UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA: INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención del título de:
INGENIERO ELECTRÓNICO

TEMA:
DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE COMUNICACIONES UNIFICADAS PARA LA EMPRESA RACOMDES S.A. EN LA CIUDAD DE QUITO

AUTOR:
GUEVARA SIGCHA JEFFERSON DAVID

TUTOR:
JOSÉ ANTONIO PAZMIÑO SANDOVAL

Quito, enero de 2016

CESIÓN DE DERECHOS DE AUTOR

Yo Jefferson David Guevara Sigcha, con documento de identificación Nº 1717489817, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de grado/titulación intitulado: "Diseño e implementación de un sistema de comunicaciones unificadas para la empresa RACOMDES S.A. en la ciudad de Quito", mismo que ha sido desarrollado para optar por el título de: Ingeniero Electrónico, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....

Nombre: Jefferson David Guevara Sigcha

Cédula: 1717489817

Fecha: enero 2016

DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación, "Diseño e implementación de un Sistema de Comunicaciones Unificadas para la empresa RACOMDES S.A. en la ciudad de Quito" realizado por Jefferson David Guevara Sigcha, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, enero 2016

Ing. José Antonio Pazmiño Sandoval

C.I. 171032183-5

ÍNDICE

INTRODUCCIÓN 1
CAPÍTULO 1 2
FUNDAMENTOS TEÓRICOS 2
1.1 Conceptos Básicos de Voz sobre el Protocolo de Internet (VoIP) 2
1.2 Protocolo IP 3
1.3 Protocolos de transporte 5
1.3.1 Protocolo TCP 5
1.3.2 Protocolo UDP 6
1.4 Protocolo de transporte de voz RTP 6
1.5 Protocolos de señalización 6
1.5.1 Protocolo SIP 6
1.6 Asterisk 8
1.7 Elastix 8
1.8 Comunicaciones unificadas en Elastix 9
1.9 Seguridad 10
1.9.1 Seguridad Física 10
1.9.2 Ataques y vulnerabilidades en una red IP 11
1.9.3 Encriptación de VoIP 11
1.10 Calidad de Servicio 12
1.10.1 Problemas y posibles soluciones en VoIP 12
1.10.2 Técnicas para lograr Calidad de Servicio (QoS) en VoIP 13
CAPÍTULO 2 14
ANÁLISIS DEL PROYECTO 14
2.1 Reseña Histórica de la Empresa RACOMDES S.A. 14
2.2 Situación actual 14
2.3 Parámetros de red e infraestructura existente 15
2.3.1 Tabla de equipos existentes 16
2.3.2 Topología de red de datos y telefonía actual 16
2.4 Problemática 17
CAPÍTULO 3 19
DESARROLLO DEL PROYECTO 19
3.1 Solución propuesta 19
3.2 Requerimientos de Red 19

3.2.1 Escalabilidad en la red 20
3.2.2 Rendimiento de red 20
3.2.3 Ancho de banda necesario para VoIP 21
3.2.4 Puertos necesarios para VoIP 23
3.2.5 Asociación de rutas analógicas a central IP. 24
3.3 Arquitectura y equipos necesarios para la implementación 26
3.4 Instalación y Configuración 27
3.4.1 Servicio de Telefonía IP en Elastix 27
3.4.2 Configuración de mensajería instantánea en Elastix 34
3.4.3 Servicio de presencia remota en Elastix 36
3.4.4 Servicio de correo electrónico Voicemail en Elastix 43
3.4.5 Servicio de video conferencia en Elastix 43
3.5 Implementación de QoS 44
3.6 Hacking Ético 45
3.7 Seguridades en el servidor Elastix. 45
CAPÍTULO 4 49
PRUEBAS DE FUNCIONAMIENTO 49
4.1 Pruebas de central de telefonía IP 49
4.2 Pruebas de mensajería instantánea 49
4.3 Pruebas de Presencia remota 50
4.4 Pruebas de video conferencia 51
4.5 Pruebas de correo electrónico 51
4.6 Pruebas de QoS 52
4.7 Pruebas de Hacking Ético 54
4.8 Pruebas de seguridades en el servidor 54
CONCLUSIONES 56
RECOMENDACIONES 58
LISTA DE REFERENCIAS 59

ÍNDICE DE FIGURAS

Figura 1. Datagrama IPv4 4
Figura 2. Representación dirección IP y notación punto-decimal 4
Figura 3. Dirección IP con números binarios. 5
Figura 4. Protocolos involucrados en una llamada SIP 7
Figura 5. Establecimiento de una llamada a través de SIP 8
Figura 6. Esquema General de los componentes de Elastix..... ...9
Figura 7. QoS Calidad de servicio para VoIP 13
Figura 8. Central Telefónica Analógica y teléfonos empresa RACOMDES S.A..... 14
Figura 9. Rack de equipos de Telecomunicaciones empresa RACOMDES S.A..... 16
Figura 10. Topología actual de red y telefonía Empresa RACOMDES S.A. 17
Figura 11. Cableado de red y telefonía actual empresa RACOMDES S.A. 18
Figura 12. Puertos usados en SIP 23
Figura 13. Configuración de red Gateway Gransdtream 24
Figura 14. Configuración SIP Server 25
Figura 15. Configuración líneas FXO 25
Figura 16. Configuración de Canales 26
Figura 17. Diseño de Red para servidor de comunicaciones unificadas RACOMDES S.A. 26
Figura 18. Selección de particionamiento en servidor Elastix 27
Figura 19. Ingreso de contraseña servidor Elastix 28
Figura 20. Interfaz WEB de Elastix 29
Figura 21. Configuración de troncal SIP entre servidor Elastix y GW Grandstream 30
Figura 22. Configuración de Ruta de salida servidor Elastix..... 32
Figura 23. Configuración de Ruta de entrada de servidor Elastix 33
Figura 24. Configuración de extensiones en servidor Elastix 34
Figura 25. Diagrama de conexión de Elastix con celular Android par servicio de mensajería 34
Figura 26. Ingreso a Addon Developer 35
Figura 27. Datos ingresados en Módulo GSM de Elastix 36
Figura 28. Página de acceso WEB a Elastix, ingreso a OpenVPN 37
Figura 29. Parámetros para creación de archivo VARS en OpenVPN 38
Figura 30. Configuración de IPTABLES en servidor de red 39
Figura 31. Configuración del Server de OpenVPN 40

Figura 32. Configuración del Server de OpenVPN 42
Figura 33. Pestaña de OpenVPN Status 42
Figura 34. Configuración Voicemail. 43
Figura 35. Habilitación Códecs de Video 44
Figura 36. Asignación de Vlans en Switch CISCO 44
Figura 37. IPTables servidor de Elastix 46
Figura 38. IPTables Servidor de Red 46
Figura 39. Fail2Ban sobre SSH servidor de red RACMODES S. A. 47
Figura 40. Firewall de servidor Elastix vía WEB 48
Figura 41. Pruebas de conexiones SIP de central Elastix 49
Figura 42. Pruebas de Elastix para envío masivo de mensajes 50
Figura 43. Pruebas de asistencia remota sobre celular Android 50
Figura 44. Pruebas de video conferencia 51
Figura 45. Pruebas Voicemail 52
Figura 46. Pruebas consumo de ancho de banda 53
Figura 47. Reporte QoS de Elastix 53
Figura 48. Pruebas de Hacking ético 54
Figura 49. Pruebas de seguridad con fail2ban en servidor de red CentOS y Elastix respectivamente 55

ÍNDICE DE TABLAS

Tabla 1. Datos Ancho de Banda códec G.729 22
Tabla 2. Reglas de marcado Servidor Elastix 31

ÍNDICE DE ANEXOS

Anexo 1. Especificaciones técnica de los equipos empresa RACOMDES S.A. …..61

Anexo 2. Teléfonos IP instalados en la empresa ……..63

Anexo 3. Condiciones actuales del rack de Comunicaciones.…….63

RESUMEN

La empresa RACOMDES S.A. brinda servicios de radiocomunicaciones para varias provincias en Ecuador, al tener una gran demanda de usuarios muchas veces existen problemas primordialmente en la comunicación, lo que provoca pérdidas y molestias con los clientes; hasta el momento no se ha buscado una solución efectiva y se han mantenido sistemas analógicos que no brindan fiabilidad ni la posibilidad de asociación con otros sistemas que permitan optimizar la comunicación y por ende el trabajo dentro de la empresa para con los clientes.

El presente proyecto tienen como objetivo brindar una solución que unificará servicios tales como: telefonía, correo electrónico, comunicación remota, mensajería y video; permitiendo a los empleados de la empresa brindar en todo momento la atención adecuada a los clientes que requieran soporte, para que se desarrolle este proyecto se deben cambiar los equipos analógicos por equipos que soporten el protocolo de Internet (IP).

El proyecto de Comunicaciones Unificadas se desarrollará en un servidor con software libre de ELASTIX basado en ASTERISK que es una plataforma que proporciona todas las funcionalidades para servicio de telefonía IP, dentro de este servidor se instalará la Central IP, misma que contará con cinco líneas analógicas de entrada y tendrá veinte y cinco extensiones para los empleados, con posibilidad de crecimiento futuro.

El servidor de Comunicaciones Unificadas se va a desarrollar en su totalidad sobre el protocolo IP y la central va a ser expuesta en una dirección IP Pública, por lo que un factor muy importante a tomar en cuenta es la seguridad, por este motivo se van a realizar varios análisis y se tomarán las medidas de seguridad necesarias para evitar posibles ataques a la red que perjudiquen el correcto funcionamiento del sistema y eviten que personas no autorizadas accedan a la información de la empresa.

ABSTRACT

RACOMDES S.A. offers services for radio broadcasting in many provinces around the country. Since the demand from users is very high, there are usually problems concerning communication, which brings losses and discomfort among clients. There hasn't been found an effective solution yet, and analog systems have been kept, which neither are reliable nor have the possibility of being associated with other systems in order to optimize the communication and the service provided.

The aim of this project is to provide an alternative that will unify services such as telephones, e-mail, remote communication, messaging and video; allowing employers to always offer proper customers service who require support. In order to develop this project, analog equipment needs to be changed by newer equipment compatible with internet protocol (IP).

The Project of Unified Communications will be developed with a free software server from ELASTIX, based on ASTERISK, which is a platform that provides all functionalities of IP telephony. The IP Core will be installed in this server, consisting of five analogic inlet lines, and twenty-five extensions for employers, open to future development.

The Unified Communications server is going to be totally developed on IP protocol, while the core is to be exposed with a public IP address. Because of this, a very important factor to be considered is security. For this reason, many analysis will be performed, as well as, many security measures will be implemented to prevent possible attacks that can damage the well-functioning of the system. This way, no unauthorized people can gain access to the information of the company.

INTRODUCCIÓN

En el presente trabajo se presentan los principales conceptos correspondientes a la instalación de un sistema de comunicaciones unificadas, en donde se mencionan: el sistema operativo sobre el cual funcionará el servidor, los protocolos y códecs necesarios para que el sistema funcione y algunos criterios de seguridad y calidad de servicio a aplicarse.

Se realiza además un análisis del proyecto y se analiza la situación actual de la empresa, los equipos existentes, la infraestructura con la que cuenta la empresa y los problemas evidenciados antes de la instalación del servidor de comunicaciones unificadas.

Posteriormente se expone el desarrollo del proyecto con la instalación del servidor y cada uno de los complementos que conforman el servidor de comunicaciones unificadas como son: telefonía IP, Elastix Email System, mensajería instantánea, video conferencia, y ciertos parámetros de QoS y seguridades que se aplicarán.

Finalmente se muestran las pruebas de funcionamiento de cada uno de los complementos que conforman el servidor de comunicaciones unificadas y el nivel de seguridad y calidad de servicio implementado a través de softwares de monitoreo y realización de llamadas.

CAPÍTULO 1

FUNDAMENTOS TEÓRICOS

1.1 Conceptos Básicos de Voz sobre el Protocolo de Internet (VoIP)

La VoIP es una tecnología que transmite señales de voz a través de un ancho de banda, es decir que la voz se transmite en paquetes de información; cuando un usuario realiza una llamada mediante VoIP la voz se agrupa en paquetes de información utilizando el mecanismo de Procesamiento Digital de Señales (*DSP por sus siglas en inglés)* que hace paquetes más pequeños que llegarán al receptor; por esto VoIP permite la relación de voz, video y datos a través de una sola red, generando ahorros significativos para los usuarios que opten por esta tecnología (Veneta & Ladrón , 2009, pág. 68).

La tecnología de VoIP ha sido revolucionaria puesto que su objetivo es reducir significativamente el costo de llamadas telefónicas y presenta grandes ventajas ya que da lugar a la asociación con casi todas las aplicaciones que se manejan a través de la red (Veneta & Ladrón , 2009, pág. 69)

Existen innumerables ventajas en VoIP ya que tiene desarrolladores a nivel mundial que realizan investigaciones tanto en la construcción de nuevas aplicaciones como en la solución de problemas que se pueden ir presentando, entre las principales ventajas se pueden nombrar las siguientes:

- La VoIP se puede aprovechar utilizando una infraestructura de red ya existente y es además independiente de los medios de transmisión lo que permite realizar varias conversaciones simultáneas.

- Permite la comunicación remota sin que sea necesario utilizar el sistema de telefonía analógico lo que provoca un ahorro significativo.

- El costo beneficio de instalar un sistema VoIP es grande, ya que para empezar no requiere de grandes inversiones y tiene gran escalabilidad, además permite la reutilización de equipos analógicos.

- Al funcionar sobre el protocolo TCP/IP puede utilizar su ancho de banda para envío de imágenes, video, texto tal como se hace en una red o en el internet.

- VoIP utiliza varias técnicas de compresión y evita también el envío de información en los momentos de silencio haciendo así más eficiente el uso del ancho de banda (Molina & Polo, 2014, pág. 322).

1.2 Protocolo IP

IP es un protocolo de la capa de red que no está orientado a conexión, está basado en datagramas es decir que divide la información en pequeños fragmentos o paquetes, al no ser orientado a conexión cada datagrama viaja independientemente lo que hace que los paquetes puedan llegar en desorden o duplicados, por esta razón es un protocolo no fiable (Santos, 2014, pág. 124).

El protocolo IP tiene como objetivo transmitir información a través de paquetes en un grupo entrelazado de redes hasta que cada paquete alcance su destino, para esto proporciona la información necesaria para que cada host o equipo sepa cómo llegar; en resumen el protocolo IP hace que un gran grupo de redes enlazadas y enrutadores funcionen como una sola y gran red (Herrera, 2003, pág. 260).

La transmisión de datos en el protocolo IP se realiza a través de datagramas, cada datagrama consta de una cabecera y una parte de datos, los datagramas pueden alcanzar un tamaño de 65 Kbytes. En la figura 1 se muestra como está conformado un datagrama IP.

Estructura IPV4

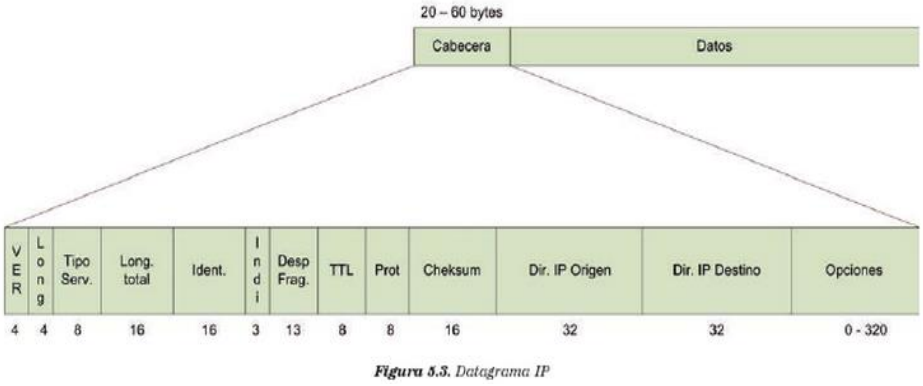


Figura 5.5. Datagrama IP

Figura 1. Datagrama IPv4.

Fuente: (Santos, 2014)

El direccionamiento lógico es una de las funciones principales del protocolo IP, este direccionamiento se utiliza para definir la importancia de los identificadores para cada host que se encuentra dentro de la red, por esta razón cada dispositivo final debe tener una dirección única en la red, a esta dirección se la conoce como dirección IP.

