USER AGENT (UA) O AGENTES USUARIOS.**

Los usuarios agentes son aplicaciones que se subdividen en agentes usuario clientes (UAC) y agentes usuario servidor (UAS), o mejor conocidos como cliente y servidor. El cliente se encarga de iniciar las peticiones tipo SIP y actúa como el agente de llamadas del usuario, mientras que el Servidor recibe las peticiones y retorna respuestas en nombre del usuario.

- **SERVIDORES DE RED**

Existen tres tipos de servidores de redes SIP, los cuales son los servidores Proxy, los servidores de redirección, y los servidores de registro.

Los Proxy básicamente actúan en nombre de otros clientes y contienen funciones tanto de servidor como de cliente. Un servidor Proxy es capaz de interpretar y de reescribir en las cabeceras de las solicitudes antes de que estas pasen a otros servidores, de esta manera se identifica al Proxy como el creador de la solicitud y se asegura de que la respuesta siga la misma ruta de regreso hacia el Proxy en lugar de al cliente.

Los servidores de Redirección principalmente aceptan peticiones SIP y envían una respuesta redirigida hacia el cliente la cual contiene la dirección del próximo servidor, este tipo de servidores no aceptan llamadas.

Los servidores de registro se encargan de registrar las direcciones SIP y sus direcciones IP asociadas, por lo general están localizados en los servidores Proxy y en los de Redirección. Solo pueden aceptar mensajes de solicitud Register, haciendo posible

el registro correspondiente de los usuarios. Esto se hace debido a que por ejemplo, en conexiones vía ISP y en usuarios móviles, la dirección IP de dichos usuarios puede cambiar.

2.3.12.4.2. MENSAJES SIP.

Existen dos tipos de mensajes SIP: Solicitudes, las cuales son iniciadas por los clientes y Respuestas, que son originadas desde los servidores. Cada mensaje contiene una cabecera que describe los detalles de la comunicación a establecerse. SIP es un protocolo basado en texto cuya sintaxis de mensajes y campos de cabecera son iguales a las del protocolo http, los mensajes SIP se pueden enviar sobre TCP o UDP (User Datagram Protocol – Protocolo de Datagrama de Usuario).

- **SOLICITUDES DE MENSAJE.**

SIP tiene seis tipos de solicitudes de mensaje. Estas solicitudes, que en ocasiones son llamadas métodos, habilitan a usuarios y servidores de la red para localizar, crear y monitorear llamadas. Los seis tipos de solicitudes son las siguientes:

- ✓ **Invite:** Este método indica que el usuario o servicio es invitado a participar en una sesión, incluye la descripción de la sesión a realizarse y en el caso de llamadas full dúplex, el agente que llama indica el tipo de datos que se van a transferir.
- ✓ **ACK:** Este mensaje corresponde a la respuesta de los mensajes Invite, representan la última confirmación del usuario final y concluyen la transacción iniciada por la solicitud invite. Si la estación que llama incluye la descripción de la sesión en su

solicitud ACK, no se utilizan parámetros adicionales en la sesión. En caso de que no haya una descripción de la sesión de los parámetros contenidos en el mensaje invite, estos se toman por defecto.

- ✓ **BYE:** Permite la liberación de una sesión anteriormente establecida. Corresponde al mensaje RELEASE de los protocolos ISUP y Q.931. Un mensaje BYE puede ser emitido por el que genera la llamada o el que la recibe.
- ✓ **Register:** es usado por un UAC con el fin de indicar al registrar la correspondencia entre su Dirección SIP y su dirección de contacto (ejemplo: dirección IP).
- ✓ **Cancel:** Se usa para pedir el abandono de la llamada en curso pero no tienen ningún efecto sobre una llamada ya aceptada. De hecho, solo el método “BYE” puede terminar una llamada establecida.
- ✓ **Options:** Sirve para interrogar las capacidades y el estado de un UAC o de un UAS. La respuesta contiene sus capacidades (ejemplo: tipo de medios siendo soportados, idioma soportado) o el hecho de que el UA sea indisponible.

- **RESPUESTAS SIP.**

A continuación se presenta una lista de los tipos de respuestas usados por el protocolo SIP:

- ✓ **1xx:** Es una respuesta provisoria, indica la petición recibida. Las respuestas provisionales, también conocidas como respuestas informativas, indican que el servidor contactado está realizando una cierta acción y todavía no tiene una respuesta definitiva. Un servidor envía una respuesta 1xx si calcula que le llevará

más de 200 ms obtener una respuesta final. Las respuestas 1xx no son transmitidas en forma confiable. Nunca hacen al cliente enviar un ACK. Las respuestas provisionarias (1xx) pueden contener cuerpos de mensaje, incluyendo descripciones de la sesión.

- ✓ **2xx:** Se refieren al éxito de alguna acción, la cual fue recibida, entendida y aceptada con éxito.
- ✓ **3xx:** Redirección, indican que algunas acciones adicionales necesitan ser tomadas para terminar la petición.
- ✓ **4xx:** Error de cliente, la petición contiene sintaxis errónea o no se puede llevar a cabo en este servidor
- ✓ **5xx:** Error de algún servidor, este no pudo llevar a cabo una petición válida.
- ✓ **6xx:** Existe alguna falla global, la petición no se puede satisfacer en ningún servidor.

- **CABECERAS SIP.**

En la cabecera del mensaje se especifica la estación que está llamando, la que recibe la llamada, la ruta y el tipo de mensaje de la llamada. Se definen tres grupos de cabecera del mensaje:

- ✓ Cabecera general: Se refiere a solicitudes y respuestas.
- ✓ Cabeceras de Entidad: Contiene información sobre el tipo de mensaje y la longitud del mismo.

- ✓ Cabeceras de respuesta: habilita al servidor para incluir información adicional de respuesta.

2.3.12.4.3. Direccionamiento SIP.

Los nodos SIP son referenciados usando URI (Uniform Resources Indicator), con la siguiente estructura:

sip:usuario@servidor_sip

Esta convención indica tanto el usuario al que quiere alcanzarse como el servidor SIP, que se espera que conozca la dirección SIP del usuario final. Aquellas conexiones que requieren una encriptación para la señalización usaran el prefijo "sips", en lugar de "sip" en la descripción de sus URI's. La encriptación de dichas señales hará uso de la capa de transporte seguro (SSL).

2.3.12.5. Descripción de SDP.

El protocolo SDP (Session Description Protocol) RFC 2327 se utiliza para describir sesiones multicast en tiempo real, siendo útil para invitaciones, anuncios, y cualquier otra forma de inicio de sesiones.

La propuesta original de SDP fue diseñada para anunciar información necesaria para los participantes y para aplicaciones de multicast MBONE (Multicast Backbone). Actualmente, su uso está extendido para el anuncio y la negociación de las capacidades de una sesión multimedia en Internet.

Puesto que SDP es un protocolo de descripción, los mensajes SDP se pueden transportar mediante distintos protocolos con SIP, SAP, RTSP, correo electrónico con aplicaciones MIME o protocolos como HTTP. Como el SIP, el SDP utiliza la codificación del texto. Un mensaje del SDP se compone de una serie de líneas, denominados campos, donde los nombres son abreviados por una sola letra, y está en una orden requerida para simplificar el análisis. El SDP no fue diseñado para ser fácilmente extensible.

2.3.13. Comparación entre SIP Y H.323.

A continuación mencionaremos algunas diferencias entre los protocolos SIP Y H.323:

- H.323 es un estándar extenso, complejo y rígido, que especifica todo el conjunto de protocolos en cada capa del modelo de referencia OSI lo que facilita la tarea de interoperabilidad pero es difícil de adaptar a las nuevas aplicaciones.
- SIP es un protocolo de Internet típico que funciona intercambiando líneas cortas de texto ASCII, interactúa bien con otros protocolos de Internet. Es altamente modular y flexible, y se puede adaptar con facilidad a las nuevas aplicaciones.
- H323 especifica servicios mientras que SIP especifica señalización e inicialización.
- H323 codifica la información en binario mientras que SIP codifica en modo texto.
- La interconexión con la PSTN es fundamental para el éxito de la telefonía IP, H.323 cuenta con un punto a su favor en este aspecto al estar definida la compatibilidad con la PSTN en el propio estándar.
- H.323 no establece relación con protocolos de la red como HTTP, o los de correo electrónico (SMTP, POP3, etc.). Mientras que SIP si lo hace.

A continuación se presenta una tabla comparativa entre SIP y H.323:

Tabla 8.

Tabla comparativa de entre los Protocolos SIP y H.323.

| <i>ELEMENTO</i> | <i>H.323</i> | <i>SIP</i> |
|------------------------------|-----------------------------|--------------------------------|
| Diseñado por | ITU | IETF |
| Arquitectura | Distribuida | Distribuida |
| Control de Llamadas | Gatekeeper | Servidor Proxy, Redirección |
| Endpoints | Gateway, Terminal | User Agent |
| Compatibilidad con PSTN | Si | Ampliamente |
| Señalización de llamadas | Q.931 sobre TCP | SIP sobre TCP o UDP |
| Formato de mensajes | Binario | ASCII |
| Transporte de medios | RTP/RTCP | RTP/RTCP |
| Llamadas de múltiples partes | Si | Si |
| Direccionamiento | Host o número telefónico | URL's |
| Encriptacion | Si | Si |

Fuente: Diseño de un Sistema de Telefonía de voz y video sobre IP para la ONG CREAB (Proyecto de Pregrado).

2.3.14. Redes Privadas Virtuales (VPN).

Una Red Privada Virtual (VPN, Virtual Private Network), es una red privada que utiliza la infraestructura de una red pública para poder transmitir información.

Una VPN combina dos conceptos: Redes Virtuales y Redes Privadas. En una red virtual, los enlaces de la red son lógicos y no físicos. La topología de esta red es independiente

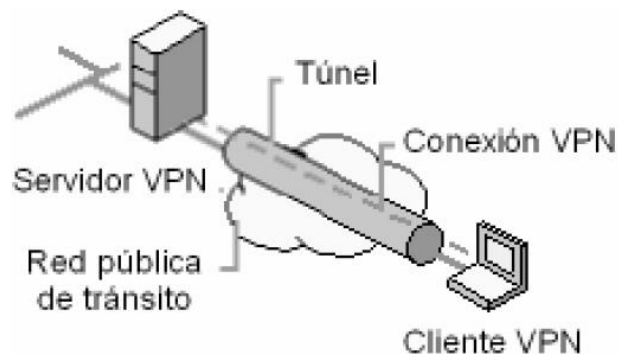
de la topología física de la infraestructura utilizada para soportarla. Un usuario de la red virtual no será capaz de detectar la red física, el solo podrá ver la red virtual (Gonzáles, 2006).

