UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Estudio y diseño de un sistema de comunicaciones unificadas VoIP basado en Elastix con seguridad perimetral

AUTOR:

Ing. Pablo Enrique Espinoza De La Cuadra

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL GRADO ACADÉMICO DE MAGÍSTER EN TELECOMUNICACIONES

TUTOR:

M. SC. NÉSTOR ARMANDO ZAMORA CEDEÑO

Guayaquil, 29 de octubre de 2021

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

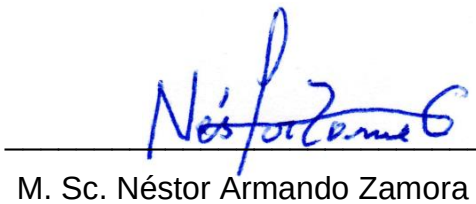
MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación Estudio y diseño de un sistema de comunicaciones unificadas VoIP basado en Elastix con seguridad perimetral, fue realizado en su totalidad por Pablo Enrique Espinoza De La Cuadra como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones.

Guayaquil, 29 de octubre de 2021

TUTOR



M. Sc. Néstor Armando Zamora Cedeño.

DIRECTOR DEL PROGRAMA

M. Sc. Manuel de Jesús Romero Paz

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

YO, Pablo Enrique Espinoza De La Cuadra

DECLARO QUE:

El trabajo de titulación “Estudio y diseño de un sistema de comunicaciones unificadas VoIP basado en Elastix con seguridad perimetral”, previo a la obtención del grado Académico de Magíster, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación del Grado Académico en mención.

Guayaquil, 29 de octubre de 2021

EL AUTOR

Ing. Pablo Espinoza De La Cuadra

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

YO, Pablo Enrique Espinoza De La Cuadra

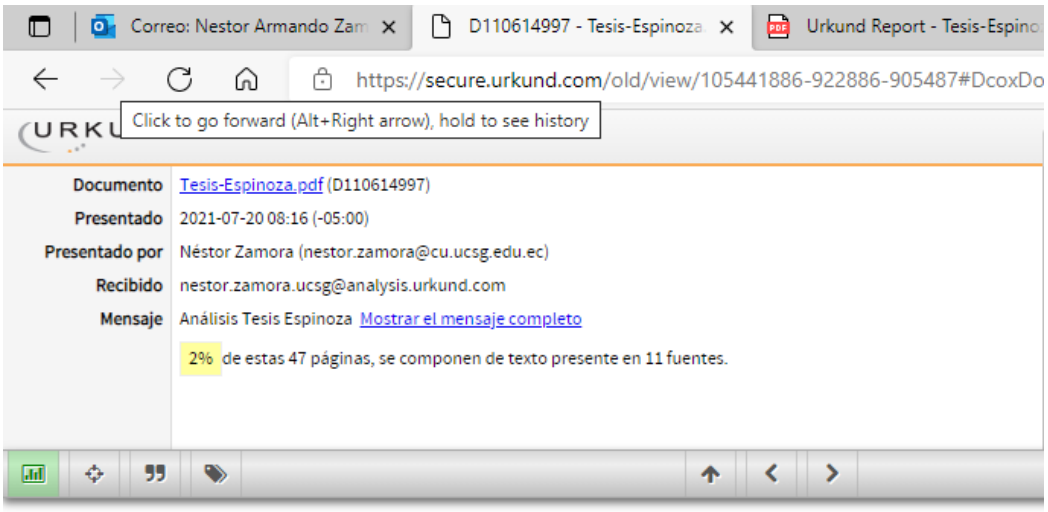
Autorizo, a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución del Trabajo de Titulación de Maestría titulado: “Sistema de comunicaciones basado en Elastix con seguridad perimetral”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, 29 de octubre de 2021

EL AUTOR

Ing. Pablo Espinoza De La Cuadra

REPORTE DE URKUND



SISTEMA DE POSGRADO MAESTRÍA EN TELECOMUNICACIONES TÍTULO DE LA TESIS: Estudio y diseño de un sistema de comunicaciones unificadas VoIP basado en Elastix con seguridad perimetral. Previa la obtención del Grado Académico de Magíster en Telecomunicaciones ELABORADO POR: Ing. Pablo Espinoza De La Cuadra Guayaquil, 2021

II SISTEMA DE POSGRADO CERTIFICACIÓN Certificamos que el presente trabajo fue realizado en su totalidad por el Magíster Pablo Enrique Espinoza De La Cuadra como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones. Guayaquil,

a los 18 días del mes Julio año 2021 DIRECTOR DE TESIS _____ M. Sc. Néstor Armando Zamora Cedeño. REVISORES: _____ M. Sc. Edwin Fernando Palacios Meléndez _____ M. Sc. Luis Silvio Córdova Rivadeneira

DIRECTOR DEL PROGRAMA _____ M. Sc. Manuel de Jesús Romero Paz

III SISTEMA DE POSGRADO DECLARACIÓN DE RESPONSABILIDAD YO, Pablo Enrique Espinoza De La Cuadra DECLARO QUE: La tesis "Sistema de comunicaciones basado en Elastix con seguridad perimetral", previa a la obtención del grado Académico de Magíster,

ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que

Dedicatoria

Dedico este trabajo a Dios que me guía siempre aun en contra de mis necios desvaríos; a mi amada esposa Xiomara Arcentales y mis hijos Alejandro y Santiago, quienes son mi razón de ser y mi vida; a mis padres, que siguen siendo desde el cielo la luz que me ilumina siempre; a mis hermanos, porque de ellos es también cada uno de mis logros; a mis suegros y mis cuñados, quienes han sido para mí una nueva familia.

Agradecimientos

Agradezco a Dios por la infinita bondad con que ha de tolerar mis faltas y la fortaleza que me da para seguir después de cada tropiezo; a mi amada esposa Xiomara Arcentales, por la energía que me transmite, la paciencia, el amor y la fe incondicional que tiene en mí; a mis hijos Alejandro y Santiago, por ser el motor que me hace seguir, a mis padres, por haber sido durante toda mi vida el amor incondicional en la tierra y desde el cielo me alumbran y cuidan; a mis hermanos, porque ellos siempre se preocupan por mí y me animan a seguir; a mis suegros, porque han sido un poco mis padres que están en la tierra.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

ING. NÉSTOR ARMANDO ZAMORA CEDEÑO, MSc.

TUTOR

f. _____

ING. CORDOVA RIVADENEIRA LUIS. MSc.

REVISOR

f. _____

ING. QUEZADA CALLE EDGAR. MSc.

REVISOR

f. _____

ING. ROMERO PAZ MANUEL DE JESÚS, MSc

DIRECTOR DEL PROGRAMA

ÍNDICE GENERAL

Índice de Figuras

Capítulo 2:

Capítulo 3:

Capítulo 4:

Índice de Tablas

Capítulo 2:

Capítulo 3:

Resumen

En este proyecto se realizará un análisis de las amenazas que afronta una red VoIP basada en Elastix y cómo se puede dar protección y fiabilidad al funcionamiento de la misma; se describirá la configuración de una red VoIP con diferentes conexiones de hosts telefónicos y equipos de computación; se describirá la instalación de una central telefónica IP Elastix y su funcionamiento en la red VoIP; se establecerá una protección perimetral de la red por medio de un firewall. Ya en el entorno de funcionamiento de la red, se analizará diferentes formas de ataques a la central telefónica Elastix; se analizará y describirá la configuración de políticas de protección en el firewall de tal forma que se brinde protección contra las direcciones externas para cercar el perímetro externo de la red; de otro lado, se podrá definir la protección de la central para ataques desde la red interna, es decir protección en el perímetro interno.

Palabras clave: Telefonía, VoIP, Elastix, Seguridad, Amenazas.

Abstract

In this project, an analysis of the threats faced by a VoIP network based on Elastix will be carried out and how it can provide protection and reliability to its operation; The configuration of a VoIP network with different connections of telephone hosts and computer equipment will be described; The installation of an Elastix IP telephone exchange and its operation in the VoIP network will be described; perimeter protection of the network will be established by means of a firewall. In the network operating environment, different forms of attacks on the Elastix telephone exchange will be analyzed; The configuration of protection policies in the firewall will be analyzed and described in such a way as to provide protection against external addresses to surround the external perimeter of the network; on the other hand, it is possible to define the protection of the control panel for attacks from the internal network, that is to say protection in the internal perimeter.

Keywords: Telephony, VoIP, Elastix, Security, Threats.

Capítulo 1: Descripción del proyecto de intervención.

1.1. Introducción.

El crecimiento constante de los sistemas de comunicación convergentes ha tenido varios efectos positivos en los negocios empresariales y las instituciones de servicios privados y públicos, entre los más importantes están los económicos ya que la unificación de servicios en una sola red ha permitido abaratar los costos. Hasta hace unos pocos años había una existencia paralela de las redes de datos y las de telefonía, ambas desarrollándose de forma separada debido a las tecnologías incompatibles que utilizaban. En la actualidad esa incompatibilidad tecnológica ya no es tal; con el desarrollo de la tecnología VoIP (Voz sobre IP), se han logrado desarrollar sistemas completamente convergentes de redes de datos y de telefonía.

Por otro lado, la velocidad con que se incrementa el acceso a la red de Internet debido al aumento de la capacidad de transmisión de datos es el resultado del desarrollo de tecnologías que pasaron de los Mbps a los Gbps tanto a nivel de equipos de comunicación como de servidores Aplicaciones y base de datos. Actualmente la infraestructura de red ha migrado de HFC a GPON lo cual permite la integración de todos los servicios básicos de comunicación por una sola red de FO: TV, Telefonía e Internet. La inminente desaparición de la TV y la telefonía como servicios individuales solo dejará al Internet como servicio principal puesto que la TV y la telefonía ya pueden ser ofertados dentro de esta red.

Sin embargo, uno de los aspectos que surgen como resultado de la unificación de las redes de datos y de telefonía, es el de la seguridad. Tal como lo dice Juan Oliva en su publicación Seguridad en implementaciones de Voz sobre IP, “esta tecnología digital está expuesta a vulnerabilidades propias de los entornos de red. En la actualidad hay poca exposición y documentación sobre problemas de seguridad existentes y emergentes”(Oliva & Estrella, 2014).

La convergencia de las diferentes redes de comunicaciones en una sola red unificada que brinde todos los servicios de voz y datos, ha generado múltiples beneficios, la flexibilidad y escalabilidad de las redes de comunicaciones actuales traducen estos beneficios en ahorro en el ámbito económico.

1.2. Antecedentes.

En el año 1995 se dio inicio al sistema que permite transmitir la voz utilizando el protocolo VoIP (Voz sobre IP), fue la empresa VocalTec la primera en realizar este sistema que permitía la compresión de la voz en paquetes de datos para ser transmitidos por Internet. A este paso le siguió la conexión de VoIP con las líneas telefónicas de la red PSTN (*Public Switched Telephone Network*) convencional. El sistema tenía problemas de lentitud y desconexiones que no garantizaban la calidad del servicio: estos problemas se fueron minimizando con el uso de protocolos como el H.323 y posteriormente el Ethernet para lograr mayor calidad y rapidez. Para 1998 se logra la conexión de un PC con teléfono y teléfonos entre sí por medio de Internet.

1.3. Definición del problema.

Una de las aplicaciones más importantes de la convergencia es el incremento de implementaciones de sistemas VoIP en las mayorías de empresas privadas y públicas. En el ámbito de la seguridad se deben establecer los riesgos y detectar las vulnerabilidades que estas redes unificadas tienen actualmente.

Ese aumento de las redes de comunicación VoIP, trae como efecto que las vulnerabilidades también se incrementen, puesto que quedan expuestos huecos de seguridad, que los atacantes podrían usar para diferentes propósitos maliciosos.

1.4. Justificación del Problema a Investigar.

Antes de la telefonía IP, la red telefónica convencional afrontaba problemas de seguridad diferentes a los de una red IP. Para poder explorar actualmente las vulnerabilidades que se presentan en una red VoIP se debe analizar, identificar y controlar esas vulnerabilidades mediante métodos que actualmente existen en las redes IP, como la utilización de Firewalls y analizadores de tráfico para establecer la seguridad perimetral de la red integrada VoIP.

1.5. Objetivos.

1.5.1. Objetivo General:

Diseñar un Sistema de Comunicaciones Unificadas VoIP basado en Elastix con Seguridad Perimetral.

1.5.2. Objetivos específicos:

- ✓ Configurar una central telefónica VoIP Elastix para una pequeña empresa.
- ✓ Levantar los servicios telefónicos de llamadas locales, nacionales, internacionales y celulares.
- ✓ Habilitar las opciones de video llamadas y video conferencia y comprobar su funcionamiento.
- ✓ Configurar un firewall para protección perimetral de la red y la central VoIP con análisis de tráfico y protección contra amenazas.

1.6. Hipótesis o Idea a Defender.

La configuración de técnicas de protección perimetral de la red VoIP permite contrarrestar los ataques, minimizar los riesgos y descartar las vulnerabilidades de la Red VoIP unificada.

1.7. Metodología de investigación.

El método de investigación es analítico; por cuanto se procede con el análisis estructural de los diferentes elementos constitutivos de una red VoIP, se analizan funcionalmente dichos elementos para determinar las

vulnerabilidades y amenazas de las redes VoIP, finalmente se realizan pruebas con políticas de protección contra los diferentes ataques a la red de voz y datos para, en base a los resultados, sacar conclusiones, observaciones y recomendaciones.

Capítulo 2: Fundamentación Teórica.

2.1. Redes de datos.

Una Red está conformada por una serie de elementos de comunicación interconectados entre sí a través de medios físicos, para intercambiar información entre emisores y receptores. Entre los elementos que intervienen en una red se cuentan: emisor, receptor, mensaje, canal, ruido, etc. (DORDOIGNE, 2015)

La comunicación que se inicia desde uno de los extremos; se emite un mensaje hacia otro, una vez que el mensaje se envía, intervienen los protocolos de comunicación para identificar los extremos (emisor, receptor), establecer el canal de comunicación y organizar el intercambio de mensajes. La red de datos utiliza dispositivos de comunicación y periféricos que intervienen para convertir las señales digitales en eléctricas y trasmitirlas por los canales de comunicación.(DORDOIGNE, 2015; Tenenbaum, 1997)

Una red de datos, es una red de comunicaciones donde los emisores y receptores son equipos de computación, telefónicos, de comunicación y demás periféricos conectados a la red. Intervienen en la red los equipos clientes denominados hosts, los equipos servidores, los equipos de comunicaciones. (DORDOIGNE, 2015)

Para poder diseñar, analizar, diferenciar la estructura de la red, los tipos de redes se han clasificado según la topología en: Estrella, Anillo, Árbol, Bus, Doble anillo, Malla, Mixta. (Tenenbaum, 1997)

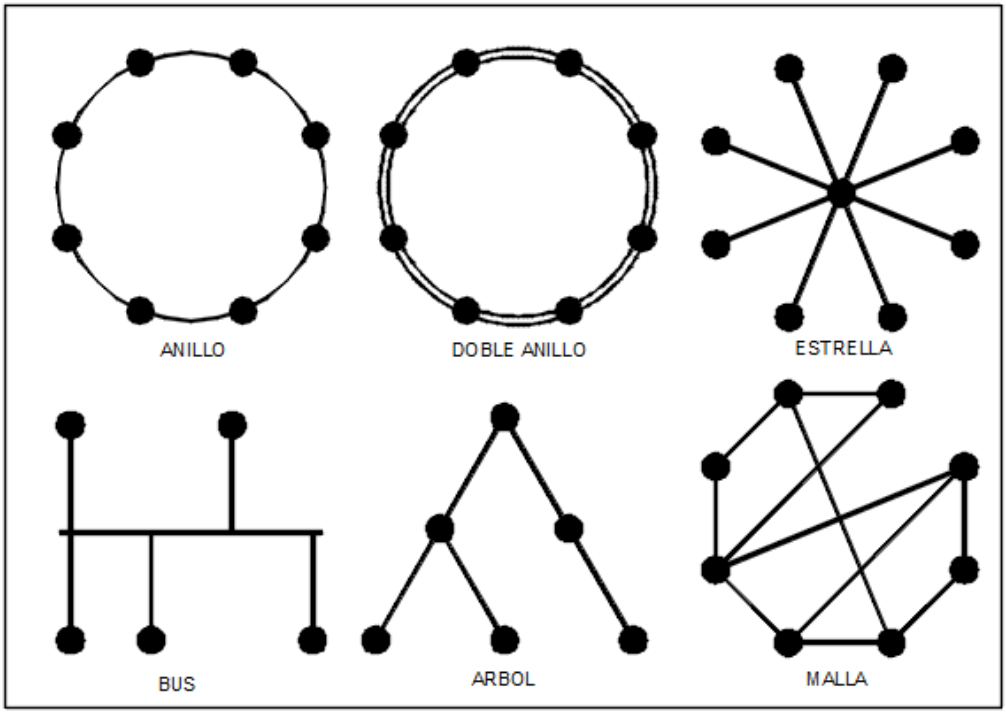


Figura 2.1: Topología de redes
Fuente: Autor

2.1.1. Tipos de redes.

Otra clasificación de las redes de datos y la más conocida de acuerdo a su tamaño, extensión de cobertura, alcance y amplitud física, es la que define a las redes de datos como: PAN, LAN, MAN, WAN. (Tenenbaum, 1997)

2.1.1.1. Redes PAN

Las redes PAN (*Personal Area Network*) son de uso doméstico, donde se conectan en red varios dispositivos y periféricos de uso personal o familiar, por ejemplo, un computador personal, la impresora, el teléfono celular, la Tablet, las cámaras de vigilancia, los sensores de movimiento, entre otros. Son muy comunes actualmente ya que con los AP o routers inalámbricos instalados en la mayoría de los hogares se implementan este tipo de redes. (Tenenbaum, 1997)

2.1.1.2. Redes LAN

Las redes LAN (Local Area Network) son de uso empresarial y están circunscritas a edificaciones de varios ambientes o pisos como centros comerciales, edificios corporativos, condominios, instituciones públicas, aeropuertos, terminales, call centers, entre otros. Se pueden habilitar con equipos de comunicación como switches o hubs, se administran con servidores de aplicaciones que brindan servicios (DHCP, correo, acceso a Internet, gestión de clientes, etc.) a computadores, impresoras, escáneres, cámaras IP, lectores biométricos, y demás periféricos. (*Redes de computadoras—Andrew S. Tanenbaum—Google Libros*, 2013, p. 16)

2.1.1.3. Redes MAN

Las redes MAN se forman cuando se unen varias redes LAN, la comunicación interna puede llegar a abarcar la extensión de una ciudad. Son usadas cuando una empresa o grupo empresarial tiene varios edificios o complejos empresariales dentro de una ciudad, las redes LAN se unen por medio de enlaces de datos, generalmente de fibra óptica, formando una sola red MAN. (Tanenbaum,2013, p. 18)

2.1.1.4. Redes WAN

Las redes de área extensa (WAN por sus siglas en inglés Wide Área Network) se forman cuando se conectan varias redes ubicadas a grandes distancias que trascienden los límites de una ciudad o un país, un ejemplo es una red para brindar servicio de Internet, la que es implementada por los proveedores del servicio navegación a sus clientes. (Tanenbaum, 2013, p. 19)

2.1.2. Protocolos

Los protocolos son normas que permiten estandarizar los procesos de transmisión de datos. Inicialmente los fabricantes establecieron sus protocolos de acuerdo a las necesidades de sus equipos de comunicación, es por eso que se encontraban en el mercado diferentes protocolos de comunicación no compatibles entre sí, dificultando la

interoperabilidad entre equipos de diferente marca.(*Protocolos y Modelo OSI,* Tolosa, 2014)

2.1.2.1. Protocolo IPX/SPX

IPX (*Internetwork Packet Exchange* por sus siglas en inglés) es un protocolo creado por Novell para interconexión de redes que tienen como host clientes y servidores Novell NetWare. Es un protocolo orientado a enrutamiento de paquetes mas no a conexión, no asegura la entrega de paquetes, por eso trabaja sobre el protocolo SPX que a diferencia del anterior si es orientado a conexión.(Análisis de Seguridad de Transferencia VoIP y Desempeño de los Protocolos en Redes con Clientes Inalámbricos, Iturralde, 2006, p. 91)

2.1.2.2. Protocolo TCP

TCP (Protocolo de Control de Transmisión), es orientado a conexión, es decir que la información de origen se entrega en el destino de forma confiable. Divide los paquetes en varios segmentos y los transmite por diferentes caminos de red, en el destino los ensambla de nuevo para obtener el mensaje original. Para lo cual realiza funciones como: reordena segmentos, monitorea el flujo de datos, realiza multiplexión de datos, determina el comienzo y el fin de la comunicación. (Análisis de Seguridad de Transferencia VoIP y Desempeño de los Protocolos en Redes con Clientes Inalámbricos, Iturralde, 2006, p. 92)

2.1.2.3. Protocolo IP

IP (Protocolo de Internet) Es un protocolo basado en conmutación de paquetes, no es orientado a conexión, es decir no garantiza la entrega final de los paquetes de información. Su sistema consiste en encontrar la mejor ruta para enviar los paquetes de información. (Análisis de Seguridad de Transferencia VoIP y Desempeño de los Protocolos en Redes con Clientes Inalámbricos, Iturralde, 2006, p. 92)

2.1.2.4. Protocolo TCP/IP

TCP/IP Es el estándar de comunicación entre redes diferentes que permitió el nacimiento de Internet. Uno de los problemas más grandes para la comunicación entre redes es que los enlaces de datos dependían de los hosts de inicio y de llagada, dado que estos pertenecían a redes de diferente arquitectura sus protocolos de comunicación no eran compatibles. El protocolo TCP/IP corrige ese problema al asumir la comunicación entre Hosts sin depender de los extremos sino más bien de los equipos de transmisión o Gateway que se encargan de ser la puerta de entrada y salida de la red. (Moromencho, 2013)

2.1.2.5. Protocolo ETHERNET

En 1973 Robert Metcalfe se dio cuenta de que podía mejorar el sistema Aloha o el acceso arbitrario a los canales de comunicaciones compartidos y elaboró una tesis doctoral donde planteó teóricamente esas mejoras. Metcalfe desarrolló un nuevo sistema que incluía un mecanismo que detectaba cuando se producía una colisión (detección de colisión). El sistema también incluía "escuchar antes de hablar", en el cual la estación escuchaba la actividad (detección de operador) antes de transmitir y admitía el acceso a un canal compartido por varias estaciones (estaciones múltiples). (Márquez Díaz et al., 2001)

Poniendo todos estos componentes juntos se puede ver por qué el protocolo de acceso al canal Ethernet se llama Acceso múltiple de detección de portadora con detección de colisiones (CSMA/CD). Metcalfe también desarrolló un algoritmo de retroceso más sofisticado que, en combinación con el protocolo CSMA / CD, permitió que el sistema Ethernet funcionara con una carga de hasta el 100%. (Márquez Díaz et al., 2001)

2.1.2.6. Protocolo UDP

UDP (*User Datagrm Protocol*) es un protocolo orientado a datagramas, no hay seguridad de que los paquetes lleguen a su destino y en caso de que lleguen tampoco se garantiza el orden de llagada de los mismos. UDP Es más sencillo que el TCP, pero menos confiable, sin embargo, puede ser más rápido sobre todo en aplicaciones simples cuya ejecución requiere que los datos sean transmitidos más rápido. Aunque con menos fiabilidad. (Dimas & Morales, 2009)

2.1.3. Modelos de referencia.

La necesidad de estandarizar los métodos de acceso a redes y de transporte de datos para facilitar la compatibilidad y la interoperabilidad hizo que se creen estándares universales conocidos como modelos de referencia. Entre los más conocidos están el modelo OSI y el TCP/IP. (Tolosa, 2014)

2.1.3.1. TCP/IP

Modelo que describe los protocolos usados en la red ARPANET, predecesora de Internet. Los protocolos como el TCP/IP se basan en el principio de que el mecanismo de funcionamiento debe ser implementado en los extremos o nodos (principio de extremo a extremo). (Atelin & Dordoigne, 2006)

A mediados de los años 70, ARPANET adopta un nuevo modo de comunicación con el *Transmision Control Protocol/Internet Protocol* (TCP/IP). En 1980, la agencia DARPA, decide no utilizar el TCP/IP por el secreto militar. Al mismo tiempo la versión de UNIX *Berkeley Software Development* (BSD) proporciona gratuitamente a las universidades incluso los códigos fuente TCP/IP. (Atelin & Dordoigne, 2006)

EL modelo TCP/IP está formado por 4 capas: Aplicación, Transporte, Internet y Red. En la capa de Aplicación se encuentran los protocolos TFTP, Telnet, NFS, SMTP, DNS, LDP, SNMP, RLOGIN, FTP, HTTP entre otros. En la de Transporte los protocolos TCP y UDP. En la capa de

Internet se encuentran los protocolos ICMP, ARP, RARP e IP. En la de Red se encuentra Ethernet, FastEthernet, PPP, FDDI, ATM, Toking Ring, Frame Relay, HDLC.