La dirección IP está conformada por 2 partes; la primera es la parte de red y la segunda la parte de host, esta dirección tiene una connotación punto-decimal la cual será representada en la figura 2.

Notación punto decimal IPV4

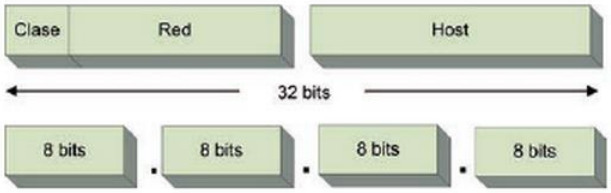


Figura 2. Representación dirección IP y notación punto-decimal.

Fuente: (Santos, 2014)

Cada número decimal de la dirección IP es representado por un número binario de 8 bits también llamado octeto y el rango posible que puede tener es de 0 a 255. En la figura 3 se muestra el formato de la dirección IP en números binarios.

Números Binarios IPV4

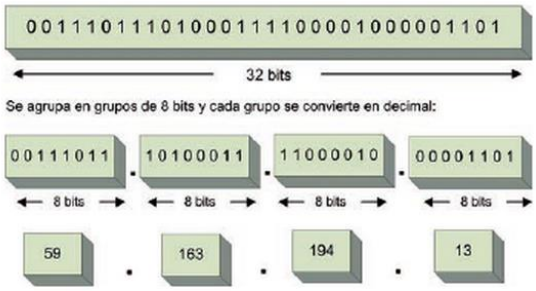


Figura 3. Dirección IP con números binarios.

Fuente: (Santos, 2014)

1.3 Protocolos de transporte

Los protocolos de transporte como su nombre lo indica permiten la transmisión de la información de origen a destino para lo cual utilizan varios métodos de trasporte o incluyen información en los paquetes, existen 2 tipos de protocolos: TCP y UDP.

1.3.1 Protocolo TCP

El Protocolo de Control de Transmisión es un protocolo de transporte que está orientado a la conexión, las funciones principales de TCP son evitar errores en los paquetes, controlando el correcto orden de llegada de los paquetes a su destino, en el caso de que algunos paquetes se pierdan TCP a través de varios mecanismos intenta que los paquetes sean reenviados.

TCP asegura la correcta recepción de todos los paquetes pero al utilizar recurso hace que la comunicación se torne más lenta(Atelin & Dordoigne, 2007, pág. 25), todo el trabajo que realiza TCP para que los paquetes lleguen a su destino implica un carga extra de información a ser enviada, por lo que para el caso de aplicaciones en tiempo real como VoIP no se considera óptimo, de todas formas es muy utilizado en otros protocolos utilizados por Elastix.

1.3.2 Protocolo UDP

UDP (User Datagram Protocol) es un protocolo de transporte que no prioriza la llegada de paquetes en orden o si éstos presentan errores sino simplemente se encarga de que los paquetes lleguen, esta es la diferencia principal con el protocolo TCP; UDP envía datagramas que son enviados dentro de los paquetes IP, al no adicionar más carga de información en el envío de los paquetes el protocolo UDP es mucho más rápido y efectivo para transmisiones de tiempo real como VoIP (Barceló, Íñigo, & Llorente, 2008, pág. 13).

1.4 Protocolo de transporte de voz RTP

En este caso se refiere al protocolo que transporta la carga útil denominado RTP (Real-time Transport Protocol), que cumple la función de transportar la voz con la menor cantidad de pérdida o retraso posible; para que este protocolo entre en funcionamiento es necesario que en el protocolo de señalización se establezca primero la llamada RTP trabaja junto con el protocolo RTCP que corrige problemas en la congestión de la red aunque utiliza otro puerto diferente.

1.5 Protocolos de señalización

Los protocolos de señalización se encuentran en la capa 5 del modelo OSI y dentro de VoIP cumplen las funciones de: inicio y final de sesión, progreso de llamadas, entre otras. La ITU o el IETF han desarrollado varios protocolos de señalización soportados para VoIP entre los que se tiene: SIP, IAX2, H.323, MGCP, SCCP.

Los protocolos más utilizados para telefonía y en la plataforma Asterisk son SIP e IAX2, para el presente trabajo de titulación se tomó en cuenta el protocolo SIP.

1.5.1 Protocolo SIP

SIP *(Session Initiation Protocol)* es un protocolo de aplicación creado por el IETF.SIP da lugar a que los usuarios participen en sesiones de intercambio de información,

utilizando mecanismos de establecimiento, modificación, finalización de llamada y además varios protocolos como se muestra en la figura 4:

Protocolos de una llamada IP

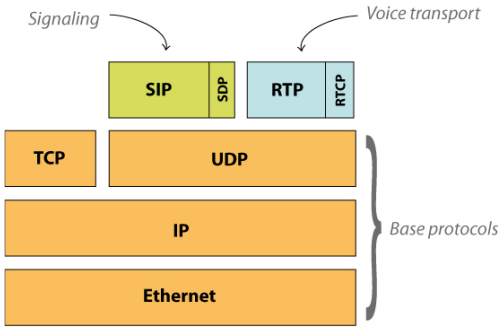


Figura 4. Protocolos involucrados en una llamada SIP.

Fuente: (Landivar, 2011)

SIP puede realizar varias acciones para el establecimiento y terminación de comunicaciones multimedia, entre las que se tiene:

- Localización de usuarios.
- Intercambio / negociación de capacidades de los terminales.
- Disponibilidad de usuarios
- Establecimiento de llamada
- Mantenimiento de llamada.

Al ser SIP un protocolo basado en el modelo Servidor-Cliente, los clientes SIP pueden realizar peticiones y respuestas que van a permitir el establecimiento y la finalización de la llamada, para esto también es necesario establecer los parámetros de recepción de audio y el puerto por el que se van a transmitir y recibir los datos (Porter, Kanclirz, & Zmolek, 2006, pág. 152).

En la figura 5 se muestra el establecimiento de una conexión entre 2 usuarios por medio de SIP.

Proceso de una llamada SIP

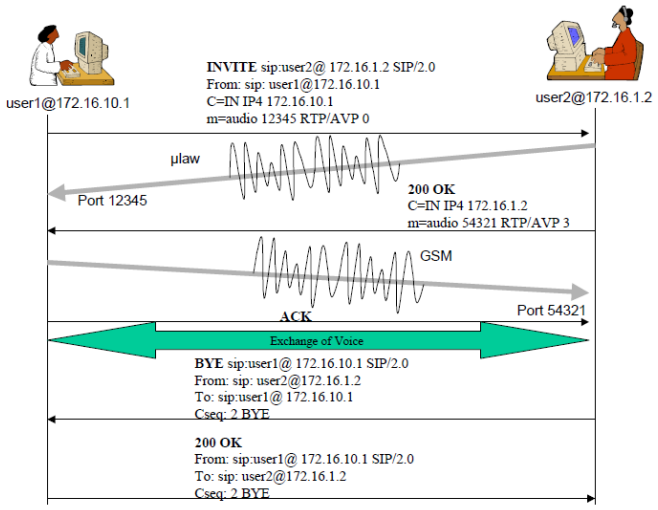


Figura 5. Establecimiento de una llamada a través de SIP.

Fuente: (Porter, Kanclirz, & Zmolek, 2006)

Es importante aclarar que para el software libre Asterisk, la implementación de SIP solo está disponible en UDP.

1.6 Asterisk

Como indica (Gómez, 2008) Asterisk es un software que funciona bajo licencia libre desarrollado para telefonía y que soporta aplicaciones de VoIP, debido a esto gran cantidad de empresas han tomado este modelo para telefonía lo que hace que usuarios e incluso hackers aporten con soluciones a inconvenientes y también al desarrollo de nuevas tecnologías embebidas en este sistema; entre las aplicaciones más destacadas que funcionan en Asterisk se tiene: transferencia de llamadas, contestación automática de llamadas, opción de no molestar, monitoreo y grabación de llamadas, contestación de una llamada a una extensión remota, monitoreo y/o grabación de llamadas, voicemail, conferencias, colas de atención, llamada en espera, IVR *Interactive Voice Response*, entre varias más (Triana, 2014).

1.7 Elastix

Elastix es un servidor de comunicaciones unificadas, distribuido también bajo software libre que permite la asociación de varias tecnologías de comunicación entre las que se tiene: VoIP PBX, mensajería instantánea, email, presencia remota.

El sistema operativo de Elastix está desarrollado en Linux en la versión de CentOS, éste también trabaja en 4 programas de software como Asterisk, Hylafax, Openfire y Postfix que permiten las funciones de la central PBX, Fax, Mensajería Instantánea e Email, respectivamente (Landivar, 2011).

En la figura 6 se muestra un esquema con los componentes de Elastix.

Componentes de Elastix

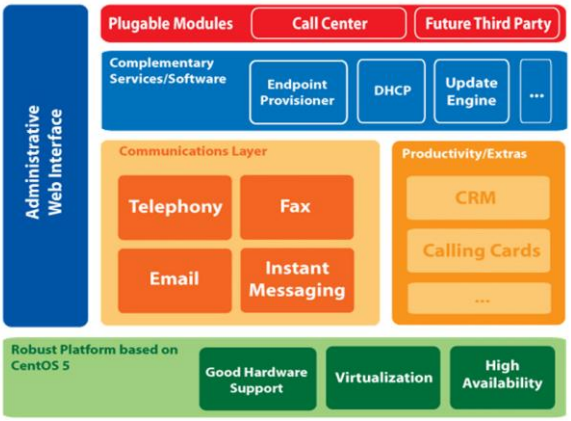


Figura 6. Esquema General de los componentes de Elastix

Fuente: (Landivar, 2011)

1.8 Comunicaciones unificadas en Elastix

La asociación de varias aplicaciones en un mismo servidor permite un mejor control, mayor eficiencia y sobre todo un ahorro en recursos del sistema, es por eso que agrupar varios servicios de comunicación en un servidor en este caso Elastix ha tenido tanto éxito en grandes empresas.

Las aplicaciones y las características que se asocian dentro del servidor Elastix son:

Elastix Email System (Correo Electrónico)

- Servidor de Email multi-dominio con administración por Web.
- Soporte de protocolo para transferencia simple de correo *SMTP* por sus siglas en inglés.
- Configuración de email relay.
- Soporte para cuotas en las cuentas de email.
- Funcionalidad de listas de distribución.

Mensajería Instantánea

- Servidor de mensajería instantánea basado en el protocolo de mensajes cortos par a par *SMPP*.
- Envío de correos masivos.
- Configuración completamente basada en Web.
- Soporta conexiones server-to-server para compartir usuarios.
- Reporte de sesiones de usuarios.
- Soporte de plugins en Elastix.

Videoconferencia

- Servidor de video asociado a la central PBX.
- Configuración en teléfonos con soporte flash y protocolo de video H263.
- Conferencias programables con accesos restringidos.
- Integración con SOFPHONES compatibles (Flanagan, 2012, pág. 162).

1.9 Seguridad

Se debe intentar en la medida de lo posible hacer un sistema fiable en donde la información no corra ningún tipo de peligro, para esto se debe analizar tanto la seguridad física como la seguridad dentro de la red.

1.9.1 Seguridad Física

Aunque parezcan problemas muy simples son una de las principales causas de fallos en las seguridades de un sistema, la desconexión de algún cable o provocar daños físicos en los equipos para dañar el sistema es algo muy simple de realizar, para contrarrestar este tipo de problemas es importante tener en cuenta las siguientes consideraciones: Limitar la cantidad de usuarios que tienen acceso al servidor, no usar el usuario Root, jamás dejar sesiones de conexión abiertas, cambiar las claves por defecto de Elastix (Porter, Kanclirz, & Zmolek, 2006, pág. 417).

1.9.2 Ataques y vulnerabilidades en una red IP

Denegación de servicio: Se define a este ataque como la intrusión o inmersión a una computadora o red, que causa que los administradores o usuarios reales no tengan acceso a sus equipos.
Este ataque se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor presente sobrecargas e imposibilite que los servicios sigan funcionando.

Ataques de inundación SIP (SIP Flooding): Es un ataque de denegación de servicio en el cual se realiza un envió excesivo de paquetes tipo INVITE en el servidor SIP el cual permanecerá esperando que se establezcan llamadas y provocará fallas y saturación en el sistema.

- **Sniffing:** Consiste en oír y capturar el tráfico que pasa por la red, es una práctica bastante general y hay aplicaciones denominadas sniffers que realizan este proceso (Porter, Kanclirz, & Zmolek, 2006, pág. 419).

1.9.3 Encriptación de VoIP

Para no permitir que se intercepte la red es necesaria la encriptación de la información; existen algunas opciones para esto como son:

SRTP (Secure RTP): Esta variación de protocolo proporciona cifrado, identificación del mensaje, protección e integridad frente a envíos a RTP en aplicaciones que manejan unicast y multicast (Calero, 2015).

VPN (Virtual Private Network): Muy usada ya que permite simular una red privada sobre los parámetros de una red pública, pero al ser una red pública se corren riesgos propios de internet, para evitar ataques se usa el *tunneling* que es la encriptación de los datos enviados sobre la red pública, aislando la información e incorporando varios protocolos seguros (Johnston & Piscitello, 2006).

1.10 Calidad de Servicio

Calidad de servicio o *QoS* por sus siglas en inglés, está directamente relacionado con el término *throughput* que se refiere a que una cantidad de información se transmita en cierto tiempo dado asegurando así un buen servicio. Los problemas más importantes que pueden afectar QoS en la red son generalmente Jitter, eco, latencia y la pérdida de paquetes que a través de varias pruebas han sido resueltos (Triana, 2014, pág. 25).

1.10.1 Problemas y posibles soluciones en VoIP

A continuación se describirán los problemas más comunes que se producen sobre VoIP y las recomendaciones que pueden solucionar dichos problemas.

Jitter

Causas: El jitter es el cambio constante en la llegada de los paquetes provocado por congestión de red, desincronización o por la variación de rutas en el envío de paquetes para llegar a su destino.

Valores recomendados

El jitter en el establecimiento de la comunicación no debe superar el valor de 100 ms. Si dicho valor es inferior a 100 ms el jitter puede ser equiparado correctamente, caso contrario debería ser mermado (ELASTIXTECH, 2014).

Posibles soluciones

La solución generalmente escogida es la utilización del jitter buffer; que consiste en establecer un pequeño encolamiento para ir recibiendo los paquetes y usarlos con un mínimo retraso.

Latencia

Causas: Se define como el tiempo que tardará un paquete en ser transmitido desde su origen hacia su destino; la congestión o enlaces lentos hacen que este problema aparezca.

Valores recomendados

La latencia o retardo tendría que ser inferior a 150 ms. Los seres humanos tienen la capacidad de asimilar hasta 250 ms en su rango audible. Si se supera ese valor la comunicación se vuelve irregular.

Posibles soluciones

Se debe analizar donde se encuentra el problema, para esto es necesario revisar los valores de ancho de banda y de en la medida de lo posible aumentarlos priorizando los paquetes importantes es decir los que interesan que sean transmitidos (ELASTIXTECH, 2014).

1.10.2 Técnicas para lograr Calidad de Servicio (QoS) en VoIP

En la figura 7 se muestran los trabajos principales que garantizan QoS:

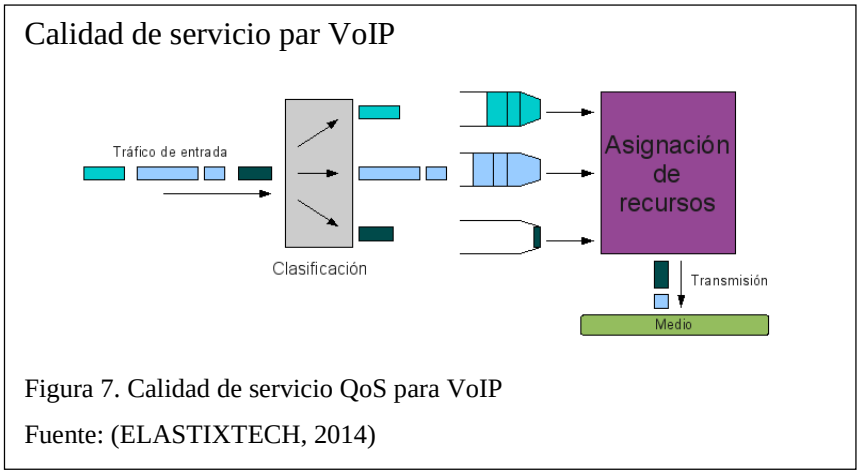


Figura 7. Calidad de servicio QoS para VoIP

Fuente: (ELASTIXTECH, 2014)

Como se puede ver, todo el tráfico que entra es clasificado de acuerdo a la información que posee, siendo segmentado en diferentes canales para posteriormente pasar a la asignación de recursos, estas 2 acciones son primordiales y son explicadas a continuación.

