Diseño e implementación de un sistema de acceso y alarma comunitaria basado en pbx voip virtuales para áreas residenciales

Cellere Guaman, Jonathan Marcelo y Nuñez Camacho, Berner Eduardo

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Trabajo de titulación, previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones

Ing. Aguilar Salazar, Darwin Leónidas

17 de junio del 2021

Curiginal

Document Information

Analyzed document	Tesis_v2(2)_versión final.docx (D107421108)
Submitted	6/1/2021 8:49:00 PM
Submitted by	
Submitter email	dlaguilar@espe.edu.ec
Similarity	5%
Analysis address	dlaguilar.espe@analysis.urkund.com

Sources included in the report

W	URL: https://docplayer.es/amp/30496924-Estudio-de-una-aplicacion-voz-sobre-ip-voip.html Fetched: 10/30/2019 8:11:22 PM	1
SA	**Tesis Laboratorio IP - Maestria Teleco.docx** Document Tesis Laboratorio IP - Maestria Teleco.docx (D12122484)	1
W	URL: http://www.emb.cl/gerencia/articulo.mvc?xid=2356&ni=telefonia-ip-cambio-de-paradigma-en-lascomunicaciones-empresarialesBhutani, Fetched: 6/1/2021 8:52:00 PM	2
SA	**Tesis_PazminoSantiago.docx** Document Tesis_PazminoSantiago.docx (D61978246)	6
SA	**Tesis de grado.docx** Document Tesis de grado.docx (D14319450)	1
W	URL: https://www.timetoast.com/timelines/1519798 Fetched: 6/1/2021 8:52:00 PM	1
W	URL: http://www.repositorio.usac.edu.gt/3752/1/Mauricio%20Gerardo%20L%C3%B3pez%20Maldonado.pdf Fetched: 4/16/2021 10:28:09 PM	1
W	URL: https://ddd.uab.cat/pub/trerecpro/2010/hdl_2072_117457/PFC_TomasVelazquezGarcia.pdf Fetched: 10/15/2019 7:01:11 PM	2
W	URL: http://www.estrellateyarde.org/wp-content/uploads/file/sistema-voip-basado-en-asterisk-antonio-sierra.pdf Fetched: 4/25/2021 1:30:20 PM	1
W	URL: https://iie.fing.edu.uy/ense/asign/ccu/material/docs/Codificacion%20de%20voz%20y%20video%20(presentacion).pdf Fetched: 6/1/2021 8:52:00 PM	4
SA	**TESIS_GIOVANY_GUDINO_FINAL4_BACKUP.pdf** Document TESIS_GIOVANY_GUDINO_FINAL4_BACKUP.pdf (D20033899)	1
SA	**Proyecto de grado (final).docx** Document Proyecto de grado (final).docx (D23730812)	1

1/57

Firmado electrónicamente por:
DARWIN LEONIDAS
AGUILAR SALAZAR

.....

Ing. Aguilar Salazar, Darwin Leónidas

CC: 1103036826

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Diseño e implementación de un sistema de acceso y alarma comunitaria basado en pbx voip virtuales para áreas residenciales**" fue realizado por los señores **Cellere Guaman, Jonathan Marcelo y Nuñez Camacho, Berner Eduardo** el cual ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí,01 de junio del 2021

Firmado electrónicamente por:
DARWIN LEONIDAS AGUILAR SALAZAR

Ing. Aguilar Salazar, Darwin Leónidas

CI: **1103036826**

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

RESPONSABILIDAD DE AUTORÍA

Nosotros, **Cellere Guaman, Jonathan Marcelo y Nuñez Camacho, Berner Eduardo**, con cedulas de ciudadanía n° 1723073472 y 1723045025, declaramos que el contenido, ideas y criterios del trabajo de titulación**: "Diseño e implementación de un sistema de acceso y alarma comunitaria basado en pbx voip virtuales para áreas residenciales"** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 17 de junio del 2021

Cellere Guaman, Jonathan Marcelo

CC: 1723073472

Nuñez Camacho, Berner Eduardo

CC: 1723045025

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERIA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, Cellere Guaman, Jonathan Marcelo y Nuñez Camacho, Berner Eduardo, con cedulas de ciudadanía n° 1723073472 y 1723045025, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Diseño e implementación de un sistema de acceso y alarma comunitaria basado en pbx voip virtuales para áreas residenciales"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi/nuestra responsabilidad.