2.1.3.2. Modelo OSI

El modelo de Interconexión de Sistemas Abiertos (OSI) fue creado en 1984 por la Organización Internacional para la Normalización (ISO), con el propósito de lograr compatibilidad e interoperabilidad entre tecnologías de comunicación de los diferentes fabricantes (Atelin & Dordoigne, 2006).

El modelo OSI está formado por 7 capas, a diferencia del TCP/IP que solo tiene 4 capas. La división de la comunicación de red en capas establece normas para los componentes de red a fin de permitir el desarrollo y el soporte de los productos. Las capas son las siguientes:

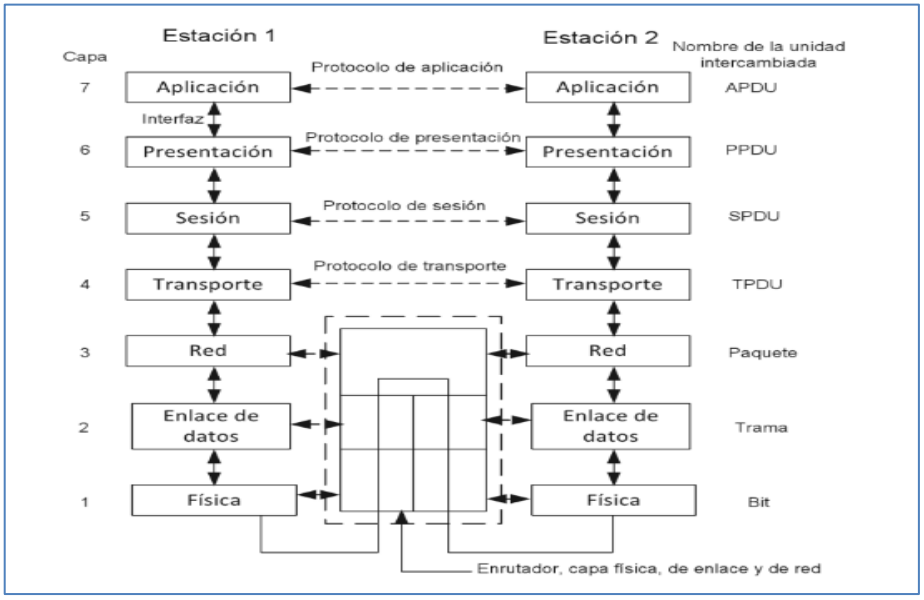


Figura 2.2: Modelo OSI
Fuente: (Oliva Alonso, 2013)

2.1.3.2.1. Capa de Aplicación

En la capa de aplicación es donde operan todos los programas que interactúan con el usuario. Aquí se encuentra protocolos de servicios a usuario como TELNET, FTP, SMTP, POP, HTTP, DHCP, NAT, SNMP, DNS, TFTP, entre otros., estos servicios proveen una interfaz con el usuario. La capa de aplicación es la puerta de entrada del usuario a la red de comunicación por medio de las aplicaciones. (L. Moreno, 2003) (Tolosa, 2014)

2.1.3.2.2. Capa de Presentación

En esta capa se definen los formatos y estructura de los datos para que sean legibles por el receptor en la dirección de destino, es decir que aquí se traduce la sintaxis de los datos a un formato estándar (universal) legible por el nivel inferior. Además, aquí se realiza la encriptación y compresión de los datos cuando se han solicitado los protocolos de seguridad de cifrado.(Tolosa, 2014; Moromencho, 2013)

2.1.3.2.3. Capa de Sesión

Debe establecerse aquí el inicio, mantenimiento y finalización de sesiones entre aplicaciones, aquí se establecen los procedimientos que permiten la conversación entre las diferentes herramientas de software y aplicaciones. Aquí se organiza y sincroniza la comunicación a través de funciones para el diálogo entre las aplicaciones. (Tolosa, 2014; Moromencho, 2013)

2.1.3.2.4. Capa de Transporte

En esta capa se establecen todos los aspectos del transporte de datos entre dos equipos remotos, tales como: (Tolosa, 2014; Moromencho, 2013)

- Confiabilidad del transporte de datos.
- Crear mantener y terminar circuitos virtuales de comunicación entre hosts.
- Detección de errores de transmisión, reordenamiento y recuperación los datos.

- Control del flujo de la información.
- Eliminación de paquetes repetidos.

2.1.3.2.5. Capa de red

En esta capa se establece el encaminamiento por la mejor ruta y se conectan dos sistemas remotos. En este nivel los datos se fragmentan en paquetes y se envían de manera independiente, para ella se elige la mejor ruta (menor tiempo y saturación) para enviar los paquetes de información, entre las funciones adicionales más relevantes se encuentran: (Tolosa, 2014; Moromencho, 2013)

- Conexión y desconexión entre redes.
- Sincronización.
- Control de flujo.
- Detección y recuperación de errores.
- Evitar la congestión.

Las unidades de información son los paquetes.

2.1.3.2.6. Capa de enlace de datos.

En la capa de enlace se establece la transferencia confiable de los datos a través de la red, para esto actúan los protocolos realizan los diferentes procesos como:

- Direccionamiento físico,
- Topología de red,
- Notificaciones de errores,
- Control de secuencia y de flujo.

Las unidades de información son las tramas, en proceso de encapsulación se agregan los bits de control antes de pasar la trama a la capa física. En proceso de des encapsulación se detectan y retiran esos bits antes de pasar a la capa superior de red. (Tolosa, 2014; Moromencho, 2013)

2.1.3.2.7. Capa Física.

En la capa física se produce la transmisión de los bits o binaria, recibe mensajes y transmite bits. Se definen las características del enlace y la interface:

- Mecánicas (medios físico y conectores)
- Eléctricas (duración del bit, niveles de voltaje, etc)
- Funcionales (Asignación de señales a los pines)

Intervienen los parámetros de transmisión como velocidades de flujo de datos y voltajes, tipos de cable, conectores. EL medio físico de transmisión puede ser cable de cobre, fibra óptica o inalámbrico. Las funciones principales de la capa física se pueden resaltar como:

- Los componentes físicos
- La codificación de datos
- Señalización

Los componentes físicos son el medio físico de transmisión, los conectores, los dispositivos electrónicos, etc. La codificación es el proceso de conversión de una trama en bits de datos para su transmisión. La señalización es el método de representación de los bits. (Tolosa, 2014; Moromencho, 2013)

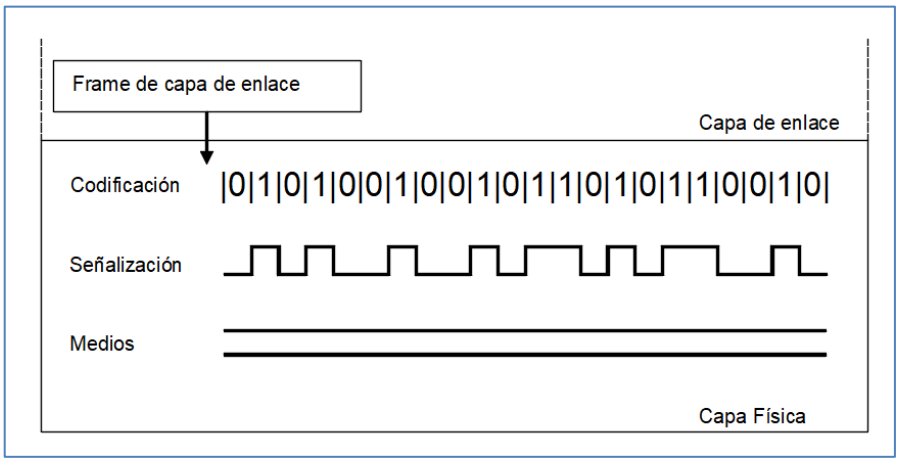


Figura 2.3**:** Funciones principales de la capa física
Fuente: El autor

2.2. Telefonía

La telefonía analógica había sido hasta la llegada de la red de Internet y VoIP la opción de comunicación global, sin embargo, los obstáculos tecnológicos que no permitían la unificación de los servicios de transmisión de datos con los telefónicos por ser redes de tecnología diferente fueron el impulso necesario para acelerar los esfuerzos por encontrar una opción diferente de brindar el servicio telefónico. La opción de transmitir la voz humana digitalmente a través de conductores, tubo relevancia en el camino hacia la digitalización de las señales auditivas y con el teorema de Nyquist como herramienta fundamental de muestreo se allanó ese camino. (Semeria, 2015)

2.2.1. Transmisión de la voz humana

La voz humana está compuesta por ondas acústicas que viajan a través del aire a la velocidad del sonido, esto es a 1,244 Km/h (o 340 m/s). Pero esta velocidad no significa que se puedan comunicar fácilmente dos puntos distantes, pues la voz humana se atenúa rápidamente, perdiendo energía a medida que viaja. Luego de unos pocos metros, la señal es tan débil que no se puede escuchar una conversación.(Edgar Landívar, 2009)

2.2.2. Rango de frecuencia de la voz humana

Otra característica importante de la voz humana es que las cuerdas vocales modulan la voz en un amplio espectro de frecuencias que van de graves a agudos en un rango aproximado de 20Hz a 20kHz. Actualmente se sabe que para transmitir voz "entendible" solo es necesario transmitir un rango mucho menor de frecuencias y esto hace más fácil la transmisión. Por lo tanto, los teléfonos comerciales solo transmiten un rango aproximado de 400Hz a 4kHz. Esto distorsiona levemente la voz, pero de todas maneras se puede entender. Es por eso que al oír a alguien por teléfono su voz suena ligeramente diferente que en la vida real pero aun así se puede entender la conversación. (*Comunicaciones Unificadas con Elastix Volumen 1, Edgar Landívar, 2009*, p. 18)

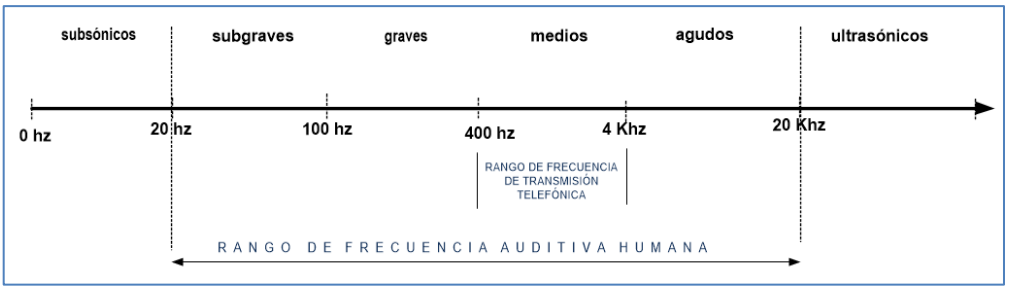


Figura 2.4: Rango de frecuencia auditiva humana
Fuente: El autor

2.2.3. Ancho de banda

El ancho de banda es una magnitud de frecuencia por lo tanto se mide en Hertz, es la diferencia entre la máxima y la mínima frecuencia que puede pasar por un canal de comunicación. (Semeria, 2015)

$$\mathrm{AB} = \mathrm{f}_{\mathrm{max}} - \mathrm{f}_{\mathrm{min}}$$

Ancho de banda en Informática es un término algo difícil de entender, pues es un concepto bastante amplio. En general se puede decir que ancho de banda es una medida de la cantidad de información que puede transmitir por un medio por unidad de tiempo. Debido a que es una medida por unidad de tiempo muchas veces se hace una analogía con la velocidad. (Arribas, 2010)

Medidas comunes para expresar el ancho de banda son los bits por segundo. Esta medida también equivale a bits/s, bps o baudios. El ancho de banda es un término muy importante cuando se habla de telefonía pues las comunicaciones en tiempo real necesitan un ancho de banda mínimo asegurado para entregar una comunicación de calidad en destino.(Arribas, 2010)

2.2.4. Digitalización de la voz

Las redes digitales de transmisión de voz y datos presentan algunas ventajas en comparación con las redes analógicas, por ejemplo:

- Conservan mejor la integridad de la señal durante su recorrido. Es decir que la señal está menos expuesta a los factores externos como el ruido eléctrico.
- Provee de métodos para verificar de cada cierto tiempo la integridad de la señal.

Digitalizar una señal de voz, al igual que otro tipo de señales, consiste en tomar muestras de la amplitud de la señal analógica a intervalos de tiempo regulares, para obtener una señal discreta y transformar esos valores discretos a binarios. Proceso que se conoce como muestreo. (Semeria, 2015)

2.2.5. Teorema de Nyquist

Para digitalizar la señal a través del muestreo existía el dilema de cuan fidedigna puede ser la señal en relación al número de muestras tomadas para que pueda ser reconstruida en el proceso contrario de pasarla de digital a analógica. Está claro que, a mayor número de muestras, mayor fidelidad de la señal; es decir que, a mayor frecuencia de muestreo la señal digitalizada será más parecida a la original luego de su reconstrucción. (Semeria, 2015)

Sin embrago, para evitar es importante poder determinar ¿cuánto es necesario muestrear la señal? o ¿cuál es la frecuencia de muestreo mínima para que la señal sea reconstruida satisfactoriamente? En 1928 Henry Nyquist, un ingeniero suizo que trabajaba para AT&T, resolvió el dilema con su teorema propuesto: La frecuencia de muestreo debe ser como mínimo el doble de la frecuencia de la señal original. (Semeria, 2015)

Se define con la expresión:

$$f_m \geq 2BW_S$$

Partiendo del teorema de Nyquist, se puede encontrar cual sería la frecuencia de muestreo para convertir una señal de voz humana a digital que garantice su reconstrucción en el destino. Se sabe que es suficiente transmitir un rango de frecuencias de entre 400Hz a 4000Hz para que la voz humana sea entendible. Por lo tanto, según Nyquist, una señal de voz se debería muestrear como mínimo al doble de la frecuencia mayor (4000 Hz), es decir a 8000Hz.(Semeria, 2015)

Ahora se entiende por qué la frecuencia de muestreo de 8000Hz se usa en la mayoría de Codecs.

2.2.6. Redes orientadas a circuitos

Cuando la comunicación entre dos nodos se establece únicamente después de que asigna un circuito exclusivo ente los dos extremos, se observa lo que se define como una red orientada a circuito; mientras dure la comunicación entre los nodos en circuito permanecerá cautivo. En momentos en los cuales no haya circuitos disponibles no podrá haber nuevas comunicaciones. (J. Moreno et al., 2006)

Las redes orientadas circuitos también pueden transportar datos digitalmente. Otra de las características de este tipo de redes es que tienen ancho de banda fijo para la transmisión.

2.2.7. Redes orientadas a paquetes

Cuando la comunicación se realiza por un mismo medio, pero la información está fragmentada y los fragmentos o paquetes pueden o no pertenecer a un mismo origen o estar dirigidos al mismo destino, se está ante una red orientada a paquetes; por un mismo medio trafican simultáneamente diferentes flujos de información. En una red orientada a paquetes, se divide el tráfico de cada flujo de información en diferentes fragmentos o paquetes que se envían intercaladamente; en el destino, dichos fragmentos o paquetes deben ser re-ensamblados para reproducir el mensaje original. (Fajardo, 2004)

La red IP es una red orientada a paquetes, dentro del conjunto de redes IP se tiene las redes MAN, LAN, WAN y la más famosa red conocida como Internet. En estas redes, que trabajan bajo el esquema OSI, los dispositivos de comunicación se encargan de realizar el proceso de empaquetamiento de datos antes ser transmitidos por los medios físicos. De tal forma que, por cada línea de transmisión pueden circular, decenas, centenas de circuitos dependiendo del número de equipos conectados a la red y la cantidad de transmisiones realizadas. (DORDOIGNE, 2015; Fajardo, 2004)

En una red orientada a paquetes el tráfico aumenta de acuerdo a la cantidad de transmisiones que se estén realizando en forma simultánea, es decir de acuerdo a la cantidad de segmentos o paquetes que están siendo transmitidos. El ancho de banda aumenta o disminuye en función del tráfico, pero está limitado por la capacidad del canal de transmisión.

2.2.8. Protocolos de Señalización Digital

Los protocolos de señalización se utilizan para gestionar el canal de comunicación, es decir para transmitir información de control, información de estado del canal de comunicaciones (esta información puede ser indicar que el canal está “desconectado”, “timbrando”, “respondido”), y otro tipo de información como DTMFs, caller ID, entre otros. (González Lumbreras, 2014)

Hay dos tipos de protocolos de señalización: de canal asociado CAS (por sus siglas en inglés: *Channel Associated Sgnaling*) y de Señalización de canal común CCS (por sus siglas en inglés: *Common Channel Signaling*). En el CAS se transmite la señalización por el mismo canal junto con la información, en el CCS se transmite la señalización por otro canal diferente al de la información. En la transmisión por canal compartido de la señalización junto con la información, por el protocolo CAS, hay mayor consumo de ancho de banda, esto significa menor disponibilidad de capacidad del canal para la transmisión de la

información útil. Razón por la cual es más utilizado el protocolo de señalización CCS. (González Lumbreras, 2014)

2.2.8.1. Señalización Asociada al Canal (CAS)

El protocolo CAS es conocido como robbed-bit (bit robado) y es usado en circuitos T1 y E1. Robbed-bit toma el octavo bit de cada canal de comunicación cada seis Frames y lo reemplaza por información de señalización. El bit original robado se pierde de la información. En la transmisión de la voz, ese bit perdido no representa un efecto muy distorsionador de la señal original siendo este el bit menos significativo. Sin embargo, significa pérdida por degradación en la calidad de la señal.

Otro protocolo CAS que aún subsiste en nuestros días es R2. Se trata de un protocolo que fue popular en los años 60s. En realidad, R2 es una familia de protocolos en donde cada implementación se denomina "variante". Existen variantes dependiendo del país o inclusive de la compañía telefónica que lo ofrece. (Edgar Landívar, 2009, p. 31)

2.2.8.2. Señalización de Canal Común (CCS)

2.2.8.2.1. SS7

Es el protocolo de señalización más utilizado y que alcanzó un nivel de estandarización global por brindar: alta flexibilidad, alta capacidad, alta velocidad; y porque, además implica menores costos al brindar mayor rango de servicios y usar menor hardware. (Campoverde & Ferrerosa, 2010)

SS7 es un conjunto de protocolos de señalización telefónica y el más usado globalmente. Se encarga del establecimiento y finalización de llamadas. Otra de las acciones que realiza es proporcionar los mecanismos de tarificación pre-pago y el envío de mensajes cortos. (Campoverde & Ferrerosa, 2010)

SS7 para las telecomunicaciones es un estándar global definido por la ITU-T. El estándar define el protocolo y los procedimientos mediante los cuales los elementos de la red de telefonía intercambian información sobre una red digital para realizar enrutamiento, establecimiento y control de llamadas. (Campoverde & Ferrerosa, 2010)

Para mantener y entregar servicios, los componentes de una llamada intercambian información, este proceso se conoce cómo Señalización. El protocolo SS7 dispone de una estructura estándar para señalización, interconexión, mensajería y mantenimiento en redes de telefonía. Realiza establecimiento de llamada, intercambio de información de usuario, enrutamiento de llamada, estructura de abonados diferentes y soporta servicios en redes inteligentes.

2.2.8.2.2. ISDN (Integrated Services Digital Network)

La Red Digital de Servicios Integrados, permite la transmisión simultánea de voz y datos sobre pares de cobre telefónicos con mejor calidad en comparación con las líneas analógicas.

ISDN facilita las conexiones digitales de tal forma que estas puedan ofrecer una gama más amplia de servicios integrados. Para cumplir con este fin, ISDN utiliza dos interfaces:

- **BRI**: Basic Rate Interface
- **PRI**: Primary Rate Interface

Un BRI contiene 2 canales útiles (canales B) de 64Kbit/s cada uno más un canal de señalización de 16Kbit/s (canal D) que en total suman 144Kbit/s. BRI, que debía ser un estándar residencial, tuvo muy poca acogida en este segmento del mercado en los Estados Unidos. Fue más utilizado en Europa.

PRI es la opción para usuarios corporativos como negocios o empresas ya que puede agrupar más canales B. Se transmite sobre circuitos T-carrier y E-carrier.

2.3. Redes VoIP

Las redes VoIP marcaron el inicio de la convergencia de las redes de datos con las de telefonía. Si bien es cierto el servicio telefónico de las redes VoIP nació como un servicio que se entregaba a través del Internet, con la ayuda de herramientas como Net2Phone, Skype entre otras; el incremento de la tasa de transferencia de datos del servicio de Internet ofertado por los ISP del orden inicial de los Kbps a Mbps, como efecto de la implementación de redes de FO para el transporte y la última milla, hizo que rápidamente aparecieran herramientas alternativas a las centrales telefónica analógica de la telefonía convencional, es decir aparecieron las centralitas IP que podían operar desde la red de datos (ethernet). (López & Rodríguez, 2008)

2.3.1. Voz sobre IP, VoIP o Transmisión de voz sobre protocolo IP.

Las redes IP diseñadas para datos, no pueden disimular algunas desventajas para la transmisión de voz, ya que la data de voz es muy sensible a retardos y problemas de transmisión por muy pequeños que estos sean. La tecnología ha evolucionado para disminuir en gran medida de aquellos problemas inherentes a las redes IP que perjudican la calidad de voz. (López & Rodríguez, 2008)

2.3.2. Protocolos VoIP

Los protocolos que intervienen en la transmisión de Voz sobre IP son los mismos que la transmisión de datos, dentro de esos se encuentra el propio protocolo IP. Los protocolos de la etapa de transporte como el TCP o UDP. Por arriba de los protocolos de transporte se encuentran los de señalización de voz y otras tantas opciones de protocolos de señalización. Esto se puede explicar mejor en base al siguiente gráfico. (Martín & Aversa, 2014)

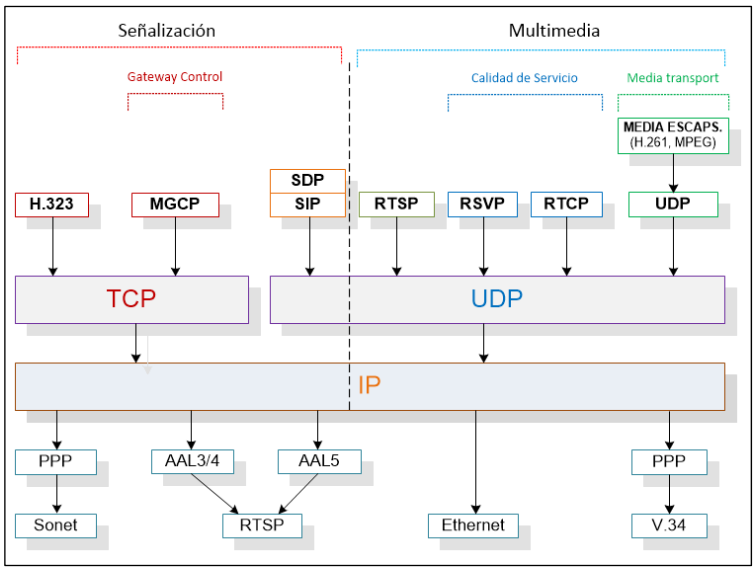


Figura 2.5: Protocolos VoIP
Fuente: (López & Rodríguez, 2008, p. 27)

Los paquetes VoIP (Audio y video) se encuentran en RPT y se encapsulan en UDP para su transporte. El protocolo UDP no tiene control sobre el orden en que llagan loa paquetes, los entrega sin verificar si hay perdidas de paquetes o retardo de llegada. (Martín & Aversa, 2014)

2.3.2.1. Clasificación de protocolos VoIP

Se puede clasificar a los protocolos que intervienen en una red VoIP en tres grupos:

- **Protocolos de señalización**

Al igual que los protocolos de señalización de la telefonía tradicional, los de VoIP cumplen funciones como: tareas de establecimiento de sesión, control del progreso de la llamada, entre otras. En el modelo OSI, se enmarcan en la capa de Sesión. diferentes fabricantes u organismos como la ITU o el IETF, han desarrollado diferentes protocolos de señalización que están soportados por Asterisk. como: (González, 2011)

- SIP
- IAX
- H.323
- MGCP
- SCCP

De los cuales, los más utilizados en el entorno de Asterisk son SIP e IAX.