Clasificación: El tráfico que ha entrado al terminal o equipo para ser transmitido debe ser clasificado, para lo cual existen varios juicios entre los que se tiene: por equipo destino, por marcas en los paquetes, por aplicación, entre otros; este proceso se debe realizar necesariamente para asegurar la calidad del servicio. La clasificación se encarga de ubicar semejanzas en los parámetros de QoS que negocia cada paquete, los parámetros más comunes son: latencia máxima, tráfico máximo en ráfaga, tráfico mínimo sostenido y variación en la latencia.

Asignación de recursos: Al tener dividido el tráfico y la información necesaria de los requerimientos de QoS se da paso a que los paquetes sean transmitidos al medio.

CAPÍTULO 2

ANÁLISIS DEL PROYECTO

2.1 Reseña Histórica de la Empresa RACOMDES S.A.

Las empresas que conforman el Grupo Maxi son RACOMDES S.A. y MAXIDISTRIBUCIONES CÍA LTDA, la primera empresa en mención instituida en los años 90 se encarga de la instalación y gestión de sistemas de radiocomunicación troncalizados en la frecuencia de 800MHz asignada dentro del territorio ecuatoriano, la empresa fue tomada por el Grupo Maxi en el año 2009.

La empresa ofrece además un gran stock de productos referentes a radiocomunicación como: repetidoras analógicas y digitales, radios móviles y portátiles y brinda además soporte, asesoría e implementación en proyectos a nivel Nacional.

2.2 Situación actual

La empresa en la actualidad cuenta con un sistema analógico de telefonía, mismo que está constituido por una central telefónica de marca Panasonic TEM824, que cuenta con 3 líneas analógicas y 17 extensiones con teléfonos analógicos marca Panasonic KX-TS520LX; para la recepción se utiliza un teléfono de marca Panasonic KXT-7730, tal como se muestra en la figura 8.

Equipos actuales empresa RACOMDES S.A.

Figura 8. Central Telefónica Analógica y teléfonos empresa RACOMDES S.A.

Elaborado por: Jefferson Guevara

La empresa no cuenta con servicio de mensajería y para correo electrónico cuenta con su propio servidor y dominio.
Este sistema aunque ha permitido la comunicación con los clientes, no da opciones para mejorar y optimizar el trabajo, provocando en muchas ocasiones conflictos con los usuarios y representando pérdidas para la empresa.

Para el manejo de red se tiene la gestión a través de un servidor HP ProLiant ML110 G7 que cuenta con un sistema operativo basado en CENTOS en el que se configuran además seguridades y calidad de servicio.

2.3 Parámetros de red e infraestructura existente

Los parámetros de red con los que cuenta la empresa son:

- Un ancho de banda dedicado contratado al proveedor de servicios de internet Telconet de 2.5 Megabytes de subida y 2.5 Megabytes de bajada.

- El proveedor de internet usa un router HP modelo A-MSR 900, en el cual a través de un enlace de fibra óptica asigna 4 direcciones IP públicas para la empresa, además del direccionamiento privado para los enlaces privados de radiocomunicaciones.

- Se usa cable UTP categoría 6 para la distribución de puntos de red en la empresa.

- La empresa cuenta con 2 servidores: el primero de marca HP ProLiant ML110 que gestiona la red interna, en donde se conecta el switch de distribución marca CISCO Small Business que provee un punto de red a cada host dentro de la empresa y el otro servidor marca Servidor HP Proliant ML310E GEN8 V2 usado para la administración de los enlaces de radiocomunicación existentes y en el cual se va a instalar el servidor de comunicaciones unificadas.
- La infraestructura interna en la empresa ya provee de un punto de red y de telefonía para cada usuario.

En la figura 9 se observa el estado actual del rack de comunicaciones con los servidores y el switch.

Rack de comunicaciones empresa RACOMDES S.A.

Figura 9. Rack de equipos de Telecomunicaciones empresa RACOMDES S.A.
Elaborado por: Jefferson Guevara

2.3.1 Tabla de equipos existentes

En el Anexo 1 se pueden observar las características técnicas de cada uno de los equipos tanto de telefonía como de red con los que cuenta la empresa RACOMDES S.A., y se detalla el funcionamiento que cumplen en dicha infraestructura

2.3.2 Topología de red de datos y telefonía actual

Como se puede observar en la figura 10 la telefonía y el servicio de datos son totalmente independientes uno de otro, lo cual hace que la administración sea más complicada y no se optimice el rendimiento de estas funciones.

Topología de red y de telefonía actual

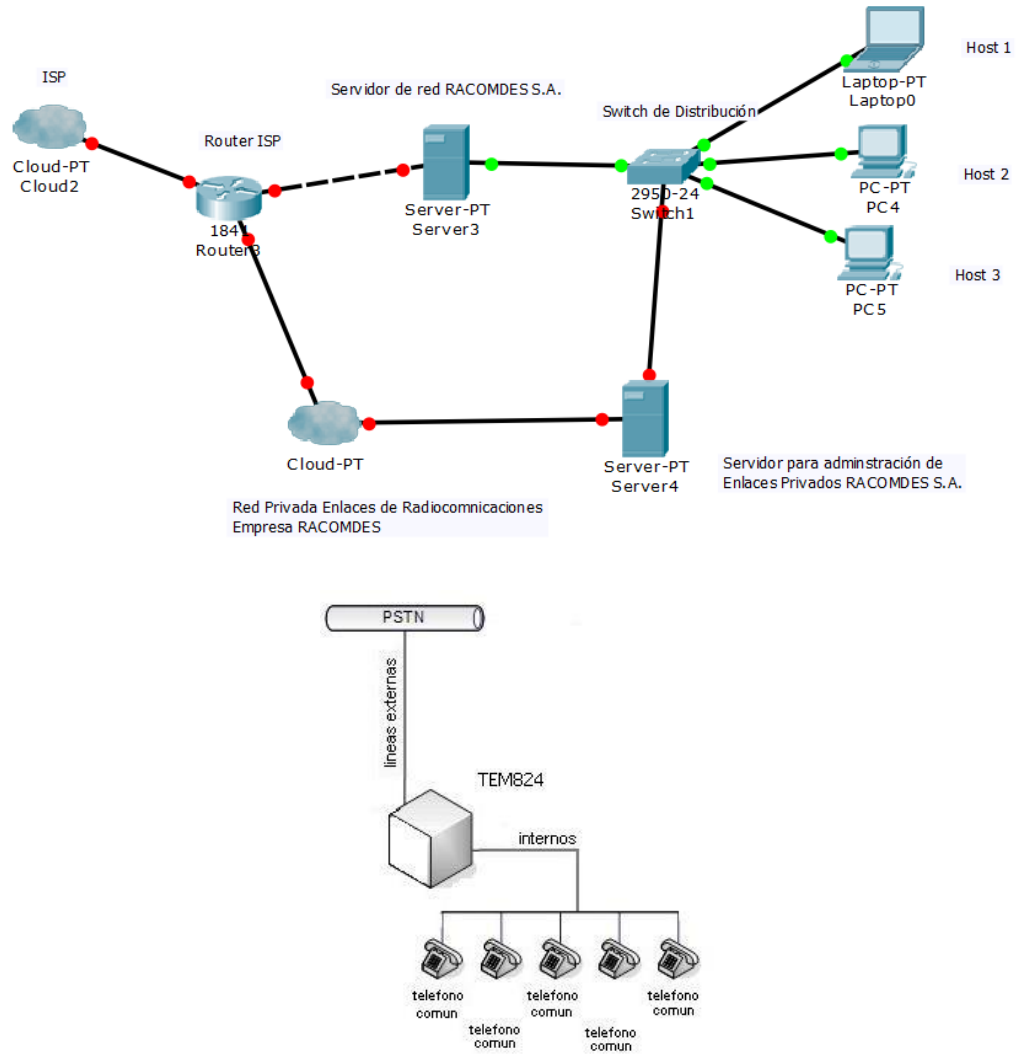


Figura 10. Topología actual de red y telefonía Empresa RACOMDES S.A.

Elaborado por: Jefferson Guevara

2.4 Problemática

A nivel de infraestructura dentro de la empresa no se cuenta con etiquetado para cada puno de red, lo que hace que la administración sea complicada, tampoco se cuenta con las identificaciones necesarias dentro de la central de telefonía analógica y el cableado no tiene estructura, esto da lugar a que si hay algún problema en determinada extensión telefónica o a su vez en un equipo final de red, la identificación y solución al problema tome más tiempo del necesario.

En la figura 11 se puede observar cómo se encuentra el cableado de red y telefonía actualmente.

Cableado actual empresa RACOMDES S.A.

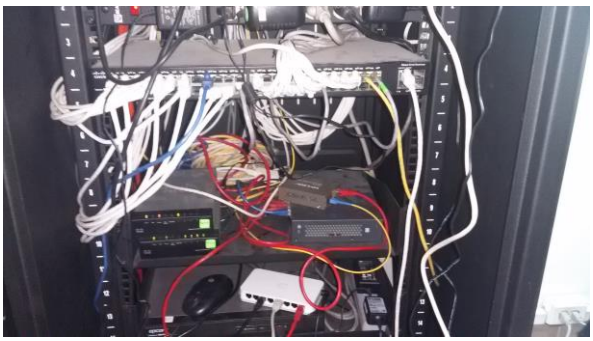


Figura 11. Cableado de red y telefonía actual empresa RACOMDES S.A.
Elaborado por: Jefferson Guevara

La falta de organización en la telefonía actual de la empresa provoca poca eficacia en la comunicación con los clientes puesto que no se redirigen correctamente los requerimientos, ya que la central maneja aún tecnología analógica no se puede optimizar la atención a través de la asistencia remota o la asociación de los mensajes a través de correo electrónico, todos los servicio se encuentran separados y eso hace que la administración de cada uno sea más compleja.

CAPÍTULO 3

DESARROLLO DEL PROYECTO

3.1 Solución propuesta

Para solucionar los problemas expuestos de telefonía y en general de comunicaciones dentro de la empresa, se ha visto la necesidad de instalar un sistema de comunicaciones unificadas que funcionará bajo el software libre de Elastix en un sistema operativo CENTOS, el mismo que va a ser instalado en el servidor HP Proliant ML310E GEN8 V2 con el que ya cuenta la empresa, y tiene las características suficientes para que el sistema operativo funcione sin inconvenientes.

El sistema de Elastix instalado en el servidor se va a conectar con las 5 líneas telefónicas analógicas que posee la empresa a través de un enlace troncal con un Gateway Grandstream GWX4108 que soporta hasta ocho puertos y que ha sido escogido debido a su compatibilidad con el servidor Elastix; en cada una de las extensiones se colocarán teléfonos IP de marca YEALINK que son completamente compatibles con el sistema y han sido escogido ya que presentan una administración WEB de uso fácil para la configuración de parámetros para el usuario

Las demás aplicaciones de comunicaciones unificadas como mensajería, correo electrónico, asistencia remota y videoconferencia se van a instalar y configurar dentro del sistema Elastix y van ser personalizadas para cada usuario.

3.2 Requerimientos de Red

Para definir las características físicas que debe tener el servidor de comunicaciones unificadas con el fin de garantizar una calidad de servicio óptimo a los usuarios, se realizó un análisis, tomando en cuenta:

- Escalabilidad
- Rendimiento de red
- Ancho de banda necesario para VoIP

- Cantidad de rutas entrantes analógicas
- Puertos necesarios para VoIP

3.2.1 Escalabilidad en la red

La escalabilidad es la capacidad que tiene un sistema para cambiar su tamaño y su configuración, para esto se analiza el futuro crecimiento y cómo la red está preparada para mantener la calidad de servicio (Hillar, 2009, pág. 157).

Para el caso del servidor de comunicaciones unificadas la empresa cuenta actualmente con 20 extensiones, se calcula un crecimiento aproximado de 3 extensiones adicionales por año, además se requiere a futuro la comunicación con una sucursal ubicada en la ciudad de Guayaquil.

De acuerdo a los requerimientos expuestos y considerando que el diseño de red con el que cuenta la empresa satisface completamente las exigencias para trabajar en telefonía IP, el servidor de comunicaciones unificadas ha sido dimensionado para un crecimiento de hasta 200 extensiones, con características de 4Gb de memoria RAM, 500Gb de almacenamiento interno y un procesador de 3,1 GHz que permiten brindar todos los servicios sin ninguna complicación.

3.2.2 Rendimiento de red

Para garantizar un rendimiento de red adecuado en cuanto al desempeño del servidor Elastix, se analizan dos tipos de problemas que afectan directamente a la parte de comunicaciones, como son la pérdida de paquetes y el ancho de banda insuficiente.

Pérdida de Paquetes

Al estar basadas en el protocolo UDP orientado a la no conexión, si en el proceso de transferencia de información se produce una pérdida de paquetes, estos no serán reenviados, produciendo un gran problema al perderse paquetes muy seguidos (ELASTIXTECH, 2014).

- **Valor Recomendado**

La pérdida de paquetes máxima que se permite para que no se generen problemas en la comunicación no debe superar 1%, se recomienda usar el códec G.711 que cumple con este porcentaje y permite una comunicación más fiable además de ser gratuito (ELASTIXTECH, 2014).

- **Posible Solución**

Para impedir la pérdida de paquetes una técnica eficientes no transmitir los silencios, ya que casi todas las conversaciones tienen silencios, la solución sería solo transmitir el audio, liberando así los enlaces y evitando tráfico en la comunicación (ELASTIXTECH, 2014).

Ancho de Banda Insuficiente

Se debe partir con el principio de que el ancho de banda en comunicaciones es limitado, ya que siempre va a estar compartido con otras aplicaciones, al ser este el caso, se debe asegurar la mejor calidad de servicio QoS, lo que garantiza una óptima comunicación de Voz sobre IP.

- **Valor Recomendado**

El ancho de banda está directamente relacionado con el códec al utilizar el G.729 se consume un menor ancho de banda ya que codifica la voz a 8 Kbps, el mismo que al añadirle las cabeceras para empaquetar se necesitaría de aproximadamente 24 Kbps de ancho de banda para una solo conversación, es uno de los códecs con menor consumo de ancho de banda, su inconveniente es que es pagado.

- **Posible Solución**

Para garantizar una calidad de servicio QoS óptima se realizará un análisis en cuanto a generación de tráfico de llamadas a través de un programa llamado SIPP, que determinará el desempeño máximo del servidor Elastix simulando una sobrecarga en llamadas(ELASTIXTECH, 2014).

3.2.3 Ancho de banda necesario para VoIP

Para calcular el ancho de banda que se utilizará en la empresa se deben tomar en cuenta 2 factores:

- **El número de llamadas concurrentes.**

Las llamadas concurrentes son un aproximado de la cantidad máxima de llamadas simultáneas que se realizarán sobre un enlace.

Esta aproximación debe tomar en cuenta la cantidad de llamadas telefónicas simultáneas entre diferentes puntos y el posible margen de crecimiento y las políticas de la organización al respecto.

- **El ancho de banda para dirigir cada conversación telefónica.**

Existen varios parámetros que definen el tamaño del ancho de banda que tendrá la llamada, entre los que están: códec, opciones de compresión, enlaces sobre los que se enrutarán las llamadas, entre otros.

En la Tabla No. 1 se muestra los datos para calcular el ancho de banda en VoIP para la empresa RACOMDES S.A.

Tabla 1.

Datos Ancho de Banda códec G.729

Velocidad	8 Kbps
Carga Útil	20 Bytes
Cabecera Ethernet	18 Bytes
Cabecera Capa 2	6 Bytes
Cabecera IP/UDP/RTP	2 Bytes
Sobrecarga IP	20 Bytes
Sobrecarga UDP	8 Bytes

Nota: Elaborado por Jefferson Guevara

A continuación se muestran los cálculos a partir de los datos anteriormente enunciados.