2.3.14.1. Componentes Básicos De Una VPN.

El cifrado y las medidas de seguridad son la base de las Redes privadas virtuales. En cierto modo las VPN están sustituyendo a las WAN, a pesar de que estas se pueden operar más fácilmente y tienen un bajo costo, pero no ofrecen seguridad apropiada para las empresas (Gonzáles, 2006). Los componentes que forman parte de una VPN son:

Figura 22.

Componentes de una VPN.



Fuente: Redes Privadas Virtuales (Monografía de Pregrado).

- **Servidor VPN.** Es la Computadora que acepta conexiones VPN de clientes VPN. Encargado de administrar todos los clientes VPN y proporcionar la seguridad de la red.

- **Cliente VPN.** Computadora que inicia una conexión VPN con un servidor VPN.
- **Túnel.** Es la Porción de la conexión en la que los datos son encapsulados. Es la Conexión VPN.- Porción de la conexión en la cual los datos son encriptados. Para conexiones VPN seguras, los datos son encriptados y encapsulados en la misma porción de la conexión. Nota: Es posible crear un túnel y enviar los datos a través del túnel sin encriptación. Esta no es una conexión VPN porque los datos privados viajan a través de la red pública o compartida en una forma no encriptada y fácilmente visible e insegura.
- **Protocolos de túnel.** Se utilizan para administrar los túneles y encapsular los datos privados. Existen varios protocolos de túnel que se estudiarán más adelante.
- **Datos del túnel.** Datos que son generalmente enviados a través de un enlace punto a punto.
- **Red de tránsito.** Red pública o compartida que permite el tránsito de los datos encapsulados. La red de tránsito puede ser Internet o una intranet privada. para simular un vínculo punto a punto en una VPN, los datos se empaquetan con un encabezado que proporciona la información de enrutamiento que permite a los datos recorrer la red pública hasta su destino. Para simular un vínculo privado los datos se cifran para asegurar la confidencialidad. Los paquetes interceptados en la red pública no se pueden descifrar si no se dispone de las claves de cifrado. La parte de la conexión en la que se encapsula y cifran los datos privados se denomina conexión VPN.

2.3.14.2. Arquitectura de una VPN.

Existen dos tipos básicos de arquitecturas de VPN, las cuales son:

1. **VPN de Acceso Remoto.** Este tipo de VPN proporcionan acceso remoto a intranet o extranet empresarial. una VPN de acceso remoto ahorran dinero a las empresas ya que, en lugar de realizar llamadas de larga distancia, solo con establecer una conexión con el ISP local. el usuario solo debe hacer una conexión al servidor ISP de la compañía, a través de Internet, una vez que el usuario hizo conexión, podrá hacer uso de los recursos de la intranet privada de la empresa (González, 2006).

Las VPN de acceso remoto se subdividen en VPN Dial-Up y VPN directa.

- **VPN Dial-Up.** En este tipo de VPN el usuario realiza una llamada local a ISP utilizando el modem, aunque se trata de una conexión más lenta es también la más común, este tipo de VPN se usa más entre los usuarios móviles, ya que no se puede tener una conexión de alta velocidad a todos los lugares a los que viaja.
- **VPN Directa.** Este tipo de VPN se utilizan las tecnologías de conexión a Internet de alta velocidad, como DSL y modem de cable las cuales ya ofrecen muchos ISP. se ocupa principalmente entre los teletrabajadores, también se emplea para obtener conexiones desde el hogar.

- 2. VPN de Sitio A Sitio.** Esta alternativa a Frame Relay o a las redes WAN de línea alquilada permite a las empresas llevar los recursos de la red a las sucursales, las oficinas instaladas en casa y los sitios de partners comerciales (González, 2006).

Las VPN de sitio a sitio se subdividen en VPN Intranet y VPN Extranet.

- **VPN Intranet.** Una VPN de intranet se utiliza para la comunicación interna de una compañía, enlazan la oficina central con todas las sucursales, se rigen por las mismas normas como en cualquier red privada. Un enrutador realiza la conexión VPN de sitio a sitio que conecta dos partes de una red privada. el servidor VPN proporciona una conexión enrutada a la red que está conectado el servidor VPN. (Shinder, 2004)
- **VPN Extranet.** La característica de VPN Extranet es que permite a los proveedores de servicios de distribución del contenido de multidifusión IP se originé a partir de un sitio de la empresa a otros sitios de la empresa. Esta característica permite a los proveedores de servicios puedan ofrecer la próxima generación de servicios de extranet flexibles, lo que ayuda para que las asociaciones empresariales entre los diferentes clientes de la empresa VPN.

2.3.14.3. Requerimiento de una Red Privada Virtual (VPN).

Para garantizar que una red privada virtual sea segura, este disponible y sea fácil de mantener es necesario cumplir con ciertos requisitos esenciales que una empresa debe tomar en cuenta antes de implementar una Red Privada Virtual (González, 2006).

Los requerimientos se detallan a continuación:

- **Disponibilidad:** La disponibilidad se aplica tanto al tiempo de actualización como al de acceso. No basta que el usuario tenga autorización para acceder a los servidores corporativos, si no puede conectarse debido a problemas de la red, por tanto se debe asegurar la disponibilidad en la parte física de la red.
- **Control:** El control debe ser implementado por el supervisor o administrador de la Red Privada Virtual, sea este interno o externo dependiendo de la como se realizó la implementación de VPN. Debemos tomar en cuenta que por muy grande que sea la organización es posible tener una solo VPN, lo que facilitará al administrador de la VPN el control sobre la misma.
- **Compatibilidad:** Debido que al utilizar tecnologías de VPN y de internet estas se basan en protocolo IP, por lo que la arquitectura interna del protocolo de red de la compañía debe ser compatible con el protocolo IP.
- **Seguridad:** Hablar de seguridad y de red privada virtual, hasta cierto punto se podría decir que son sinónimos. La seguridad en una VPN abarca todo, desde el proceso de cifrado que se implementa hasta los servicios de autenticación de usuarios. Es necesario que se tenga muy en cuenta este término de seguridad, ya que se puede afirmar que una VPN sin seguridad no es una VPN.
- **Interoperabilidad:** La interoperabilidad de una red privada virtual, es muy importante para la transparencia en la conexión entre las partes involucradas. Confiabilidad.- La confiabilidad es uno de los requisitos importantes que debe poseer en una Red Privada Virtual, pero esta confiabilidad se ve afectada en gran porcentaje

en la VPN de Acceso Remoto en las que se sujeta a la confiabilidad que se tiene por parte del ISP, ya que si el servicio del ISP se interrumpe la conexión también y nosotros no se podrá hacer nada hasta que el ISP nuevamente brinde su servicio a los clientes.

- **Confiabilidad:** La confiabilidad es uno de los requisitos importantes que debe poseer en una Red Privada Virtual, pero esta confiabilidad se ve afectada en gran porcentaje en la VPN de Acceso Remoto en las que se sujeta a la confiabilidad que se tiene por parte del ISP, ya que si el servicio del ISP se interrumpe la conexión también y nosotros no se podrá hacer nada hasta que el ISP nuevamente brinde su servicio a los clientes.
- **Autenticación de datos y usuarios:** La autenticación de datos y de usuarios es sumamente importante dentro de cualquier configuración de Red privada Virtual. La autenticación de datos afirma que los datos han sido entregados a su destinatario totalmente sin alteraciones de ninguna manera. La autenticación de usuarios es el proceso en el que se controla que solos los usuarios admitidos tengan acceso a la red y no sufrir ataques por usuarios externos y maliciosos.
- **Sobrecarga de tráfico:** La sobrecarga de tráfico es un problema de cualquier tipo de tecnología de redes, y por ende también es un problema inevitable, especialmente si tenemos una red privada virtual a través de un ISP. Tomando en cuenta que un paquete enviado en una VPN es encriptado y encapsulado lo que aumenta de manera significativa la sobrecarga de tráfico en la red.
- **Mantenimiento:** El mantenimiento, aspecto del que no se puede olvidar. Si la red privada virtual es implementada con los propios recursos de la empresa es necesario

considerar que el mantenimiento debe estar soportado por el propio personal del departamento de sistemas, el cual debe estar capacitado para este fin. De no poseer el personal capacitado es preferible contratar servicios externos que se encarguen de la implementación y mantenimiento de la red privada virtual de la empresa.

- **Sin repudio:** Consiste en el proceso de identificar correctamente al emisor, con la finalidad de tener claro desde donde proviene la solicitud. Si se considera que una VPN va a servir para contactar con los clientes, es necesario que este bien identificado de dónde proviene el pedido. Para poder realizar cualquier transacción comercial (comercio electrónico) por internet es necesario que esta transacción sea un proceso sin repudio. Nos podemos dar cuenta que nuevamente se está hablando de seguridad, una de las características fundamentales en una VPN. (Ramírez, 2013).

2.3.14.4. Ventajas De Las Redes Privadas Virtuales (VPN).

El simple hecho de hablar de redes privadas virtuales, como se indicó anteriormente, viene a la mente el término de seguridad, así como también el bajo costo que esta tecnología necesita para implementarla y además su facilidad de uso.

En resumen, se puede decir que la implementación de una red privada virtual nos hace pensar en tres aspectos fundamentales y beneficiosos, que son:

- **Ahorro en costos.** El ahorro en costos de las redes privadas virtuales está asociado con diferentes factores que influyen en el paso de una tecnología anterior a una tecnología de redes privadas virtuales. La eliminación de líneas rentadas, al igual que las líneas por marcación son dos factores fundamentales que permitirán el ahorro en

la implementación de una VPN, tomando en cuenta que al eliminar este tipo de comunicación también se eliminan los costos de los demás dispositivos involucrados como puede ser equipos pbx, equipos de acceso remoto. También se eliminarán costos de instalación y configuración de dichos equipos de acceso remoto, entre otros costos.

- **Beneficios para el usuario final.** El usuario final se ve muy beneficiado, ya sea un usuario que pertenezca a la propia empresa o un cliente. En la actualidad las empresas deben llegar al cliente, sin importar donde se encuentre éste, es por eso que se hace necesario que el cliente tenga acceso a los servicios y ya no se lo haga con comunicaciones telefónicas de larga distancia que son muy costosas, sino a través de un ISP local con un enlace más eficiente y menos costoso y además un enlace que va a estar disponible las 24 horas del día los 365 días del año. El mismo beneficio tendrán los usuarios remotos, facilitándoles el acceso a la información de la empresa en el momento que lo deseen, independiente del lugar en el que se encuentren.