Sangolquí, 17 de Junio del 2021

Cellere Guaman, Jonathan Marcelo

CC: 1723073472

Nuñez Camacho, Berner Eduardo

CC: 1723045025

Dedicatoria

Dedico este trabajo a mi madre, por ser uno de los pilares más importantes de mi vida, por siempre demostrarme su cariño, su apoyo incondicional y así nunca darme por vencido y siempre perseverar por alcanzar mis sueños. A mi padre que siempre se esforzó para que nunca me falte nada y de esta manera tener una buena educación y lograr trazar mi camino con éxito. A mis dos hermanas Alexandra y Kerlly por estar conmigo en todo momento, gracias por brindarme su apoyo incondicional. A mi tía Blanca, a quien quiero como una madre, por compartir momentos significativos. También va dedicado a toda mi familia, amigos y profesores que han aportado y orientado con sus consejos y de esta manera poder crecer tanto profesional y como ser humano.

Berner Eduardo Nuñez Camacho

Dedicatoria

En mi vida he logrado aprender muchas cosas diferentes y esto es gracias a mis hermanos, mi madre, mis abuelos y toda mi familia, por ello debo dedicar este trabajo y esfuerzo a todos ellos, ya que me han ayudado y apoyado de manera incondicional, agradezco a mis abuelos de manera especial por los valores que siempre me inculcaron y su confianza en mí. A mis hermanos quienes siempre me han ayudado y apoyado para trazar con éxito un nuevo rumbo en mi vida, a mi madre que ha hecho lo mejor por mí y mis hermanos, inculcándonos sus valores, de igual forma, debo dedicar este trabajo a mis amigos y compañeros que me han ayudado en todo el trayecto que he tenido dentro de la universidad, ya que me han ayudado a superarme como persona y de manera profesional.

.

Jonathan Marcelo Cellere Guaman

Agradecimiento

Agradezco a Dios por darme las fuerzas necesarias para no decaer o rendirme en alguna etapa de mi carrera y así poder culminar este objetivo de mi vida con éxito. A mis Padres por haberme enseñado que, con esfuerzo, dedicación puedo alcanzar mis sueños, me dieron su apoyo incondicional para no decaer cuando todo parecía complicado e imposible. A mi tutor de tesis, por haberme brindado su apoyo, su conocimiento y por haberme ayudado a desarrollarme profesionalmente.

Berner Eduardo Nuñez Camacho

Agradecimiento

Mi agradecimiento principal es con Dios por cuidarme y guiarme durante mi vida, debo agradecer a mis abuelos, hermanos y mi madre por ayudarme en todo el camino y dificultades que han debido suceder para alcanzar esta meta, gracias por su apoyo y guía incondicional. Agradezco de igual forma a mi tutor por darnos su apoyo y tiempo para inculcar en nosotros nuevos conocimientos y ayudarnos a desarrollarnos de manera profesional.

Jonathan Marcelo Cellere Guaman

Índice de Contenidos

Urkund.....2
Certificación.....3
Responsabilidad de Autoría.....4
Autorización de publicación.....5
Dedicatoria.....6
Agradecimiento.....8
Resumen.....19
Abstract.....20
Capítulo I.....21
Planteamiento del problema de investigación.....21
Antecedentes.....21
Justificación.....22
Alcance.....24
Objetivos.....24
Objetivo General.....24
Objetivos Específicos.....24
Capítulo II.....26
Fundamento Teórico.....26
Introducción......26
Telefonía Tradicional (PSTN).....26
Historia de la telefonía IP.....27
Estructura de una red VoIP.....28
Diferencias entre VoIP y Telefonía IP.....31
Estándar VoIP.....32
Protocolos.....32

SIP 33

RTP 38

Cabecera RTP 40

RTCP 42

Cabecera RTCP 43

SRTP 47

Cabecera SRTP 48

Arquitectura VoIP 50

Terminales IP 52

Gateways y adaptadores analógicos 52

Tipos de PBX 53

Asterisk 55

FreeSwitch 55

FreePBX 56

Issabel 57

VitalPBX 57

Elección de la plataforma de desarrollo 58

Códecs 59

Valores de medición 64

Cloud-Hosting 67

Asterisk 68

Introducción 68

Definición 69

Principales características de Asterisk 70

Arquitectura 71

Zabbix 73

No-IP 74

Fail2ban 74

Capítulo III 75

Análisis, Diseño e Implementación del Sistema 75

Introducción 75

Definición de los escenarios 76

Requerimientos de la Urbanización 77

Análisis de la propuesta de diseño e implementación 78

Sistema de monitoreo y control de acceso 78

Sistema de monitoreo y control de acceso 79

Análisis de implementación del sistema de control de acceso en contraste con los requerimientos de los usuarios 79

Análisis para la elección del plan de alojamiento del Servidor de Telefonía 79

Software 82

Acrobits Groundwire 83

Linphone 83

SessionTalk SIP 83

Softphone 84

Zoiper 84

Elección del softphone 84

Análisis de implementación del sistema de Alarma Comunitaria contraste con los requerimientos de los usuarios. 87