Tamaño del Paquete = Cab.Capa2 + Cab.IP/UDP/RTP + Q.Útil

Tamaño del Paquete = 6 + 2 + 20 = 28 Bytes

*Tamaño del Paquete = 28*8 = 224 bits*

$$PPS = \frac{Tasa\ de\ bits\ codec}{Carga\ Útil}$$

$$PPS = \frac{8\ Kbps}{20\ Bytes} = \frac{8000\ bps}{160\ bits} = 50$$

*Bandwidth = Tamaño del Paquete * PPS*

*Bandwidth = 224*50 = 11,200 bps*

Con lo cual para garantizar la realización de una llamada con calidad óptima de voz se necesita una red con un mínimo de 11,2 Kbps.

3.2.4 Puertos necesarios para VoIP

En los sistemas telefónicos Asterisk-Elastix trabajan varios protocolos para que se pueda realizar una llamada entre dos o más teléfonos IP, originalmente se utilizan los protocolos IAX2 y SIP, pero en este caso específico se utilizó únicamente líneas SIP.

Puertos UDP/TCP en el protocolo SIP

SIP se complementa con SDP (*Session Description Protocol)* y RTP (*Real Time Protocol)*, el primero para el envío de detalles de contenido como pueden ser direcciones IP y el códec a utilizar, y RTP netamente para la transmisión de datos.

En la figura 12 se puede observar la forma en que se produce el intercambio de comunicación así como también los puertos asociados para el establecimiento de la misma.

Puertos protocolo SIP

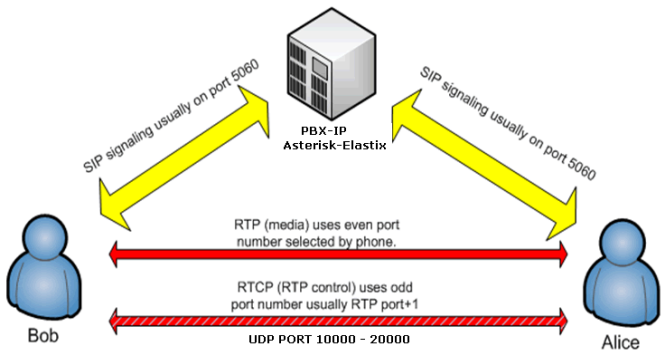


Figura 12. Puertos usados en SIP

Fuente: (ELASTIXTECH, 2014)

Es importante tener en mente que la comunicación es bidireccional, por lo tanto los puertos UDP 10000 a 20000 se deben abrir para permitir el tráfico de entrada y salida,

así como el correspondiente al protocolo SIP el puerto UDP/TCP 5060, adicionalmente si existe un corta fuegos de por medio en cada localidad, se deben configurar para permitir este tráfico en cada una de las redes IP donde existan teléfonos IP, de lo contrario no van a poder comunicarse(ELASTIXTECH, 2014).

3.2.5 Asociación de rutas analógicas a central IP.

Para integrar las líneas telefónicas provenientes del PSTN (*Public Switched Telephone Network),* hacia el servidor Elastix se utilizó un gateway Grandstream 4108, ya que dicho dispositivo de red convierte las llamadas de voz a tiempo real, entre una red telefónica conmutada, a una red VoIP y viceversa.

Para el caso del diseño de red propuesto en el presente trabajo de titulación se toma en cuenta los siguientes aspectos:

Como se puede observar en la Figura 13, lo primero a tener en cuenta es el direccionamiento que tendrá el Gateway, mismo que se alojara de forma estática en la dirección 192.168.1.160/24.

Gateway Grandstream

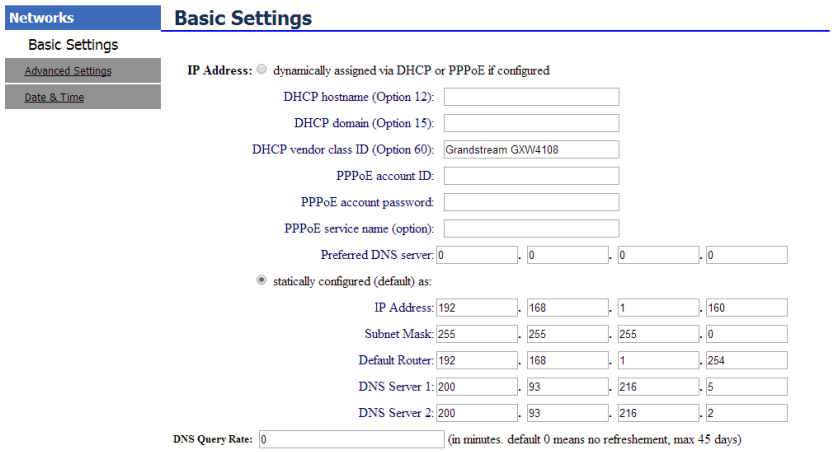


Figura 13. Configuración de red Gateway Gransdtream.

Elaborado por: Jefferson Guevara

De la misma forma como se establece un direccionamiento para el Gateway se debe indicar cuál es el SIP server, en este caso Elastix esta con la dirección 192.168.1.170,

y como se observa en la Figura No. 14 será el servidor donde se alojarán todos los servicios.

SIP Server gateway Grandstream

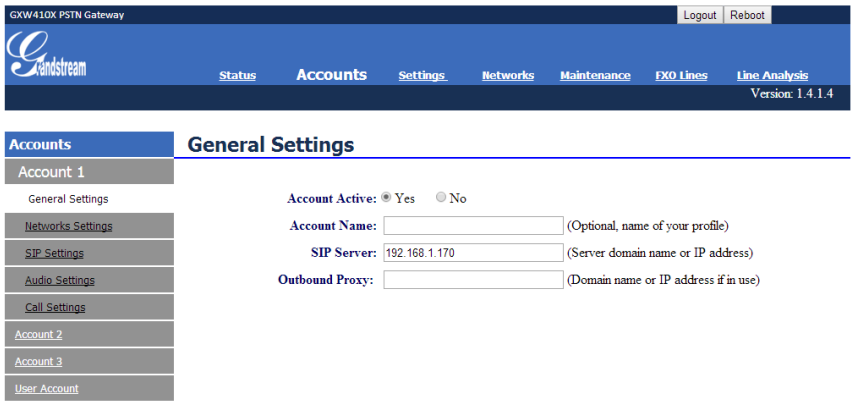


Figura 14. Configuración SIP Server.

Elaborado por: Jefferson Guevara

Un aspecto importante son los tonos de llamada en progreso, en cuanto al tono de marcado, de remarcado y ocupado, así como también la cadencia telefónica, ya que dicha característica es propia de cada país, en la Figura No. 15 se aprecia la configuración de cada uno de los tonos.

Líneas FXO gateway Grandstream

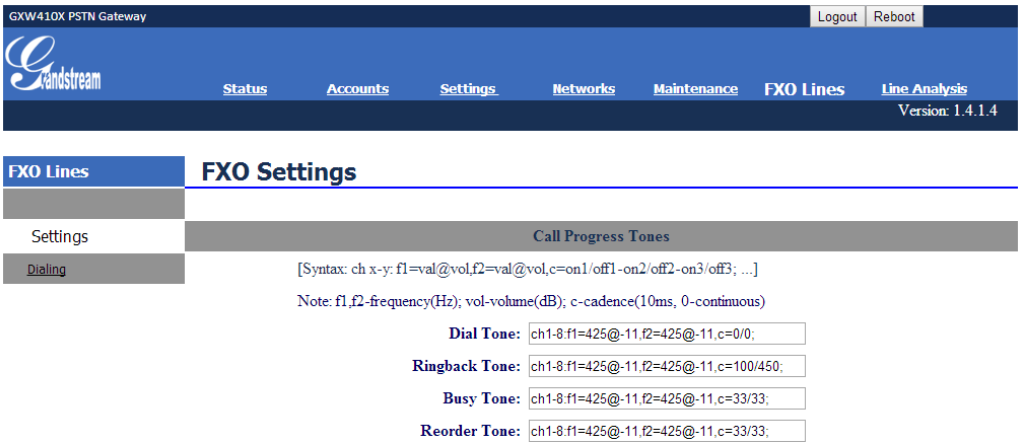


Figura 15. Configuración líneas FXO.

Elaborado por: Jefferson Guevara

Como última característica a tomarse en cuenta es el método DTMF RFC2833, ya que sin el cual no se puede discar directamente a ninguna de las extensiones, opción que disminuiría aspectos tales como el Direct Dial y el IVR, tal como se observa en la Figura No. 16 se evidencia la configuración del SIP channel como de los ID's usados para la central VoIP.

Canales gateway Granstream

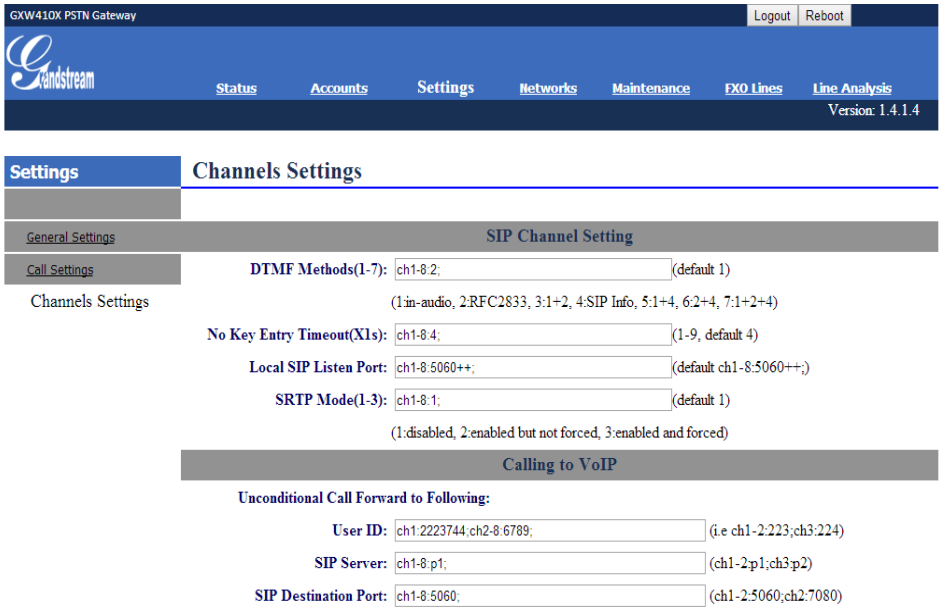


Figura 16. Configuración de Canales.

Elaborado por: Jefferson Guevara

3.3 Arquitectura y equipos necesarios para la implementación

Para la instalación del sistema de comunicaciones unificadas se va a usar la infraestructura existente y se van a aumentar sobre ésta los equipos necesarios para poner el sistema en marcha

En la siguiente figura se muestra como quedara la arquitectura de red telefónica en la empresa.

Diseño de red propuesto

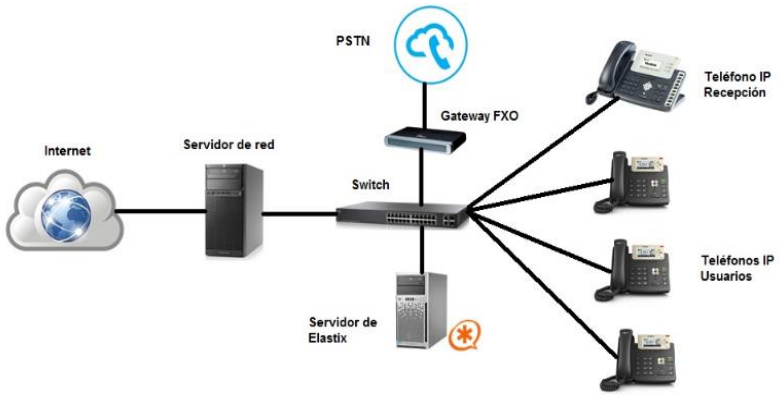


Figura 17. Diseño de Red para servidor de comunicaciones unificadas RACOMDES S.A.

Elaborado por: Jefferson Guevara

Se observa que el servidor donde se coloca el sistema de comunicaciones unificadas está a su vez conectado con el servidor de red. Dentro de la red se coloca también un Gateway FXO de 8 puertos de marca Gradstream que es el encargado de asociar las líneas analógicas emitidas por la PSTN con la central IP; finalmente se conectan a la red los teléfonos IP habiendo diferencias únicamente en el teléfono a instalarse para recepción puesto que incluye botoneras.

3.4 Instalación y Configuración

El servidor de comunicaciones unificadas va a tener en funcionamiento para la empresa RACOMDES S.A. los servicios de: telefonía IP, mensajería, presencia remota, correo electrónico y video conferencia.

3.4.1 Servicio de Telefonía IP en Elastix

Para realizar la instalación del servidor Elastix se debe realizar el siguiente procedimiento:

- Una vez introducido el disco o la imagen ISO dentro del servidor el proceso de instalación iniciará automáticamente, las primeras pantallas son configuraciones de idioma, hora y fecha, luego se escoge el tipo de particionamiento y se selecciona según el requerimiento como se muestra en la figura 18.

Configuración Elastix

Figura 18. Selección de particionamiento en servidor Elastix

Elaborado por: Jefferson Guevara

Se debe confirmar que se va a borrar la partición y se da clic en NO en la ventana de revisar y modificar la capa de particiones.

- Se realiza la configuración de las interfaces de red, para el caso de la empresa RACOMDES S.A. el servidor tiene 2 interfaces, la primera para el direccionamiento interno que es la red 192.168.1.0 y la segunda red 172.16.2.0 que va a permitir la comunicación con una oficina remota en Guayaquil.
  Además se configura el Gateway con la dirección 192.168.1.254 que es la dirección del servidor de red con el que cuenta la empresa y los DNS que son asignados por el proveedor de internet.
  Una vez que se completan todos los parámetros de red se va a pedir la configuración de zona horaria.

- Un paso importante es el ingreso de la contraseña de root que va a permitir el acceso a la consola del servidor, se recomienda colocar una clave robusta. La ventana de ingreso se muestra en la figura 19.

Contraseñas en Elastix

Figura 19. Ingreso de contraseña servidor Elastix

Elaborado por: Jefferson Guevara

- Ya se han ingresado los datos necesarios para la instalación y se debe dar clic en aceptar y esperar varios minutos, durante el proceso se pedirán claves para usuario root de MySQL y para el usuario admin de la Interfaz Web.

Una vez terminado el proceso de instalación se debe ingresar a la consola del servidor con el usuario root y la contraseña asignada y también se tiene acceso a la interfaz

WEB colocando la dirección IP asignada al servidor tal como se muestra en la figura 20.

Elastix WEB

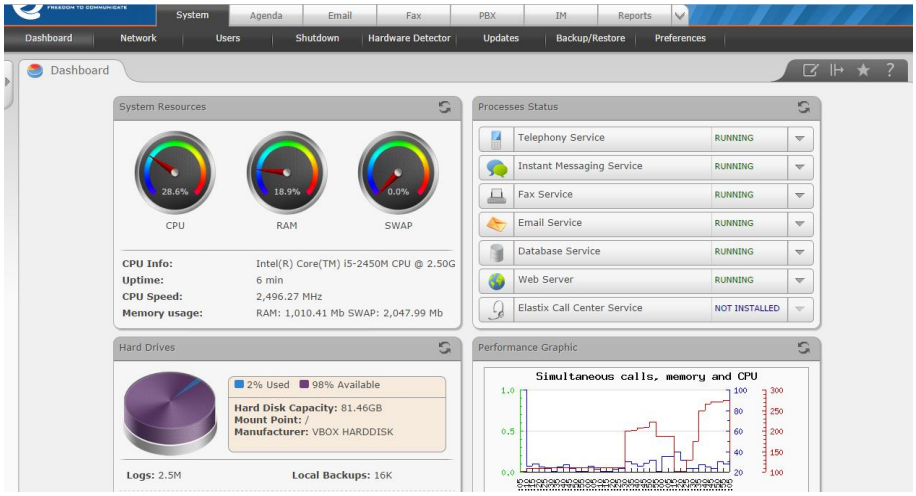


Figura 20. Interfaz WEB de Elastix

Elaborado por: Jefferson Guevara

Configuración de troncal SIP en Elastix

Para asociar el servidor de telefonía con las líneas analógicas existentes en la empresa, se configuró un gateway Grandstream, esta configuración ya fue detallada en la sección *Asociación de rutas analógicas a central IP*. Dentro de Elastix se debe configurar una troncal SIP que realice la conexión del servidor con el Gateway y este a su vez se comunique con las líneas analógicas de la empresa.