2.3.15. Asterisk.

Asterisk es una central software (PBX) de código abierto. Al ser una central PBX híbrida permite interconectar teléfonos IP, análogos, etc., y conectar dichos teléfonos a la red telefónica convencional. Su nombre se deriva del símbolo Asterisco en inglés y se debe al uso del mismo como comodín para poder representar casi cualquier cosa (Marín & Luis, 2013).

Asterisk corre bajo el Sistema Operativo Linux y provee todas las funcionalidades que se pueden esperar de un Conmutador. A pesar de que Asterisk es un software de implementación de centrales telefónicas VoIP, también es capaz de inter-operar con todos los equipos telefónicos basados en estándares diferentes, usando terminales cuyos costos son bajos al compararlos con otras soluciones.

Asterisk provee los siguientes servicios:

- Voicemail con Directorio.
- Conferencias.
- Colas de llamadas.
- Menús interactivos (IVR)

Con Asterisk se puede acceder a la PSTN mediante un proveedor, utilizando una tarjeta analógica conectada al equipo, sin embargo para comunicarse mediante VoIP no se necesita hardware adicional. Para interconexión con equipos telefónicos tanto analógicos como digitales Asterisk acepta un buen número de dispositivos, soporta una amplia gama de Protocolos TDM para el manejo y transmisión de voz sobre interfaces telefónicas tradicionales y también permite señalización que es comúnmente usada en América y Europa, la cual usan los equipos telefónicos empresariales. Asterisk no sólo soporta equipos telefónicos tradicionales, también permite agregar a ellos capacidades adicionales de manera transparente.

Si bien toda implementación de un nuevo sistema supone una inversión inicial importante, el costo de instalar una central telefónica Asterisk es bastante reducido en

comparación con otras soluciones de telefonía. En primer lugar el software es gratis y está disponible para ser descargado por cualquier persona que lo desee. Por otro lado, el hardware requerido no tiene que cumplir con los últimos avances del mercado, una computadora sencilla puede servir para crear una red VoIP de pequeña o mediana envergadura. Por último Asterisk soporta la comunicación a través de softphones, los cuales también se encuentran disponibles on-line de manera gratuita en sus versiones más sencillas, a diferencia del costo que supondría instalar teléfonos para cada una de las extensiones que conforman el sistema telefónico. Es importante resaltar que el costo de implementación de Asterisk dependerá del tamaño de la red que se desee implementar.

2.3.15.1. Paquete Dahdi.

A pesar de que Asterisk es un gran producto de software, necesita de algunos complementos para realizar todo el trabajo, uno de los principales complementos es el paquete conocido como DAHDI por su siglas en inglés Digium/Asterisk Hardware Device Interface, básicamente DAHDI es un conjunto de drivers que sirve para controlar hardware telefónico como tarjetas PCI que permiten la conexión hacia la red PSTN.

Estos drivers se comunican con Asterisk a través de módulos los cuales se configuran en un archivo llamado `sytem.conf`, ubicado en el directorio `/etc/dahdi`, mientras que los canales DAHDI son configurados en un archivo llamado `chan_dahdi.conf` (Marín & Luis, 2013).

2.3.16. Elastix.

Elastix es un software de código abierto para el establecimiento 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 reportación para llamadas de Asterisk y fue liberado en marzo del 2006. Posteriormente el proyecto evolucionó hasta convertirse en una distribución basada en Asterisk.

Sin embargo Elastix no solamente provee telefonía, integra otros medios de comunicación para hacer más eficiente y productivo su entorno de trabajo.

Elastix es una distribución libre de Servidor de Comunicaciones Unificadas que integra en un solo paquete:

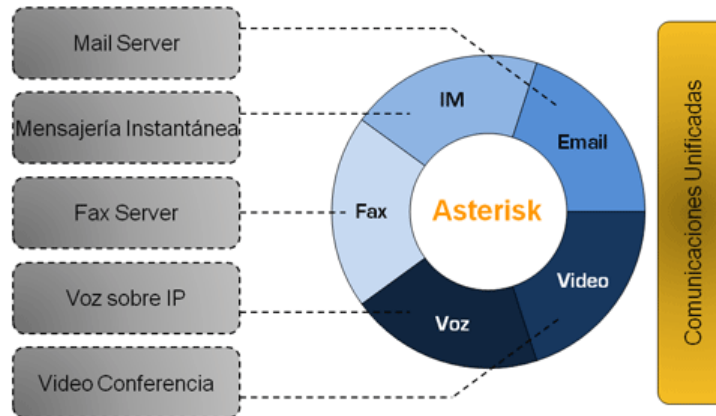
- VoIP PBX
- Fax
- Mensajería Instantánea
- Correo electrónico
- Colaboración

Elastix implementa gran parte de su funcionalidad sobre cuatro programas de software muy importantes como son Asterisk, Hylafax, Openfire y Postín. Estos brindan las funciones de PBX, Fax, Mensajería Instantánea y Correo electrónico respectivamente. Elastix corre sobre CentOS como sistema operativo y actualmente su versión más estable es Elastix 2.3.0

Elastix incluye en su solución los siguientes medios de comunicación:

Figura 23.

Características básicas de Elastix.



Fuente: VoIP y Asterisk: Redescubriendo la Telefonía

Algunas de las características básicas de Elastix incluyen:

- Correo de Voz
- Fax-a-email
- Soporte para softphones
- Interfase de configuración Web
- Sala de conferencias virtuales
- Grabación de llamadas
- Least Cost Routing
- Roaming de extensiones
- Interconexión entre PBXs
- Identificación del llamante
- CRM
- Reportación avanzada

2.4. DESCRIPCIÓN DE LA METODOLOGÍA.

La metodología utilizada para el desarrollo del proyecto es la Metodología de Diseño de Redes CISCO (TOP – DOWN NETWORK DESIGN). El diseño de red top-down es una disciplina que creció del éxito de la programación de software estructurado y el análisis de sistemas estructurados. El objetivo principal del análisis de sistemas estructurado es representar más exacto las necesidades de los usuarios, que a menudo son lamentablemente ignoradas. Otro objetivo es hacer el proyecto manejable dividiéndolo en módulos que pueden ser más fácil de mantener y cambiar.

El diseño de red top-down es una metodología para diseñar redes que comienza en las capas superiores del modelo de referencia de OSI antes de mover a las capas inferiores. Esto se concentra en aplicaciones, sesiones, y transporte de datos antes de la selección de routers, switches, y medios que funcionan en las capas inferiores. El proceso de diseño de red top-down incluye exploración divisional y estructuras de grupo para encontrar la gente para quien la red proporcionará servicios y de quien usted debería conseguir la información valiosa para hacer que el diseño tenga éxito.

La Metodología TOP – DOWN de CISCO consta de 6 fases, descritas a continuación:

2.4.1. Fase 1: Analizar Requerimientos.

En esta fase, de análisis se desarrolló mediante la observación y entrevista a los usuarios y al personal para conocer los objetivos técnicos del diseño de cableado de la red. La principal tarea es reconocer la tecnología existente en

ZOFRACOBIIJA, incluyendo la topología lógica y física y el rendimiento de la red. El último paso en esta fase es analizar el actual y futuro tráfico de la red, además se hace un análisis del tipo de señal, frecuencia y protocolo de transmisión de la red inalámbrica. En esta primera fase se deben completar los siguientes puntos:

- Analizar metas del negocio.
- Analizar metas técnicas.
- Analizar red existente.
- Analizar tráfico existente.

2.4.2. Fase 2: Desarrollar Diseño Lógico.

Se efectuó una evaluación de la red de ZOFRACOBIIJA en su diseño lógico, verificando el ya implementado para ver la factibilidad de soportar la implementación del proyecto. En esta fase se agrega la seguridad de datos, la configuración de la red, identificación de los proveedores de los servicios para reunir los accesos lúvidos y remotos. En esta segunda fase se deben completar los siguientes puntos:

- Diseñar topología de red
- Diseñar modelos de direccionamiento y hostnames
- Seleccionar protocolos para Switching y Routing
- Desarrollar estrategias de seguridad
- Desarrollar estrategias de administración de red

2.4.3. Fase 3: Desarrollar Diseño Físico.

Durante esta fase se identificara y seleccionara los recursos tecnológicos para la implementación de la red. Diseño del cableado estructurado usando normas y estándares. En esta tercera fase se deben completar los siguientes puntos:

- Seleccionar tecnologías y dispositivos para redes de campus
- Seleccionar tecnologías y dispositivos para redes empresariales

2.4.4. Fase 4: Probar, optimizar y documentar diseño.

En esta fase se debe realizar las pruebas pertinentes para verificar el correcto funcionamiento de la misma u observando deficiencias, pudiendo de esta manera Optimizar el diseño de red para obtener los resultados esperados. Al final se debe documentar todo el trabajo realizado en esta fase. Se deben cumplir los siguientes pasos:

- Probar el diseño de red
- Optimizar el diseño de red
- Documentar el diseño

2.4.5. Fase 5: Implementar y probar la red.

En esta fase se implementara el proyecto en base a toda la información recolectada y trabajo realizado en las fases anteriores, probando permanentemente la red ya con la puesta en marcha del proyecto. Se deben cumplir los siguientes puntos:

- Realizar cronograma de implementación
- Implementación del diseño de red (final)
- Realizar pila de pruebas

2.4.6. Fase 6: Monitorear y Optimizar la Red.

En esta fase se debe monitorear la red de datos con la implementación de proyecto y el óptimo rendimiento del servidor de telefonía. En caso que así lo requiera se debe realizar una optimización de cualquiera de los componentes del sistema de comunicación. Se deben tomar en cuenta los siguientes puntos:

- Operación de la red en producción
- Monitoreo de la red
- Optimización de la red

CAPITULO III

3. MARCO APLICATIVO.

3.1. FASE I: ANALIZAR REQUERIMIENTOS.

3.1.1. Analizar la Red Existente.

Actualmente ZOFRACOBIIJA cuenta con una red de datos interconectados entre ellas mediante la red de redes. La de mayor cantidad de equipos conectados se encuentra en la oficina central sobre la carretera Cobija – Porvenir y las otras con pocos equipos necesarios para las tareas a realizar según sus actividades.