- **Protocolos de transporte de voz**

Son protocolos de transporte de data de voz o de lo que se denomina carga útil. EL protocolo más conocido es RTP (*Real-time Transport Protocol*) y tiene la función de transportar la data de voz con el menor retardo posible. Este protocolo inicia su funcionamiento después que el protocolo de señalización ha establecido la llamada entre los usuarios participantes. (Sousa & Carrapatoso, 2003)

- **Protocolos de plataforma IP**

Son los protocolos convencionales en redes IP y constituyen la base sobre la cual se sostienen los protocolos de voz transporte de voz y de señalización. Los protocolos de la plataforma IP son entre otros: TCP, UDP, IP, Ethernet. (Martín & Aversa, 2014)

2.3.3. Arquitectura de la red VoIP.

Las redes VoIP son una nueva arquitectura para las comunicaciones donde la unión de las redes de Voz con las de Datos ha permitido incorporar nuevos servicios de Red, tales como: conferencias, video llamadas, chats internos, llamadas Internacionales, interconexión con la red celular, comunicación múltiple durante juegos en línea, entre otros. Es adaptable y versátil a las nuevas demandas de servicios. (Martín & Aversa, 2014)

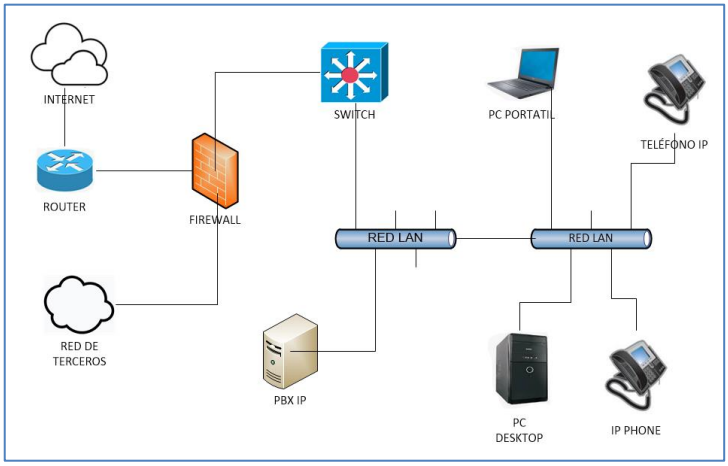


Figura 2.6: Arquitectura de red VoIP
Fuente: El autor

2.3.4. Codecs

La codificación y decodificación de las formas de onda para transformarlas en números discretos, es decir, para ser digitalizadas, tiene gran aplicación en las señales de audio y video. Tanto los teléfonos digitales como los teléfonos IP utilizan los Codecs (algoritmos codificadores y decodificadores) para sintetizar, comprimir y descomprimir la voz humana. Así también para la transmisión de video se codifica y decodifica por medio de Codecs de video. (Joskowicz, 2013)

2.3.4.1. Codecs de audio

Los algoritmos de compresión de voz se pueden clasificar de acuerdo con:

- Su tecnología
- La tasa de bits
- La calidad del audio codificado
- Su complejidad
- El retardo que introducen

Según el ancho de banda de la señal de entrada.

- Banda angosta (narrowband)
- Banda ancha
- Banda Super ancha
- Banda completa

En las tablas siguientes se resumen los algoritmos de compresión de voz más conocidos:

Tabla 2. 1: Codecs de Banda Angosta

Codec	Nombre	Bit rate (kb/s)	Retardo (ms)	Comentarios
G.711	PCM: Pulse Code Modulation	64, 56	0.125	Codec "base", 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 originalmente para video conferencias en la PSTN, es actualmente utilizado en sistemas de VoIP
G.728	LD-CELP: Low-Delay code excited linear prediction	40, 16, 12.8, 9.6	1.25	Creado para aplicaciones DCME (Digital Circuit Multiplex Encodin
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 kb/s
AMR	Adaptive Multi Rate	12..2 a 4.75	20	Utilizado en redes celulares GSM

Fuente: (Joskowicz, 2013, p. 6)

Tabla 2. 2: Codecs de Banda Ancha

Codec	Nombre	Bit rate (kb/s)	Retardo (ms)	Comentarios
G.722	Sub-band ADPCM	48,56,64	3	Inicialmente diseñado para audio y videoconferencias, actualmente utilizado para de telefonía de calidad en VoIP
G.722.1	Transform Coder	24,32	40	Usado en audio y videoconferencias
G.722.2	AMR-WB	6.6 a 23.85	259375	Estándar en común con 3GPP (3GPP TS 26.171). gran inmunidad a los ruidos de fondo en ambientes adversos (por ejemplo celulares)
G.711.1	Wideband G.711	64, 80, 96	11875	Amplía el ancho de banda del codec G.711, optimizando su uso para VoIP
G.729.1	Wideband G.729	8 a 32 kb/s	<49 ms	Amplía el ancho de banda del codec G.729, y es "compatible hacia atrás" con este codec. Optimizado su uso para VoIP con audio de alta calidad

RtAudio	Real Time Audio	8.8, 18	40	Codec propietario de Microsoft, utilizado en aplicaciones de comunicaciones unificadas (OCS)

Fuente: (Joskowicz, 2013, p. 6)

Tabla 2. 3: Codecs de Banda Super ancha

Codec	Nombre	Bit rate (kb/s)	Retardo (ms)	Comentarios
SILK	SILK	8 a 24	25	Utilizado por Skype

Fuente: (Joskowicz, 2013, p. 6)

Tabla 2. 4: Codecs de Banda Completa

Codec	Nombre	Bit rate (kb/s)	Retardo (ms)	Comentarios
G.719	Low-complexity, full-band	32 a 128	40	Es el primer codec "fullband" estandarizado por ITU
Opus	Opus	6 a 510	Hasta 60	Incorpora tecnología de SKYPE RFC 6716 (propuesta en set 2012)

Fuente: (Joskowicz, 2013, p. 6)

2.3.4.2. Codecs de Video

Los Codecs de video, son algoritmos para digitalización de videos, entre las técnicas usadas se tiene: Predicción, Transformación, cuantización, Codificación entrópica.

Predicción: Predecir el valor de ciertas muestras en función de otras, para enviar solamente como información la diferencia.

Transformación: Los valores relacionados a las muestras pueden ser transformados en otro conjunto de valores equivalentes que representan la misma información de una forma diferente. En video se utiliza le transformada discreta del coseno (DTC).

Cuantización: Se asigna un valor entero a un número real, en función de la cantidad de enteros utilizados, el proceso de cuantización puede introducir más o menos distorsión respecto al valor original.

Codificación entrópica: Representa los valores cuantizados tomando ventaja de las frecuencias relativas con las que aparece cada símbolo. Códigos de largo variable (VLC).

Algunos de los Codecs de video más conocidos son: JPEG, MPEG-1, MPEG-2, MPEG-4, H.264/AVC, SVC, MVC.

MPEG-1: Originalmente diseñado por la Moving Picture Experts Group de la ISO. Pensado para el almacenamiento y reproducción digital de aplicaciones multimedia
desde dispositivos CDROM.

MPEG-2: Pensado para proveer calidad de video desde la obtenida con NTSC/PAL y hasta HDTV, con velocidades de hasta 19 Mbps.

MPEG-4: Es la evolución de MPEG-1 y 2, y provee la tecnología base para la codificación en base a contenidos y su almacenamiento, transmisión y manipulación.

H.264/AVC: Con AVC (Advancede Video Coding) para una misma calidad de video se logran mejoras en el ancho de bande requerido de aproximadamente el 50% respecto a estándares anteriores.

2.3.5. Protocolos de Señalización.

Un protocolo es un conjunto de reglas y acuerdos que los computadores y dispositivos deben seguir para que puedan comunicarse entre ellos. Los protocolos que se utilizan en las redes de voz sobre IP son: MGCP, H.323 y SIP, entre otros; todos definidos por instituciones y organismos reguladores con normativas de control como: la ITU T, la IETF, el ETSI o el EIA TIA. Estos protocolos tienen interfaces abiertas y estándares definidos, y cuentan con una buena infraestructura de paquetes. (Patiño Cardona, 2014, p. 56)

2.3.5.1. Protocolo SIP

El Protocolo de Iniciación de Sesión (SIP) es un protocolo de señalización por medio del cual se crea, modifica y termina sesiones con uno o más usuarios destino. Las sesiones permiten llamadas telefónicas por Internet, conferencias y distribución de datos multimedia. El protocolo SIP utiliza servidores Proxy para encaminar peticiones hasta el usuario destino, también para autenticar y autorizar a usuarios, implementar políticas de direccionamiento y brindar servicios a los usuarios. SIP permite registrar las localizaciones actuales de los usuarios en los servidores Proxy. Trabaja sobre algunos protocolos de transporte. (Patiño Cardona, 2014, p. 59)

El protocolo SIP se asemeja a HTTP o SMTP, por el tipo de mensaje que incluye un encabezado y un cuerpo de mensaje, los cuales se definen en el protocolo de descripción de sesión (SDP). SIP es un protocolo basado en texto con codificación UTF8, para señalización utiliza el puerto 5060 para los protocolos TCP y UDP y para transmisión de voz por RPT usa el rango de 10000 a 20000. (Salcedo et al., 2012)

2.3.5.1.1. Mensajes SIP.

SIP es un protocolo de texto que se asemeja al HTTP, se realizan peticiones mediante los UAC37 y por medio de los UAS38 se responde a las peticiones de los usuarios. SIP establece la comunicación por medio de dos tipos de mensajes: Las solicitudes y las respuestas, emplean el formato de mensaje genérico definido den RFC 2822.

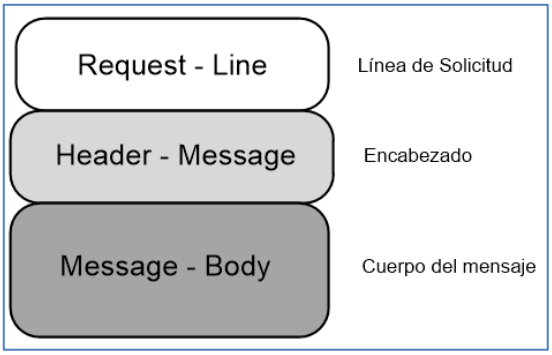


Figura 2.7: Mensaje SIP
Fuente: (Patiño Cardona, 2014)

- La línea de solicitud o petición inicial también tiene información sobre la versión del protocolo y las direcciones que intervienen.
- El encabezado contiene información de la llamada: origen, destino de la petición; y la contiene en forma de texto.
- El cuerpo del mensaje o carga útil (PAYLOAD) lleva la información.

2.3.5.1.2. Métodos SIP

Las peticiones SIP se encuentran en la línea inicial del mensaje: Request-Line, donde se describe el nombre del método, el identificador del destinatario de la solicitud (Request-URI) y la versión del protocolo SIP. SIP define algunos métodos, de los que se detallan a continuación: (Patiño Cardona, 2014)

- SIP invite: Para iniciar sesiones o modificar parámetros en una sesión ya existente.
- SIP ack: Confirma que la llamada se ha establecido.
- SIP Option: Solicita información sobre las capacidades de un servidor
- SIP Bye: Termina una sesión
- SIP Cancel: Cancela una invitación pendiente
- SIP Register: registra una ubicación en un servidor
- SIP re-invite: Cambia una sesión actual

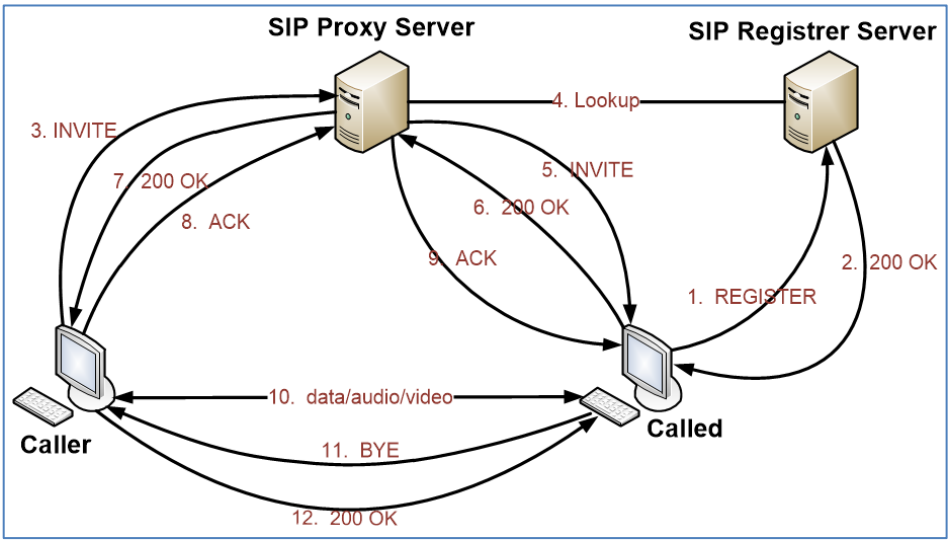


Figura 2.8: Llamada SIP
Fuente: (López & Rodríguez, 2008, p. 23)

Extensiones de métodos SIP de otros RFCs

- **SIP Info**: Extensión en RFC 2976
- **SIP notify**: Extensión en el RFC 2848 PINT
- **SIP subscribe**: Extensión en el RFC 2848 PINT
- **SIP unsubscribe**: Extensión en el RFC 2848 PINT
- **SIP update**: Extensión en RFC 3311
- **SIP message**: Extensión e n RFC 3428
- **SIP refer**: Extensión en RFC 3515
- **SIP prack**: Extensión en RFC 3262
- **SIP Specific Event Notification**: Extensión en RFC 3265
- **SIP Message Waiting Indication**: Extensión en RFC 3842
- **SIP publish**: La extensión es RFC 3903. (Patiño Cardona, 2014)

2.3.5.1.3. Respuestas SIP

Después de la recepción e interpretación del mensaje de solicitud SIP, el receptor destino responde con un mensaje similar al anterior, pero diferente en la línea inicial llamada *Status-Line*, que indica la versión de SIP, el código de la respuesta (*Status–Code*) y una descripción (*Reason-Phrase*). El código de la respuesta está formado por tres dígitos que permiten clasificar los diferentes códigos existentes. La clase de la respuesta se define por el primer dígito. (Patiño Cardona, 2014)

- **Código Clase**

  El primer dígito del Status-Code define la categoría de respuesta.

  1xx - Mensajes provisionales.

  2xx - Respuestas de éxito.

  3xx - Respuestas de redirección.

  4xx - Respuestas de fallo de método. Error de cliente

  5xx - Respuestas de fallos de servidor.

  6xx - Respuestas de fallos globales. (Patiño Cardona, 2014)

2.3.5.1.4. Cabecera.

En la cabecera SIP se agregan algunos parámetros necesarios para el transporte del paquete SIP. Algunos de los campos más importantes se detallan a continuación: (Patiño Cardona, 2014)

- **Via**: Indica el transporte usado para el envío e identifica la ruta del request, por ello cada proxy añade una línea a este campo.
- **Max-Forward**: Se utiliza para limitar el número de saltos que esta petición se puede tomar antes de llegar al destinatario. Es decrementado por uno en cada salto ya que es necesario evitar que la solicitud viaje en forma indefinida en caso de que sea atrapada en un bucle.
- **From**: Indica la dirección del origen de la petición.
- **To**: Indica la dirección del destinatario de la petición.
- **Call-Id**: Identificador único para cada llamada y contiene la dirección del host. Debe ser igual para todos los mensajes dentro de una transacción.
- **Cseq**: Se inicia con un número aleatorio e identifica de forma secuencial cada petición. Se utiliza para detectar la no entrega de un mensaje o entrega de los mensajes fuera de orden.
- **Contact**: Contiene una (o más) dirección que pueden ser usada para contactar con el usuario.
- **User Agent**: Contiene el cliente agente que realiza la comunicación.
- **Content-Type**: Contiene una descripción del cuerpo del mensaje (no se muestra).
- **Content-Length:** Se trata de un octeto (byte) que es la cuenta del tamaño del cuerpo del mensaje. (Patiño Cardona, 2014)

2.3.5.1.5. Formato de Solicitudes SIP

INVITE enviada por User1.

INVITE sip:user2@server2.com SIP/2.0

Via: SIP/2.0/UDP pc33.server1.com; branch=z9hG4bK776asdhds Max-forwards: 70

To: user2 <sip:user2@server2.com>

From: user1 <sip:user1@server1.com>; tag=1928301774

Call-ID: a84b4c76e66710@pc33.server1.com

CSeq: 314159 INVITE

Contact: <sip:user1@pc33.server1.com>

Content-Type: application/sdp

Content-Length: 142

---- User1 Message Body Not Shown ----

La primera línea del mensaje codificado se llama Request Line. Identifica que el mensaje es una petición. (Patiño Cardona, 2014)

2.3.5.1.6. Formato de Respuesta SIP

SIP/2.0 200 OK

Via: SIP/2.0/UDP

site4.server2.com;branch=z9hG4bKnashds8;received=192.0.2.3

Via:SIP/2.0/UDP

site3.server1.com;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2

Via: SIP/2.0/UDP

pc33.server1.com;branch=z9hG4bK776asdhds;received=192.0.2.1

To: user2 <sip:user2@server2.com>;tag=a6c85cf

From: user1 <sip:user1@server1.com>;tag=1928301774

Call-ID: a84b4c76e66710@pc33.server1.com

CSeq: 314159 INVITE

Contact: <sip:user2@192.0.2.4>

Content-Type: application/sdp

Content-Length: 131

---- User2 Message Body Not Shown ---- (Patiño Cardona, 2014)

2.3.5.1.7. Esquema de funcionamiento

Registro de usuarios: Deben registrarse los usuarios para que puedan ser encontrados por otros. Los terminales envían la petición REGISTER, donde los campos “from” y “to” pertenecen al usuario a registrar. El servidor Proxy actúa como “Register” y consulta si el usuario puede ser autenticado, en caso positivo envía un mensaje de OK. (López & Rodríguez, 2008)

Establecimiento de sesión: El usuario origen hace una petición INVITE al Proxy. En seguida, para detener las retransmisiones, el Proxy envía un TRYING 100 y reenvía una petición al usuario Destino. Cuando el teléfono comienza a sonar, el destino envía un RINGING 180 el cual también es reenviado por el Proxy hacia el usuario origen. Finalmente, con el OK 200 se acepta la llamada. El usuario destino toma el auricular. (López & Rodríguez, 2008)

Llamada establecida. Funciona el protocolo de transporte RTP con los parámetros determinados en la negociación a través del protocolo SDP. Dichos parámetros son: puertos, direcciones, codecs, etc. (López & Rodríguez, 2008)

Finalización de llamada: La finalización se realiza con una petición BYE que se envía al Proxy y seguidamente reenviada al usuario destino, éste contesta enviando un OK 200 y confirma que se recibió el mensaje de finalización de forma correcta. (López & Rodríguez, 2008)

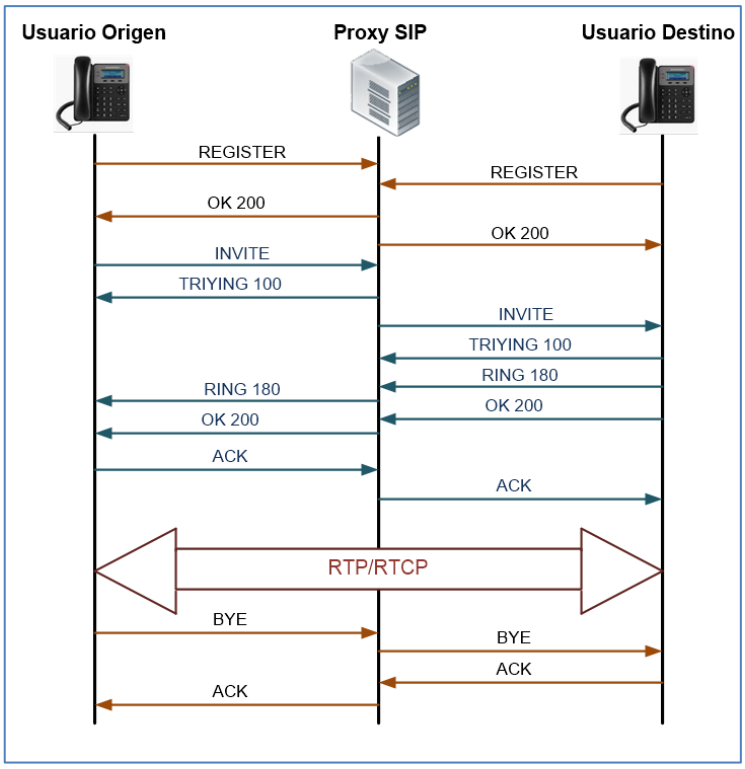


Figura 2.9: Esquema del funcionamiento de una llamada SIP
Fuente: (Patiño Cardona, 2014, p. 65)

2.3.5.1.8. Protocolos usados por SIP

- **TCP/UDP:** Se utiliza en el transporte de la información de señalización. (López & Rodríguez, 2008)
- **DNS:** En la resolución de nombres de servidores en base a la dirección de destino**.** (López & Rodríguez, 2008)
- **RTP (***Real Time Protocol***):** En el transporte de voz, datos y video a través de varios Codecs. (López & Rodríguez, 2008)
- **RTSP (***Real Time Streaming Protocol***):** Para control del envío de media streaming. (López & Rodríguez, 2008)
- **XML (***eXtensible Markup Language***):** En la transmisión de información de eventos. (López & Rodríguez, 2008)
- **MIME (***Multipurpose Internet Mail Extension***):** Para la descripción del contenido en Internet. (López & Rodríguez, 2008)
- **HTTP (***Hypertext Transfer Protocol***):** En la sintaxis y semántica, los mecanismos de autenticación, etc**.** (López & Rodríguez, 2008)

- **SAP (***Sesion Advertisement Protocol***):** Via multicast, en la publicación de sesiones multimedia, durante la comunicación bajo el protocolo SIP el usuario es el dueño de su sesión. (López & Rodríguez, 2008)

2.3.5.1.9. Agentes de Usuario (User Agent, UA)

- **Agente de usuario cliente** (UAC): Hace las peticiones SIP y recepta las respuestas. (López & Rodríguez, 2008)
- **Agente de usuario servidor** (UAS): Da respuesta a las peticiones. (López & Rodríguez, 2008)

Los Agentes realizan acciones como estas:

- Localizan a un usuario re-direccionando la llamada.
- Si no hay respuesta, implementan servicios de redirección como reenvío.
- En función del origen o el destino de las llamadas, implementan filtrado.
- Guardan información sobre administración de llamadas.