Para poder realizar esta configuración se debe dar clic en la pestaña PBX, luego en la sección Trunks y en Add SIP Trunk; dentro de esta ventana los parámetros que se deben modificar son los siguientes:

- **Trunk Name:** Nombre de la troncal para el servidor Elastix se colocó GrandGW1 como nombre.
- **Outbound Caller ID:** Identificador para asociación con el Gateway. Para el servidor se colocó 6789
- **Dialed Number Manipulation Rules:** Se colocan los planes de marcación para tener acceso a las PSTN.

- **Outgoing Settings:** Se modifica el apartado de PEER Details que son los parámetros a configurarse para que establezca la conexión.

En la figura 21, se muestra la configuración de la troncal para el servidor Elastix de la empresa RACOMDES S.A.

Troncal SIP

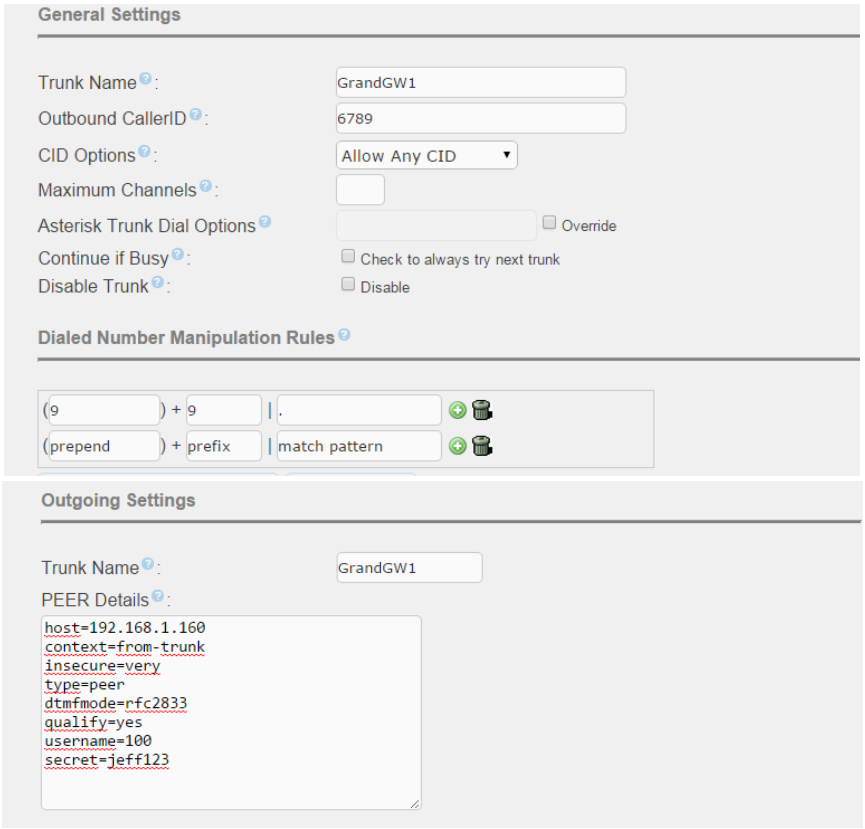


Figura 21. Configuración de troncal SIP entre servidor Elastix y GW Grandstream

Elaborado por: Jefferson Guevara

Cuando ya se establece la troncal SIP entre el servidor ELASTIX y el Gateway Grandstream, se deben colocar rutas de entrada y salida para que se establezcan los caminos por donde se van a realizar y van a ingresar las llamadas telefónicas.

Configuración de Rutas salientes Outbound Routes

Para agregar rutas salientes se da clic en la pestaña superior PBX y en la parte izquierda se ingresa a la opción de *Outbound Routes;* para la empresa se agregó una ruta llamada *salida* y se modificaron los siguientes parámetros:

- **Route name:** Nombre de la ruta
- **Route CID:** Identificador para la asociación con la troncal
- **Dial Patterns that will use this Route:** Reglas de marcado para la ruta de salida. Para el servidor se escogieron las reglas mostradas en la tabla 2.

Tabla 2.

Reglas de marcado Servidor Elastix

Necesidad	Patrón de marcado
Llamadas para provincias en Ecuador	0XXXXXXXX
Llamadas con para números con formato 1800-000-000	1X00XXXXXX
Llamadas a entidades públicas	1XX
Llamadas locales en Pichincha	XXXXXXX

Nota: Elaborado por Jefferson Guevara

- **Trunk Sequence for Matched Routes:** Se escoge la troncal creada para la asociación con la ruta de salida en este caso GrandGW1.

En la figura 22 se muestran las configuraciones de la ruta de salida.

Rutas de salida

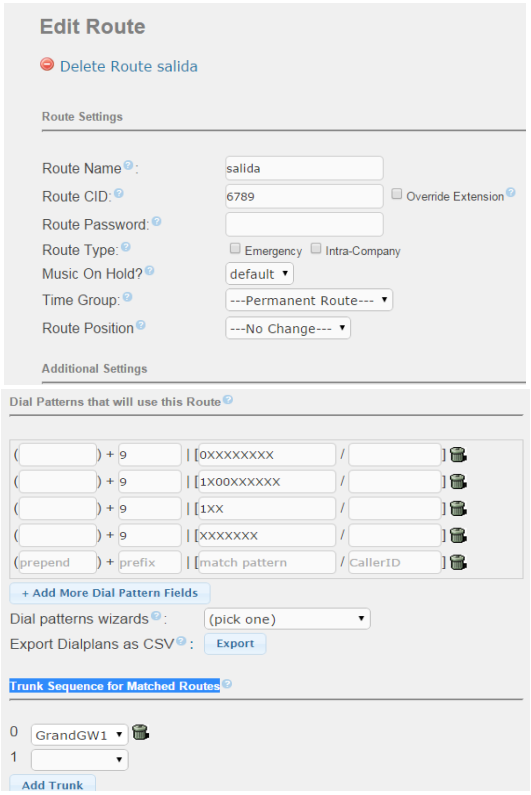


Figura 22. Configuración de Ruta de salida servidor Elastix

Elaborado por: Jefferson Guevara

Configuración de Rutas Entrante Inbound Routes

En la ruta entrante se deben configurar los siguientes parámetros:

- **Description:** Nombre para identificar a la ruta en el caso del servidor se colocó *entrante*.
- **DID Number:** Identificador para la asociación con la troncal SIP. En el caso del servidor es 6789.
- **Set Destination:** Selección del destino de las llamadas entrantes, puede ser el ingreso a una extensión, a una contestadora y varias opciones más. Para el servidor instalado se seleccionó el acceso a una contestadora o IVR personalizado para la empresa.

En la figura 23 se muestra la configuración para la ruta de entrada.

Rutas de entrada

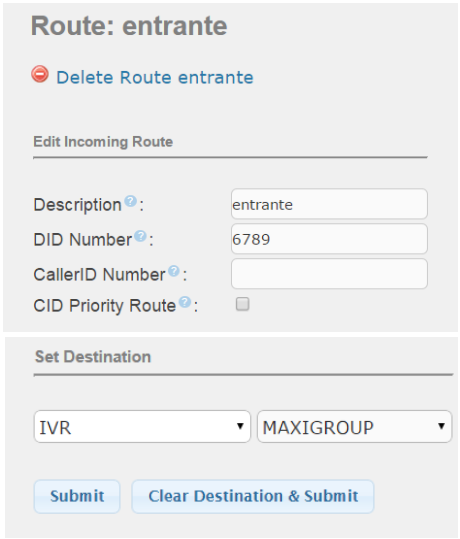


Figura 23. Configuración de Ruta de entrada de servidor Elastix

Elaborado por: Jefferson Guevara

Configuración de Extensiones

Las extensiones se crean en la pestaña PBX sección Extensions, se escogió extensiones SIP para todos los trabajadores de la empresa.

Los parámetros a modificar en la creación de extensiones son:

- **User Extension:** El número de extensión para el usuario específico. Este número se deberá configurar además en el respectivo teléfono IP.
- **Display Name:** El nombre que aparecerá en pantalla
- **Secret:** La contraseña para la asociación con el teléfono IP.
- **Voicemail:** Este apartado se configura si el usuario va a tener asociación con el correo electrónico y es necesario habilitar el servicio y agregar un correo y una clave.
- Los demás parámetros se configuran por defecto y se pueden modificar si el usuario requiere algo adicional como por ejemplo el desvío si la línea está ocupada o si no contesta una llamada.

En la figura 24 se muestra la configuración para las extensiones.

Extensiones

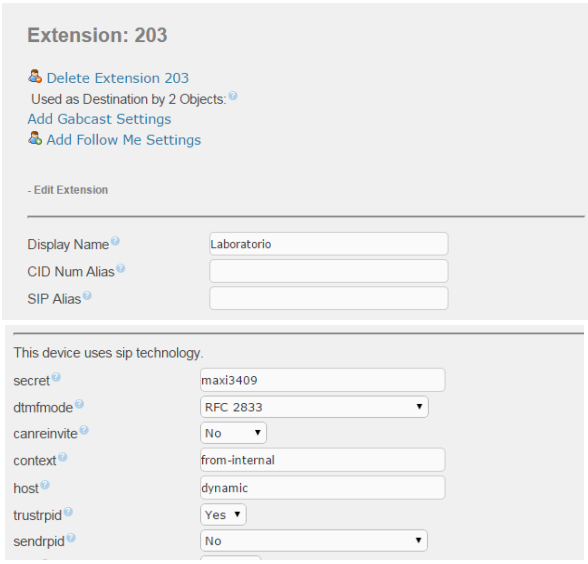


Figura 24. Configuración de extensiones en servidor Elastix

Elaborado por: Jefferson Guevara

Para la empresa se han configurado un total de 21 extensiones ya que esta la cantidad de usuarios actuales.

3.4.2Configuración de mensajería instantánea en Elastix

Para la configuración de mensajería en el servidor de Elastix se escogió trabajar con un celular Android que a través de la aplicación gratuita *Ozeki* trabajará como un router que soporte el protocolo de intercambio de mensajes SMPP.

Para poder realizar la configuración es necesario que el celular esté dentro de la misma red que el servidor. En la figura 25 se observa un diagrama de cómo se va a realizar la configuración.

Mensajería instantánea

Figura 25. Diagrama de conexión de Elastix con celular Android par servicio de mensajería

Fuente: (ELASTIXTECH, 2014)

Una vez ya instalada la aplicación en el celular, se ingresa y presiona el botón *Start*, inmediatamente después aparece la dirección IP, el puerto, el usuario y la clave que se deberán ingresar en la troncal SMPP que se creará en el servidor Elastix.

En el servidor Elastix para crear la troncal SMPP, se debe instalar el módulo SMS, para lo cual primero de debe descargar el archivo elastix-sms-beta-0.3.tar.gzque es el módulo GSM que se instalará en el Elastix; el archivo se descarga en formato .tar.gz que es un comprimido para Linux, luego se debe cargar este módulo en el servidor, para esto se debe instalar primero el Addon Elastix-Developer que es un archivo adicional, una vez instalado se accede a la pestaña como se muestra en la figura 26.

Addons en Elastix

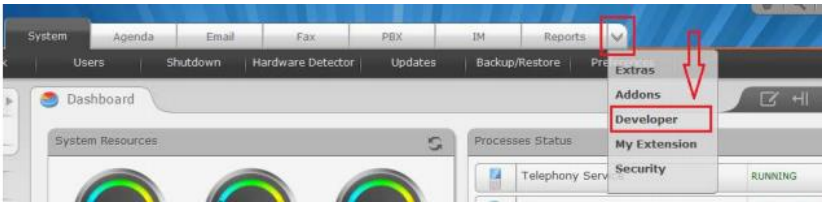


Figura 26. Ingreso a Addon Developer

Fuente: (ELASTIXTECH, 2014)

Dentro de *Elastix-Developer* aparecen 4 pestañas y se debe dar clic en la pestaña *Load Module* luego se da clic en el botón examinar, en este momento se busca el archivo elastix-sms-beta-0.3.tar.gz que se descargó previamente y se selecciona, se da clic en *Save* y ya se tiene el módulo GSM cargado en Elastix.

En la Figura 27 se muestra los campos a completar con los datos tomados del programa que se instala en el celular con Android:

Módulo GSM Elastix

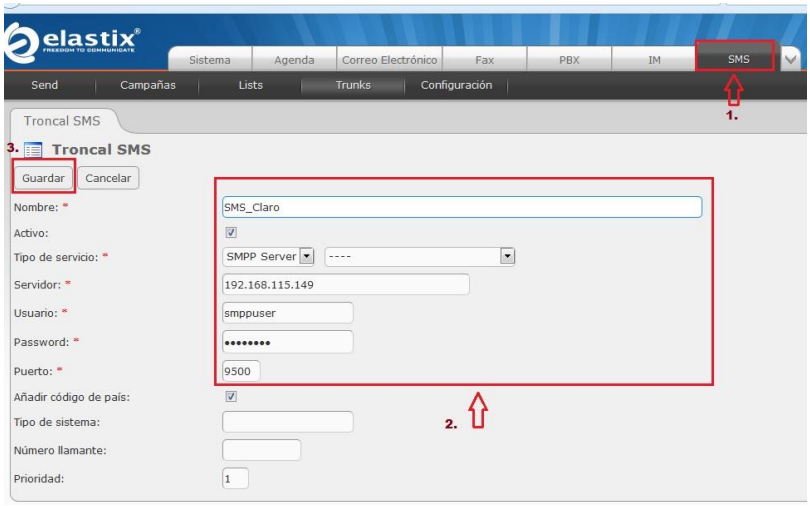


Figura 27. Datos ingresados en Módulo GSM de Elastix

Fuente: (ELASTIXTECH, 2014)

Se puede confirmar que la troncal SMPP se configuró correctamente viendo en la pantalla del celular Android un mensaje que el cliente se conectó satisfactoriamente y ya se pueden crear campañas de mensajería a través de Elastix.

3.4.3 Servicio de presencia remota en Elastix

La configuración de presencia remota en el servidor de comunicaciones unificadas se va a desarrollar a través de la creación de una VPN mediante el complemento Open VPN. Para instalar este servicio VPN se debe colocar en el servidor el comando:

```
# yum install Elastix -easyvpn
```

Una vez terminada la instalación se debe ingresar a la página de administración de Elastix a través de la web y se dirige a la pestaña Seguridad – OpenVPN, para configurar el servicio, como se muestra en la figura 28.

Open VPN en Elastix

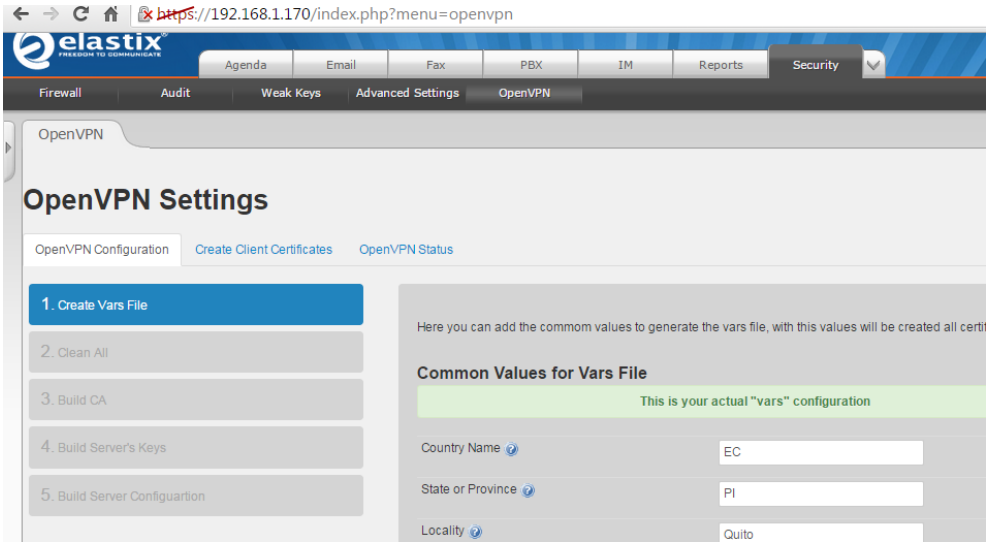


Figura 28. Página de acceso WEB a Elastix, ingreso a OpenVPN.