En la oficina central de la institución se tiene una topología de red Híbrida y fibra óptica, cumple con todos los estándares y actualmente se encuentra certificada.

Con la información recolectada y verificada, puedo concluir que la red de datos de ZOFRACOBIIJA cumple todos los requerimientos para que se pueda implementar el presente proyecto.

3.1.2. Analizar el Tráfico Existente.

ZOFRACOBIIJA cuenta con cuatro redes LAN ubicadas en distintas partes del radio urbano de la ciudad de Cobija. Siendo la que cuenta con mayor cantidad de equipos y usuarios la oficina central ubicada en el km. 14 ½ carretera Cobija – Porvenir, asimismo alberga todos los servicios y aplicaciones dentro de la Red LAN y a la vez se proporciona la salida a internet de todos los usuarios.

Se pudo evidenciar que se comienza a generar el tráfico a partir de las 09:00, llegando a alcanzar sus picos mas alto entre las 11:00 a 12:00 y de 14:00 a 16:00, verificándose un menor uso de la red en el receso por el horario del almuerzo. De la misma manera se pudo

observar que existía un gran consumo de tráfico de diferentes direcciones IP's, que en algunos de los casos justificaba por el trabajo que realizaban los funcionarios y en una gran mayoría no, lo que fue tomado en cuenta por el administrador de la red.

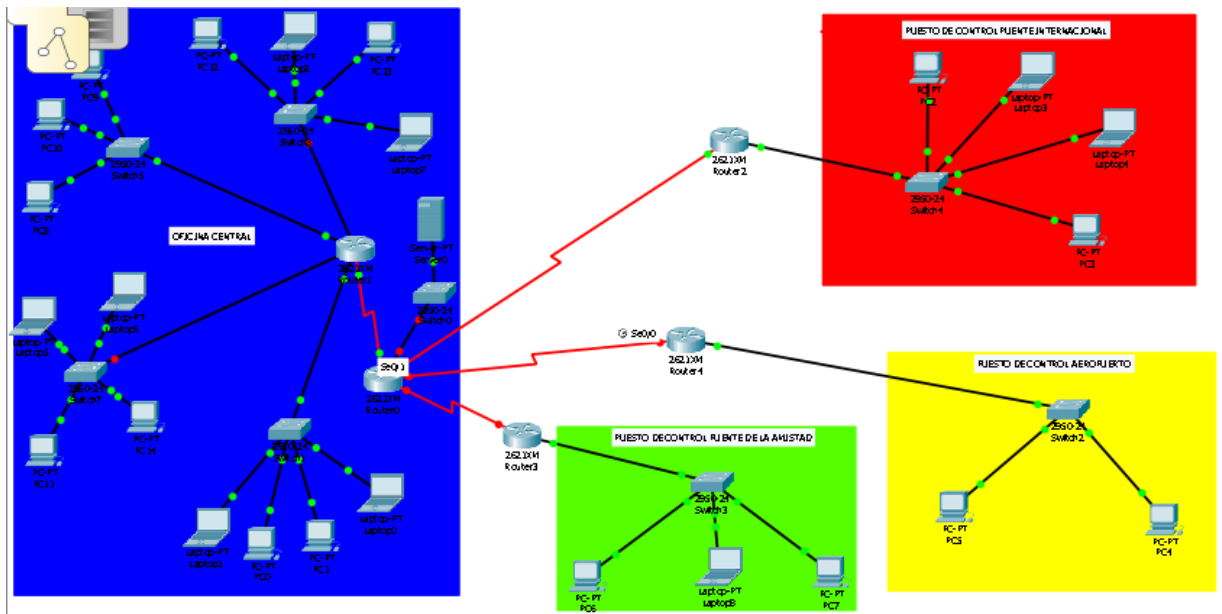
3.2. FASE 2: DESARROLLO DEL DISEÑO LÓGICO.

3.2.1. Diseñar Topología de Red.

Actualmente ZOFRACOBIA ya cuenta con una topología de red Híbrida certificada en la oficina central. Se crearon VLAN's para agrupar los diferentes puestos de trabajo de acuerdo a la función y de los servidores además de mejorar la eficiencia de la red en un menor consumo de ancho de banda de la LAN. Se reutilizara toda la tecnología con la que cuenta la institución para la implementación del presente proyecto. A continuación se muestra el diseño lógico de red de ZOFRACOBIA.

Figura 24.

Diseño Lógico de las redes de ZOFRACOBIIJA.



Fuente: Elaboración propia.

3.2.2. Diseñar Modelos de Direccionamiento y HostName.

En base al relevamiento de información realizado, en cumplimiento a la metodología y según los requerimientos de la población entrevistada se pudo tener una base de la cantidad de terminales telefónicas necesarias en las dependencias de cada una de las unidades funcionales de la institución. Según el siguiente detalle:

Tabla 9.

Tabla de direccionamiento.

| ITEM | NOMBRE DEL FUNCIONARIO | CARGO |
|------|------------------------|----------------------------|
| 1 | Rodolfo Añez Domínguez | Director General Ejecutivo |
| 2 | María R. Siviora | Secretaria Dirección |

| | | |
|----|--------------------|------------------------------------|
| 3 | Einar Hurtado | Asesoría Jurídica |
| 4 | María P. Heredia | Responsable Área de RR.HH. |
| 5 | Gabriel Farah | Jefe Unidad Adm. Financiera |
| 6 | Lila Fukumoto | Secretaria Unidad Adm. Financiera |
| 7 | David Gonzales | Jefe de Contabilidad y Presupuesto |
| 8 | Bella L. Mendoza | Secretaria Unidad de Planif. Est. |
| 9 | Jamilton Sosa | Jefe Unidad de Planificación Est. |
| 10 | José Garín Román | Responsable de Relaciones Públicas |
| 11 | Victor Rangel | Jefe Unidad de Transparencia |
| 12 | Osvaldo Alarcón | Jefe Unidad de Fiscalización |
| 13 | Sabina Quiñones | Fiscal de Pólizas |
| 14 | Robin E. Hassan F. | Responsable de BB.SS. |
| 15 | Siliane Vidal. R. | Encargada de Almacén |
| 16 | Maquelia Hurtado | Jefe Auditoría Interna |
| 17 | Raúl Aguada R. | Jefe Unidad de Operaciones |
| 18 | Jhoseline Soria | Responsable Archivo |
| 19 | Diego H. Menacho | Responsable Área Operaciones |
| 20 | Diether Beltran | Supervisor Tranca |
| 21 | Serguey Ojopi | Supervisor Amistad |
| 22 | Anibal Chupinagua | Supervisor Internacional |
| 23 | Marisol M. Vigo | Responsable. Aeropuerto |

Fuente: Elaboración propia.

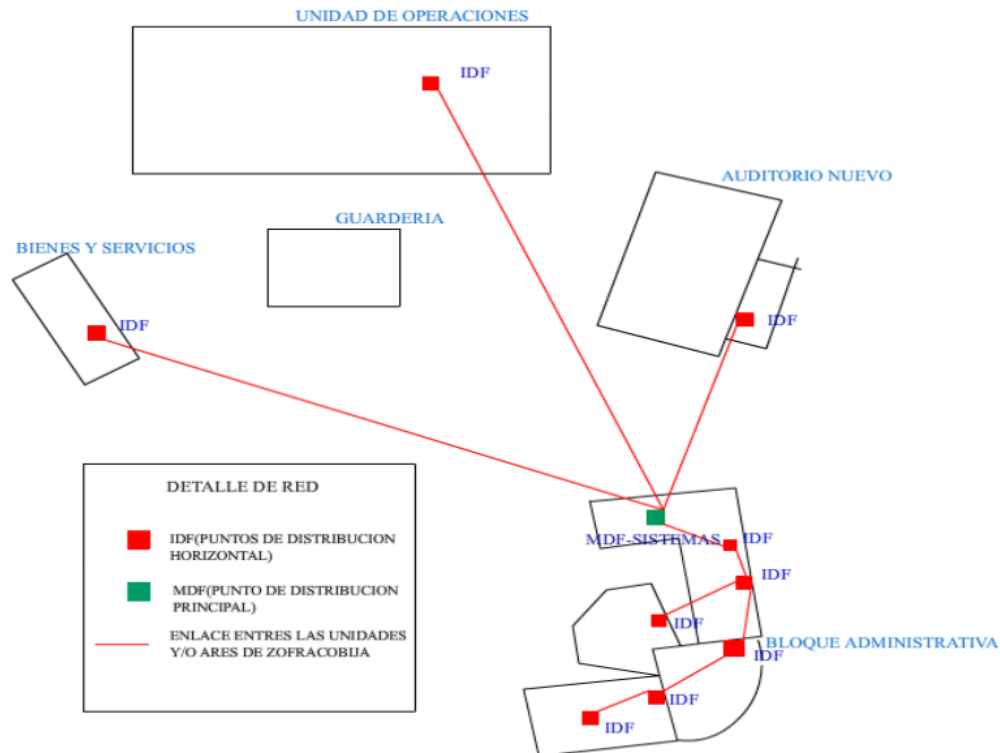
3.3. FASE 3: DESARROLLAR DISEÑO FÍSICO.

3.3.1. Seleccionar Tecnologías y Dispositivos para redes de campus.

La oficina central de ZOFRACOBIJA cuenta con una red horizontal de datos conectada mediante fibra optica, la misma será reutilizada para la implementación de nuestro proyecto. Como se puede observar en el gráfico el punto principal de distribución de la red se encuentra en el Área de Sistemas desde donde se amplía a los puntos de distribución horizontal para de esta manera llegar a cada uno de las terminales de los funcionarios.

Figura 25.

Diseño Físico de red oficina central.



Fuente: Área de Sistemas ZOFRACOBIA.

De acuerdo a los puntos de distribución que se tiene en la red de datos de la oficina central de la administración de ZOFRACOBIA, a continuación se detalla la cantidad de equipos que se encuentran conectados a la misma:

Tabla 10.

Detalle equipos de la Red ZOFRACOBIA km. 14 1/2.

| CANTIDAD | TIPO | DETALLE | OBSERVACIONES |
|----------|-----------|-----------|-------------------|
| 51 | Monitores | Completos | En funcionamiento |

| | | | |
|----|----------------------------|--------------------------|----------------------|
| 51 | CPU | Completos | En Funcionamiento |
| 51 | Estabilizadores de energía | Completos | Sin observación |
| 03 | Televisores 65" | Completos | Monitoreo de cámaras |
| 03 | Rack | Con todos sus accesorios | Sin observación |
| 01 | Servidor Dedicado | Completos en uso | En funcionamiento |
| 03 | Mikrotics | funcionamiento | Sin observación |
| 03 | Swicht | En uso | De 24 puertos |
| 02 | Firewall | En uso | Sin observación |
| 03 | Router | Inalámbrico | Sin observación |

Fuente: Elaboración propia.