2.3.5.1.10. Servidores SIP

- **Proxy Server**: Es un dispositivo intermedio que actúa como cliente y servidor para establecer llamadas entre los usuarios. Realizan retransmisiones de solicitudes y eligen el otro servidor al cual deben remitir, si es necesario, alteran los campos de la solicitud. Hay dos tipos: Statefull Proxy y Stateless Proxy. (Patiño Cardona, 2014)

- **Statefull Proxy:** Durante el procesamiento de las peticiones SIP, mantienen las transacciones en su estado. (Patiño Cardona, 2014)

- **Stateless Proxy:** Durante el procesamiento de las peticiones, no mantienen las transacciones en su estado, únicamente reenvían mensajes. (Patiño Cardona, 2014)

- **Registrer Server:** Acepta las peticiones de registro de los usuarios y guarda la información de estas peticiones para brindar un servicio de traducción y localización de direcciones en el dominio que controla. (Patiño Cardona, 2014)

- **Redirect Server:** Genera respuestas de redirección por cada petición que recibe. Este servidor re-direcciona las peticiones hacia el servidor siguiente. (Patiño Cardona, 2014)

2.3.5.2. Protocolo IAX / IAX2

El protocolo IAX (*Inter-Asterisk eXchage protocol*) es utilizado para gestionar conexiones VoIP ya sea entre servidores Asterisk, o entre servidores y clientes. El objetivo con el que se creó este protocolo fue minimizar la tasa de bits requerida en las comunicaciones VoIP y tener un soporte nativo para traspasar dispositivos de NAT (*Network Address Translation*). 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. Surge también, para corregir algunos de los problemas principales del protocolo SIP. (Patiño Cardona, 2014)

- Minimiza el ancho de banda de las transmisiones de control y multimedia
- Cambia el protocolo de texto a protocolo binario.
- Evita problemas de NAT (*Network Address Trnaslation*). Usa UDP sobre el Puerto 4569 para pasar información de señalización y datos.
- Soporta transmisión de planes de marcación. (Patiño Cardona, 2014)
- La estructura básica de IAX se fundamenta en la multiplexación sobre un solo puerto UDP de la señalización y el flujo de datos entre dos sistemas. IAX2 utiliza solo un puerto UDP (4569) para comunicaciones entre terminales VoIP para señalización y datos. El tráfico de voz es transmitido junto con la voz *(in-band*), es casi transparente a los corta fuego. (Salcedo et al., 2012)

IAX2 soporta *Trunking*, por lo tanto, puede enviar datos y señalización de varios canales por un mismo enlace, como un multiplexor. Cuando está en modo troncal, un datagrama IP puede contiene información de una o de varias llamadas sin aumentar latencia. No tener que enviar la cabecera IP varias veces resulta en una disminución de la tasa de bits y del retraso de paquetes. IAX2 es un compendio de estándares de señalización y de transmisión de datos seleccionados de otros protocolos como SIP, MGCP y RTP. (López & Rodríguez, 2008)

2.3.5.2.1. Tramas de IAX2

Hay dos tipos de tramas IAX2: Tramas F (*Full Frames*) y Tramas M (*Mini Frames*). Las tramas completas se transmiten cuando las cabeceras llevan la información necesaria para establecer la comunicación, en las tramas menores las cabeceras suprimen esta información porque la comunicación ya está establecida y se está transmitiendo solo la voz. (Patiño Cardona, 2014)

- **Trama F (Full Frame):** Las tramas F contienen una cabecera con muchos campos, los mensajes F se deben responder de manera explícita. (Patiño Cardona, 2014)

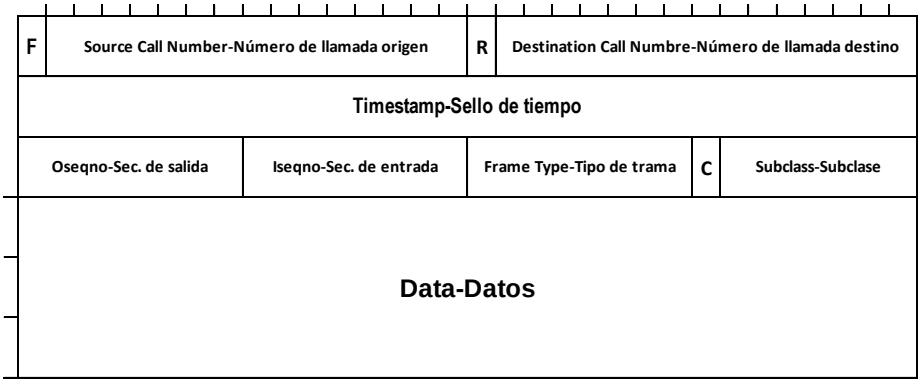


Figura 2.10: Esquema de una trama F
Fuente: (López & Rodríguez, 2008, p. 37)

- **Trama M (Mini Frame):** Se envía mucho menos información en la cabecera de las tramas M y no hay la obligación de ser respondidas,

podrían perderse durante la transmisión y solo serían descartadas. (Patiño Cardona, 2014)

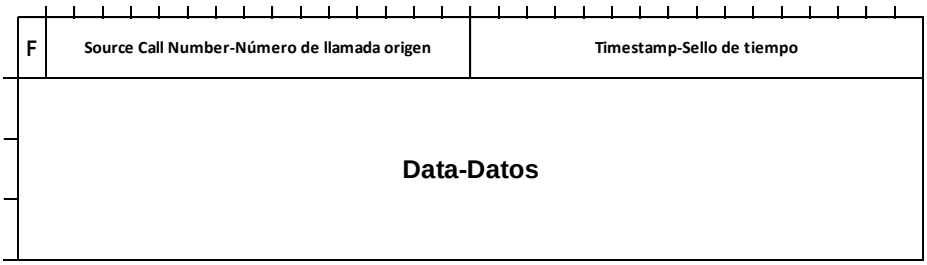


Figura 2.11: Esquema de una trama M
Fuente: (López & Rodríguez, 2008, p. 37)

2.3.5.2.2. Fases de una llamada IAX2.

- **Establecimiento de la llamada:** El terminal A Origen inicia una conexión y manda un mensaje "new". El terminal B Destino responde con "*accept*" y el origen le responde con "Ack". Seguidamente, el origen envía las señales de "*ringing*" y el Destino confirma la recepción del mensaje con un "Ack". Finalmente, el Destino acepta la llamada con un "*answer*" y el llamante confirma ese mensaje.(López & Rodríguez, 2008)

- **Flujo de datos o flujo de audio:** Se envían los Frames M y F en ambos sentidos con la información de voz. Los Frames M contienen una única cabecera de 4 bytes para ofrecer el uso en el ancho de banda. Los Frames F son completos e incluyen información de sincronización. (Patiño Cardona, 2014)

- **Liberación de la llamada o desconexión:** La liberación es igual a enviar un mensaje de "*hangup*" y confirmarlo. (Patiño Cardona, 2014)

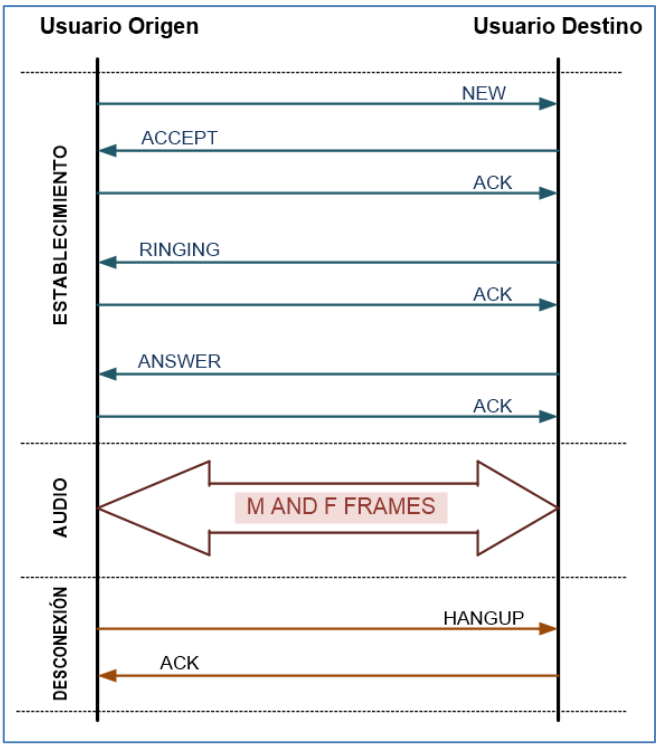


Figura 2.12: Fases de llamada IAX2
Fuente: (López & Rodríguez, 2008)

2.3.5.3. Protocolo SDP

SDP: "*Session Description Protocol*" (Protocolo de descripción de sesión). Establece un procedimiento estándar en la definición de los parámetros durante el intercambio de media streaming entre dos endpoints (puntos finales). Publicado por el IETF en la RFC 4566. El SDP es normalmente encapsulado dentro del protocolo SIP en las aplicaciones de Telefonía IP. El protocolo SDP es una declaración, por un endpoint media, de sus especificaciones de recepción y capacidades; una declaración SDP realiza las siguientes especificaciones: (Sousa & Carrapatoso, 2003)

Especificaciones de recepción

- Identifica la dirección IP que está lista para recibir la transmisión de media entrante.
- El tipo de media que está esperando recibir el endpoint.
- Identifica el protocolo que está esperando el endpoint para intercambiar información, normalmente el protocolo RTP.

- Identifica el tipo de codificación de compresión puede utilizar el endpoint para decodificar (*codec*). (Sousa & Carrapatoso, 2003

Capacidades

- Cuál número de puerto está escuchando para la transmisión de media entrante. (Sousa & Carrapatoso, 2003

- En una configuración de sesión, participan dos endpoints, donde cada uno envía un SDP para informar al otro endpoint sobre sus especificaciones y capacidades. SDP solo se limita a la negociación de un conjunto de especificaciones y capacidades compatibles para el intercambio de parámetros de media, no transmite media; las transmisiones de media son realizadas por un canal y protocolo diferente.(Sousa & Carrapatoso, 2003)

2.3.5.4. Protocolo RTP

RTP (*Real-time Transport Protocol*) Protocolo de nivel de aplicación por medio del cual se puede transmitir información (audio o vídeo) en tiempo real, extremo a extremo sobre una red de fragmentos o paquetes. Después de su publicación en 1996 tuvo varias actualizaciones. Permite transmisión y entrega de datos con multidifusión (multicast: método de envío de información a múltiples destinos en una misma transmisión) para aplicaciones de videoconferencia, streaming y otras. RTP no garantiza la calidad del servicio ni el no-retraso en la entrega de datos, deja ese trabajo a capas más bajas que controlen la reserva de recursos (Sousa & Carrapatoso, 2003)

RTP trabaja junto al protocolo de control, RTCP. RTP envía los paquetes de datos y RTCP provee servicios de control entre otras funciones. Hay una versión llamada SRTP (*Secure* RTP) que se emplea para incluir características de cifrado al canal RTP. (Sousa & Carrapatoso, 2003)

RTCP (*RTP Control Protocol*) proporciona calidad de servicio mediante el envío de información de control en la sesión RTP entre el emisor y el receptor que facilitan la verificación de extremo a extremo. El protocolo RCTP soporta solo las necesidades más básicas de comunicación de una aplicación. RTCP permite a los receptores de una sesión informar al emisor sobre la calidad de su recepción, el número de paquetes perdidos, la variación en la latencia (*jitter*) y el tiempo que le tomó a un paquete en hacer el trayecto, ser entregado en el extremo receptor y volver al extremo emisor (RTT: *Round Trip Time*). (Sousa & Carrapatoso, 2003)

Los paquetes RTCP no incrementan el tráfico en proporción al aumento de la cantidad de agentes que participan en una sesión, ajustan de acuerdo al tráfico los intervalos en que se envían los paquetes. RTCP transmite periódicamente a todos los participantes de una sesión los paquetes de control. (Sousa & Carrapatoso, 2003)

RTSP (*Real-Time Streaming Protocol*) es un protocolo que se usa para optimizar el flujo de datos de tipo multimedia. Trabaja a nivel de Aplicación y tiene similitud con el protocolo HTTP por su sintaxis y funcionamiento, con peticiones que pueden ser solicitadas desde el cliente o el servidor. Sin embargo, se distingue del HTTP en que, el protocolo RTSP requiere conservar información de estado. (Sousa & Carrapatoso, 2003)

Debido a su parecido con el HTTP, tiene como ventajas que: puede ser adaptado tanto a proxys como a firewalls y tiene compatibilidad con la difusión del tipo multicast, eso le da la capacidad de enviar en un solo paso la información a un grupo de clientes. Por otro lado, sobre la capa de transporte, puede utilizar de manera independiente tanto TCP como UDP. (Sousa & Carrapatoso, 2003)

Entre sus desventajas se destaca que: su funcionamiento es vulnerable cuando hay congestión de red, esto hace que, durante la

transmisión la pérdida de paquetes no se puede evitar ni predecir; y, cuando la transmisión es en modo *unicast*, requiere de gran ancho de banda. (Sousa & Carrapatoso, 2003

El protocolo RSVP (*Resource ReserVation Protocol*), sirve para garantizar la calidad de servicio en la transmisión, tomando en cuenta la longitud variable de los paquetes IP y que el tráfico de datos se envía como ráfagas de bits. El RSVP se encarga de eliminar las veces en las que la voz se pierde por efecto de una ráfaga de datos que existe en la red. Cuando existe congestión en un router, RSVP solicita ancho de banda, particiona los paquetes de datos más grandes y prioriza a los paquetes de voz. La calidad de servicio que ofrece RSVP no llega a ser comparable a la de redes avanzadas como ATM, que proveen QoS (Quality of Service) por defecto de forma estándar. (Sousa & Carrapatoso, 2003)

2.3.5.5. Protocolo H.323

Predecesor del SIP, el H.323 fue el protocolo con el que inició VoIP, sin embargo, hoy está en desuso, ya que el protocolo SIP se creó para solucionar los problemas que presentaba. H.323 inicialmente fue creado para establecer sesiones multimedia sobre redes locales, es un grupo de estándares para la transmisión de elementos multimedia sobre redes que no ofrecen calidad de servicio (QoS). (López & Rodríguez, 2008)

El protocolo H.323 fue pionero en facilitar la convergencia de voz, video y datos en las comunicaciones multimedia. H.323 utiliza en características de un grupo de protocolos que cubren los distintos aspectos de la comunicación. Es un protocolo cliente-servidor utiliza dos tipos de señalización: (López & Rodríguez, 2008)

- **Señalización de control de llamada (H.225):** Para el control de registro y localización. Este protocolo tiene dos funcionalidades:

- ✓ Cuando hay un **Gatekeeper** en la red, define el procedimiento de registro de un terminal en el gatekeeper. Este proceso se denomina RAS (Registration, Admission and Status) y usa un canal separado identificado como canal RAS. (López & Rodríguez, 2008)

- ✓ Cuando no hay un **Gatekeeper**, define procedimiento de dos terminales para establecer o terminar llamadas entre sí procedimiento conocido como *Señalización de llamada*. (López & Rodríguez, 2008)

- **Señalización de control de canal (H.245**): Para el control del establecimiento de llamadas.

  Cuando un Gatekeeper está presente en la red, se usa RAS. El Gatekeeper es un dispositivo opcional que se usa para cumplir la función de control de admisión; permite el establecimiento de llamadas estando como intermediario entre los puntos terminales. Otras de las funciones es direccionar la señalización hacia otro dispositivo para ejecutar otras acciones como desvío de llamadas. (López & Rodríguez, 2008)

2.3.5.5.1. Fases de la comunicación usando H.323

Los aspectos de la comunicación H323 se definen en varias fases:

- **Direccionamiento o establecimiento de la llamada**

El direccionamiento se realiza mediante el protocolo RAS, este protocolo de comunicaciones permite a una estación H.323 localizar a otra estación H.323 cuando hay en la red un Gatekeeper intermediario entre las estaciones. H.323 también puede realizar la función de direccionamiento por medio del protocolo DNS, de forma análoga al protocolo RAS, pero por medio de un servidor DNS. (Dimas & Morales, 2009; López & Rodríguez, 2008)

- **Transmisión de voz**

H.323 utiliza el protocolo UDP para la *transmisión de datos*; lo importante es utilizar los recursos de mayor velocidad de transmisión de UDP en comparación con TCP, aun cuando UDP no garantice la integridad de los datos. (Dimas & Morales, 2009; López & Rodríguez, 2008)

En la fase de *transmisión de voz*, se inicia una negociación mediante el protocolo H.245 (control de canal); también se realiza el intercambio de los mensajes (petición y respuesta) entre los dos terminales. (Dimas & Morales, 2009; López & Rodríguez, 2008)

Además, para la función de *temporización*, se utiliza el protocolo de tiempo real RTP que se encarga dicho proceso, etiquetando los paquetes UDP para que sean identificados durante la entrega de estos en recepción. (Dimas & Morales, 2009; López & Rodríguez, 2008)

- **Control de la transmisión o Audio**

Para la función de control de la transmisión entre los terminales, se utiliza el protocolo RTCP que puede detectar la congestión en la red y aplicar acciones de corrección. (Dimas & Morales, 2009; López & Rodríguez, 2008)

- **Desconexión**

En la fase de desconexión, cualquiera de los usuarios participantes activos (terminales) en la comunicación puede dar inicio al proceso de finalización de llamada, una vez iniciado, ambos terminales tienen que informar al Gatekeeper que la comunicación ha finalizado. (Dimas & Morales, 2009)

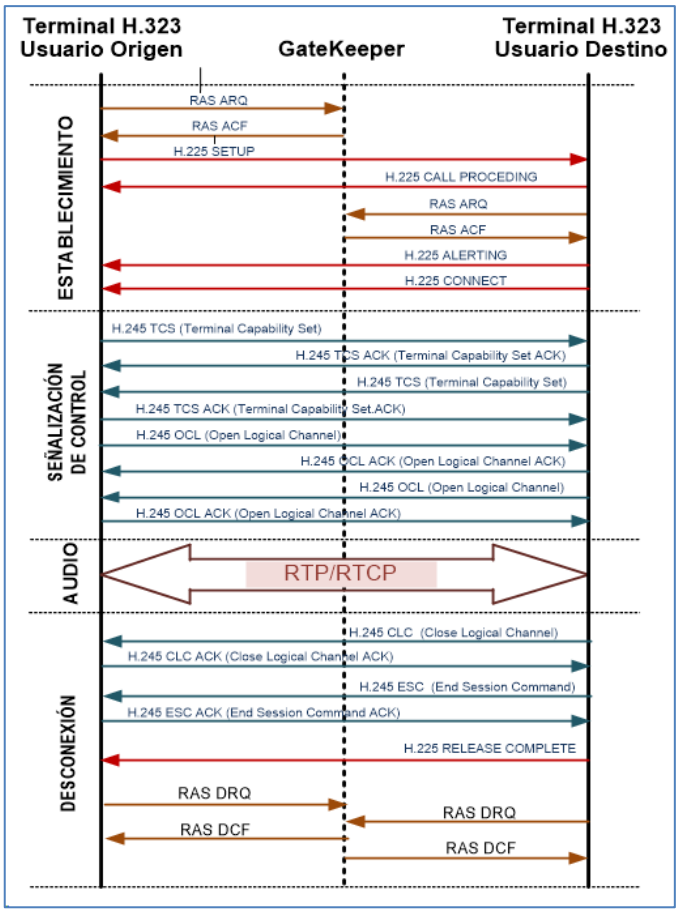


Figura 2.13: Llamada usando H323

Fuente: Autor

2.3.5.5.2. Componentes del protocolo H323

Para el análisis de los componentes del protocolo H.323 a continuación se mencionan los principales:

• **Terminal:** Los terminales son los puntos extremos de la red, un terminal H.323 envía comunicaciones bidireccionales con otro terminal, un gateway o un MCU (Unidad de Control Multipunto). (Dimas & Morales, 2009; González, 2011)

• **Gateway**: Un gateway H.323 es un dispositivo de borde que proporciona, en tiempo real, comunicaciones de doble dirección entre terminales H.323 de una red IP con terminales o gateways de una red conmutada, entre otros. Su objetivo es ser transductor para reflejar las características de un extremo en la red IP hacia otro en una red

conmutada y viceversa de manera transparente. (Dimas & Morales, 2009; González, 2011)

• **Gatekeeper**: El gatekeeper es un elemento que hace el control de acceso a la red de los terminales H.323, Gateways y MCUs, además la traducción de direcciones. El Gatekeeper realiza dos funciones de control de llamadas. Una es la gestión del ancho de banda y la segunda.es la traslación de direcciones de los terminales de la red LAN a las IP correspondientes. (Dimas & Morales, 2009; González, 2011)

• **MCU**: La Unidad de Control Multipunto tiene la función de soportar la comunicación entre tres o más puntos, bajo el estándar H.323. (Dimas & Morales, 2009)

• **Controlador Multipunto**: Es un componente de H.323 que, para mantener los niveles de las comunicaciones, proporciona capacidad de negociación con todos los terminales. (Dimas & Morales, 2009; González, 2011)

• **Procesador Multipunto:** Mezcla, conmuta y procesa audio, vídeo y flujo de datos para los participantes de una conferencia. Es un componente H.323 de hardware y software especializado. (Dimas & Morales, 2009; González, 2011)

• **Proxy H.323:** Es un servidor que provee acceso a redes seguras a los usuarios, es decir, les permite el acceso de unas a otras redes confiando en la información de la recomendación H.323, se envía información en tiempo real a un destino seguro. (Dimas & Morales, 2009)

2.3.6. Centrales PBX-IP

Las señales digitales han desplazado a las analógicas y la tendencia mundial es hacia la Transformación digital. Esta corriente transformadora ya tiene más de una década y actualmente existe una gran competencia para convertir todos los dispositivos eléctricos y electrónicos en parte de la red mundial IP desde la cual controlar su funcionamiento. (Soler Palacín, 2009)

Una de esas transformaciones se produjo como consecuencia de la Convergencia de las redes, en el campo de la telefonía tradicional - PSTN - cuando esta tecnología se ha visto desplazada por aquella que utiliza el protocolo IP para transmitir también la voz - PBX-IP -, tal es así que actualmente hablar de centrales telefónicas analógicas dentro de una empresa privada es casi imposible, Múltiples alternativas PBX-IP tanto propietarias como de código abierto han desplazado las centrales análogas, y hoy en día se han implementado en la mayoría de las empresas para abaratar costos y unificar servicios. (Soler Palacín, 2009)

2.3.7. Asterisk

Asterisk es un software libre (de código abierto o de licencia GPL) que funciona como una centralita telefónica IP, está basado en Linux y fue creada por Marc Spencer en el año 1999. Asterisk funciona como un PBX-IP (*Private Branch Exchange*) pero es administrado desde un computador personal. Como cualquier PBX, se puede conectar una cantidad determinada de teléfonos dentro de una red privada para hacer llamadas entre sí como extensiones y además conectar a un proveedor de VoIP o a una RDSI tanto básicos como primarios. (García de Vinuesa Ordovás, 2012)

Asterisk algunas funciones que anteriormente sólo estaban disponibles en sistemas propietarios PBX. Los programadores pueden crear nuevas funcionalidades escribiendo un dial plan usando el lenguaje de script de Asterisk o incluyendo módulos escritos en algún lenguaje de

programación soportado en GNU/Linux. Asterisk ofrece una variedad de funciones avanzadas como: (García de Vinuesa Ordovás, 2012)

- Gestión de llamadas con menús interactivos **IVR:** *Interactive Voice Response*.
- Encaminamiento de llamadas por el proveedor VoIP más económico **LCR:** *Least Cost Routing*.
- Integración con todo tipo de aplicaciones externas **AGI:** *Asterisk Gateway Interface*
- Gestión y control remoto de Asterisk **AMI:** *Asterisk Management Interface*.
- Base de datos **BB.DD**: Información de usuarios, llamadas, extensiones, proveedores

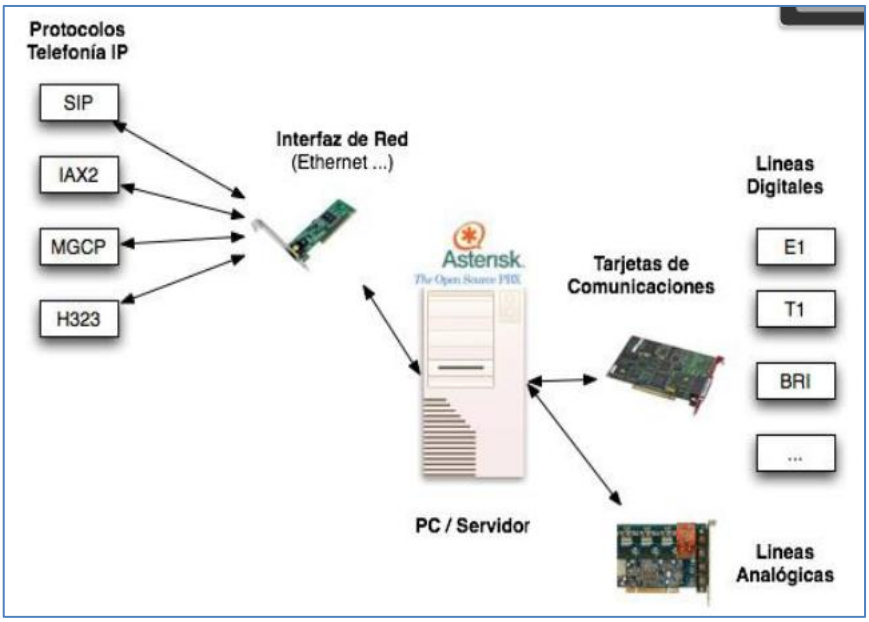


Figura 2.14: Esquema de conexión Asterisk
Fuente: (López & Rodríguez, 2008, p. 36)

Asterisk permite que la Telefonía IP pueda realizar todas las funciones características de la Telefonía Tradicional, Además incorpora una serie de nuevas funciones como: Grabación, Monitoreo y Transferencia de llamadas, Música y Llamadas en espera, Llamadas de emergencia, Autenticación e Identificación de usuarios, Administración e integración de Bases de Datos, Interfaz web, tráfico y otras funciones. Por

el tipo de tecnología y la convergencia con la red IP, la central Asterisk le otorga a la Telefonía IP marcadas ventajas respecto a la telefonía tradicional, algunas de las cuales se indican a continuación. (García de Vinuesa Ordovás, 2012)

Menores costos en instalación y mantenimiento: Es más fácil contratar proveedores de servicios, actualmente todos operan en línea a través de Internet y dan servicio desde cualquier localización. La integración de los dos servicios voz y datos en una misma red, la de datos, también genera ahorro en mantenimiento e instalación. Se puede ahorrar entre un 60% a un 80% en el costo de las llamadas con respeto al costo actual en llamadas de la telefonía convencional. (García de Vinuesa Ordovás, 2012)

- Mejora de la productividad y la atención al cliente que permite Asterisk le dan a la telefonía IP una ventaja competitiva respecto de la telefonía convencional.

- Mayor movilidad: La posibilidad que brinda la Telefonía IP de trasladar la línea telefónica o la extensión a cualquier lugar del mundo a través de Internet facilita la movilidad.

- Escalabilidad: La arquitectura de la Telefonía es escalable y muy flexible. Su instalación y configuración son simplificadas y conforme a la red del administrador. (Dimas & Morales, 2009)

- Compatibilidad: La telefonía IP está basada en estándares lo que incluye protocolos de comunicación de la capa OSI, por este motivo es compatible con hardware de diferentes fabricantes y proveedores de equipos de comunicación. (Dimas & Morales, 2009; López & Rodríguez, 2008)

- Flexibilidad: Por las diferentes opciones de formas de acceso: por Líneas Dedicadas, Cable-módem (coaxial, fibra óptica, UTP), ADSL, etc.