Elaborado por: Jefferson Guevara

Dentro de OpenVPN se deben seguir 5 pasos para configurar el equipo:

- **Primer paso: Creación del archivo Vars**

El archivo Vars permite el ingreso de información de nombre del país, provincia, nombre de la organización, entre otros. Dicha información crea los certificados para el servidor y el cliente. Si no se completan correctamente los pasos no se puede avanzar.

Una vez que se hayan llenado todos los campos se da clic en el botón *CreateVars File*, inmediatamente el campo en donde se encuentra el texto VarsExists? se llenará con la palabra YES, finalmente se da clic en el botón *YES* para avanzar al siguiente paso. Las configuraciones se muestran en la figura 29.

- **Segundo paso: Limpieza de certificados**

Este paso elimina las llaves y los certificados que se crearon antes, únicamente se debe presionar el botón *Clen all* y posteriormente *Next* para pasar al siguiente paso.

- **Tercer Paso: Creación del Certificado ca.crt**

Se realiza la creación del certificado ca.crt el cual es indispensable para la configuración de la VPN. Únicamente se debe dar clic en el botón *Create CA* para generar el archivo. El proceso toma unos 20 segundos y al finalizar al igual que en primer paso el campo Certificate Exist? se llenará con la palabra YES, para avanzar al cuarto paso se da clic en *Next* para pasar al cuarto paso.

- **Cuarto Paso: Creación de las llaves del servidor y Diffie-Hellman**

Al igual que el tercer paso estos certificados se crean dando clic en el botón *Create Server Keys*, posteriormente el sistema desplegará la imagen que indica que el sistema está generando las llaves (Calazacón, 2015).

Este proceso tarda 2 minutos aproximadamente y al finalizar como en pasos anteriores los campos se llenarán con la palabra YES

- **Quinto Paso: Configuración del Server de OpenVPN**

Este es uno de los pasos más importantes ya que se crearán las reglas de VPN y también la porción de red que la red privada virtual utilizará para formar los túneles de conexión(Calazacón, 2015).

Creación de VARS en Open VPN

Figura 29. Parámetros para creación de archivo VARS en OpenVPN.
Elaborado por: Jefferson Guevara

A continuación se describe cómo se debe llenar cada uno de los campos requeridos:

IP or HOST: En este campo se debe colocar la IP pública o privada, para el caso de la empresa RACOMDES, ya que el servidor de comunicaciones unificadas está conectado a su vez con un servidor de enlaces se va a colocar la dirección IP pública de este servidor que es: 190.95.222.226 para que se puedan comunicar extensiones remotas. Posteriormente se debe configurar el servidor de enlaces abriendo y redireccionando los puertos necesarios a través de IPTABLES tal como se observa en la figura 30.

IPTABLES en Elastix

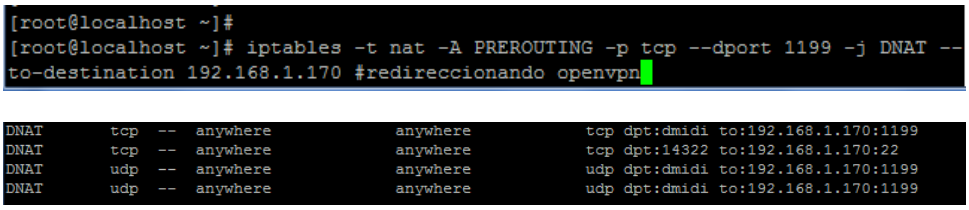


Figura 30. Configuración de IPTABLES en servidor de red

Elaborado por: Jefferson Guevara

Listening Port: Se debe colocar un número válido en el rango de puertos UDP o TCP para escuchar las conexiones entrantes del servicio de OpenVPN. Para la empresa se asignó el puerto 1199.

Dev: Se puede elegir entre 2 dispositivos virtuales de red TUN y TAP. El primero es un dispositivo Túnel de Kernel y trabaja en la capa de red empleando paquetes IP, mientras el dispositivo TAP es un dispositivo que opera en la capa 2 usando tramas Ethernet. Por defecto esta seleccionado el valor TUN. (Calazacón, 2015).

Server Network: En esta opción se establece la porción en la red que se empleará para q los túneles de la VPN se puedan vincular. Para el servidor de comunicaciones unificadas se va a usar la red 10.1.1.0 ya que se maneja esta red para administración interna (Calazacón, 2015).

Server Mask: En esta sección se establece la máscara de red que tendrá la red escogida previamente. Para el servidor se escogió la máscara de red 255.255.255.0 para permitir la conexión de varios hosts.

Keepalive: Se establece el momento en que se realizan pings a los clientes, lo que permite saber si se tiene conexión. El valor por defecto es 10s (Calazacón, 2015).

Timeout: En este campo se establece el máximo tiempo previo a que se defina a un usuario como fuera del aire, el valor se relaciona KeepAlive. Para el servidor se ha definido un tiempo de 120 segundos que es valor por defecto (Calazacón, 2015).

Advanced Options: Este campo es usado para ingresar configuraciones avanzadas en el servidor, para el caso del servidor de la empresa se colocaron los parámetros **push "route 192.168.0.0 255.255.0.0"** ya que al no estar el servicio de VPN asociado directamente al servidor de comunicaciones unificadas sino a un servidor de enlaces se necesita conocer el direccionamiento privado que utilizará el servidor de

comunicaciones unificadas que en este caso es la red 192.168.0.0 con máscara de red 255.255.0.0 (Calazacón, 2015).

Una vez definidos estos parámetros se da un clic en *Create Server Configuration* y se formará el archivo de configuración para posteriormente llena con YES *Configuration File Exist* y *Server.conf Exist*(Calazacón, 2015).

En la figura 31 se muestran los parámetros configurados para la empresa.

Para concluir las configuraciones de OpenVPN simplemente se da clic en el botón *Finish* y el sistema ya puede generar certificados. Inmediatamente después aparecen dos nuevas pestañas: *Creat Client Certificates* y *OpenVPN Status* que se ubican junto a la pestaña de *OpenVPN Configuration.*

Parámetros en Open VPN

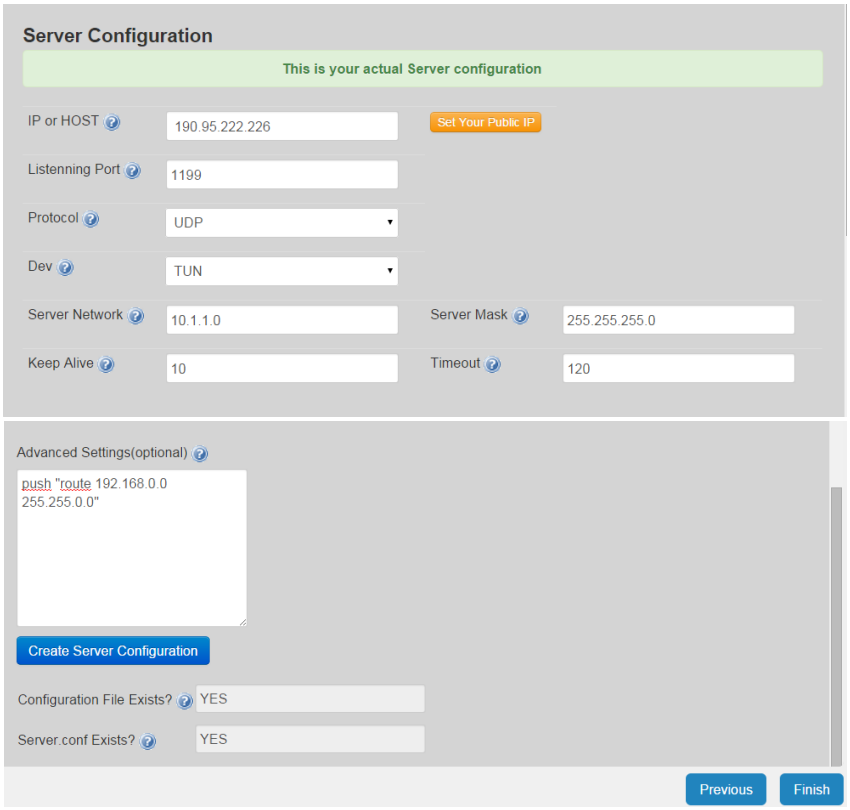


Figura 31. Configuración del Server de OpenVPN

Elaborado por: Jefferson Guevara

El siguiente paso es la creación de certificados para clientes, para esto se ingresa a la pestaña *Creat Client Certificates.*

Se pueden crear varios tipos de certificados para diferentes tipos de clientes, los parámetros a modificar en esta sección son:

ClientType: Se puede elegir el tipo de cliente para poder generar el certificado. El sistema actualmente cuenta con estos tipos de cliente:

- **Linux Client:** Genera certificados para equipos con el sistema operativo Linux los mismos que son: ca.crt, nombre.conf, nombre.crt y nombre.key. Estos certificados se deben descargar y deben ser copiados en el cliente VPN que a su vez debe estar instalado en el host cliente.
- **Windows Client:** Se generan 4 archivos necesarios para sistemas Windows que son: ca.crt, nombre.key, nombre.ovpn, y nombre.crt.
- Estos certificados se deben descargar y deben ser copiados en el cliente VPN que a su vez debe estar instalado en el host cliente.
- **YealinkPhone FW < V71 [TAR]** (Cliente Teléfono Yealink firmware menor a 71): Con esta opción se crea un archivo con extensión TAR que usarán los teléfonos de marca Yealink, se debe considerar que la versión no supere la 71. Este certificado será copiado al teléfono siempre y cuando soporte el enlace vía VPN(Calazacón, 2015).

La Figura 32 muestra algunos archivos creados en el servidor.

Creación de clientes Open VPN

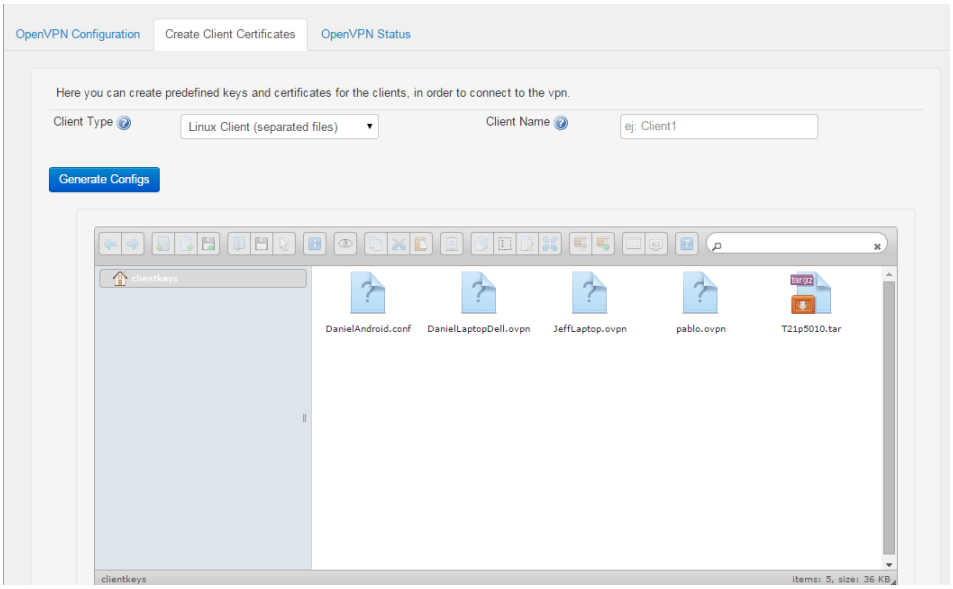


Figura 32. Configuración de clientes Server de OpenVPN

Elaborado por: Jefferson Guevara

Para finalizar se analiza el contenido de la pestaña *OpenVPN Status*, en la cual se encontrará en tiempo real la lista de los clientes conectados al servidor, la lista de todos los certificados creados y la lista de los certificados revocados y la opción de inicio, finalización o la detención de la aplicación OpenVPN tal como se puede ver en la figura 33(Calazacón, 2015).

Estado de OpenVPN

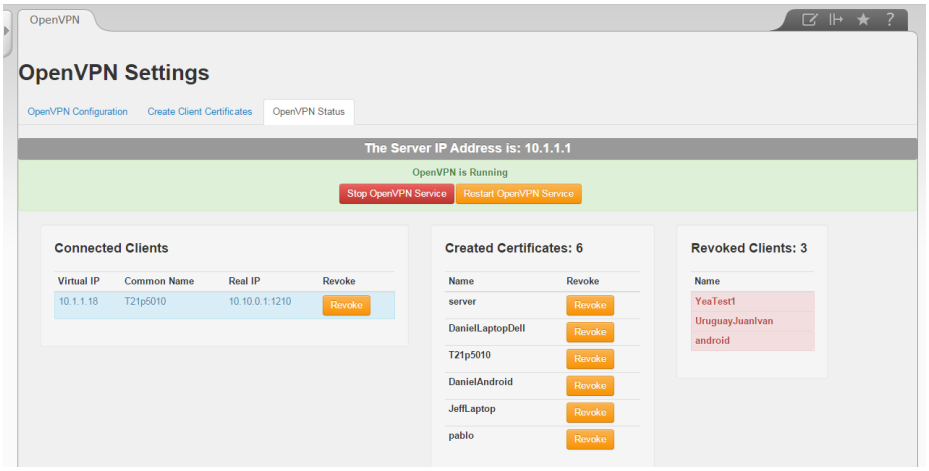


Figura 33. Pestaña de OpenVPN Status

Elaborado por: Jefferson Guevara

3.4.4 Servicio de correo electrónico Voicemail en Elastix

El servicio de Voicemails en Elastix es de gran utilidad, ya que al no estar presente una persona en su lugar de trabajo se procede a dejar un mensaje de voz para el propietario de la extensión; ahora el trabajo de Voicemails consiste en que dicha grabación va a ser almacenada temporalmente en un espacio de memoria asignado para dicha prestación y la misma será enviada en formato WAV a un email determinado por cada usuario.

Su configuración se hace habilitando el servicio de Voicemails con un correo electrónico válido y su respectiva clave de acceso como se muestra en la figura 34

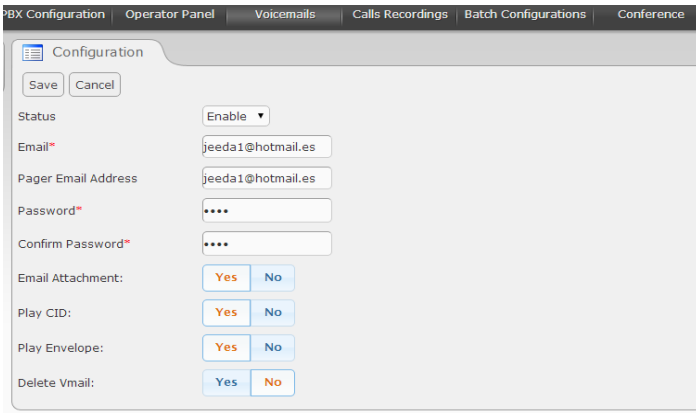


Figura 34. Configuración Voicemail.

Elaborado por: Jefferson Guevara

Cabe recalcar que hay ciertos inconvenientes si se tiene un servidor de correo electrónico privado puesto que en varias ocasiones existen bloqueos para la llegada de correos y el servicio de voicemail de Elastix puede llegar como Spam.

Lo último a realizar es asignar y habilitar el servicio de Voicemail es cada una de las extensiones.

3.4.5 Servicio de video conferencia en Elastix

La configuración del servicio de video llamada es relativamente fácil, puesto que Elastix cuenta ya con los códecs de video, y lo único que se debe hacer es habilitarlos en el archivo *sip.conf* desde consola, tal como se evidencia en la Figura 35.

Códecs de video

```
;------------------------------------------------
[general]

videosupport=yes
maxcallbitrate=386
allow=h261
allow=h263
allow=h263p
allow=h264
callevents=yes
disallow=all
allow=ulaw
allow=alaw
allow=gsm
allow=g729
allow=g711u
```

Figura 35. Habilitación Códecs de Video.

Elaborado por: Jefferson Guevara

Una vez habilitado el video support, se procede a configurar los códecs que soportan video llamada en cada una de las extensiones que se deseen contar con dicho servicio.