3.3.1.1. Requerimiento de Hardware.

Adicionalmente a todos los equipos y tecnología con la que ya cuenta la institución en la oficina central, se tienen los siguientes requerimientos, para la implementación y puesta en marcha del proyecto:

Tabla 11.

Requerimiento de Hardware para el Servidor de Telefonía IP.

| CANTIDAD | ACCESORIO | DESCRIPCIÓN Y CAPACIDAD |
|-----------------|------------------|--------------------------------|
| 1 | Procesador Intel | Core (TM) i7-2630QM 3GHz |

| | | |
|---|---------------|-----------|
| 1 | Placa Madre | Intel |
| 1 | Memoria RAM | DDR2 6 GB |
| 1 | Disco Duro | 2 TB |
| 1 | Lector de DVD | BLUE RAY |

Fuente: Elaboración propia.

Tabla 12.

Requerimiento de equipos terminales móviles.

| CANTIDAD | ACCESORIO | DESCRIPCIÓN Y CAPACIDAD |
|-----------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7 | Celular Móvil | Android 8.0 ó superior - 3G HSDPA / HSUPA, Wi-Fi Direct - Bluetooth v4.0 A2DP, - microUSB 2.0 - Reproductor de vídeo, MP4/H.264/H.263 - Reproductor de audio MP3/eAAC+/AC3 |

Fuente: Elaboración propia.

Tabla 13.

Requerimiento de equipos terminales Teléfonos IP's.

| CANTIDAD | ACCESORIO | DESCRIPCIÓN Y CAPACIDAD |
|-----------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 19 | Teléfonos IP | GXP 1610 GrandStream Telefono IP 1 Línea SIP 2 puertos eth10/100mbps DC5v Display Matricial 3 Teclas Programables Conferencia de 3 vías Soporte Multi idioma Soporta Auricular |

Fuente: Elaboración propia.

3.3.2. Seleccionar Tecnologías y Dispositivos para Redes Empresariales.

Las oficinas de los diferentes puestos de control de ZOFRACOBIIJA se encuentran distantes físicamente, por tal motivo se encuentran comunicados en una red Vertical. Para interconectarlas la institución cuenta con IP's públicas utilizadas en las VPN's, aprovechando todas las potencialidades que tienen estas tecnologías haciendo énfasis en la seguridad de todos los datos que viajan sobre la red. De la misma manera se cuenta con las potencialidades de las VLAN's implementándose una en cada puesto de control para de esta manera poder agrupar cada una de las tecnologías y diferentes niveles de usuarios.

- ✓ **Red Puente Internacional.** Esta red cuenta con pocos equipos terminales los mismos que se encuentran conectados a internet, mencionados a continuación:

Tabla 14.

Detalle de equipos de la Red ZOFRACOBIIJA Puente Internacional.

| CANTIDAD | TIPO | DETALLE | OBSERVACIONES |
|-----------------|----------------------------|--------------------------|----------------------|
| 04 | Monitores | Completos | En funcionamiento |
| 04 | CPU | Completos | En Funcionamiento |
| 04 | Estabilizadores de energía | de Completos | Sin observación |
| 01 | Rack | Con todos sus accesorios | Sin observación |
| 01 | Mikrotics | En funcionamiento | |

| | | | |
|----|--------|-------------------|----------------------------------|
| 01 | Swicht | En uso | Sin observación De 24 puertos |
| 01 | Router | En funcionamiento | Sin observación |

Fuente: Elaboración propia.

- ✓ **Red Puente de la Amistad.** En esta red solamente se cuenta con dos equipos terminales, mencionados a continuación:

Tabla 15.

Detalle de equipos de la Red ZOFRACOBIIJA Puente de La Amistad.

| CANTIDAD | TIPO | DETALLE | OBSERVACIONES |
|-----------------|----------------------------|--------------------------|----------------------|
| 02 | Monitores | Completos | En funcionamiento |
| 02 | CPU | Completos | En Funcionamiento |
| 02 | Estabilizadores de energía | Completos | Sin observación |
| 01 | Rack | Con todos sus accesorios | Sin observación |
| 01 | Mikrotics | En funcionamiento | Sin observación |
| 01 | Swicht | En uso | De 24 puertos |
| 01 | Router | | Sin observación |

En
funcionamiento

Fuente: Elaboración propia.

- ✓ **Red Aeropuerto Internacional.** En esta red solamente se cuenta con dos equipos terminales, mencionados a continuación:

Tabla 16.

Detalle de equipos de la Red ZOFRACOBILJA Aeropuerto Internacional.

| CANTIDAD | TIPO | DETALLE | OBSERVACIONES |
|-----------------|----------------------------|--------------------------|----------------------|
| 02 | Monitores | Completos | En funcionamiento |
| 02 | CPU | Completos | En Funcionamiento |
| 02 | Estabilizadores de energía | Completos | Sin observación |
| 01 | Rack | Con todos sus accesorios | Sin observación |
| 01 | Mikrotics | En funcionamiento | Sin observación |
| 01 | Swicht | En uso | De 24 puertos |
| 01 | Router | En funcionamiento | Sin observación |

Fuente: Elaboración propia.

3.3.2.1. Requerimiento de Hardware.

Adicionalmente a todos los equipos y tecnología con la que ya cuenta la institución en los puestos de control, se tienen los siguientes requerimientos que serán distribuidos equitativamente en cada uno de ellos:

Tabla 17.

Requerimiento de equipos terminales CPU's.

| CANTIDAD | ACCESORIO | DESCRIPCIÓN Y CAPACIDAD |
|-----------------|------------------|--------------------------------|
| 3 | Procesador Intel | Core (TM) i5 2320 CPU 3GHz |
| 3 | Placa Madre | Intel, asrock, etc. |
| 3 | Memoria RAM | DDR2 1024 Mb. O superior |
| 1 | Disco duro | 60 Gb o superior |
| 1 | Lector de DVD | |
| 1 | Parlantes | 4.1 o superior |
| 1 | Micrófono | Normal o Tel. USB |

Fuente: Elaboración propia.

Tabla 18.

Requerimiento de equipos terminales móviles.

| CANTIDAD | ACCESORIO | DESCRIPCIÓN Y CAPACIDAD |
|-----------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3 | Celular Móvil | Android 8.0 ó superior · 3G HSDPA / HSUPA, Wi-Fi Direct - Bluetooth v4.0 A2DP, - microUSB 2.0 - Reproductor de vídeo, MP4/H.264/H.263 - Reproductor de audio MP3/eAAC+/AC3 |

Fuente: Elaboración propia.

Tabla 19.

Requerimiento de equipos terminales Teléfonos IP's.

| CANTIDAD | ACCESORIO | DESCRIPCIÓN Y CAPACIDAD |
|-----------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3 | Teléfonos IP | GXP 1610 GrandStream Telefono IP 1 Linea SIP 2 puertos eth10/100mbps DC5v Display Matricial 3 Teclas Programables Conferencia de 3 vias Soporte Multi idioma Soporta Auricular |

Fuente: Elaboración propia.

3.4. FASE 4: PROBAR, OPTIMIZAR Y DOCUMENTAR DISEÑO.

3.4.1. Probar el Diseño de Red.

Se realizaron las pruebas necesarias a la red que ya tiene implementada ZOFRACOBIJA básicamente haciendo énfasis en primera instancia en la oficina central, para luego proceder con los otros puestos de control.

Se realizó la verificación de la red en horarios picos de tráfico de datos, teniendo una muy buena respuesta ya que no existió perdidas de paquetes retardos en la llegada de los paquetes.

Se verifico la conectividad entre la oficina central y los puestos de control haciendo uso de las IP's públicas con las que cuenta la institución mediante la VPN, obteniendo resultados positivos.

3.4.2. Documentar el Diseño.

La red de datos de ZOFRACOBIJA actualmente con los estándares de cableado estructurado por tal motivo se encuentra certificada como corresponde. La misma cuenta con toda la documentación de la implementación de la red, así como también de la certificación de la misma.

3.5. FASE 5: IMPLEMENTAR Y PROBAR LA RED.

3.5.1. Implementación del Diseño de Red (Final).

La instalación del servidor se realizó sobre el sistema Operativo Ubuntu 18.04.5, descargado desde la página oficial www.ubuntu.com. De la misma manera se procedió con la descarga e instalación de Asterisk en su versión 1.6.1.1 y Elastix en su versión 5.0, de sus páginas oficiales www.asterisk.org y www.elastix.org respectivamente.

3.5.1.1. Instalación y Configuración del Servidor Elastix.

Al iniciar la instalación de nuestro servidor de telefonía IP, nos aparece la primera pantalla:

Figura 26.

Inicio de instalación de Elastix.



Fuente: Impresión de pantalla del proceso.

Pulsamos enter para continuar, insertando todos los datos necesarios para el funcionamiento adecuado de nuestro servidor. Una vez de haber ingresado todos los datos necesarios y seleccionado lo que corresponde se concluye con la instalación de Elastix, el equipo se reiniciara automáticamente para luego solicitar el usuario y la contraseña creadas anteriormente, una vez ingresada nos remite a una dirección IP para ingresar al panel de administración de la central telefónica, en nuestro caso 192.168.1.11:

Figura 27.

Ingreso al servidor de telefonía IP.

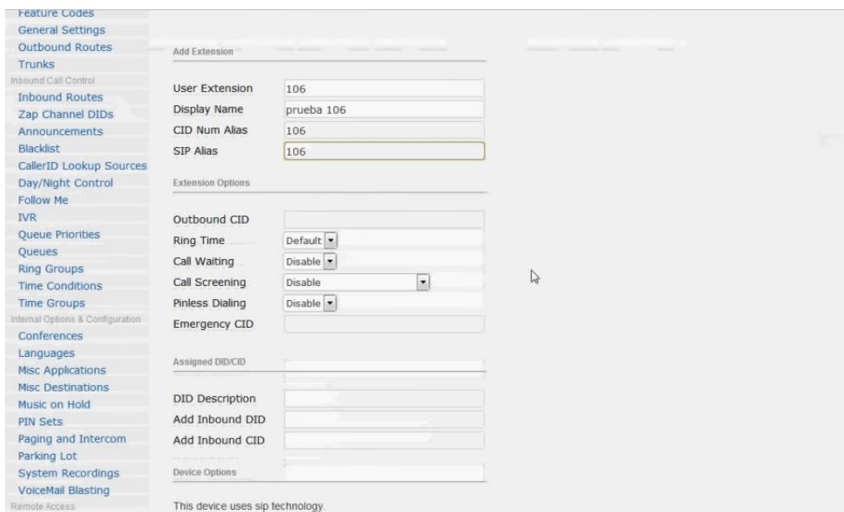


Fuente: Impresión de pantalla del proceso.