- Integración: Tanto los proveedores de servicios de telecomunicaciones como los usuarios de redes privadas pueden integrar los servicios datos, voz, video e Internet en una misma red, esta integración ha dado paso a la convergencia de las Telecomunicaciones. (Dimas & Morales, 2009; González, 2011)

2.3.7.1. Conceptos de Asterisk

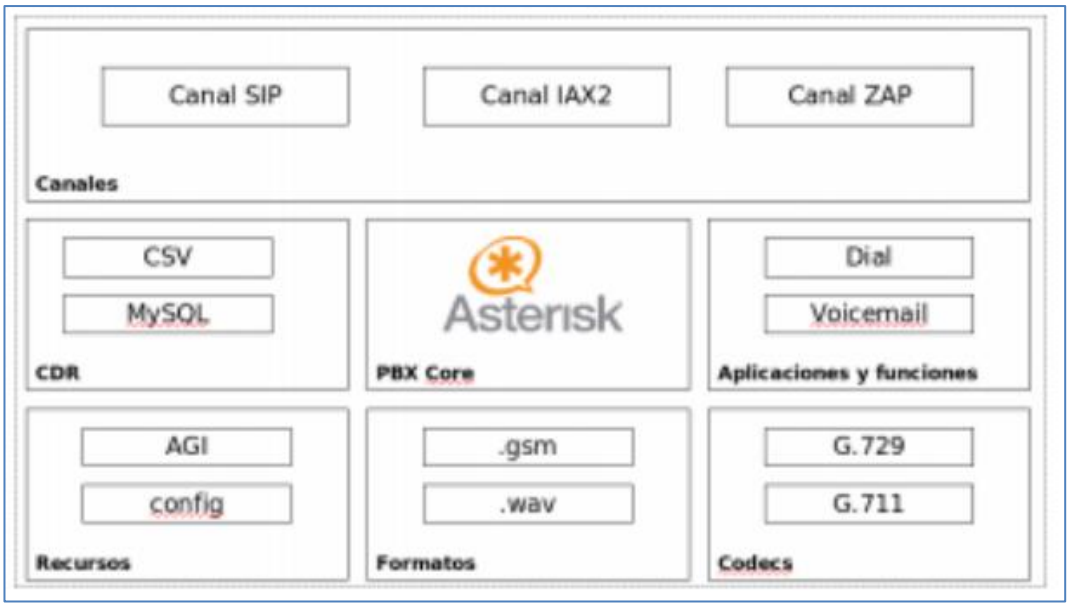


Figura 2.15: Módulos de Asterisk
Fuente: (López & Rodríguez, 2008, p. 37)

Canal: Una conexión que conduce una llamada entrante o saliente hacia o desde la red telefónica IP es un canal. De la misma manera la conexión puede venir desde o dirigirse hacia un sistema analógico tradicional, digital u otro sistema VoIP. Por defecto, Asterisk soporta una serie de canales para conducir información, los más relevantes: (López & Rodríguez, 2008)

- Canales: H.323, IAX2, SIP, MGCP

- Consola
- Canales Zap: Para líneas analógicas y digitales.

Dial plan: Un plan de discado es la configuración de la centralita Asterisk donde se programa el proceso que sigue una llamada desde que entra o sale del sistema VoIP hasta que se establece la comunicación con el terminal llamado. (López & Rodríguez, 2008; Patiño Cardona, 2014)

Extensión: Una extensión es una conexión interna programada en la centralita para ocupar un canal lógico y transmitir voz a través de dicho canal. En Asterisk, una extensión es una lista de comandos a ejecutar y no necesita estar asociada a una línea telefónica como ocurre en la telefonía analógica. (López & Rodríguez, 2008)

Contexto (**Context):** Un contexto es un grupo de extensiones que se clasifican de acuerdo el tipo de llamadas que se realizan, cada grupo o contexto tiene su programación dentro del Dial plan de Asterisk. (López & Rodríguez, 2008; Patiño Cardona, 2014)

2.3.7.2. Codificación de la Voz

En el diseño de una red IP telefónica, se deben considerar todos los parámetros que pueden afectar positiva o negativamente la calidad de la voz, para lo cual se deben utilizar los Codecs adecuados que funcionen mejor y se adapten a las características de la red. Hay una relación proporcional entre la calidad de voz y la velocidad de datos: a mayor velocidad de datos, mayor calidad de voz.

Antes de ser transmitida a través de la red IP, la voz debe ser codificada, esa es la función de los Códec de audio. Los Codecs son algoritmos que realizan la codificación y compresión del audio antes de la transmisión utilizando diferentes métodos: perceptual, paramétrico, de forma de onda o híbrido; para su posterior decodificación y descompresión antes de poder generar un sonido utilizable. Depende del

tipo de Códec implementado en la transmisión, determina el ancho de banda mayor o menor a ocupar. (Patiño Cardona, 2014)

G.711: Estándar de codificación y compresión digital de voz PCM de 64 Kbps. En G.711, la voz es codificada para su transmisión digital sobre la PSTN. Antes de su codificación se realiza la compresión de la señal. Existen dos métodos de compresión que utilizan palabras de 8 bits a 8000 muestras por segundo, es decir 64Kbps: (*G.711 : Modulación por impulsos codificados (MIC) de frecuencias vocales*, s/f)

- μ Law: Se usa en Japón y EEUU
- A Law: Se usa en Europa, Sudamérica y resto del mundo.

G.726: Estándar de Modulación por impulsos codificados diferencial adaptativa MICDA a 40, 32, 24 y 16 Kbps. La aplicación principal de los canales a 24 y 16 kbit/s es para canales de sobrecarga que transportan señal vocal en Equipos de multiplicación de circuitos digitales (EMCD). La aplicación principal de los canales de 40 kbit/s es la del transporte de señales de módem de datos en EMCD, especialmente en módems que funcionan a velocidades superiores a 4800 bit/s. (*G.726 : 40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)*, s/f, p. 1)

G.728: Basado en el concepto de compresión de predicción lineal excitada de código de bajo retardo (LD-CELP). G.728 es muy utilizado para aplicaciones de telefonía sobre redes de paquetes, especialmente VoIP donde se requiere un bajo retraso. Además, G.728 se incluye como parte del estándar internacional de videoconferencia H.320. Opera en tramas de 2.5 milisegundos de voz de entrada, correspondiente a 20 muestras de 16 bits a una velocidad de muestreo de 8000 muestras por segundo. El codificador G.728 comprime cada trama de voz en 40 bits; estos 40 bits se almacenan en 4 palabras de 16 bits, pero solo los 10 bits inferiores son significativos. Para su transporte hacia o sobre la PSTN, la codificación LD-CELP debe convertirse a formato de telefonía pública.

(*G.728 : Codificación de señales vocales a 16 kbit/s utilizando predicción lineal con excitación por código de bajo retardo*, s/f)

G.729: Algoritmo de compresión de voz en segmentos de 10 ms, opera a una tasa de 8 Kbps, pero hay actualizaciones que ofrecen tasas de 64 y 11.8 Kbps. Son cuatro actualizaciones de este estándar, G.729, G.729A, G.729B y G.729AB, cuya diferencia radica esencialmente en la complejidad del algoritmo. La finalidad de los CODEC es reducir la cantidad de bytes de información para ahorrar Ancho de Banda de la red de transmisión de datos además ahorrar espacio de almacenamiento en los dispositivos grabación de la información. La comprensión puede ser: (*G.729 : Codificación de la voz a 8 kbit/s mediante predicción lineal con excitación por código algebraico de estructura conjugada*, s/f)

- Sin pérdidas reales: Se descarta la información redundante.
- Sin pérdidas subjetivas: Se descarta la información redundante y también la irrelevante.
- Con pérdidas: Se descarta la información redundante, irrelevante y parte de la básica. Se obtiene una información semejante a la original, pero con cierta degradación de su calidad.

2.3.7.3. Servicios de Asterisk

En Asterisk se pueden configurar importantes servicios telefónicos como: ACD *System*, IVR, conferencias, *voicemail*, y grabación de llamadas, entre otros.

- **ACD** System (*Automatic Call Distributor*): Un sistema “Distribuidor Automático de Llamadas”, realiza la función de direccionar o encaminar las llamadas entrantes a diferentes operadoras o agentes según el nivel de disponibilidad de estos. Este sistema se encarga de administrar colas de llamadas, inicia en el momento que ingresa una llamada entonces realiza el trabajo de ubicarla en una cola de espera para ser atendida por una operadora cuando esta esté disponible. El ACD distribuye de manera balanceada las llamadas telefónicas

entrantes entre los agentes disponibles del centro de llamadas. (Puente, 2015)

Los recursos necesarios para el funcionamiento del ACD System son:

- Recursos de Software: Asterisk PBX, *Softphone*.
- Recursos de Hardware: terminales IP, como teléfonos IP, diadema con micrófono y audífonos (*headphones*)

- **VoiceMail** (Buzón De Mensajes): Servicio que permite asignar un buzón de mensajes de voz para cada extensión telefónica, este servicio se configura en el archivo voicemail.conf, desde el mismo se puede enviar un mensaje a una dirección de correo electrónico incluido un archivo de audio adjunto. Además, en el archivo voicemail.com se incluye la configuración de todos los procesos relacionados con el buzón de voz. (Puente, 2015)

  Este servicio evita el problema de tener un teléfono con grabadora incluida, para dejar un mensaje de voz. Si se realiza una llamada a un usuario SIP mientras éste no está disponible o no puede contestar, entonces la llamada es re-direccionada al buzón de voz, allí podrá dejar el mensaje, dicho mensaje será enviado al correo electrónico del usuario SIP llamado, cuyo buzón ha sido previamente configurado en dicha extensión. (Puente, 2015)

- **IVR** (Respuesta Interactiva De Voz): Servicio de interacción de la central telefónica con el usuario que realiza una llamada, haciéndole escuchar un menú de voz pregrabado a través del cual se le dan opciones que puede seleccionar por medio del teclado de su teléfono. (Puente, 2015) (Alvarado-Kravarovich, 2012)

  Este servicio está orientado a:

- Direccionar la llamada de acuerdo a la información que da y que recibe el usuario llamante.
- Entregar información automatizada al usuario y almacenar información del mismo por medio de su teléfono a manera de encuestas.
- vender y promocionar servicios adicionales desde la línea telefónica a los clientes.
- Permitir a las empresas que reciben altos flujos de llamadas manejar tráfico de llamadas entrantes por medio del menú interactivo y el servicio de llamada en espera.

Conferencia telefónica: Servicio que permite realizar diálogos simultáneos entre tres o más usuarios a manera de estar dentro de una sala virtual, este servicio se lo utiliza para realizar reuniones telefónicas entre varios usuarios remotos. (Puente, 2015; Patiño Cardona, 2014)

Mensajería Instantánea: Servicio que permite, en tiempo real, el envío y recepción de mensajes. Para brindar este servicio de mensajería instantánea es necesario que los clientes utilicen los servicios de voz y datos al mismo tiempo. (Patiño Cardona, 2014)

Grabación de Llamadas: Asterisk permite que las llamadas sean grabadas entre el usuario que realiza la llamada y el agente que la atiende. Pueden realizarse grabaciones de las conversaciones en curso y ser almacenadas en un archivo ubicado en el disco duro de la central Asterisk o en una unidad externa a la que se direcciona. (Puente, 2015) Hay varios motivos por los que se puede grabar las llamadas, pero en la mayoría de los casos es para: (Puente, 2015; Patiño Cardona, 2014)

- Guardar la evidencia de buen o mal comportamiento del agente o del usuario llamante.
- Evaluar el desempeño del agente que atiende a los clientes.

- Guardar evidencia de aceptación o no de los servicios por parte de los clientes.

Transferencia atendida de llamadas: Es un servicio convencional de telefonía; consiste en la acción de transferir a una extensión la llamada que se está atendiendo, al recibir contestación de la extensión, el usuario que hace de presentador presenta al usuario llamante antes de colgar y establecer la transferencia al usuario destino. El usuario destino puede rechazar la llamada y colgar sin contestar, en ese caso, la llamada retornará a quien contestó inicialmente. Durante el proceso de transferencia, el usuario llamante externa escuchará la música "Música en espera". (García de Vinuesa Ordovás, 2012)

2.3.8. FreePBX

Es una aplicación Web de código abierto con interfaz gráfica de usuario. FreePBX gestiona una centralita IP Asterisk brindando al usuario un ambiente de configuración de líneas y servicios telefónicos. Siendo Asterisk un sistema basado en Linux se requiere un nivel avanzado de conocimientos para su configuración, FreePBX le brinda al usuario toda la funcionalidad de una centralita IP Asterisk en un entorno gráfico de fácil administración. (Chávez, 2007)

2.3.9. Openfire

Openfire es un servidor de colaboración en tiempo real (RTC) con licencia de Open Source Apache. Utiliza el único protocolo abierto ampliamente adoptado para mensajería instantánea, XMPP (también llamado *Jabber*). Es una aplicación web de mensajería instantánea basado en java. Ofrece un sistema versátil para el desarrollo de aplicaciones de mensajería y una interfaz gráfica de usuario, se caracteriza por una fácil administración. (Osorio Pazmiño & Puetate Villarreal, 2015)

2.3.10. Elastix

Elastix es un software de servidor de código abierto para sistemas de comunicaciones unificadas VoIP que agrupa funciones como: centralita telefónica IP, correo electrónico, mensajería instantánea, DHCP, entre otras; cuenta con una interface Web que permite su administración desde un sistema amigable para el usuario. Elastix está basada en otras aplicaciones de código abierto como Asterisk, FreePBX, Openfire y Postfix, aunque también tiene servicio de fax, actualmente existen múltiples opciones de transferencia de documentos.(López & Rodríguez, 2008)

Elastix fue lanzada en el 2006 por Palo Santo Solutions, empresa ecuatoriana que dio soporte hasta el 2016, fecha en la que Elastix es vendida a la empresa 3CX, y en el 2017 con el lanzamiento de 3CX versión para Linux, Elastix es reemplazada marcando el fin del proyecto como *open-source*, de ahora en adelante es propietario.(Andi & Augusto, 2015)

2.4. Seguridades en redes VoIP

2.4.1. Seguridad de la información

En una red de comunicación se debe establecer un procedimiento de seguridad que proteja la información almacenada en las unidades locales y la que circula y se comparte a través de la red. Dentro de una red, la información es el activo más importante de una empresa u organización, y es responsabilidad del administrador de la red definir las políticas de protección, tomar control de los medios de circulación de la información, establecer el proceso de conexión segura de los dispositivos de red, implementar un sistema de protección de la red interna y de las áreas estratégicas donde residen los servidores y los equipos de comunicación.

Para dar seguridad a una red se debe establecer una estrategia o método de defensa. Hasta ahora se conocen dos métodos de defensa que se definen como:

- Defensa en Profundidad
- Defensa Perimetral

2.4.2. **Defensa en profundidad**

Es una estrategia de seguridad que consiste en formar varias líneas de defensa o capas de protección por niveles, donde los elementos constituyentes de cada línea de defensa son las barreras de protección. La profundidad se logra cuando se incrementan las líneas de defensa y el nivel de protección es creciente en cada capa interior.(Jara & Pacheco, 2012, p. 16)

Línea de defensa. La idea de una línea de defensa es formar una zona de protección delimitada por el inicio de otra en orden sucesivo, cada línea estará formada por una o más barreras. Para diferenciar una línea de protección de otra, se debe establecer el tipo de amenazas y de acuerdo con ese tipo clasificar las capas.

Figura 2.16: Defensa en profundidad
Fuente: (Jara & Pacheco, 2012, p. 16)

2.4.3. **Amenazas.**

La información es uno de los activos más importantes de un negocio, para muchos negocios es el más importante; su valor llega a incrementarse debido a la relación de dependencia que existe entre el negocio y la información, los esfuerzos de la Seguridad Informática en una administración de red se centran en mantener la información auténtica, disponible, íntegra y confidencial, si no se logra proteger la información, el negocio estará en riesgo de desaparecer. Desde este punto de vista todo lo que ponga en peligro la autenticidad, integridad, disponibilidad y confidencialidad de la información es una amenaza. (Morales et al., 2014)

Debido a la importancia de la información siempre existen agentes externos a una organización dispuestos a obtener dicha información, la misma que en el mercado negro puede ser vendida a otras organizaciones. Los agentes externos, ya sean organizaciones delictivas, hackers, agentes de gobierno, entre otros; utilizarán diferentes recursos para dirigir ataques destinados a la obtención o destrucción de la información, estos recursos de hardware y software se constituyen en amenazas que una vez dentro de la red interna de una organización pueden poner en peligro la seguridad de la información. Entre las amenazas más conocidas están: los Spam, Los malware (Software malicioso), el Phishing, los Ramsonware, los ataques de fuerza bruta, DDoS, etc. (Pilay & Manuel, 2021)

2.4.4. Vulnerabilidades.

Las redes de comunicaciones están siempre expuestas a ser atacadas por diferentes motivos, aunque ese ataque generalmente no es dirigido, un ataque es el resultado de múltiples vulnerabilidades que existen y no se han podido **prevenir, detectar, eliminar o corregir**. Los ataques provienen desde muchos frentes siempre están ahí esperando una oportunidad de activarse. Los accesos a Internet, los puertos de entrada y salida de datos, el descuido y mal uso de las claves de acceso, los errores de uso del computador, el descuido en el uso de las

herramientas de acceso como el correo electrónico, los permisos de acceso a carpetas compartidas, el uso de medios de almacenamiento infectados de virus, etc., son vulnerabilidades que existen en los entornos de red.(Pilay & Manuel, 2021)

2.4.5. Ataques.

Siempre existen agentes externos dispuestos a intentar obtener la información de una empresa, corporación, institución, entidad pública, etc, para lo cual disponen de recursos de hardware y software como herramientas de ataque. Los ataques a una red de comunicación; a los servidores, PCs, teléfonos IP, equipos de comunicación y demás host conectados en un dominio, son el resultado de la existencia de múltiples formas vulnerar la seguridad de estos equipos en las redes. Estas vulnerabilidades existentes en las redes, son objetivo de ataques que se han ido multiplicando a lo largo de la historia del Internet y las redes de comunicaciones.

2.4.6. Seguridad perimetral.

La seguridad perimetral comprende la primera línea de defensa entre las redes públicas y las redes internas privadas o corporativas de una organización. Este método está basado en el establecimiento de recursos de seguridad en el perímetro externo de la red. Sin embargo, en este método de defensa se pueden definir niveles de confianza que permiten el acceso a usuarios internos y externos a determinados servicios y denegar cualquier tipo de acceso a otros. (Morales et al., 2020)

A diferencia del método en profundidad, donde el método de defensa se analiza por capas, en el método perimetral la defensa de la red se convierte en un perímetro o anillo protector.

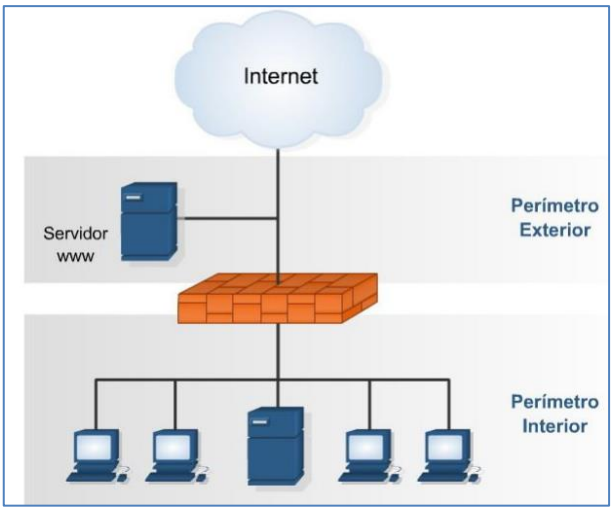


Figura 2.17: Seguridad Perimetral
Fuente: (Arellano, 2005)

Firewall.

Un Firewall (cortafuegos en español) es un equipo de comunicación que permite filtrar el tráfico de entrada y de salida entre equipos de red pertenecientes a una misma red o a redes diferentes. Un firewall es un componente electrónico (hardware) que tiene un sistema de gestión embebido (software) que permite, desde una interface gráfica de usuario o desde una línea de comandos, administrar el tráfico de datos en base a reglas programadas para permitir o denegar la comunicación de entrada o de salida entre equipos pertenecientes a redes diferentes o a una misma red, estos equipos pueden ser: computadores, servidores, equipos de comunicación (como routers, switches, VPN físicas, acces point, etc), equipos telefónicos (teléfonos IP o analógicos, diademas telefónicas, etc), cámaras de vigilancia, dispositivos inalámbricos (smartphones, smart TV, tablets, ect), UPS, lectoras magnéticas, etc. (Morales et al., 2020)

El firewall no es un administrador de ancho de banda, tampoco analizador de paquetes o sniffer, su función es poner una pared o barrera de protección para impedir o permitir la comunicación entre equipos de red. El ancho de banda máximo de trabajo del firewall está determinado por la capacidad que sus interfaces de red (NIC) permiten transmitir: 10, 100, 1000 o 10000 MBps (Mega Bytes por segundo).

2.5. Red de comunicaciones

Una red de comunicaciones es un sistema de interconexión de equipos a través de medios físicos, en una red de comunicaciones se transmite e intercambia información en forma de voz y datos entre equipos remotos a pequeñas y grandes distancias. Todo equipo remoto se convierte en host de la red cuando integra en su hardware el puerto de conexión estándar: la tarjeta de red identificada como NIC (*network interface card*); por medio de la NIC, el equipo accede al medio físico (alámbrico o inalámbrico) que lo conecta a la red. Cada NIC tiene un identificador universal único conocido como MAC (*Media Access Control*) Address, la Mac Address de cada NIC es un identificador de 6 pares de dígitos hexadecimales.

2.5.1. Elementos de una red de comunicaciones

Una red de comunicaciones puede estar conformada principalmente por elementos que se describen como equipos transmisores/receptores, medios de transmisión y datos. Por otro lado, la conectividad lógica de los equipos transmisores/receptores depende principalmente del software de administración y los protocolos de comunicación.

2.5.2. red con telefonía VoIP

Es una red IP donde se incorporan: la central y los teléfonos IP como host de red, a partir de la existencia de los protocolos de transmisión de Voz sobre IP, tales como: SIP, IAX, MGCP, H.323. Con la Telefonía IP, el concepto de red de comunicaciones se expandió, eliminando en las redes corporativas el funcionamiento separado de la red IP y la red telefónica convencional. (López & Rodríguez, 2008)

A partir de la existencia de la red VoIP han aparecido en el mercado diferentes tipos de centrales IP para brindar servicio telefónico; algunas de estas centrales están disponibles en la web y ofrecen su portal para dar servicio telefónico a través del Internet. Actualmente las empresas tienen su propia centralita telefónica, la más utilizada es la conocida como Asterisk, la misma que se instala sobre un computador y tiene su programación sobre Linux. (López & Rodríguez, 2008)

2.5.3. Equipos de comunicación

Dentro de una red de comunicaciones funcionan múltiples equipos que permiten la interconexión de los hosts, algunos de estos equipos son: switches, routers, AP, routers inalámbricos, módems, entre otros; son equipos activos que permiten la conmutación de paquetes y basan su funcionamiento en el protocolo ethernet.

2.5.4. Red de Switches

Los switches (conmutadores), son los equipos activos más usados de una red LAN, permiten la interconexión de hosts y la interconexión de redes, tienen la capacidad de aprender por medio de señales de broadcast las direcciones de red de los equipos y conmutar los paquetes de origen hacia el destino específico a través de sus puertos. Un switch puede operar como un puente entre redes o segmentos de redes, mejora la seguridad de la red. Los modos de funcionamiento de un switch más conocidos son: store-and-fordward y Cut-through; el primero almacena paquetes de datos en un buffer y luego lo envía; el segundo lee los primeros 6 bytes de información y luego encamina el paquete al puerto de salida. (Palacios Oviedo, 2018)

Un switch en su funcionamiento básico es un dispositivo electrónico de capa 2 del modelo OSI (enlace de datos), cuando tiene algunas funciones propias de un router, tales como almacenamiento de tablas de rutas entre otras, es switch capa 3 del modelo OSI (Capa de red). (Palacios Oviedo, 2018)

2.5.5. VLAN

Las VLAN (Virtual LAN) o Redes de Área Local Virtual, se utilizan para crear redes diferentes (subredes) dentro de una sola Red LAN, una técnica de separación de broadcast para brindar seguridad y mejorar la administración de la red. Dentro de un mismo dominio, un switch capa dos que pertenece a una VLAN específica no podrá enviar su broadcast a otra VLAN si no se ha permitido desde un switch capa 3 donde se administran las VLAN de red. De esta forma se pueden aislar las subredes de alta seguridad como por ejemplo la subred de servidores, de otra subred de menor seguridad, ya sea de impresoras o de teléfonos IP entre otras.