3.5 Implementación de QoS

Para asegurar la calidad de servicio en el servidor de comunicaciones unificadas se decidió separar la red de voz y la red de datos a través de redes de área local virtuales VLANS, para el servidor de comunicaciones unificadas se asigna la VLAN VOZ con el rango de direcciones desde la IP 192.168.1.125 hasta la IP 192.168.1.180, asignando un ancho de banda de 1,5 Megabytes que serán suficiente para una buena comunicación, con eso y mediante pruebas que se realizarán posteriormente con respecto al rendimiento del servidor se configura QoS sobre el servidor.

En la figura 36 se muestra la asignación de Vlans en el switch CISCO con el que cuenta la empresa.

Vlans Switch Cisco

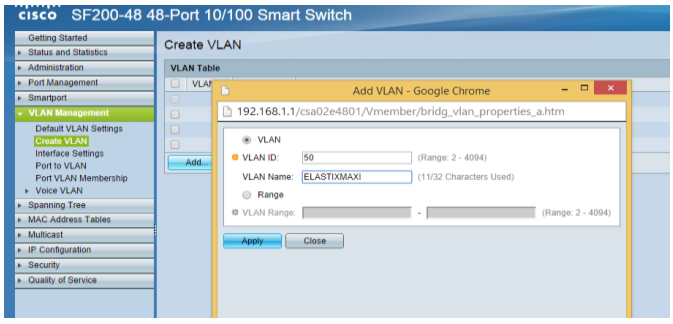


Figura 36. Asignación de Vlans en Switch CISCO

Elaborado por: Jefferson Guevara

3.6 Hacking Ético

El hacking ético permite poner a prueba las vulnerabilidades que pueda presentar el servidor de voz sobre IP a través del ingreso de un usuario no autorizado al sistema. Existen varios métodos que permiten determinar las posibles falencias en la seguridad de un servidor, para el caso del servidor de comunicaciones unificadas de la empresa se va a utilizar el programa NMAP que permite: descubrir servidores dentro de la red, identificar los puertos que se encuentran abiertos, verificar los servicios que se están ejecutando y los sistemas operativos de los host conectados.

Instalación y configuración de NMAP

Realizar hacking ético con NMAP va a permitir encontrar la dirección del servidor de comunicaciones unificadas y verificar los puertos abiertos y servicios en ejecución, para realizar el ataque controlado a la empresa se instaló NMAP basado en Linux en una computadora con CENTOS a través del comando *#yum install nmap*, una vez instalado y ejecutado el programa se procederá a realizar el ataque a la dirección 192.168.1.170 que corresponde al servidor; en el capítulo 4 de pruebas y resultados se pueden observar los resultados.

3.7 Seguridades en el servidor Elastix.

Uno de los puntos más importantes para la seguridad es la documentación de los cambios que se realicen en el servidor. Se debe cumplir con los siguientes puntos:

- Una recomendación es colocar contraseñas complejas en las que se deben tener letras mayúsculas, minúsculas, símbolos y números; para el caso de la empresa RACOMDES se asignaron contraseñas que cumplen con estos parámetros y no solo la contraseña de root y usuario sino también las contraseñas de MySQL, Free PBX, FOP, y de las extensiones.
- Otro de los puntos importantes es una vez instalado el servidor es restringir el acceso a los equipos; la manera más eficaz de realizar esto es a través de IPTables que permiten el acceso y bloqueo de ciertos puertos a ciertas

direcciones IP, sobre todo es importante que el acceso a Security Shell (SSH) y WEB se dé solo para los administradores del servidor.

En la figura 37 se observa los IPTables configurados en el servidor Elastix.

IPTABLES Elastix

```
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [133299:59193040]
:ELASTIX_FORWARD - [0:0]
:ELASTIX_INPUT - [0:0]
:ELASTIX_OUTPUT - [0:0]
-A INPUT -j ELASTIX_INPUT
-A FORWARD -j ELASTIX_FORWARD
-A OUTPUT -j ELASTIX_OUTPUT
-A INPUT -p tcp --dport 5038 -j ACCEPT
-A ELASTIX_FORWARD -j REJECT --reject-with icmp-port-unreachable
-A ELASTIX_INPUT -i lo -j ACCEPT
-A ELASTIX_INPUT -p icmp -j ACCEPT
-A ELASTIX_INPUT -p udp -m udp --dport 67:68 -j ACCEPT
-A ELASTIX_INPUT -p udp -m udp --dport 5004:5082 -j ACCEPT
-A ELASTIX_INPUT -p udp -m udp --dport 4569 -j ACCEPT
-A ELASTIX_INPUT -p udp -m udp --dport 5036 -j ACCEPT
-A ELASTIX_INPUT -p udp -m udp --dport 10000:20000 -j ACCEPT
-A ELASTIX_INPUT -p udp -m udp --dport 2727 -j ACCEPT
-A ELASTIX_INPUT -p udp -m udp --sport 53 -j ACCEPT
-A ELASTIX_INPUT -p udp -m udp --dport 69 -j ACCEPT
-A ELASTIX_INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A ELASTIX_INPUT -p tcp -m tcp --dport 25 -j ACCEPT
-A ELASTIX_INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A ELASTIX_INPUT -p tcp -m tcp --dport 110 -j ACCEPT
-A ELASTIX_INPUT -p tcp -m tcp --dport 143 -j ACCEPT
-A ELASTIX_INPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

Figura 37. IPTables servidor de Elastix

Elaborado por: Jefferson Guevara

De acuerdo a la figura 37 se observa por ejemplo que a través de IPTables en la línea –A ELASTIX_INPUT –i lo –j ACCEPT se están permitiendo conexiones locales al servidor, también entre las reglas permitidas se tiene el acceso a HTTP puerto 80 y HTTPS puerto 443 que son muy importantes para la configuración web del servidor, entre otras reglas más que permiten definir el acceso a las funciones del servidor.

Dado que el servidor de comunicaciones unificadas está a su vez conectado con un servidor de red, en este servidor que es el que tiene la dirección IP Pública, y permite las conexiones remotas también se han establecido IPTables mismas que se muestran en la figura 38.

IPTABLES servidor de red

```
# Generated by iptables-save v1.4.7 on Sun Jun 28 23:30:34 2015
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A PREROUTING -p tcp -m tcp --dport 3448 -j DNAT --to-destination 192.168.40.150:443
-A PREROUTING -p udp -m udp --dport 4569 -j DNAT --to-destination 192.168.40.150:4569
-A PREROUTING -p tcp -m tcp --dport 8686 -j DNAT --to-destination 192.168.1.1:443
-A PREROUTING -p tcp -m tcp --dport 8687 -j DNAT --to-destination 192.168.40.150:22
-A PREROUTING -p tcp -m tcp --dport 9898 -j DNAT --to-destination 192.168.1.123:80
-A PREROUTING -p tcp -m tcp --dport 2202 -j DNAT --to-destination 192.168.1.232:202
-A PREROUTING -p tcp -m tcp --dport 3449 -j DNAT --to-destination 192.168.1.232:443
-A PREROUTING -p tcp -m tcp --dport 5004:5005 -j DNAT --to-destination 192.168.1.232:5004-5005
-A PREROUTING -p tcp -m tcp --dport 2201 -j DNAT --to-destination 192.168.1.232:201
-A PREROUTING -p tcp -m tcp --dport 4040 -j DNAT --to-destination 192.168.1.81:4040
-A PREROUTING -p tcp -m tcp --dport 5050 -j DNAT --to-destination 192.168.1.123:80
-A PREROUTING -p tcp -m tcp --dport 9443 -j DNAT --to-destination 192.168.1.81:443
-A PREROUTING -p tcp -m tcp --dport 1199 -j DNAT --to-destination 192.168.1.170:1199
```

Figura 38. IPTables Servidor de Red.

Elaborado por: Jefferson Guevara

- También es importante el cambio de los puertos que se asignan por defecto a través de una traducción de puertos que se realiza generalmente en el router o servidor de red.

  Cuando se intenta realizar un ataque al servidor se buscan los puertos configurados por defecto y al cambiarlos se complicaría el trabajo del atacante. Para la empresa RACOMDES S.A. se cambiaros los puertos de SSH, de VPN y de las extensiones remotas.

- Una de las medidas más importantes a nivel de seguridad es el escaneo de logs, para esto se usa el software de Fail2Ban que identifica intentos de autentificación al servidor y si realiza una autentificación fallida después de un cierto número de intentos, se bloquea automáticamente la dirección IP del atacante.

  En el caso del servidor Elastix se puede instalar a través del comando *#yum -y install fail2ban*y se inicia el proceso a través del comando # *service fail2ban start*, al iniciarlo fail2ban se asocia con las reglas de IPTables.

  En la figura 39 se muestra la configuración de IPTables sobre SSH y los bloqueos a direcciones atacantes.

Fail2Ban servidor de red