Luego de ingresar a nuestro servidor, procedemos a configurar las 25 extensiones para los equipos PC y Smartphone.

Figura 28.

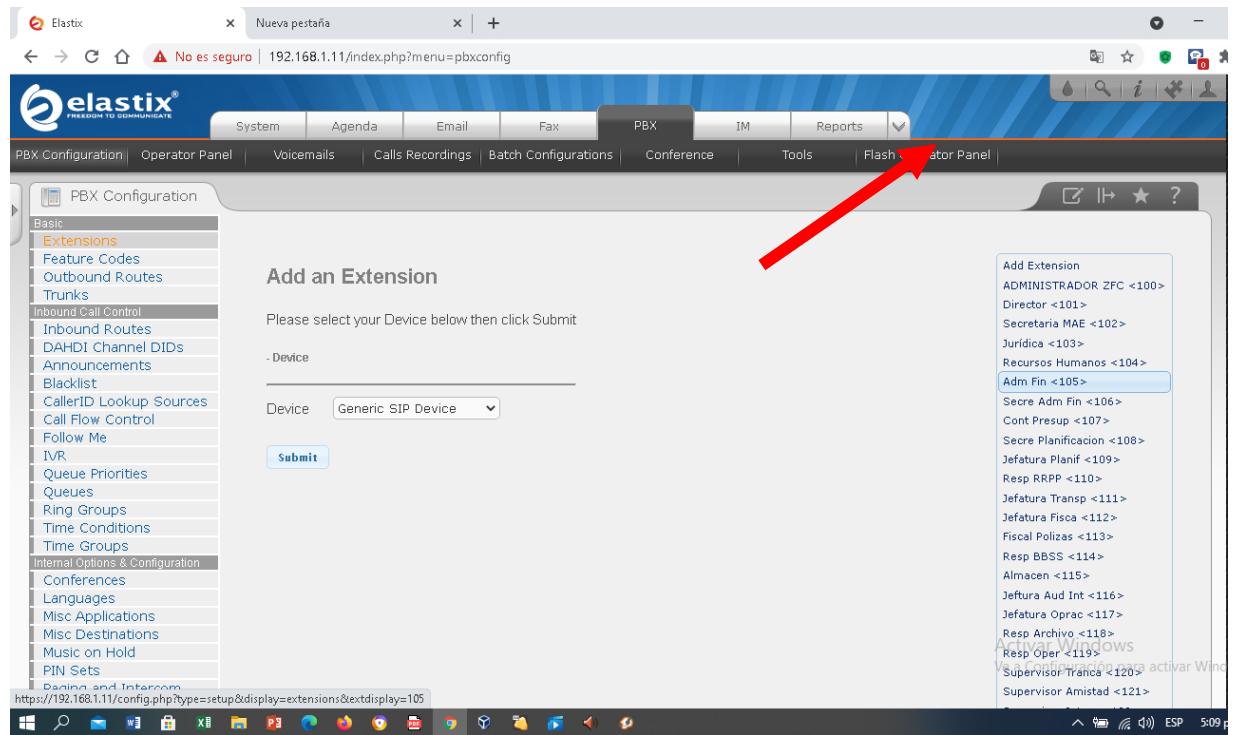
Creación de la extensiones SIP.



Fuente: Impresión de pantalla del proceso.

Todas las extensiones que creamos se irán visualizando conforme las guardemos, como se muestra en el grafico donde se creamos dos la 106 y la 107:

Gráfico 26. Configuración de extensiones SIP funcionarios.



Fuente: Impresión de pantalla del proceso.

A continuación se muestra cada una de las extensiones SIP que fueron configuradas en nuestro servidor Elastix:

Tabla 20.

Extensiones SIP configuradas.

| ITEM | NOMBRE DEL FUNCIONARIO | CARGO | DIRECCION IP | EXTENSION SIP |
|------|------------------------|----------------------------|----------------|---------------|
| 1 | Rodolfo Añez D. | Director General Ejecutivo | 192.168.16.14 | 101 |
| 2 | María R. Siviora | Secretaria Dirección | 192.168.15.238 | 102 |

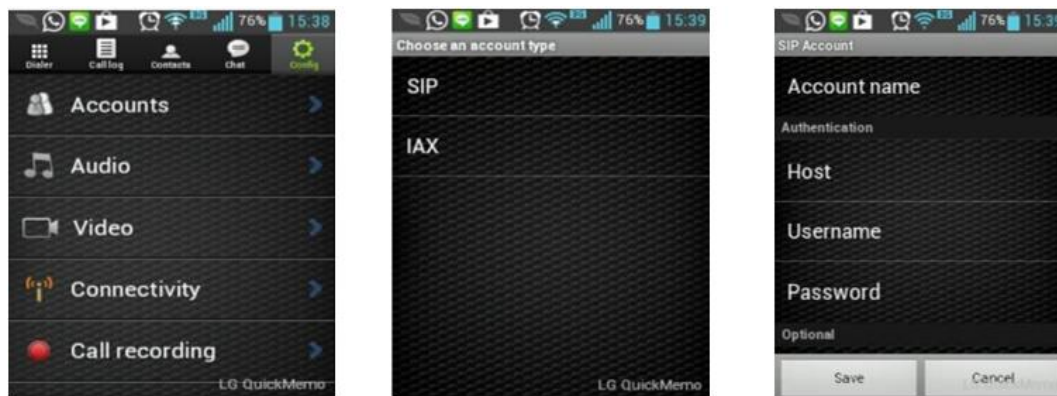
| | | | | |
|----|--------------------|-------------------------------|----------------|-----|
| 3 | Einar Hurtado | Asesoría Jurídica | 192.168.15.236 | 103 |
| 4 | María P. Heredia | Responsable Área de RR.HH. | 192.168.15.105 | 104 |
| 5 | Gabriel Farah | Jefe Unidad Adm. Financiera | 192.168.15.243 | 105 |
| 6 | Lila Fukumoto | Secretaria U. Adm. Financ. | 192.168.15.119 | 106 |
| 7 | David Gonzales | Jefe de Contab. y Presup. | 192.168.15.228 | 107 |
| 8 | Bella L. Mendoza | Secretaria U. de Planif. Est. | 192.168.15.163 | 108 |
| 9 | Hamilton Sosa | Jefe Unidad de Planif. Est. | 192.168.15.220 | 109 |
| 10 | José Garín Román | Responsable de RR.PP. | 192.168.15.248 | 110 |
| 11 | Victor Rangel | Jefe Unidad de Transparencia | 192.168.15.229 | 111 |
| 12 | Osvaldo Alarcón | Jefe Unidad de Fiscalización | 192.168.15.244 | 112 |
| 13 | Sabina Quiñones | Fiscal de Pólizas | 192.168.15.22 | 113 |
| 14 | Robin E. Hassan F. | Responsable de BB.SS. | 192.168.15.187 | 114 |
| 15 | Siliane Vidal. R. | Encargada de Almacén | 192.168.15.170 | 115 |
| 16 | Maquelia Hurtado | Jefe Auditoría Interna | 192.168.15.202 | 116 |
| 17 | Raúl Aguada R. | Jefe Unidad de Operaciones | 192.168.15.227 | 117 |
| 18 | Jhoseline Soria | Responsable Archivo | 192.168.1.1 | 118 |
| 19 | Diego H. Menacho | Responsable Área Operac. | | 119 |
| 20 | Diether Beltran | Supervisor Tranca | | 120 |
| 21 | Serguey Ojopi | Supervisor Amistad | | 121 |
| 22 | Anibal Chupinagua | Supervisor Internacional | | 122 |
| 23 | Marisol M. Vigo | Responsable. Aeropuerto | | 123 |

Luego de configurar todas las extensiones de mi servidor Elastix, se procedió con la instalación y configuración de las terminales para que se tenga conectividad entre los usuarios para ello se utilizó el Softphone **ZOIPER** por ser muy útil, de fácil instalación, configuración y requerimientos técnicos mínimos de los equipos.

Ejecutamos ZOIPER, seleccionamos Config – Accounts, elegimos la opción SIP llenando los datos de cada una de las extensiones creadas en nuestro servidor, luego llenamos los datos que nos solicita y procedemos a guardar los datos llenados.

Figura 29.

Configuración de las terminales clientes con ZOIPER.



Fuente: Impresión de pantalla del proceso.

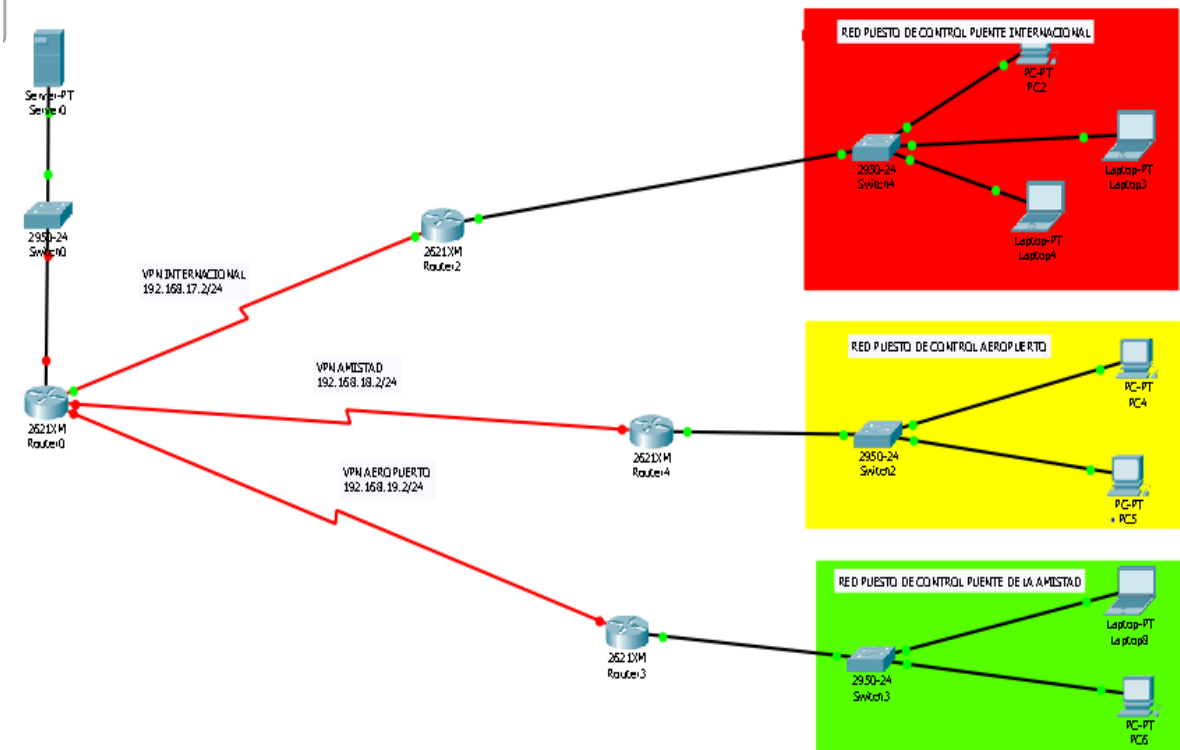
3.5.1.2. Configuración de las VPN.