Análisis de Sonorización 87

Hardware 97

Evaluación del sistema de Perifoneo 97

Implementación del sistema 112

Diseño de software 112

Instalación de Asterisk 112

Sip.conf 113

Extensions.conf 116

Voicemail.conf 121

E-mail 121

Fail2Ban 123

MariaDB 126

Zabbix 132

Página Web 136

Diseño de Hardware 141

Capítulo IV 142

Análisis de resultados 142

Introducción.....142

Análisis de la instalación.....142

Análisis de desempeño y funcionamiento del sistema considerando QoS.....145

Análisis de protocolos de seguridad para la central virtual IP.....156

Análisis de costos.....158

Capítulo V.....160

Conclusiones y recomendaciones.....160

Conclusiones.....160

Recomendaciones.....163

Trabajos futuros.....164

Referencias.....166

Anexos.....172

Índice de Tablas

Tabla 1 Tabla Resumen troncales E1 / T1 30
Tabla 2 Protocolos VoIP 33
Tabla 3 Respuestas y peticiones SIP 35
Tabla 4 Paquetes RTCP 42
Tabla 5 Clasificación de los códecs de acuerdo a su frecuencia de trabajo 60
Tabla 6 Códecs de Banda angosta (NB) 60
Tabla 7 Códecs de banda ancha (WB) 62
Tabla 8 Códecs de super banda ancha (SWB) 63
Tabla 9 Códecs de banda completa 63
Tabla 10 R-Factor y MOS 65
Tabla 11 Comparaciones de los diferentes softphone 85
Tabla 12 Niveles acústicos aproximados de la voz referente a 1 metro de distancia del hablante. 90
Tabla 13 Rango de frecuencia y niveles sonoros de algunos instrumentos 91
Tabla 14 E jemplos de Ruido con sus determinados niveles de frecuencia y nivel sonoro. 92
Tabla 15 Atenuación del sonido en base a diferentes frecuencias 94
Tabla 16 Especificaciones de parlantes IP 98
Tabla 17 Especificaciones de parlantes IP 100
Tabla 18 Especificaciones de la interfaz OPTIMUS IA-20SIP 101
Tabla 19 Especificaciones de los altavoces IP 103
Tabla 20 Especificaciones de los Gateway megafonía IP 105
Tabla 21 V alor estimado de los dispositivos IP. 107
Tabla 22 Especificaciones del altavoz HN-30P 109
Tabla 23 Especificaciones del amplificador BT-309A 110
Tabla 24 Equipos y materiales utilizados para la implementación del sistema. 141
Tabla 25 MOS obtenido de la plataforma VoIP Spear 151
Tabla 26 Latencia obtenida de la plataforma VoIP Spear 152
Tabla 27 Parámetros de QoS 153
Tabla 28 Costo del dispositivo implementado 159

Índice de Figuras

Figura 1 Capa del modelo OSI 29
Figura 2 Sesión de llamada SIP entre dos teléfonos 34
Figura 3 SIP en modelo TCP/IP 36
Figura 4 Mensajes SIP en una comunicación entre dos usuarios 37
Figura 5 Funcionamiento de un Mixer 39
Figura 6 Funcionamiento de un traductor 40
Figura 7 Estructura de un paquete Ethernet considerando RTP 41
Figura 8 Cabecera del paquete RTP 41
Figura 9 Cabecera común RTCP 44
Figura 10 Paquete sender report 44
Figura 11 Paquete Receiver report 45
Figura 12 Paquete source description 46
Figura 13 Cabecera del paquete BYE 46
Figura 14 Cabecera de paquete APP 46
Figura 15 Codificación y decodificación del protocolo SRTP 48
Figura 16 Cabecera SRTP 49
Figura 17 Arquitectura VoIP 51
Figura 18 Ejemplo de Conexión de un ATA 53
Figura 19 Comparación de códecs de banda angosta en base a MOS 66
Figura 20 Comparación de códecs de banda ancha en base a MOS 66
Figura 21 Comparación de códecs de super banda ancha en base a MOS 67
Figura 22 Características de una central Asterisk 71
Figura 23 Estructura modular de Asterisk 72
Figura 24 Planes de los Droplets disponibles en Digital Ocean. 82
Figura 25 Logo Acrobits Groundwire 87
Figura 26 Niveles de presión Sonora 89
Figura 27 Dnámica de los sonidos 90
Figura 28 Atenuación de una fuente puntual 93
Figura 29 Zona seleccionada para la instalación del parlante IP 94
Figura 30 Cálculo de la distancia en base a triángulos para obtener la atenuación del parlante 96
Figura 31 Parlantes IP de KNTECH 99
Figura 32 Parlantes IP de CINETO 101