```
:OUTPUT ACCEPT [36042:23151056]
:fail2ban-SSH - [0:0]
-A INPUT -p tcp -m tcp --dport 22 -j fail2ban-SSH
-A INPUT -p tcp -m tcp --dport 22 -j fail2ban-SSH
-A INPUT -s 31.2.128.0/17 -j DROP
-A INPUT -s 31.11.40.0/21 -j DROP
-A INPUT -s 31.14.0.0/16 -j DROP
-A INPUT -s 31.47.208.0/21 -j DROP
-A INPUT -s 31.133.24.0/21 -j DROP
-A INPUT -s 31.133.96.0/21 -j DROP
-A INPUT -s 31.173.0.0/16 -j DROP
-A INPUT -s 31.215.0.0/16 -j DROP
-A INPUT -s 31.220.128.0/21 -j DROP
-A INPUT -s 46.19.104.0/21 -j DROP
-A INPUT -s 46.20.128.0/20 -j DROP
```

Figura 39. Fail2Ban sobre SSH servidor de red RACMODES S. A.

Elaborado por: Jefferson Guevara

- Otro punto a tomar en cuenta también es el acceso de equipos remotos al servidor a través de una red privada virtual (VPN), de esta manera se asegura que la información pase por los enlaces del servidor Elastix y esté encriptada.

Para la empresa se consideró trabajar con la aplicación Easy VPN que se instaló en el servidor y para los clientes remotos se utilizó el cliente OpenVPN.

- La utilización de corta fuegos *Firewall* es fundamental para la seguridad del servidor, el servidor Elastix ya incluye en su interfaz WEB la administración de firewall como se muestra en la figura 40, pero además se ha configurado firewall en el servidor de red ya que este contiene la dirección IP pública que permite conexiones remotas.

Firewall en Elastix

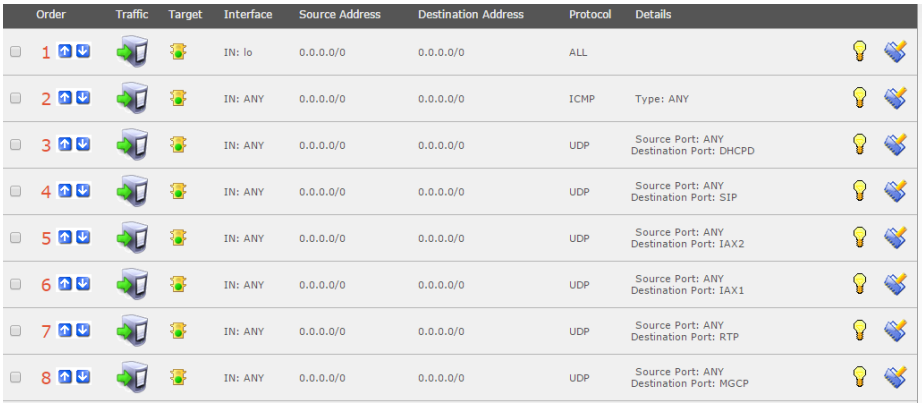


Figura 40. Firewall de servidor Elastix vía WEB.

Elaborado por: Jefferson Guevara

CAPÍTULO 4

PRUEBAS DE FUNCIONAMIENTO

4.1 Pruebas de central de telefonía IP

Para comprobar el funcionamiento de la central de telefonía IP se puede ingresar a través de la interfaz WEB de Elastix a la pestaña de reportes y se verifica el historial de llamadas realizadas por cada uno de los usuarios, esto también se puede realizar a través de la consola CLI de Asterisk se coloca el comando *sip show peers* para verificar las conexiones tanto de extensiones creadas como del enlace con el Gateway Grandstream que asocia a la central con las líneas analógicas; esto se muestra en la figura 41.

Pruebas de Telefonía IP

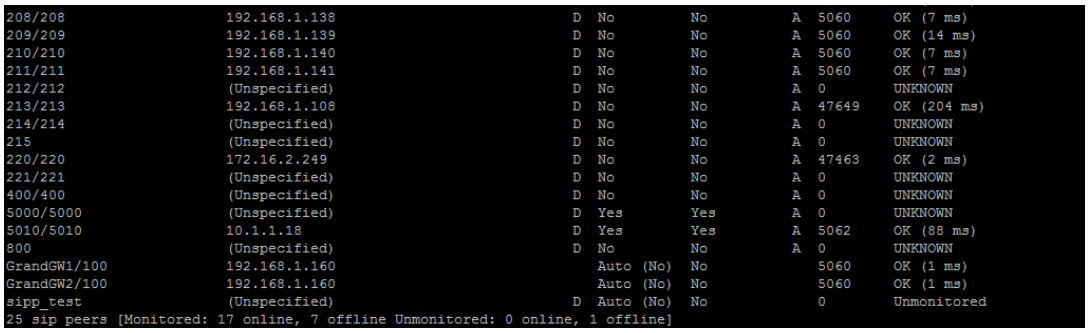


Figura 41. Pruebas de conexiones SIP de central Elastix

Elaborado por: Jefferson Guevara

En el Anexo 2 se muestran los teléfonos IP que fueron instalados en la empresa y que ahora permiten la realización y recepción de llamadas.

4.2 Pruebas de mensajería instantánea

Las pruebas de mensajería instantánea se realizan desde la plataforma Elastix con el envío de mensajes masivos a través de Ozeki que es una aplicación para celulares Android que funciona como gateway para telefonía móvil. En la figura 42 se puede observar la configuración para el envío de mensajes masivos desde la WEB de Elastix.

Pruebas mensajería instantánea

Figura 42. Pruebas de Elastix para envío masivo de mensajes

Elaborado por: Jefferson Guevara

4.3 Pruebas de Presencia remota

Para las pruebas de presencia remota, se colocó un cliente VPN en un celular con plataforma Android el cual a través de la carga del archivo generado por la central IP de Elastix mediante el servicio de OpenVPN y con la instalación de la aplicación Zoiper que es un Softphone o teléfono IP virtual se pudo acceder a la central con una extensión asignada desde cualquier red.

En la figura 43 se puede observar el servicio de OpenVPN y Zoiper funcionando en el celular Android mismo que está conectado a la red de su proveedor de telefonía móvil.

Pruebas de Presencia Remota

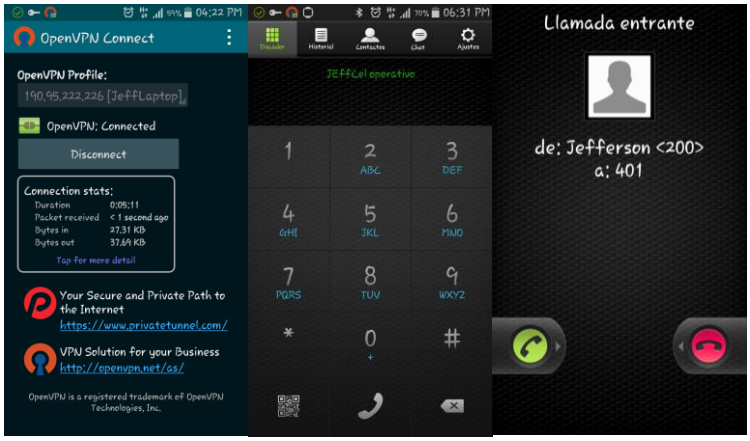


Figura 43. Pruebas de asistencia remota sobre celular Android

Elaborado por: Jefferson Guevara

4.4 Pruebas de video conferencia

Para las pruebas del servicio de video conferencia se utilizaron softphones XLITE que tienen soporte para video, es necesario realizar la activación de códecs tanto en la central como en cada uno de los teléfonos, los códecs de video que se utilizan son: H263, H263p y H264.

En la figura 44 se puede ver una foto de unavideo llamada realizada a través de 2 softphones XLITE.

Pruebas de video conferencia

Figura 44. Pruebas de video conferencia

Elaborado por: Jefferson Guevara

4.5 Pruebas de correo electrónico

La asociación con correo electrónico se va a realizar a través de voicemail, es decir que los mensajes de voz que lleguen al teléfono IP cuando la persona esté ausente, llegarán también con una notificación y un archivo con extensión .wav al correo seleccionado en la configuración de las extensiones

En la figura 45, se muestra la recepción de un mensaje dejado en la central para la extensión 200 con el archivo adjunto respectivo.

Pruebas de correo electrónico

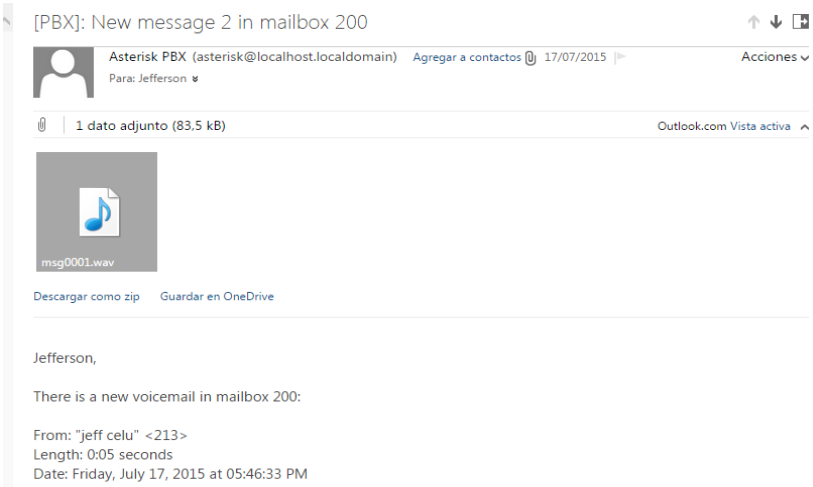


Figura 45, Pruebas Voicemail

Elaborado por: Jefferson Guevara

4.6 Pruebas de QoS

Las pruebas de calidad de servicio se realizan a través de la herramienta para Windows Wireshark que permitirá el análisis de ancho de banda usado en una llamada, además de mostrar los tiempos de latencia, jitter y pérdida de paquetes.

Para el análisis de uso de ancho de banda se va a realizar una gráfica en Wireshark donde la línea negra representa el consumo de voz en la red, la línea roja el consumo de datos en la red y la línea verde la sumatoria de datos y voz. Se verifica a través de esta herramienta que el uso de ancho de banda en una llamada SIP con duración de 30 segundos, aproximadamente es de 0.350 Megabytes que son consumidos en la red y que claramente no afectarán al desempeño de la misma.

En la figura 46 se pude observar la gráfica de Wireshark del consumo de ancho de banda utilizado en una llamada SIP del servidor Elastix.

Se decidió además para asegurar QoS, colocar a la red de voz que está en el rango de direcciones desde 192.168.1.125 hasta 192.168.1.180dentro de una VLAN configurada en el switch de distribución, definir parámetros máximos de ancho de

banda para conexión de 1,5 Mb, que resulta suficiente para el correcto funcionamiento del servidor.

Consumo de ancho de banda

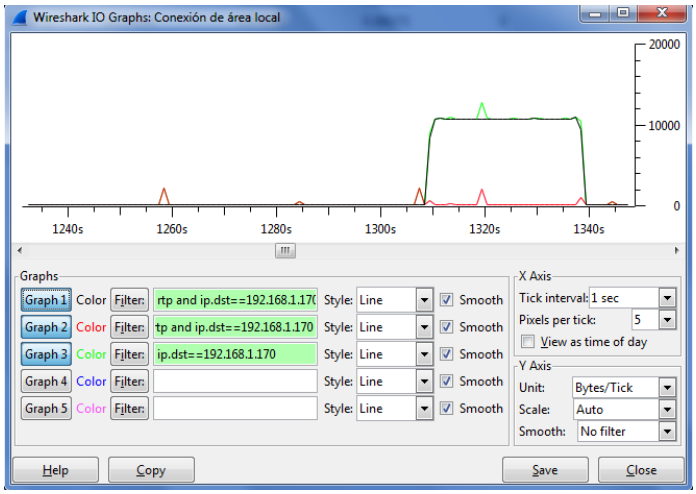
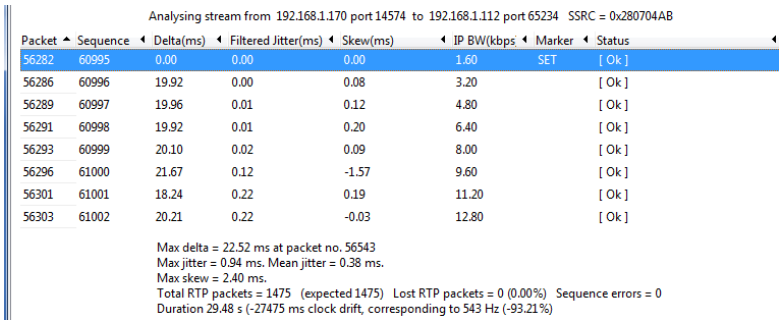


Figura 46. Pruebas consumo de ancho de banda

Elaborado por: Jefferson Guevara

Además del consumo de ancho de banda Wireshark permite monitorear el retardo, el jitter y errores en la entrega de paquetes, tal como se muestra en la figura 47.

Latencia, Jitter y pérdida de paquetes



Analysing stream from 192.168.1.170 port 14574 to 192.168.1.112 port 65234 SSRC = 0x280704AB

Packet	Sequence	Delta(ms)	Filtered Jitter(ms)	Skew(ms)	IP BW(kbps	Marker	Status
56282	60995	0.00	0.00	0.00	1.60	SET	[Ok]
56286	60996	19.92	0.00	0.08	3.20		[Ok]
56289	60997	19.96	0.01	0.12	4.80		[Ok]
56291	60998	19.92	0.01	0.20	6.40		[Ok]
56293	60999	20.10	0.02	0.09	8.00		[Ok]
56296	61000	21.67	0.12	-1.57	9.60		[Ok]
56301	61001	18.24	0.22	0.19	11.20		[Ok]
56303	61002	20.21	0.22	-0.03	12.80		[Ok]

Max delta = 22.52 ms at packet no. 56543
Max jitter = 0.94 ms. Mean jitter = 0.38 ms.
Max skew = 2.40 ms.
Total RTP packets = 1475 (expected 1475) Lost RTP packets = 0 (0.00%) Sequence errors = 0
Duration 29.48 s (-27475 ms clock drift, corresponding to 543 Hz (-93.21%)

Figura 47. Reporte QoS de Elastix

Elaborado por: Jefferson Guevara

Mediante las pruebas realizadas de calidad de servicio se puede determinar el correcto funcionamiento del servidor, pues la pérdida de paquetes no supera el 1% del total de la carga y los retardos y jitters no superan los 100ms que son los valores mínimos para una comunicación de calidad.

4.7 Pruebas de Hacking Ético

Para realizar las pruebas de hacking ético a través de NMAP es necesario usar el comando *# nmap 192.168.1.170* que va a mostrar el detalle de los puertos abiertos en el servidor, tal como se muestra en la figura 48.

NMAP en Elastix

Figura 48. Ejecución de NMAP en el servidor Elastix.

Elaborado por: Jefferson Guevara

Como se puede observar a través de este ataque voluntario con NMAP al servidor, se identifica que existen varios puertos abiertos los cuales podrían causar ingresos al servidor no deseados, los cuales deben ser contrarrestados mediante la implementación de seguridades adecuadas.

4.8 Pruebas de seguridades en el servidor

Para las pruebas de seguridad se verifica a través de fail2ban los intentos de ingreso al servidor fallidos y los bloqueos que ha tenido el servidor, debido a que el servidor de Elastix fue instalado sobre otro servidor de red con sistema operativo CentOS se ha configurado el servicio de fail2ban en los 2 servidores asegurando aún más la red.
En la figura 48 se muestran los intentos los intentos fallidos sobre el servidor de red y los que se han registrado en el servidor Elastix.

Pruebas de Fail2Ban

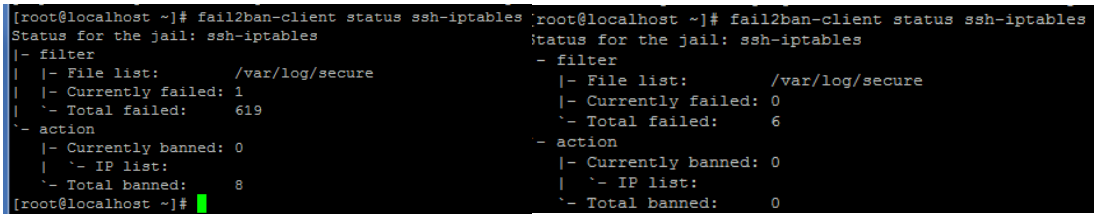


Figura 49. *Pruebas de seguridad con fail2ban en servidor de red CentOS y Elastix respectivamente*
Elaborado por: Jefferson Guevara

Con esto se verifica en las IPTABLES los bloqueos de puertos a través de firewall y que el trabajo de fail2ban se está realizando correctamente.

CONCLUSIONES

- Se diseñó e implementó un sistema de comunicaciones unificadas en base al software libre Elastix en servicios de telefonía presencial y remota, mensajería, video llamada y correo electrónico; dicho software permite quelos empleados tengan una comunicación permanente con los clientes sin importar si están o no dentro de la empresa y permite la administración de todas las aplicaciones en una sola consola haciendo más fácil la administración de los servicios.

- Se determinaron requerimientos mínimos para el correcto funcionamiento del sistema de comunicaciones unificadas dentro de la empresa, con el análisis de parámetros de ancho de banda con un valor de 2,5 Mbytes, cantidad de usuarios que serán 21 en total, tráfico en la red 512 Kilobytes y cantidad de llamadas que se realizan en el servidor que son un aproximado de 10 llamadas concurrentes.

- Se implementó seguridad a través de fail2ban que informa por medio de correo electrónico y reportes desde la consola de los intentos de ingreso externos al servidor y bloquea a las direcciones que intenten este registro, evitando posibles ataques en el sistema y dando información en tiempo real del tráfico, llamadas, problemas de conexión e intentos de ingreso dentro del servidor.

- Se configuró el servidor de acuerdo a los requerimientos individuales de cada empleado de la empresa limitando el acceso de varias aplicaciones de administración y configurando contraseñas individuales, dando así acceso a los usuarios únicamente a sus respectivas cuentas y evitando cambios en el servidor que afecten el funcionamiento del sistema.

- Se configuraron algunos valores en la opción de parámetros de progreso de llamadas en el gateway Grandstream, entre estos parámetros están: dial tone, ring back tone, busy tone y reorder tone, en los cuales se fijaron frecuencias de 425 Mhz, puesto que estos valores permiten a través de la sincronización de tiempo, el correcto y preciso funcionamiento de marcado y colgado en la realización de una llamada.

- Con respecto a las pruebas realizadas sobre el servidor de comunicaciones unificadas se verificó el cumplimiento de parámetros mínimos para el correcto funcionamiento, tales como: la pérdida de paquetes máxima que por medio de la herramienta Wireshark se comprobó no supera el 1%, otros valores comprobados fueron la latencia y el jitter que presentaron valores inferiores a los 100ms entre el inicio y finalización de una llamada permitiendo así una comunicación de calidad.

RECOMENDACIONES

- Se recomienda colocar un servidor redundante y sacar un respaldo de configuraciones para realizar un reemplazo en caso de que se presente una falla en el servidor principal, al colocar un servidor redundante en un caso de emergencia se tendría toda la información respaldada y sobre todo la empresa no se quedaría incomunicada por un largo periodo de tiempo.

- Se debe colocar un equipo de almacenamiento externo que puede ser un arreglo de discos o memorias externas que permitan la grabación de llamadas y correos que lleguen a la empresa, evitando así la saturación en la memoria interna del servidor, puesto que al llenar esta memoria el servidor empieza a presentar fallas en la comunicación y con las funciones de comunicaciones unificadas.

- Se recomienda asociar un correo electrónico que reciba un reporte diario de logs o eventos que ocurran en el servidor, permitiendo tener una información diaria del rendimiento del servidor y dando lugar en caso de errores a soporte y mantenimiento remoto.

- Se recomienda tener al servidor de comunicaciones y en general al rack de comunicaciones con un respaldo de energía para no permitir por fallas de energía cortes abruptos en los servicios y evitando posibles errores en la inicialización de los servicios del sistema de comunicaciones unificadas.

- Se recomienda el uso de un switch PoE *Power over Ethernet*, puesto que los teléfonos están conectados a la energía eléctrica a través de adaptadores y en un posible corte de energía los teléfonos deben seguir en funcionamiento y permitir a los usuarios estar comunicados en todo momento

LISTA DE REFERENCIAS

Veneta, A., & Ladrón , A. (2009). Interacciones tecnológicas y efectos red: claves para predecir el impacto del VOIP sobre la industria de las telecomunicaciones. Madrid: Portal Universia S.A.

Atelin, P., & Dordoigne, J. (2007). *TCP/IP y protocolos de Internet.* Barcelona: ENI.

Barceló, O., Íñigo, G., & Llorente, V. (2008). *Protocolos y aplicaciones Internet.* España: UOC.

Calazacón, J. (Eenero de 2015). DESARROLLO DE PROTOTIPO DE UNA RED VOIP SEGURA MEDIANTE VPN UTILIZANDO SOFTWARE LIBRE, PARA LA COMUNICACIÓN DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR, SEDE SANTO DOMINGO. Santo Domingo, Santo Domingo, Ecuador.

Calero, C. (16 de Marzo de 2015). Rediseño e implementación de mejoras al sistema voip en la Universidad Agraria del Ecuador, Campus Guayaquil (tesis de pregrado). Guayaquil, Guayas, Ecuador.

ELASTIXTECH. (12 de Diciembre de 2014). *ElASTIXTECH Elastix.* Obtenido de http://elastixtech.com/qos-calidad-de-servicio-para-voip/

Flanagan, W. (2012). *Understanding VoIP and Unified Communications: Internet Telephony and the Future Voice Network.* Hoboken: John Wiley & Sons.

Gómez, J. (2008). *VoIP y Asterisk: redescubriendo la telefonía.* España: RA-MA.

Herrera, E. (2003). *Tecnologías y redes de transmision de datos.* México: Limusa.

Hillar, G. (2009). *Redes: diseño, actualización y reparación.* Argentina: Editorial Hispano Americana HASA.

Johnston, A., & Piscitello, D. (2006). *Understanding Voice over IP Security.*Norwood: Artech House.

Landivar, E. (07 de Julio de 2011). Comunicaciones Unificadas en Elastix. Guayaquil, Guayas, Ecuador.

Molina, F., & Polo, O. (2014). *Servicios de red e internet.* España: RA-MA.

Porter, T., Kanclirz, J., & Zmolek, A. (2006). *Practical VoIP Security*. Rockland, MA: Syngress Publishing.

Santos, M. (2014). *Sistemas Telemáticos.* España: RA-MA.

Triana, F. (21 de Julio de 2014). La telefonía IP y su incidencia en el apoyo a la gestión de la Universidad Técnica Estatal de Quevedo. Propuesta alternativa, (tesis de pregrado). Quevedo, Los Ríos, Ecuador.

ANEXOS

Anexo 1. Especificaciones técnicas de los equipos empresa RACOMDES S.A.

MODELO	IMAGEN	FUNCIÓN
Servidor HP Proliant ML310E GEN8 V2		Servidor dedicado para enlaces de radiocomunicación y servidor Elastix de la empresa RACOMDES S.A.
Servidor HP Proliant ML110 G7		Servidor dedicado para configuración de red interna de la empresa.
Switch Cisco SMALL BUSINESS		Switch de Distribución de puntos de red internos.
HP Router A-MSR 900 JF812A		Router de ISP Telconet asignación de direcciones IP públicas para la empresa
Panasonic KX-TEM824		Central Telefónica Analógica existente

Panasonic KX-TS520LX		Teléfono analógico utilizado para extensiones en la empresa
Panasonic KXT-7730		Teléfono analógico utilizado para recepción

Anexo 2. Teléfonos IP instalados en la empresa

Anexo 3. Condiciones actuales del Rack de comunicaciones