Se configuro las redes privadas virtuales para cada puesto de control: Puente Internacional, Puente de La Amistad y Aeropuerto. Según el siguiente detalle:

- VPN Puente Internacional para la red 192.168.17.0
- VPN Puente de La Amistad 192.168.18.0
- VPN Aeropuerto 192.168.19.0

Figura 30.

Configuración de las VPN's y las VLAN's.



Fuente: Elaboración propia.

3.5.2. Realizar Pila de Pruebas.

- Para comprobar el correcto funcionamiento de la red, se realizó pruebas a cada punto verificando la conexión a internet. A continuación se muestra prueba realizada de una llamada de la extensión 107 (Jefe de Contabilidad) a la extensión 106 (Secretaria del Administrativo Financiero).

Figura 31.

Llamada de la extensión 106 a la 107.



Fuente: Impresión de pantalla del proceso.

- Para verificar la calidad de los servicios de la telefonía IP, tales como: voz, datos, fax y otros; se procedió a realizar conectividad entre los funcionarios con todos los servicios, teniendo resultados muy favorables.
- A todo el personal de ZOFRACOBIA se le hizo entrega de la lista de extensiones correspondientes a cada una de las dependencias donde se instalaron las terminales.

3.6. FASE 6. MONITOREAR Y OPTIMIZAR LA RED.

3.6.1. Monitoreo de la Red.

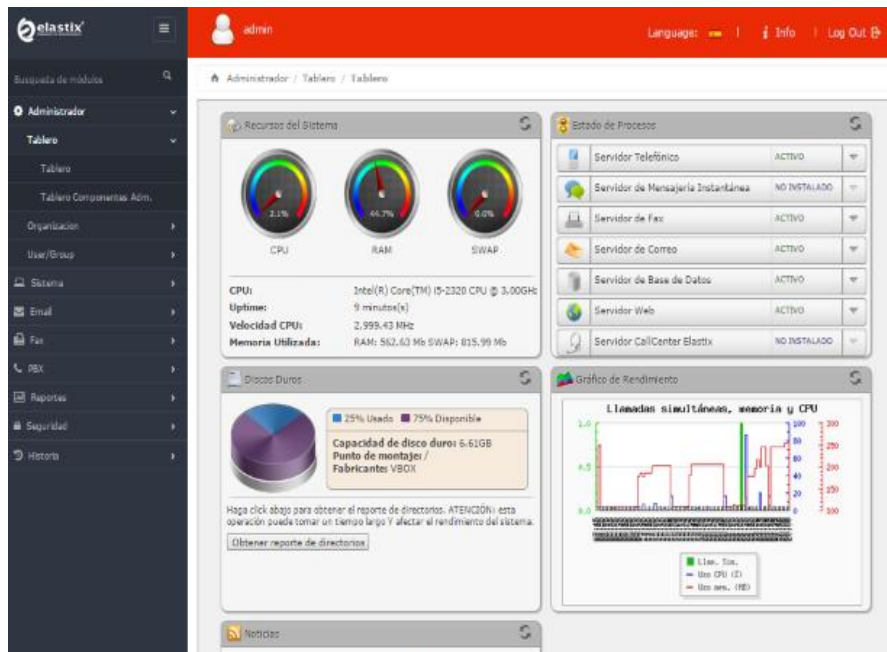
Se realizó el monitoreo de la red para garantizar el óptimo funcionamiento de la misma, aprovechando las potencialidades con las que cuenta nuestro servidor de telefonía IP.

3.6.1.1. Monitoreo y Seguimiento de los Servicios.

Se realizó el monitoreo de los recursos y servicios que se están ejecutando en el servidor Elastix, mediante su panel de monitor como se muestra a continuación:

Figura 32.

Monitoreo de los recursos y quipos.



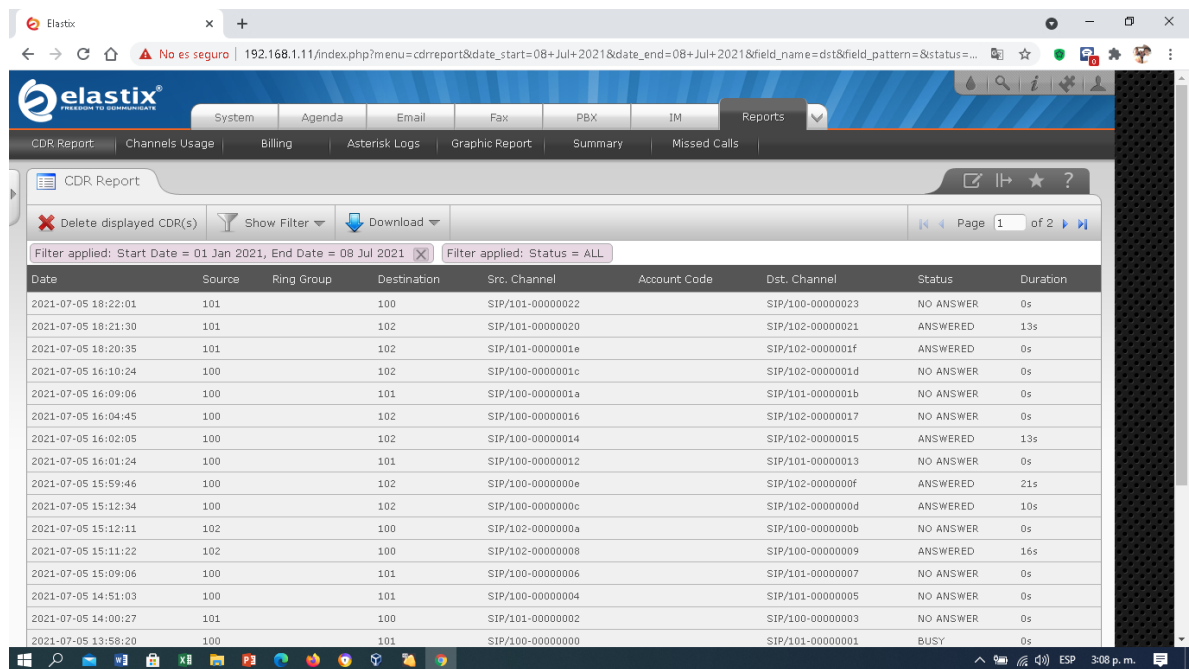
Fuente: Impresión de pantalla del proceso.

3.6.1.2. Monitoreo del Tráfico de Voz y Datos.

Para realizar el monitoreo de la voz y los datos que viajan sobre la red, Elastix cuenta con un módulo de reportes donde se puede verificar todos los datos de las llamadas efectuadas y recibidas proporcionando información que se requiera.

Figura 33.

Monitoreo de los servicios del servidor.



The screenshot displays the Elastix web interface for generating a Call Detail Record (CDR) report. The browser address bar shows the URL: 192.168.1.11/index.php?menu=cdrreport&date_start=08+Jul+2021&date_end=08+Jul+2021&field_name=dst&field_pattern=&status=... The interface includes a navigation menu with options like System, Agenda, Email, Fax, PBX, IM, and Reports. The CDR Report section is active, showing a table of call records with columns for Date, Source, Ring Group, Destination, Src. Channel, Account Code, Det. Channel, Status, and Duration. The table contains 20 rows of data, including call times, source and destination numbers, channel identifiers, and call status (e.g., NO ANSWER, ANSWERED, BUSY).

| Date | Source | Ring Group | Destination | Src. Channel | Account Code | Det. Channel | Status | Duration |
|---------------------|--------|------------|-------------|-----------------|--------------|-----------------|-----------|----------|
| 2021-07-05 18:22:01 | 101 | | 100 | SIP/101-0000022 | | SIP/100-0000023 | NO ANSWER | 0s |
| 2021-07-05 18:21:30 | 101 | | 102 | SIP/101-0000020 | | SIP/102-0000021 | ANSWERED | 13s |
| 2021-07-05 18:20:35 | 101 | | 102 | SIP/101-000001e | | SIP/102-000001f | ANSWERED | 0s |
| 2021-07-05 16:10:24 | 100 | | 102 | SIP/100-000001c | | SIP/102-000001d | NO ANSWER | 0s |
| 2021-07-05 16:09:06 | 100 | | 101 | SIP/100-000001a | | SIP/101-000001b | NO ANSWER | 0s |
| 2021-07-05 16:04:45 | 100 | | 102 | SIP/100-0000016 | | SIP/102-0000017 | NO ANSWER | 0s |
| 2021-07-05 16:02:05 | 100 | | 102 | SIP/100-0000014 | | SIP/102-0000015 | ANSWERED | 13s |
| 2021-07-05 16:01:24 | 100 | | 101 | SIP/100-0000012 | | SIP/101-0000013 | NO ANSWER | 0s |
| 2021-07-05 15:59:46 | 100 | | 102 | SIP/100-000000e | | SIP/102-000000f | ANSWERED | 21s |
| 2021-07-05 15:12:34 | 100 | | 102 | SIP/100-000000c | | SIP/102-000000d | ANSWERED | 10s |
| 2021-07-05 15:12:11 | 102 | | 100 | SIP/102-000000a | | SIP/100-000000b | NO ANSWER | 0s |
| 2021-07-05 15:11:22 | 102 | | 100 | SIP/102-0000008 | | SIP/100-0000009 | ANSWERED | 16s |
| 2021-07-05 15:09:06 | 100 | | 101 | SIP/100-0000006 | | SIP/101-0000007 | NO ANSWER | 0s |
| 2021-07-05 14:51:03 | 100 | | 101 | SIP/100-0000004 | | SIP/101-0000005 | NO ANSWER | 0s |
| 2021-07-05 14:00:27 | 101 | | 100 | SIP/101-0000002 | | SIP/100-0000003 | NO ANSWER | 0s |
| 2021-07-05 13:58:20 | 100 | | 101 | SIP/100-0000000 | | SIP/101-0000001 | BUSY | 0s |

Fuente: Impresión de pantalla del proceso.