2.5.6. Configuración de Switch

Para administrar la red se debe configurar los switches de tal forma que se puedan crear VLANs para dar seguridad a las subredes de equipos de misión crítica; por ejemplo: el datacenter, por medio de la segmentación del broadcast. Esta configuración se debe realizar en un switch capa 3: Primero se crea una red de administración de switches.

2.5.6.1. Red de Administración de Switches

En el switch capa 3, se debe configurar la red administrativa siendo la dirección IP del switch capa 3 principal la puerta de enlace de dicha red, cada switch capa 2 se configura con dirección una dirección IP de esa red de switches y como IP default Gateway se asigna la dirección IP del switch capa 3. Para que haya comunicación entre los switches, se debe configurar el VTP mode del switch capa 3 en modo SERVER y el VTP mode de todos los switches capa 2 en modo CLIENT. Se debe confirmar la comunicación utilizando el comando PING.

2.5.6.2. Creación de VLANs

Para la creación de subredes, en el switch capa 3 se configuran las diferentes VLANs con las direcciones IP designadas para cada subred, estas IPs serán la puerta de enlace de cada subred. En la configuración se asigna la descripción de cada VLAN.

Capítulo 3: Diseño y configuración de una red de comunicaciones.

3.1. Diseño de la red con telefonía VoIP

En la red VoIP los equipos telefónicos se conectan usando interfaces de red (NIC) como cualquier terminal IP, la red se administra desde un servidor Elastix; una aplicación web con interface gráfica de usuario que trabaja como una centralita telefónica basada en Asterisk. Desde la central se gestionan: la PBX IP, las líneas troncales y las extensiones telefónicas con todos los servicios que una central telefónica ofrece. Desde este servidor se configura el servicio DHCP que asigna automáticamente las direcciones IP a todos los equipos telefónicos y demás equipos de red como computadores, impresoras y demás equipos que necesiten IP por asignación automática, no así otros equipos como los servidores, UPS, routers, etc., que se configuran con IP fija desde su propia configuración de red y dichas IPs fijas deben ser reservadas en el servidor DHCP como excepciones, para que no sean asignadas automáticamente a otros equipos.

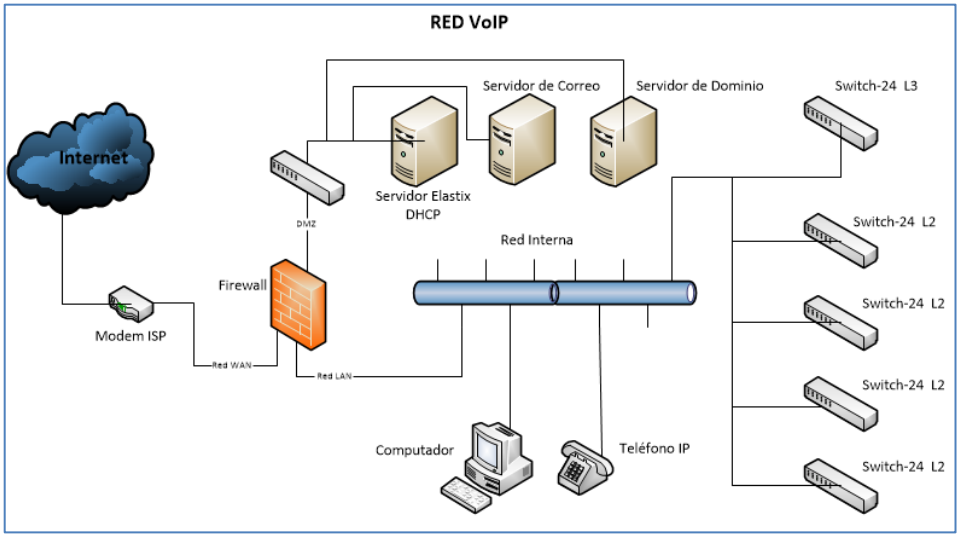


Figura 3.1: Red con telefonía VoIP
Fuente: El Autor.

3.1.1. Cálculo y configuración de la red

La red está conformada por:

- 50 computadores para estaciones de usuarios.
- 50 extensiones telefónicas,
- 1 impresora central.
- 1 servidor Elastix
- 1 Servidor de dominio, DNS y Active Directory (Windows Server)
- 1 Servidor de correo (Windows Server)
- Servidores de aplicaciones de usuario.
- Modem de acceso a Internet con 4 direcciones IP públicas
- 1 firewall cisco ASA
- 1 switch cisco capa 3
- 2 switches cisco de 24 puertos
- 3 switches PoE cisco de 24 puertos

3.1.2. Asignación de direcciones IP

Son 50 equipos de computación, clasificados en:

- 5 estaciones para cargos ejecutivos,
- 10 para cargos administrativos y
- 35 para cargos operativos.

  Las estaciones telefónicas no son compartidas, entonces se asigna la misma cantidad de teléfonos IP de acuerdo a la distribución de funciones especificada. Hay 1 servidor para dominio, DNS y Active directory, 1 servidor de correo y 1 servidor de telefonía Elastix.

- Se asigna la red 192.168.10.0/24 para servidores.
- Se asigna la red 192.168.200.0/24 para equipos de comunicación.
- Se asigna la red 192.168.20.0/24 para equipos de computación.
- Se asigna la red 192.168.30.0/24 para teléfonos.

Tabla 3. 1

RED SERVIDORES	RED SWITCHES	RED USUARIOS DATOS	RED USUARIO VOZ
Vlan 10	Vlan 200	Vlan 20	Vlan 1
192.168.10.0/24	192.168.200.0/24	192.168.20.0/24	192.168.1.0/24

Fuente: El autor

3.1.3. VLAN de Computadores y telefonía

En el switch capa 3 se configura una red LAN virtual (Vlan) para administración, este switch funciona como un ruteador (*router*) desde donde se configura la red interna de dominio y se crean las rutas de acceso a redes WAN privadas y públicas. La configuración de Vlans sirve para separar las redes por departamentos o grupos específicos de usuarios dentro de una organización, de tal forma que hay una red de computadores y equipos de datos y una red de teléfonos IP.

3.1.4. VLAN de Servidores

Se configura una red LAN virtual específica de servidores para separar y proteger todos los equipos de misión crítica dentro de la organización, por medio de reglas de configuración en los equipos de comunicación y en el firewall.

3.1.5. VLAN Administrativa de Equipos de comunicación

Los equipos de comunicación deben conectarse entre sí dentro de una red específica y para poder administrarlos se crea una Vlan administrativa de switches configurada en el switch capa 3 cuya dirección IP será el Gateway. En esta red el switch capa 3 es el Servidor VTP y los switches capa 2 los Clientes VTP.

3.1.5.1. Configuración de Red de Switches

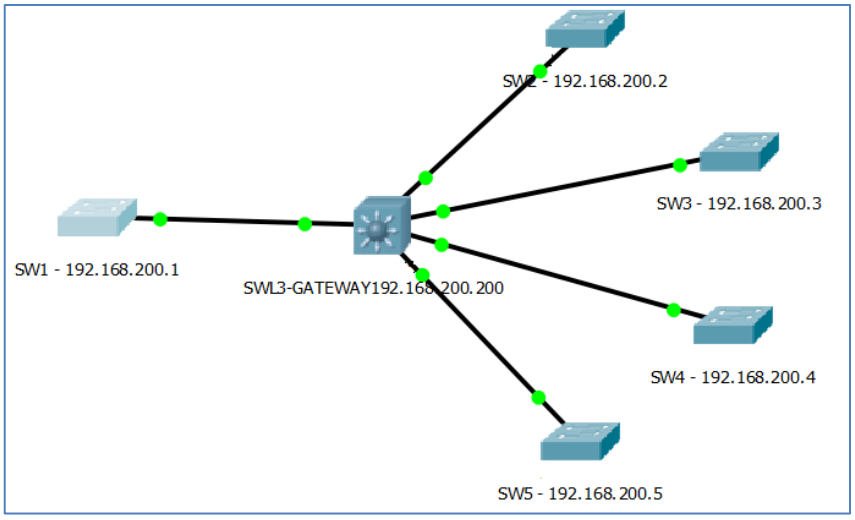


Figura 3.2: Switches en red a través de un Gateway
Fuente: El Autor.

3.1.5.2. Configuración del switch capa 3:

Se configuran y se activan las Vlan 10, 20 y 200; la Vlan 10 para la red de servidores; la Vlan 20 para la red de equipos de usuarios (voz y datos); La Vlan 200 para le red de switches.

- Dirección IP VLAN 10: 192.168.10.250
- Dirección IP VLAN 20: 192.168.20.250
- Dirección IP VLAN 200: 192.168.200.200

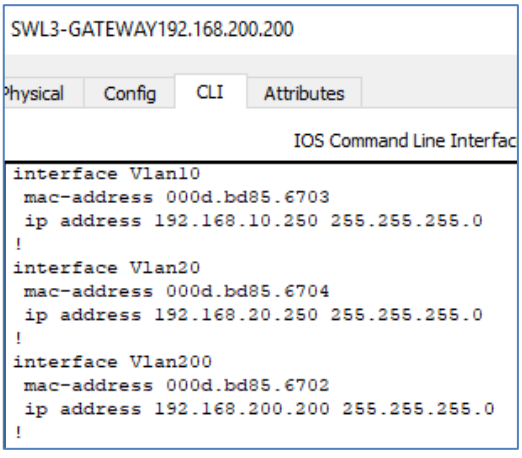


Figura 3.3: configuración vlans en switch capa 3
Fuente: El Autor.

Se configuran en **modo troncal** y se activan las interfaces fastethernet 0/1, fastethernet 0/2, fastethernet 0/3, fastethernet 0/4 y fastethernet 0/5 para la conexión de los switches capa 2.

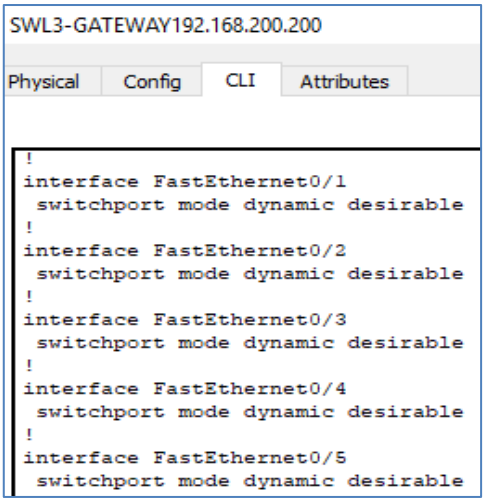


Figura 3.4: Interfaces en modo troncal
Fuente: El Autor.

Se verifica que la configuración VTP (*Vlan Trunking Protocol*) esté en modo operativo servidor (*Server*).

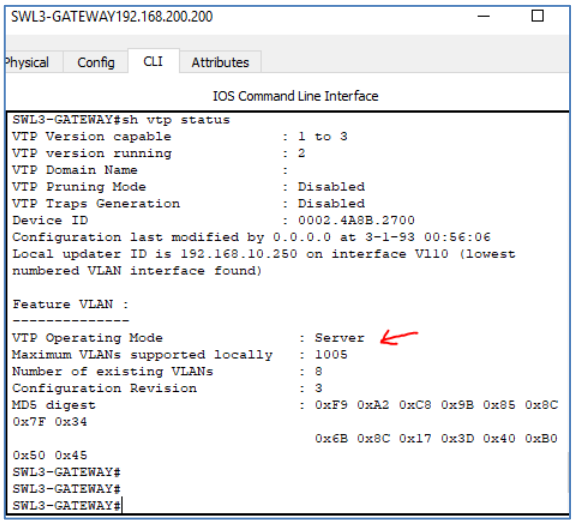


Figura 3.5: Configuración VTP
Fuente: El Autor.

3.1.5.3. Configuración de switches capa 2:

Se configuran en **modo troncal** y se activan las interfaces fastethernet 0/24 de los 5 switches capa 2 para la conexión con las interfaces fastethernet 0/1, fastethernet 0/2, fastethernet 0/3, fastethernet 0/4 y fastethernet 0/5 del switch capa 3.

En el switch 1, se configuran y se activan las Vlan 10 y 200, la Vlan 10 para la red de servidores y la Vlan 200 para la red de switches. Se configura como default Gateway para la red de switches la IP: 192.168.200.200.

Se activan las interfaces fastethernet del 1 al 23 en **modo access** para la conexión de los equipos servidores. Se verifica que la configuración VTP (Vlan Trunking Protocol) esté en modo operativo cliente (Client).

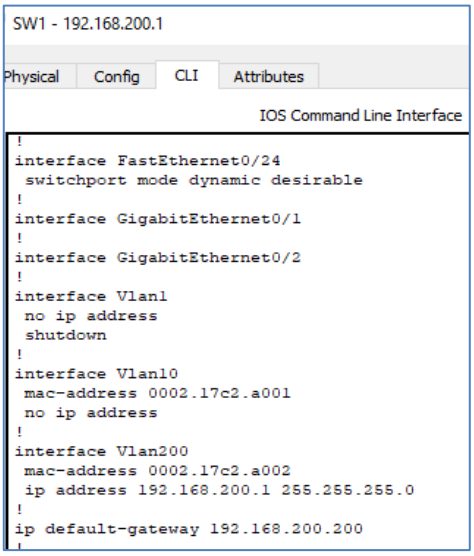


Figura 3.6: Vlan administrativa y gateway

Fuente: El Autor.

En los switches del 2 al 5, se configuran y se activan las Vlan 20 y 200; la Vlan 20 para la red de usuarios y la Vlan 200 para la red de switches. En todos los switches del 2 al 5 se configura como default

Gateway para la red de switches la IP: 192.168.200.200, que corresponde al switch capa 3.

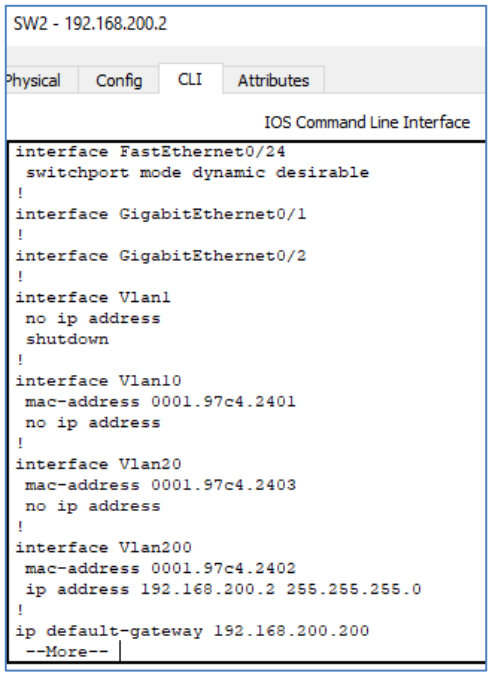


Figura 3.7: Configuración de Vlan y default gateway

Fuente: El Autor.

Se activan las interfaces fastethernet del 1 al 23 en **modo access** para la conexión de los equipos de usuarios.

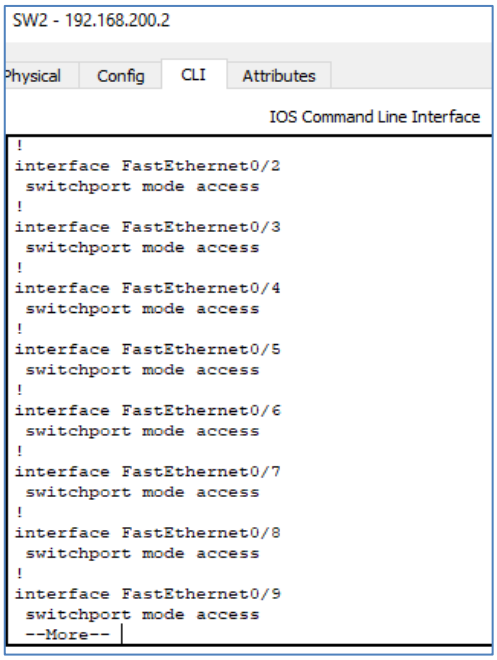


Figura 3.8: Configuración de las interfaces en modo access

Fuente: El Autor

Se verifica que la configuración VTP (Vlan Trunking Protocol) esté en modo operativo cliente (Client).

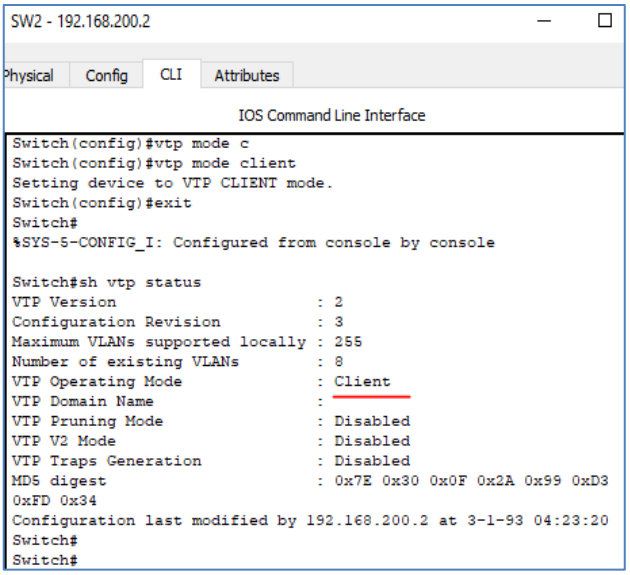


Figura 3.9: VTP en modo CLIENT

Fuente: El Autor.

3.1.5.4. Configuración de host.

Con la conexión de computadores y teléfonos IP a la red de switches se verifica la conectividad de los hosts de red, se comprueba la conectividad entre equipos utilizando el protocolo ICMP.

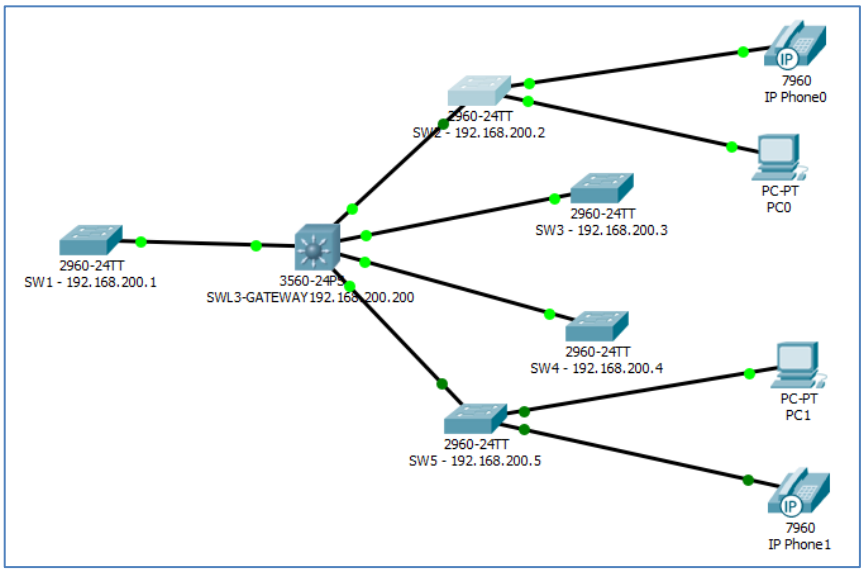


Figura 3.10: Conexión de Hosts (PC y Teléfonos IP)

Fuente: El Autor.

3.1.5.5. Instalación de la central Elastix

Se realiza la instalación del software Elastix en un computador que tenga la capacidad de hardware que soporte la herramienta en funcionamiento normal, especificaciones de referencia son: Intel Core i3, 8 GB de memoria RAM y disco duro de 500 GB a 1 TB. Al iniciar la PC desde el CD instalador de Elastix se muestra la pantalla siguiente:

Figura 3.11: Inicio de Instalación de Elastix
Fuente: El Autor.

Elección del idioma y tipo de teclado; se elige Spanish en este caso:

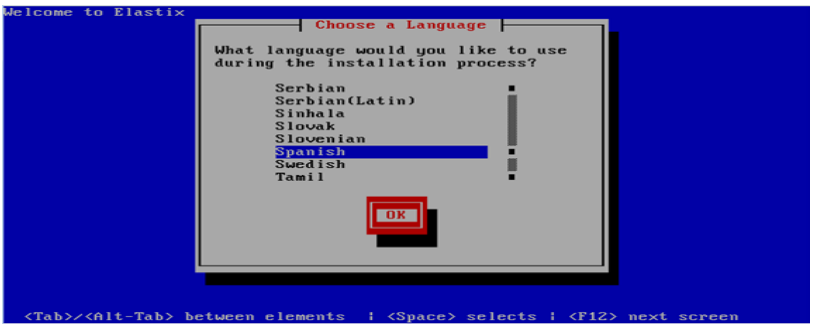


Figura 3.12: Selección de idioma
Fuente: El Autor

El sistema pide inicializar la unidad, se elige SI. Se elige la unidad a particionar con el diseño predeterminado y se da ACEPTAR. Para revisar la capa de particiones se elige SI. Se verifica que está creada la unidad de intercambio Swap, se elige ACEPTAR.

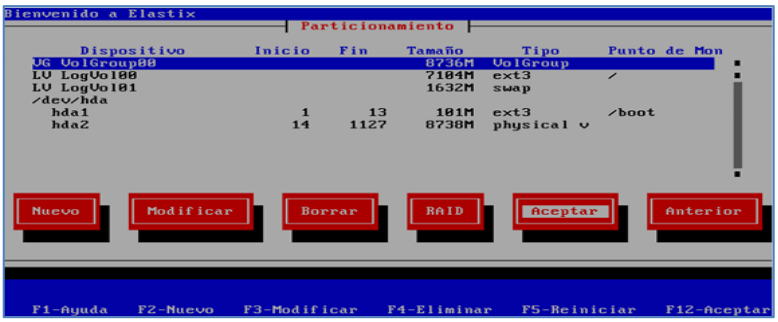


Figura 3.13: Capa de particiones
Fuente: El Autor.

Para configurar la red se elige SI. Para activar el tipo de soporte, en este caso solo IPv4, se da ACEPTAR. Se puede elegir configuración dinámica DHCP o manual, en este caso se elige manual. Se escribe la dirección IP y la máscara, en este caso es tipo C (de 24 bits igual a 255.255.255.0), se da ACEPTAR:

Figura 3.14: Configuración de IP y máscara de red
Fuente: El Autor.

Se configura la puerta de enlace y los DNS, entonces ACEPTAR. Se asigna el nombre del equipo y se da ACEPTAR. Se elige el uso horario, en este caso para Ecuador es America/Guayaquil, ACEPTAR:

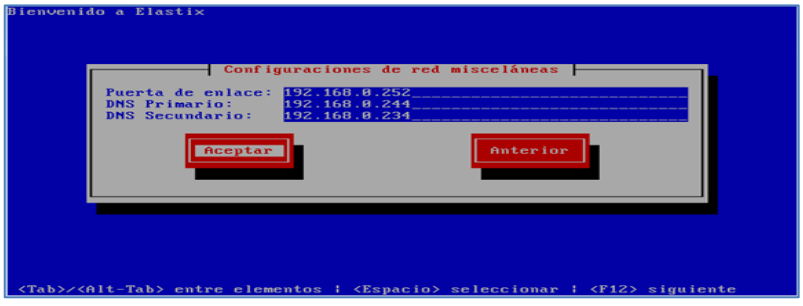


Figura 3.15: Configuración de Gateway y DNS
Fuente: El Autor.

Se ingresa y confirma la contraseña de ROOT, se da ACEPTAR:

Figura 3.16: Contraseña de root
Fuente: El Autor.

Una vez instalados los paquetes, continúa iniciando los servicios de sistema:

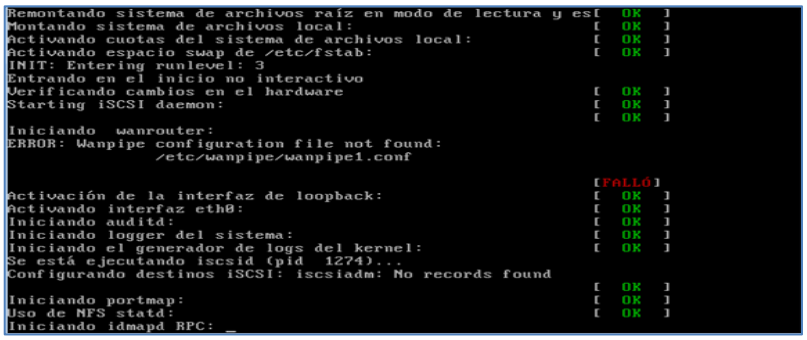


Figura 3.17: Instalación de Paquetes e inicio de servicios
Fuente: El Autor.