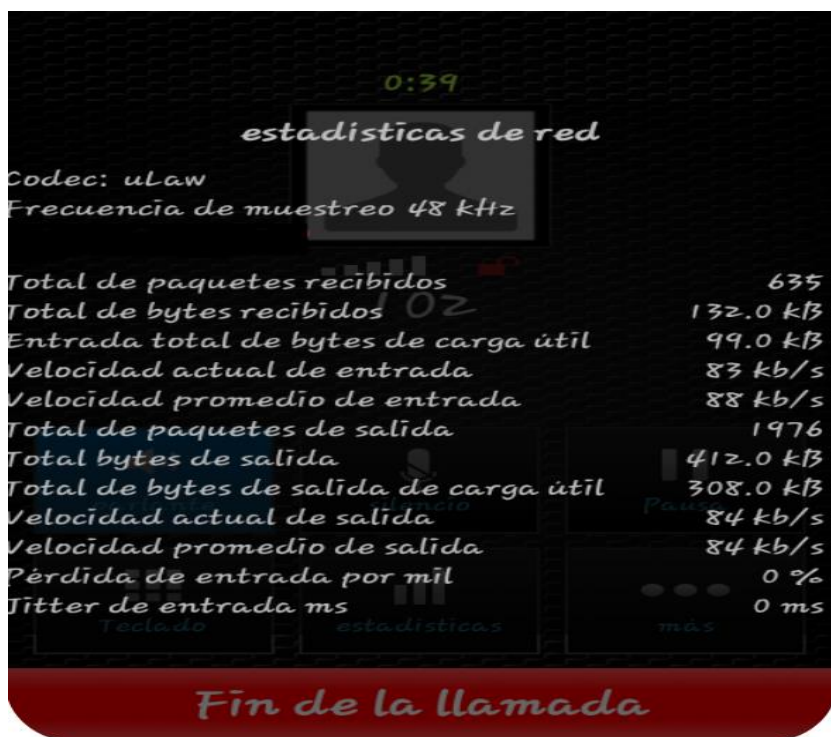
3.6.1.3. Calidad de Llamadas.

Para medir la calidad de llamadas generadas en el sistema se empleó el códec denominado ulaw, con una frecuencia de muestreo de 48 Khz, que muestra las estadísticas de la terminal al realizar cada una de las llamadas. Este códec, conocido también como G.711 ofrece un flujo de datos de 64 kbit's, lo que resulta alto con relación a otros códec's. Estos 64 kbit's son comparados con el ancho de banda que se utilizaban en el pasado para

conectarse a Internet. A continuación se muestra el cuadro generado por las llamadas realizadas durante el monitoreo de las mismas:

Figura 34.

Monitoreo de llamada realizada.



Fuente: Impresión de pantalla del proceso.

Como se puede verificar en la figura anterior toda la información reflejada nos muestra que tenemos una muy buena calidad de en las llamadas, tomando en cuenta que no se tienen pérdidas de paquetes ni retraso en los mismos.

CAPITULO IV

4.CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES.

- Con la realización del presente proyecto, se pudo observar la importancia que tiene hoy en día las tecnologías de Telefonía IP, no solo en el campo de las telecomunicaciones sino también en el área de las instituciones públicas y privadas donde cada vez más se incrementa el número de estas que quieren modificaciones o cambios en sus sistemas de telefonía para poder transmitir la voz a través del protocolo IP. Esto se debe a la fácil adquisición de distribuciones libres como Elastix, las cuales ofrecen una amplia gama de beneficios.
- La implementación de Telefonía IP en ZOFRACOBIA beneficiara a todos los funcionarios y usuarios de la institución, ya que el módulo de Elastix dispone de ciertas aplicaciones con una interfaz gráfica amistosa para el usuario.
- Se cumplieron satisfactoriamente, todos y cada uno de los objetivos planteados en los capítulos anteriores, ya que se tiene una comunicación eficaz entre los usuarios finales lo que se refleja en mayor competitividad y motivándolos a ejecutar sus compromisos y tareas institucionales, creando un excelente clima de trabajo.
- Para la culminación del presente proyecto fue muy importante el apoyo que dio cada uno de los funcionarios de la institución para la conclusión de cada una de las etapas de la metodología.
- El mayor problema que se tuvo en el transcurso de la elaboración del presente proyecto se dio por la falta de presupuesto de la institución para la adquisición de los teléfonos IP. Lo que fue subsanado con la instalación de softphones para realizar la conectividad entre los equipos.

- Los datos obtenidos en el relevamiento de información fueron concluyentes para saber con que tipo de tecnologías contaba la institución en su red y poder proyectar la solución a los posibles problemas que se tendrían en la implementación del proyecto. Se reutilizó la mayor parte de la infraestructura con la que ya contaba la administración de ZOFRACOBIIA.
- La telefonía IP constituye un gran paso para la administración de ZOFRACOBIIA en términos de innovación tecnológica, teniendo en cuenta las potenciales ventajas de esta tecnología.
- El comportamiento de cada uno de los funcionarios y usuarios del proyecto, pueden ser monitoreados de forma fácil y oportuna.
- Las pruebas realizadas desde y hacia la oficina central de ZOFRACOBIIA con los puestos de control Puente Internacional, Puente de La Amistad y Aeropuerto, fueron exitosas tanto en la transmisión de voz y de datos.

4.2. RECOMENDACIONES.

- Dar mantenimiento preventivo y correctivo de todo el equipamiento que comprende la red de la institución de manera permanente (servidores, computadoras, instalaciones de red, instalaciones eléctricas, etc.).
- Realizar auditorías internas periódicamente para poder ver posibles falencias del servidor IP.

- Actualizar el software de nuestro servidor y de los softphones, lo que mejorara la calidad del servicio, tomando en cuenta las mejoras constantes de estos softwares.
- Tomar en cuenta el consumo de la memoria RAM del servidor. Ya que esta es una limitante cuando se tiene varias llamadas simultaneas.
- En caso del incremento de la infraestructura y del número de extensiones, será necesario la habilitación de otro servidor. De acuerdo a las necesidades que el caso amerite.
- Si se piensa adicionar más elementos al sistema, es preciso se realice las pruebas respectivas de tráfico de datos, así comprobar que el sistema cuenta con el adecuado ancho de banda. Estas pruebas evitarán que haya pérdidas de datos o en el peor de los casos ocasione una congestión y como resultado el sistema quede inhabilitado.
- El proyecto contempla la conexión de voz y video IP solo mediante Internet, este puede modificarse y expandirse para utilizarse con telefonía tradicional PSTN mediante hardware telefónico.

Referencias Bibliográficas

Idobro José Manuel, M. R. (2011). *Redes de Datos y Convergencia IP*. Méjico: AlfaOmega.

Monzon, A. G. (2012). *Redes Privadas Virtuales*. Madrid.

Pepelnjack, I., & Guichard, J. (2003). *Arquitectura MPLS y VPN*. España: Pearson Education.

Saavedra, J. C. (2015). *Diseño de Red con Top - Down*. Cochabamba.

Tanenbaum, A. S. (2003). *Redes de Computadoras - Cuarta Edicion*. Mexico: Prentice Hall.

Viscaíno, J. M. (14 de 09 del 2006). Implementacion de Servicios VoIP sobre Asterisk. Tesis de Grado. Catalunha. España.

Wikipedia. (Febrero 2020).pt.wikipedia.org/.



UNIVERSIDAD AMAZÓNICA DE PANDO

25 años Abriendo Caminos de Superación

Cobija, 29 de junio del 2021

Señor:

Msc. Lic. Humberto Fernandez Calle

DOCENTE DE LA ASIGNATURA

TALLER DE MODALIDAD DE GRADUACIÓN II

Presente:

REF: CONFORMIDAD Y AVAL PARA LA PRESENTACIÓN DEL PROYECTO DE GRADO NIVEL LICENCIATURA DEL POSTULANTE UNIV: RAUL AGUADA ROMERO.

De mi mayor Consideración:

En calidad de Asesor y realizando el seguimiento continuo del desarrollo del Proyecto de Grado del postulante Univ. Raúl Aguada Romero, que ha concluido con el desarrollo del proyecto: "TELEFONIA IP UTILIZANDO UNA RED PRIVADA VIRTUAL PARA LA ZONA FRANCA COMERCIAL E INDUSTRIAL DE COBLIA", y habiéndose cumplido con todos los requerimientos exigidos, es que mediante la presente expreso ante usted, que el sistema desarrollado e implementado en el Proyecto de Grado presentado, a merita el aval para que el postulante efectúe la presentación y defensa de su trabajo de licenciatura a objeto de optar al título de **Ingeniero en Sistemas Informáticos**.

Es cuanto informo para los fines consiguientes.

Atentamente.


Ing. José Balderama Méndez
DOCENTE DE INGENIERIA DE SISTEMAS
ASESOR

C.c.: Arch



CITE/ZFC/DGE/Nº0213/-2020

Señor:

Ing. Samuel Fuentes Chambi,
**COORDINADOR DE LA CARRERA DE
INGENIERÍA DE SISTEMAS**

Presente.-

REF.: Conformidad a culminación de Proyecto de Grado,

De mi mayor consideración:

Mediante la presente me dirijo a usted con motivo de hacerle llegar conformidad de la conclusión del Proyecto de Grado **"TELEFONIA IP UTILIZANDO UNA RED PRIVADA VIRTUAL PARA LA ZONA FRANCA COMERCIAL E INDUSTRIAL DE COBIZA"**, desarrollado en nuestra institución por el Sr. Raúl Aguada Romero. Previo visto bueno del Responsable del Área de Sistema de la institución.

Sin otro particular me despido muy atentamente.

Rodolfo Añez Domínguez
**DIRETOR GENERAL EJECUTIVO
ZOFRACOBIA**