Se solicita escribir y confirmar la clave de root para la base de datos MySQL:

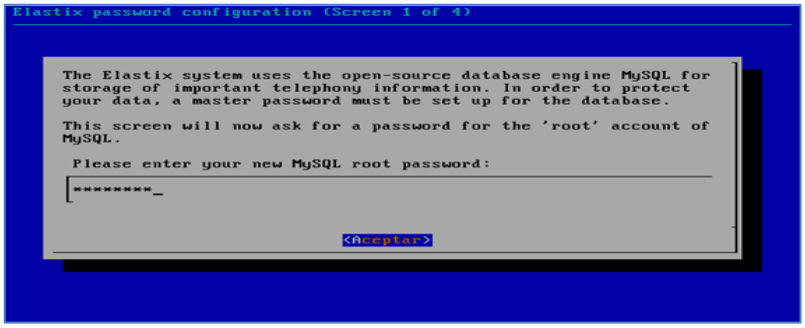


Figura 3.18: Clave de root
Fuente: El Autor.

Se solicita escribir y confirmar la clave de acceso WEB:

Figura 3.19: Clave de acceso WEB
Fuente: El Autor.

Al finalizar muestra el prompt solicitando usuario y contraseña de ingreso. Se inicia con el usuario ROOT y la clave ingresada durante la instalación:

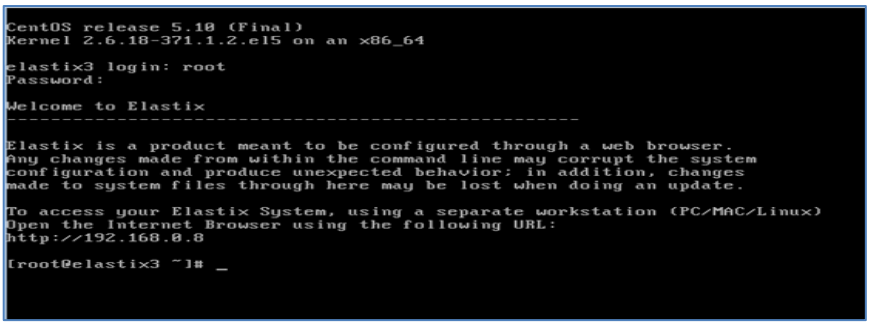


Figura 3.20: Fin de instalación de Elastix
Fuente: El Autor.

Se conecta en el Slot PCI del PC servidor Elastix, una tarjeta OpenVox de 8 puertos FXO analógicos, estas tarjetas son compatibles con los drivers DAHDI y Zaptel. En el puerto FXO #8 se conecta la base celular.

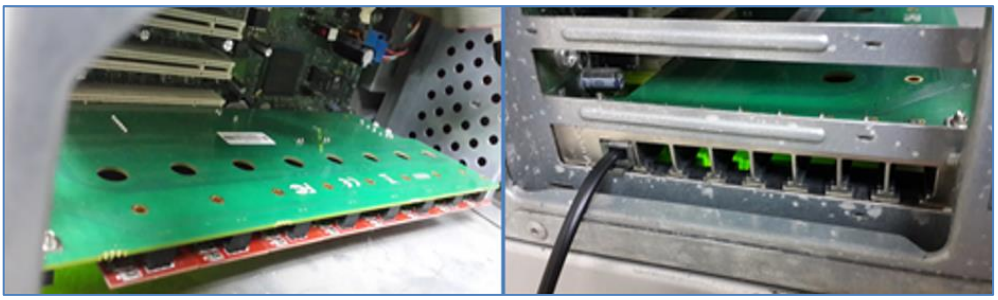


Figura 3.21: Instalación de tarjeta OpenVox.
Fuente: El Autor.

Figura 3.22: Conexión de base celular
Fuente: El Autor.

Configuración de la central Elastix

El acceso a la herramienta es por web, por lo tanto, se ingresa por http desde otro host de la misma red a la dirección IP del servidor Elastix, se autentica con el usuario *admin* y la contraseña definida durante la instalación.

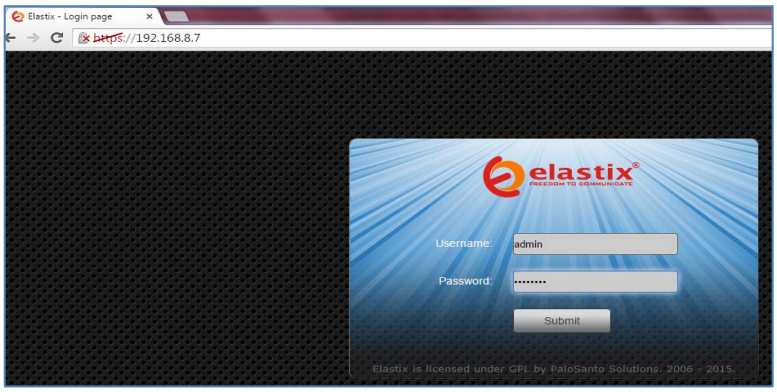


Figura 3.23: Acceso web a Elastix
Fuente: El Autor.

En la pestaña *PBX* se realiza la configuración de central. En la opción *SUDMIT* se ingresan los datos para crear extensiones; se escribe el número de extensión (*User extensión*), y el nombre en pantalla (*Display name*). Se define el

tipo DTMF (multifrecuencia de doble tono) a usar, para una línea SIP en Elastix es RFT2833. Se puede usar una clave (Secret) de seguridad, se aplica la configuración (*Apply Config*). Se define el tipo DTMF (multifrecuencia de doble tono) a usar, para una línea SIP en Elastix es RFT2833. Las extensiones creadas aparecen enlistadas en la parte derecha de la pantalla.

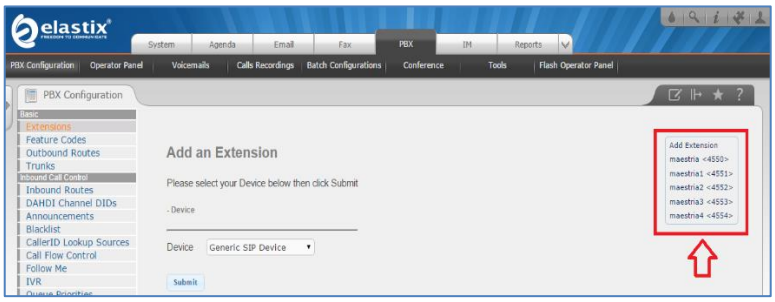


Figura 3.24: Creación de extensiones
Fuente: El Autor.

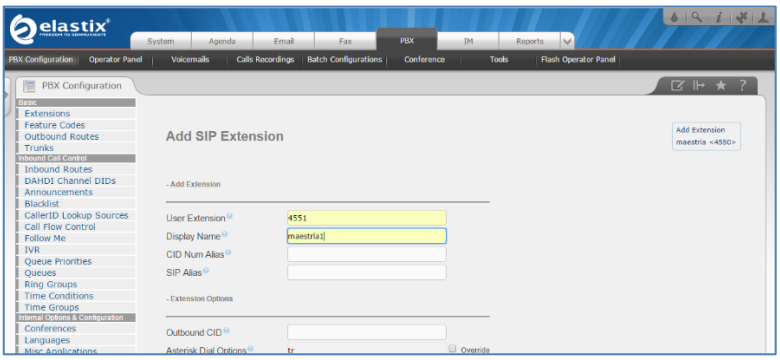


Figura 3.25: Número de extensión de usuario
Fuente: El Autor.

3.1.5.5.1. Configuración de las troncales.

En la etiqueta *System*, opción *Hardware Detector* se puede visualizar la tarjeta detectada, en el puerto FXO #8. En la etiqueta *PBX Configuration* de la PBX se elige la opción *Trunks*. En este caso la tarjeta es compatible con DAHDI, se selecciona la opción *Add DAHDI Trunk*. Se pone un nombre identificador a la troncal y se asocia al grupo identificador DAHDI, en este caso **g0**.

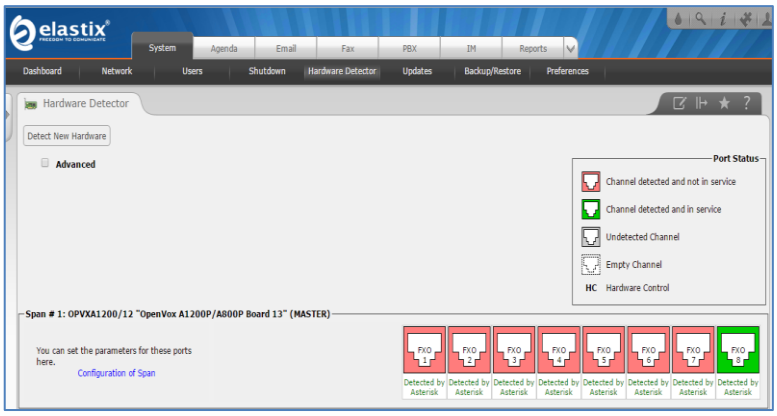


Figura 3.26: Puerto FX0#8 activo
Fuente: El Autor.

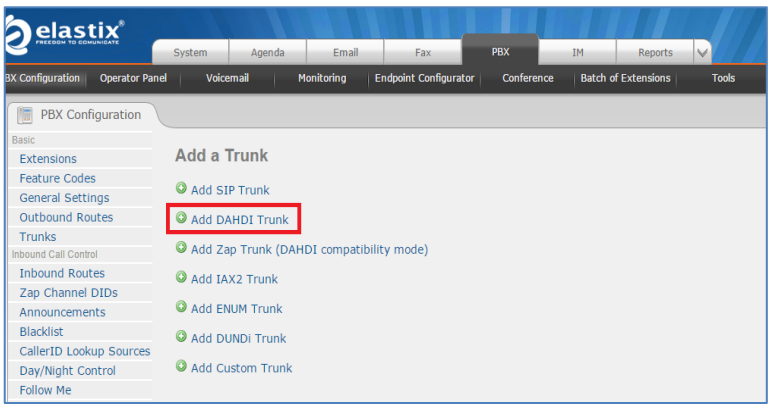


Figura 3.27: Selección de tipo de troncal
Fuente: El Autor.

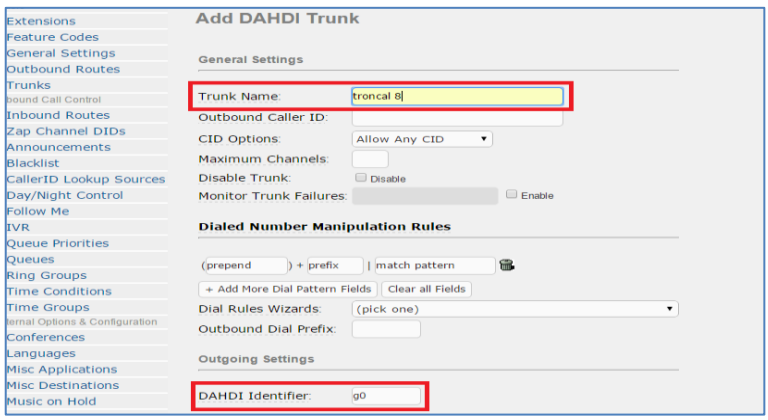


Figura 3.28: Nombre de troncal
Fuente: El Autor.

Se puede configurar el grupo identificador en Asterisk File Editor del PBX, en la columna FileName se busca el archivo *dahdi-channels.conf.*

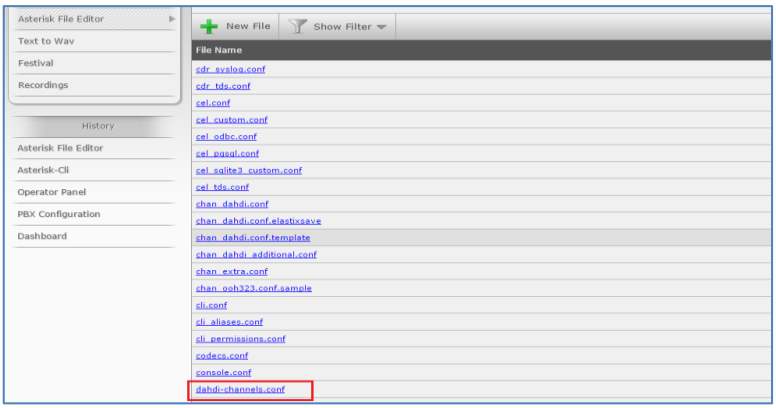


Figura 3.29: Ingreso a configuración de canales DAHDI
Fuente: El Autor.

Aquí se puede configurar el grupo y asociarlo a 1 o más canales, en este caso solo se está usando el canal 8, y el grupo es 0.

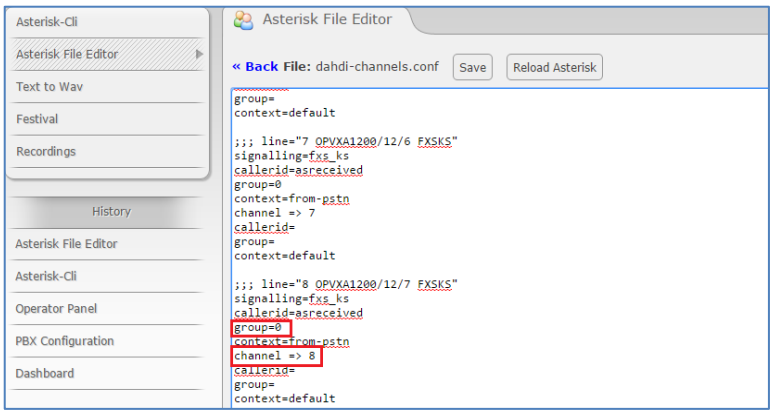


Figura 3.30: puertos asociados a canales DAHDI
Fuente: El Autor.

3.1.5.5.2. Funcionamiento de la Central Elastix.

Para realizar la prueba de la central Elastix con varios de los servicios se crea una mini red a la cual se han conectado: la central Elastix, dos computadores y dos teléfonos ip. Con esta implementación se podrá establecer la conexión telefónica entre las extensiones creadas en la central.

a) Hacer llamadas utilizando los teléfonos IP.
b) Hacer llamadas desde los computadores con una de las herramientas de softphone.
c) Hacer una llamada a celular y recibirla utilizando la conexión del Elastix con una base celular por medio de la tarjeta OpenVox.

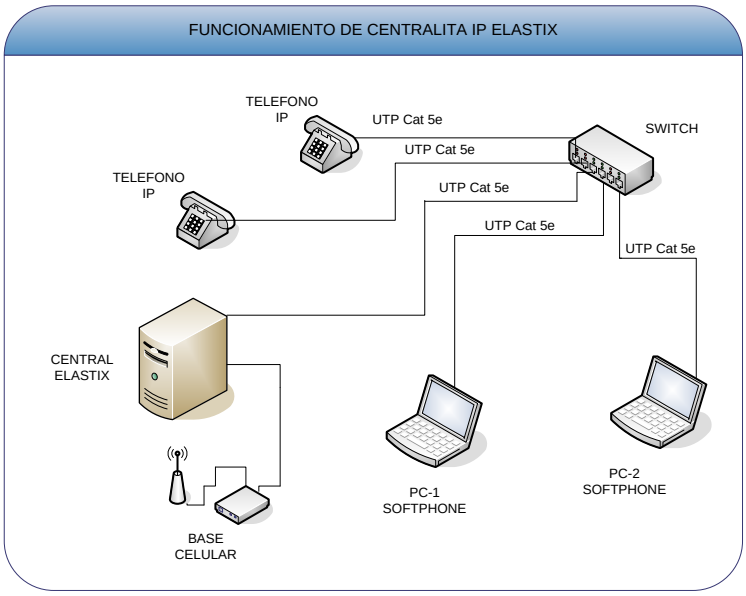


Figura 3.31: Esquema de conexión de central Elastix
Fuente: El Autor

3.1.5.5.3. Servidor DHCP de Elastix.

Una de las herramientas importantes del Elastix es el Protocolo de Configuración Dinámica de Host (DHCP) que permite administrar la asignación de direcciones IP de una red, un dominio, o cualquier entorno de red interna privada, de esta forma se facilita designar las direcciones IP para los host y teléfonos IP de usuarios y otros equipos de red como: impresoras, cámaras, lectores biométricos, turneros, televisores, etc. El DHCP genera automáticamente una dirección IP para cada host conectado a la red que detecta, la dirección IP asignada es la identificación única de cada host de la.

Una limitación del servicio DHCP de Elastix son las Redes LAN Virtuales (VLAN), la configuración DHCP no permite asignar IP para diferentes redes; este servicio si se puede configurar en el DHCP de un Windows Server o desde el switch capa 3 de Cisco.

3.1.6. Diseño de la Seguridad perimetral

La red perimetral se va a diseñar como una red protegida por un Firewall de anterior generación, ejemplo Cisco ASA 5515 y por un firewall de Nueva generación, ejemplo: CheckPoint. El Firewall Cisco ASA ofrece seguridad de puertos con políticas aplicadas a las interfaces de red.

3.1.6.1. Configuración del Firewall

Un Firewall de Próxima generación, ofrece gestión integrada de seguridad en la red, cubriendo aspectos de seguridad tales como: control de uso de aplicaciones, gestión de acceso a Internet, prevención de intrusiones, seguridad de gateways, entre otras; con herramientas diferenciadas o blades: DLP, IPS, VPN, URL Filtering, Antivirus, Aplications Control.

Control de uso de aplicaciones: Se puede limitar el uso de aplicaciones web según la relación que tengan con el trabajo. En este sentido, checkpoint tiene la opción crear reglas que programan la activación de una alarma, para permitirle al usuario certificar que el acceso a una herramienta disponible pero restringida, tiene relación con los objetivos de su trabajo; de esta forma el usuario puede decidir tomar o no el riesgo de usar una herramienta que está catalogada como restringida y de uso poco frecuente.

Gestión de acceso a Internet: La gestión del acceso a Internet se realiza por medio de políticas de configuración de

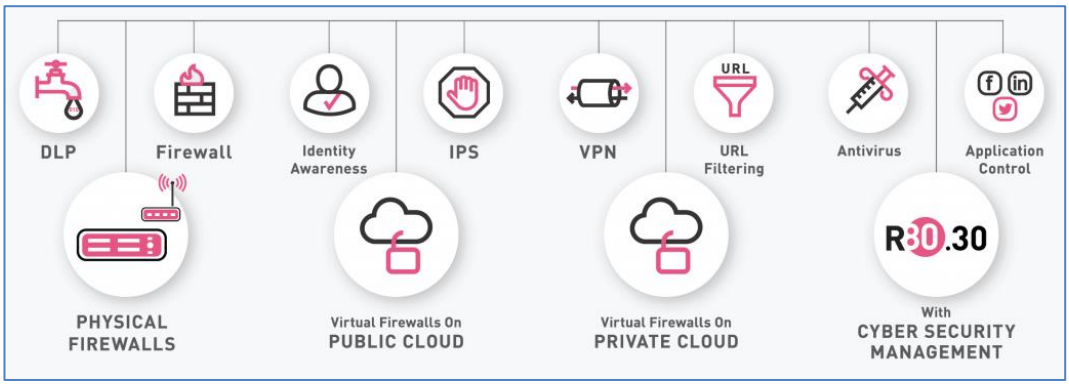


Figura 3.32: Servicios de Seguridad de Firewalls de Nueva Generación.
Fuente: https://www.checkpoint.com/quantum/virtual-systems/

Para la configuración del servidor de Checkpoint se debe tener tres consolas: una consola principal y dos nodos.

3.1.6.2. Configuración de la Salida a Internet

La configuración de la salida a Internet se realiza por medio de un Switch conectado a la red pública, a través de la interface contratada a un proveedor ISP, entre el switch y la salida a Internet se coloca el Firewall de protección perimetral. De acuerdo con la topología de la red, el puerto de salida a Internet se toma desde ese switch y se conecta a una interface Input del FW y la

interface output del mismo FW a un puerto del equipo del Proveedor de acceso a Internet, ya sea un modem, router o ambos. La conexión se realiza entre dos puertos RJ45, en cuyo caso se usa patchcords de cable UTP Cat 6, o entre dos puertos Gbits de fibra óptica usando patchcords de FO. El switch de red interna provee de acceso a Internet a toda la red. Entre el switch de red que puede ser una capa 3, y la salida a Internet se colocará el firewall de administración de políticas de acceso, para protección de las direcciones de red interna, los equipos de computación que contienen la información y los equipos de misión crítica.

En la red interna se conecta el servidor Elastix, detrás del switch principal de tal forma que se pueda administrar las conexiones de voz y datos desde el DHCP habilitado en la centralita IP.

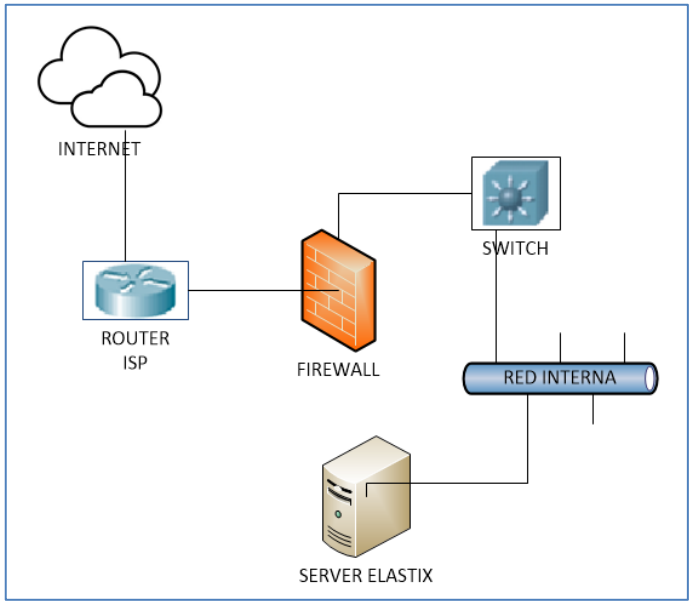


Figura 3.33: Topología con Conexión del Firewall
Fuente: El Autor

3.1.6.3. Enlaces con terceros

Hay otras conexiones de acceso controlado a la red interna por medio de VPN, estas conexiones son denominadas enlaces con terceros. La configuración de este tipo de conexiones se realiza utilizando herramientas que el Firewall tiene incorporado en sus servicios. La configuración de la VPN dentro del FW tiene incorporadas las opciones de diferentes tipos de seguridades que permiten garantizar la disponibilidad, integridad, autenticidad y confiabilidad de la información transmitida a través de un túnel VPN.

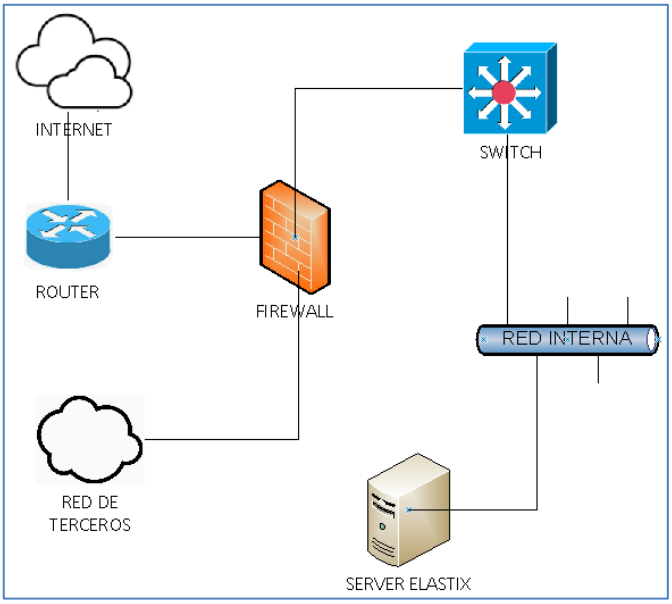


Figura 3.34: Inclusión de red de terceros
Fuente: El Autor

3.1.6.4. Configuración de la DMZ

Algunos equipos de misión crítica están expuestos, dentro de la red interna, a la acción de diferentes intrusiones o intentos de intrusiones por parte de agentes que, logrando penetrar la barrera de protección, se alojaron en el Sistema Operativo de algún computador y desde allí intentan vulnerar, por diferentes métodos, la protección de acceso de dichos equipos para extraer información o para otro tipo de acciones. Los equipos sometidos durante mucho tiempo a este tipo de ataques, cuando las protecciones de acceso por usuario y contraseña no son suficientes, podrían ser vulnerados causando un incidente de seguridad grave por perdida de información u otro tipo de daños. Para prevenir esto se crea una zona desmilitarizada DMZ de tal forma que se pone una barrera adicional de seguridad y de protección para los servidores que contienen la información más valiosa de la red interna.

3.1.6.5. Configuración de Firewall

Usando un Firewall perimetral, se puede dar seguridad a la red interna por administración del acceso a Internet, bloqueo de direcciones IP y de URL, sin embargo, hay otras fuentes de amenazas o huecos de seguridad que desde un firewall no se puede bloquear, algunas de estas fuentes o huecos de seguridad se presentan a nivel del correo electrónico, el directorio activo de usuarios, la instalación de programas desde sitios permitidos. Estas fuentes se protegen desde herramientas

complementarias como el antivirus y el control de listas negras para bloqueo de correos.

El Firewall se configura para admitir las direcciones IP y las URL que se especifican en las políticas y además bloquear todas aquellas que no, de tal forma que, al no encontrar la política que admita el acceso a una IP o URL determinada, simplemente bloquea el acceso.

Capítulo 4: Simulaciones.

4.1 Análisis del funcionamiento de la red en un ambiente real

Para la simulación se va realizar primero una descripción de la topología de la red.

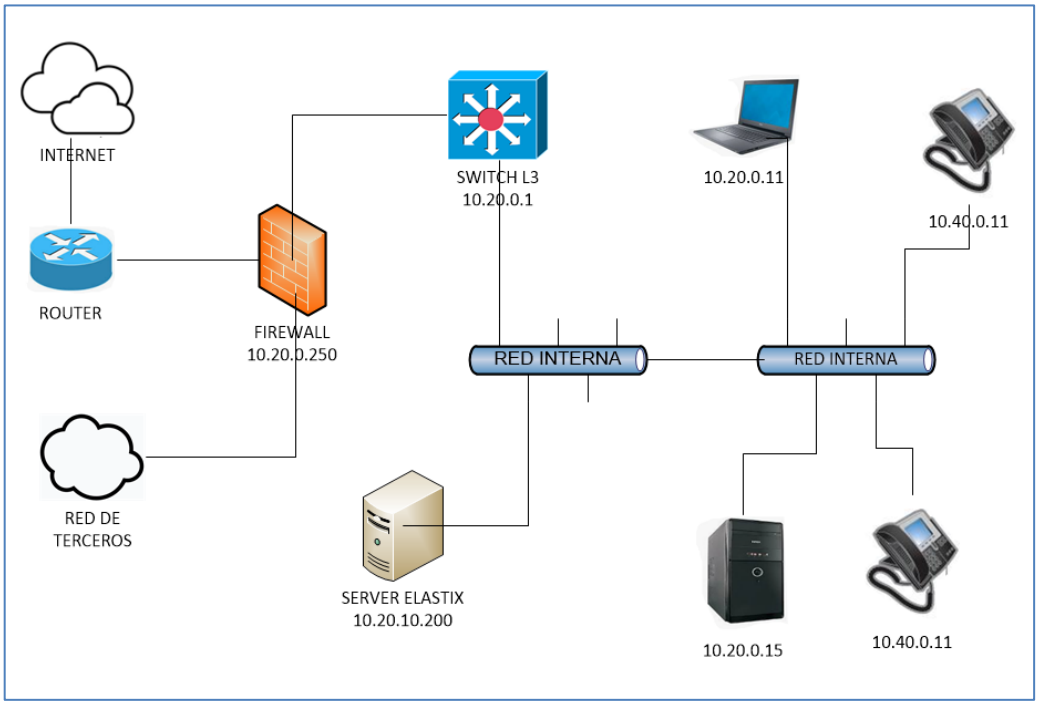


Figura 4.1: Topología de la red.
Fuente: El Autor

El servidor elastix funciona como DHCP de la red para los host como computadores y telefonos IP. En este caso, una estación de trabajo formada por un computador y un telefono IP. El proceso de asignación de dirección IP se puede ver en el cli siguiente:

DHCP Discover: Broadcast de cliente es enviado para buscar el servidor; DHCP Offer: Broadcast de servidor responde con la IP ofertada; DHCP Request: Broadcast de aceptación del cliente; DHCP Ack: Broadcast de servidor confirmación del servidor.

Una estación de trabajo formada por un computador y un teléfono es fuente de acceso a la red interna y a las externas (Internet y redes de terceros) y por lo tanto fuente de emisión de información de todo tipo,

pública, interna, confidencial o privada. La integridad, confiabilidad y disponibilidad de la Información depende de la seguridad con que se pueda transmitirla a traves de la red.

Dado que la seguridad perimetral de la red interna siempre estuvo diseñada para la protección de la red de datos y no la de voz, la implementación de defensas destinadas a la protección de las líneas telefónicas no se incluyen en la consideración de las amenazas y debilidades de la seguridad conjunta hasta la aparición de VoIP. Se trata de incluir los protocolos de la telefonía IP en la protección de la red.

Los protocolos como IAX, SIP y otros de señalización de la telefonía VoIP pueden ser vulnerables ante ataques durante la transmisión de voz. Los accesos telefónicos protegidos por nombres de usuario y contraseñas pueden sufrir ataque de Fuerza bruta para ser vulnerados. A traves de un dispositivo telefónico IP se puede acceder a la red de datos e iniciar ataques para diferentes tipos de objetivos maliciosos.

Una de las vulnerabilidades más comunes de una red telefónica y en este caso la red VoIP, es la captura temporal de la línea para venta de servicios a terceros, de esta forma la factura se endosa al dueño de la línea aunque haya sido usada fraudulentamente por un tercero. Este tipo de delito informático, se detecta despues de la emisión de la factura telefónica por parte del proveedor, una vez que el atacante ha logrado vulnerar las protecciones de red y ha utilizado la línea. A continuación se muestra un intento fallido de registro desde una IP pública externa a una central elástix, en un claro ejemplo de intrusión en el dominio interno de una entidad.

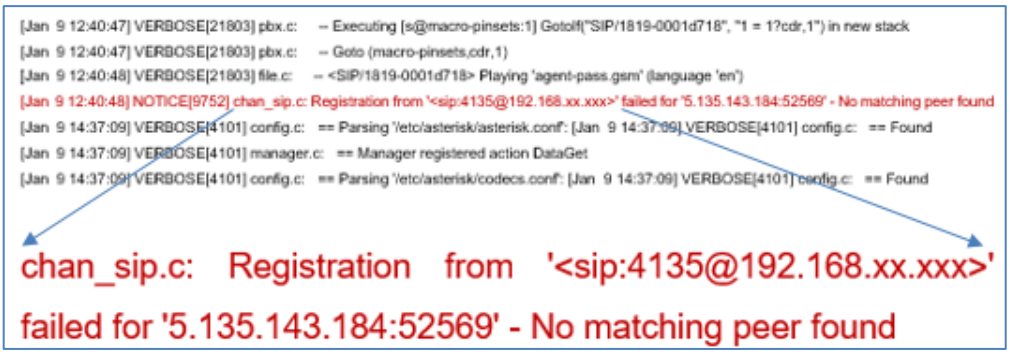


Figura 4. 2: Intento de registro en central SIP desde una IP externa.
Fuente: El Autor

Desde la IP 5.135.143.184 a traves del puerto 52569 se está realizando una violación de política de seguridad con una infiltración lógica externa o una actividad de reconocimiento, en cualquiera de los casos, esta IP logró ingresar a la red Interna vulnerando las seguridades del Firewall.

La acción: se realiza una búsqueda online del origen de la IP 5.135.143.184, se verifica que es una IP de Francia y que ha sido denunciada decenas de veces. Se procede a bloquear la IP en una Política de Firewall.

La política de firewall se configura para denegar el tráfico desde la IP externa origen hacia la red LAN interna destino, de la misma forma, se deniega el tráfico a la inversa, es decir, desde la LAN interna origen hacia la IP externa destino.

Política de Firewall 1

From: LAN

To: INTERNET

Source: Internal (se agrupan todas las redes LAN internas)

Destination: IP_5.135.143.184

Service: ALL (comprende todos los puertos y protocolos)

Action: Deny (Denegar)

From	To	Source	Destination	Schedule	Service	Users	Action
LAN	INTERNET	Internal	IP_5.135.143.184_Mali	always	ALL		Deny
INTERNET	LAN	IP_5.135.143.184_Maliciosa	Internal	always	ALL		Deny

Figura 4. 3: Política de Bloqueo de dirección IP maliciosa
Fuente: El Autor

Política de Firewall 2

Source: Any (toas las redes LAN internas)

Destination: BloqueosIPMaliciosos (grupo de direcciones a bloquear)

Service: Any (cualquier puerto o protocolo)

Action: Drop (Soltar, desechar, lanzar)

Name	Source	Destination	VPN	Services & Applicat...	Action
Bloqueo IPsMALICIOSAS&AMENAZAS	Any	BloqueosIPMaliciosos	Any	Any	Drop
Bloqueo IPsMALICIOSAS&AMENAZAS	BloqueosIPMaliciosos	Any	Any	Any	Drop

Figura 4. 4: Política de Bloqueo de dirección IP maliciosa
Fuente: El Autor

Todos los intentos de acceso detectado desde IPs públicas hacia la central telefónica IP son violaciones de políticas de seguridad y se deben bloquear por medio del FW. Los intentos de acceso son rechazados por la central al no hacer match con la base de direcciones IP permitidas, no se produce la vulneración de la central, pero se corre el riesgo de que el atacante use otros métodos como, denegación de servicios por ataques de fuerza bruta.

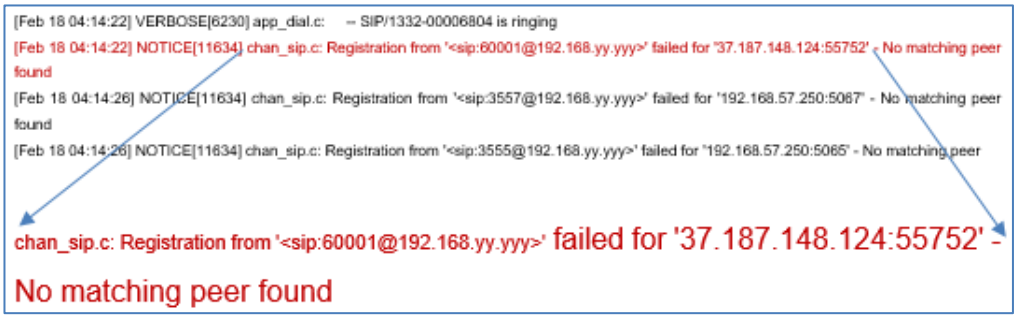


Figura 4. 5: Intento de registro en central SIP desde una IP externa
Fuente: El Autor

La política implementada en el Firewall es reactiva, pero se complementa con configuraciones de políticas de IPS, URL filtering y Aplication Control (Sistema de Prevención de Intrusos, filtrado de URL y Control de Aplicaciones), que son políticas preventivas.

Las IPs intrusas ingresan por conexiones realizadas desde la red interna una vez que algún bot o programa descargado de la web ejecute los mecanismos de reconocimiento o de intrusión.

Conclusiones

1. Se demuestra que, con políticas de protección perimetral preventivas y reactivas, se puede proteger la información de una red de comunicación VoIP, en este caso de una central Elastix, para evitar las intrusiones externas o reducir al mínimo el riesgo de ataques exitosos.

2. La verificación de ataques desde la red interna se realiza manualmente revisando la información de los archivos LOGS del sistema de archivos de Asterisk.

3. Si bien la aplicación de las políticas de seguridad no garantiza al 100% la seguridad de la red, estas permiten tener más del 90% de protección. Actualmente se han multiplicado las formas de ataques dirigidos, con objetivos específicos, como los ransomware, que usan métodos de encriptación para captura de datos. Este tipo de ataques requiere que se complemente el Firewall perimetral con el uso de un Antivirus.

4. La detección de posible acceso por suplantación de identidad que genera el secuestro de una línea telefónica, evita a la entidad dueña de la misma la pérdida de dinero.

Recomendaciones

1. Implementar el procedimiento de educación del personal en el uso de las herramientas computacionales a fin de evitar que se ingrese software malicioso a los equipos de la red por descuido o desconocimiento de las mejores prácticas.

2. Limitar el uso de medios de acceso de datos con flash memory, tomando control de los puertos USB de los computadores desde la consola de Antivirus, para, una vez bloqueados, reducir el riesgo de ingreso software malicioso por esos medios.

3. Si el sistema operativo o la herramienta de administración del o los switches permite hacer control de seguridad de puertos o permiso de acceso por MAC Address, esta política de debe aplicar para impedir la conexión de equipos no autorizados a la red.

Referencias Bibliográficas

5518.pdf. (s/f). Recuperado el 6 de julio de 2021, de https://www.dspace.espol.edu.ec/bitstream/123456789/3001/1/5518.pdf

Alvarado-Kravarovich, C. (2012). *ESCUELA SUPERIOR POLITECNICA DEL LITORAL*. http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-90816.pdf

Andi, T., & Augusto, C. (2015). *Evaluación de la Red de Telefonía IP de la FIE para la Implementación del Uso de Smartphone*. http://dspace.espoch.edu.ec/handle/123456789/4471

Arellano, G. (2005). *Seguridad Perimetral*. 27.

Arribas, D. F. G. (2010). *Dr. Jorge E. López de Vergara Méndez*. 74.

Atelin, P., & Dordoigne, J. (2006). *Redes informáticas: Conceptos fundamentales: normas, arquitectura, modelo OSI, TCP/IP, Ethernet, Wi-FI...* Ediciones ENI. https://books.google.com.ec/books?hl=es&lr=&id=7eu6qwjNam8C&oi=fnd&pg=PT5&dq=modelos+de+referencia+osi+y+tcp/ip&ots=o-HiJHzroO&sig=NDh3CRjIOP0Qgod1ox_W1h5vNd4

Campoverde, A. F. A., & Ferrerosa, R. K. J. (2010). *INGENIERO EN TELEMÁTICA*. 90.

Chávez, D. (2007). *PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ*. 96.

Dimas, J., & Morales, L. (2009). *ANALISIS DE REQUERIMIENTOS E IMPLEMENTACIÓN DE LA PLATAFORMA ASTERISK UTILIZANDO ESTANDAR H.323/IAX2*. http://www.redsegura.cl/wp-content/uploads/photo-gallery/asterisk.pdf

DORDOIGNE, J. (2015). *Redes informáticas - Nociones fundamentales (5ª edición): (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6 ...)*. Ediciones ENI.

Edgar Landívar. (2009). *Comunicaciones Unificadas con Elastix*. http://s3.amazonaws.com/academia.edu.documents/35593728/Comunicaciones_Unificadas_con_Elastix_Volumen_1_29Mar2009.pdf?AWSAccessKeyId=AKIA

J56TQJRTWSMTNPEA&Expires=1469342705&Signature=JF0gyl2CCf5%2FCm1W7OYK6m5Pp%2F4%3D&response-content-disposition=inline%3B%20filename%3DComunicaciones_Unificadas_con_Elastix.pdf

Fajardo, Á. M. M. (2004). Redes convergentes. *Ciencia e Ingeniería Neogranadina*, *14*, 64–74. https://doi.org/10.18359/rcin.1269

G.711: Modulación por impulsos codificados (MIC) de frecuencias vocales. (s/f). Recuperado el 15 de julio de 2021, de https://www.itu.int/rec/T-REC-G.711/es

G.726: 40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM). (s/f). Recuperado el 15 de julio de 2021, de https://www.itu.int/rec/T-REC-G.726-199012-I/en

G.728: Codificación de señales vocales a 16 kbit/s utilizando predicción lineal con excitación por código de bajo retardo. (s/f). Recuperado el 15 de julio de 2021, de https://www.itu.int/rec/T-REC-G.728/es

G.729: Codificación de la voz a 8 kbit/s mediante predicción lineal con excitación por código algebraico de estructura conjugada. (s/f). Recuperado el 15 de julio de 2021, de https://www.itu.int/rec/T-REC-G.729/es

García de Vinuesa Ordovás, B. (2012). *Desarrollo e implementación de un sistema de VoIP basado en Asterisk y PBX*. https://e-archivo.uc3m.es/handle/10016/16947

González Lumbreras, E. A. (2014). *Estudio del tráfico telefónico de una red celular basado en el protocolo de señalización ISUP* [Masters, Universidad Autónoma de Nuevo León]. http://eprints.uanl.mx/11774/

González, W. S. (2011). *PROTOCOLOS DE SEÑALIZACIÓN USADA ACTUALMENTE PARA TERMINALES MÓVILES E IP*. 50.

Jara, H., & Pacheco, F. (2012). *Ethical Hacking 2.0*. USERSHOP.

Joskowicz, J. (2013). Voz, video y telefonía sobre IP. *Universidad de la República, Instituto de Ingeniería Eléctrica, Facultad de Ingeniería*.

http://iie.fing.edu.uy/ense/asign/ccu/material/docs/Voz%20Video%20y%20Telefonia%20sobre%20IP%202009.pdf

López, E. E., & Rodríguez, A. S. (2008). *Instalación de un sistema VoIP corporativo basado en Asterisk*. 101.

López, E. E., & Rodríguez, A. S. (2008). *Instalación de un sistema VoIP corporativo basado en Asterisk*. 101.

Márquez Díaz, J., Pardo Sánchez, K., & Pizarro Valencia, S. (2001). *Ethernet: Su origen, funcionamiento y rendimiento*. https://www.redalyc.org/pdf/852/85200903.pdf

Martín, M. J., & Aversa, F. (2014). *Redes académicas de VoIP latinoamericanas frente al desafío de las nuevas tecnologías*. http://dspace-dev.redclara.net:8080/handle/10786/772

Microsoft Word—29Mar2009.doc—Comunicaciones_Unificadas_con_Elastix_Volumen_1_29Mar2009.pdf. (s/f). Recuperado el 24 de julio de 2016, de http://s3.amazonaws.com/academia.edu.documents/35593728/Comunicaciones_Unificadas_con_Elastix_Volumen_1_29Mar2009.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1469342705&Signature=JF0gyl2CCf5%2FCm1W7OYK6m5Pp%2F4%3D&response-content-disposition=inline%3B%20filename%3DComunicaciones_Unificadas_con_Elastix.pdf

Morales, F., Toapanta, S., & Toasa, R. (2014). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *Ingeniería del agua*, *18*(1), ix. https://doi.org/10.4995/ia.2014.3293

Morales, F., Toapanta, S., & Toasa, R. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *27*, 553–565.

Moreno, J., Soto, I., & Larrabeiti, D. (2006). *Protocolos de Señalización para el transporte de Voz sobre redes IP*. 18.

Moreno, L. (2003). *El Modelo OSI*. línea). Disponible en http://www. htmlweb. net/redes/osi/osi_3. html.(Fecha de consulta 10 de octubre, 2003). http://www.ie.itcr.ac.cr/marin/telematica/trd/01_modelo_OSI_v2.pdf

Moromencho, A. (2013). *Diseño e implementación de una red LAN y WLAN para la Escuela Fray Jodoco Ricke de la comuna de Lumbisí en el cantón Quito* [QUITO/EPN/2013]. http://bibdigital.epn.edu.ec/handle/15000/6888

Oliva Alonso, N. (2013). *Redes de comunicaciones industriales*. https://books.google.com.ec/books/about/Redes_de_comunicaciones_industriales.html?id=4TKJ9IpMSJEC&redir_esc=y

Oliva, J., & Estrella, P. (2014). *Seguridad en implementaciones de voz sobre IP*. Abril. http://blogs.elastix.org/wp-content/uploads/2015/04/Seguridad_en_Implementaciones_voip.pdf

Osorio Pazmiño, T. Y., & Puetate Villarreal, E. B. (2015). *Monitorización, medición y análisis del consumo energético de VoIP para protocolos IAX y SIP en función del tráfico de voz.* http://dspace.ups.edu.ec/handle/123456789/10182

Palacios Oviedo, D. (2018). *Diseño E Implementación De Red En Dispositivos Cisco.* http://repository.unad.edu.co/handle/10596/19905

Patiño Cardona, D. L. (2014). *IMPLEMENTACIÓN DE UNA CENTRAL IP – PBX BASADA EN ASTERISK PARA EL SISTEMA DE TELEFONÍA DE LA UNIVERSIDAD CATÓLICA DE PEREIRA*. 197.

Pilay, C., & Manuel, R. (2021). *Análisis de amenazas y vulnerabilidades informáticas basado en la Norma ISO 27002, en el proceso de citas del servidor web de una Institución*. https://repositorio.upse.edu.ec/handle/46000/5754

Puente, G. B. (2015). *Elastix Unified Communications Server Cookbook*. Packt Publishing Ltd. https://books.google.es/books?hl=es&lr=&id=gDW9BwAAQBAJ&oi=fnd&pg=PP1&dq=Elastix&ots=nGv2x-xAnV&sig=YkuH6MeSrvhGQw9V6KhF1OUnKds

Redes de computadoras—Andrew S. Tanenbaum—Google Libros. (s/f). Recuperado el 28 de agosto de 2016, de https://books.google.es/books?hl=es&lr=&id=WWD-4oF9hjEC&oi=fnd&pg=PR18&dq=modelo+TCP/IP&ots=Xyj7Wbs8Dd&sig=Bp1xa2dqEAV_g0zYSAYVEf94Zvc#v=onepage&q=modelo%20TCP%2FIP&f=false

Salcedo, O., López, D., & Hernández, C. (2012). *Estudio comparativo de la utilización de ancho de banda con los protocolos SIP e IAX*. 18.

Semeria, M. (2015). *Área: Ingeniería Informática*. 17.

Soler Palacín, E. (2009). *Diseño e implementación de una solución de VoIP*. http://upcommons.upc.edu/handle/2099.1/8373

Sousa, J. P., & Carrapatoso, E. (2003). *Uma arquitectura IPtel baseada no protocolo SIP*. 9.

Tanenbaum, A. S. (s/f). *Redes de computadoras*. Recuperado el 28 de agosto de 2016, de https://books.google.es/books?hl=es&lr=&id=WWD-4oF9hjEC&oi=fnd&pg=PR18&dq=modelo+TCP/IP&ots=Xyj7Wbs8Dd&sig=Bp1xa2dqEAV_g0zYSAYVEf94Zvc#v=onepage&q=modelo%20TCP%2FIP&f=false

Tenenbaum, A. S. (1997). Redes de computadoras. *Pearson. México. 814pp*. http://dspace.ucbscz.edu.bo/dspace/handle/123456789/18255

Tolosa, G. (2014). *Protocolos y Modelo OSI*. Recuperado de http://www. tyr. unlu. edu. ar/TYR-publica/02-Protocolosy-OSI. pdf. http://www.tyr.unlu.edu.ar/pub/02-ProtocolosOSI.pdf

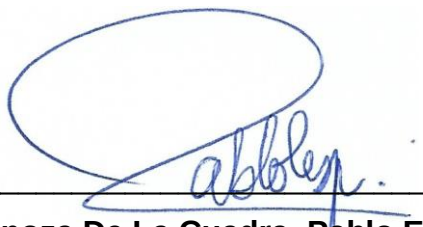
DECLARACIÓN Y AUTORIZACIÓN

Yo, **Espinoza De la Cuadra, Pablo Enrique** con C.C: # 091323425-8 autor del trabajo de titulación: Estudio y diseño de un sistema de comunicaciones unificadas VoIP basado en Elastix con seguridad perimetral, previo a la obtención del título de **Magister en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 29 de octubre de 2021



Espinoza De La Cuadra, Pablo Enrique

C.C: 091323425-8

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Estudio y diseño de un sistema de comunicaciones unificadas VoIP basado en Elastix con seguridad perimetral		
AUTOR(ES)	Espinoza De La Cuadra, Pablo Enrique		
REVISOR(ES)/TUTOR(ES)	M. Sc. Córdova Rivadeneira, Luis Silvio; M. Sc. Quezada Calle, Edgar Raúl / M. Sc. Zamora Cedeño, Néstor Armando		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Sistema de Posgrado		
PROGRAMA:	Maestría en Telecomunicaciones		
TITULO OBTENIDO:	Magister en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	Guayaquil, 29 de octubre de 2021	**No. DE PÁGINAS:**	115
ÁREAS TEMÁTICAS:	Telefonía IP, Protocolos de Señalización, Red de Comunicaciones, Seguridad de la información, Seguridad Perimetral.		
PALABRAS CLAVES/ KEYWORDS:	Telefonía, VoIP, Elastix, Seguridad, Amenazas.		

RESUMEN: En este proyecto se realizará un análisis de las amenazas que afronta una red VoIP basada en Elastix y cómo se puede dar protección y fiabilidad al funcionamiento de la misma; se describirá la configuración de una red VoIP con diferentes conexiones de hosts telefónicos y equipos de computación; se describirá la instalación de una central telefónica IP Elastix y su funcionamiento en la red VoIP; se establecerá una protección perimetral de la red por medio de un firewall. Ya en el entorno de funcionamiento de la red, se analizará diferentes formas de ataques a la central telefónica Elastix; se analizará y describirá la configuración de políticas de protección en el firewall de tal forma que se brinde protección contra las direcciones externas para cercar el perímetro externo de la red; de otro lado, se podrá definir la protección de la central para ataques desde la red interna, es decir protección en el perímetro interno.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** 0979253373	E-mail: penrique11@hotmail.com
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	**Nombre:** Manuel Romero Paz	
	Teléfono: 0994606932	
	E-mail: manuel.romero@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	