Figura 33 Equipo IA-20SIP 102
Figura 34 A ltavoces IP de CYSER SYSTEM 104
Figura 35 Gateway megafonía IP 106
Figura 36 TV-BOX Tx3 Mini 108
Figura 37 Altavoz HN-30P 110
Figura 38 Amplificador BT-309ª 111
Figura 39 Estado de la plataforma Asterisk activado 113
Figura 40 Correo recibido 120
Figura 41 Configuración de Asterisk en Fail2ban en el archivo jail.conf 124
Figura 42 Configuración de Asterisk en Fail2ban en el archivo jail.local 125
Figura 43 Estado de la herramienta Fail2ban para el servicio de Asterisk 126
Figura 44 Configuración para acceso remoto de la base de datos 130
Figura 45 Configuración del archivo odbcinst.ini 130
Figura 46 Configuración del archivo odbc.ini 131
Figura 47 Configuración del archivo res_odbc.conf 132
Figura 48 Configuración del archivo cdr_adaptive_odbc.conf 132
Figura 49 Configuración del archivo snmpd.conf 133
Figura 50 Configuración del Host en Zabbix 133
Figura 51 Creación y configuración de una aplicación en Zabbix 134
Figura 52 Aplicaciones creadas en Zabbix para el monitoreo de Asterisk 135
Figura 53 Vista de la página Web urbanización San Francisco 136
Figura 54 Vista de la pestaña Acerca de nosotros de la página web 138
Figura 55 Vista de la pestaña información de la página web 138
Figura 56 Vista de la pestaña cartelera de la página web 139
Figura 57 Vsta de la pestaña login de la página web 139
Figura 58 Vista del registro de llamadas de la página Web 140
Figura 59 Diagrama de bloques 142
Figura 60 Instalación de la bocina 144
Figura 61 Ingreso de personas externas 145
Figura 62 Calidad de sonido 146
Figura 63 Calidad de video 147
Figura 64 Seguridad de la urbanización 147
Figura 65 Perifoneo 148
Figura 66 I nstalación del sistema (Softphone) 149
Figura 67 Preferencia de dispositivos para utilizar el sistema 150

Figura 68 Cantidad de llamadas procesadas por la centralita VoIP medidas a través de Zabbix 155
Figura 69 Captura de tráfico de la llamada sin el protocolo SRTP 157
Figura 70 Captura de tráfico de la llamada con el protocolo SRTP 158

Resumen

En el presente proyecto de titulación se desarrolló un sistema de acceso y alarma comunitaria basado en PBX VoIP virtuales para áreas residenciales en el cual se utilizó el software Asterisk para realizar la implementación de la central de telefonía IP, la cual está alojada en un Cloud Services, en consecuencia, se realizó un estudio del estado del arte comparando las diferentes soluciones que hoy en día están disponibles y se comercializan en el mercado, puesto que en la actualidad existen un sinfín de soluciones, de las cuales no todas se adaptan a las necesidades requeridas por los moradores de las áreas residenciales.

Se diseñó e implementó un sistema sencillo con múltiples funcionalidades como es el sistema de accesos a través de audio y video, avisos de eventos particulares mediante un altavoz los mismos que pueden ser enviados mediante correo electrónico a los usuarios del sistema y activación de una alarma comunitaria, al mismo tiempo, se realizaron diferentes configuraciones para garantizar la seguridad del sistema y de la privacidad de los datos de los usuarios.

Por otra parte, para mejorar la experiencia del usuario se realizó una página web diseñada especialmente para la urbanización en la cual se realizó la implementación, conviene destacar que una de las principales funcionalidades es que se puede visualizar el registro de llamadas que contiene varios detalles de las mismas como la duración de la llamada, el número de origen y de destinatario, entre otros.

PALABRAS CLAVE:

- **ASTERISK**
- **CLOUD SERVICES**
- **TELEFONÍA IP**

Abstract

To begin with in this project developed a community Access and alarm system base on Virtual PBX VoIP for residential areas in which Asterisk software was used to implement the IP PBX phone system, which is hosted in a Cloud Services. consequently, a state of the art study was carried out comparing the different solutions that are available and marketed in the market today, however today there are countless solutions, of which not all adapt to the needs required by the residents of the residential areas.

It was designed and implemented a simple system with multiple functionalities such as the system of access via audio and video, notices of particular events by means of a speaker the same ones that can be sent by e-mail to the users of the system and activation of a community alarm, at the same time, different configurations were made to ensure the security of the system and the privacy of user data.

On the other hand, to improve the user experience, a web page designed especially for the urbanization in which the implementation was carried out was made. it should be noted that one of the main features is that you can view the call log that contains various call details such as call duration, source and recipient number, among others.

KEYWORDS:

- **ASTERISK**
- **CLOUD SERVICE**
- **TELEPHONY IP**

Capítulo I

Planteamiento del problema de investigación

Antecedentes

Al día de hoy ha existido un gran crecimiento en las redes IP (LAN,WAN, MAN), por esto y otros factores el protocolo IP se ha convertido en uno de los más utilizados en varias aplicaciones que van desde servicios de red hasta la comunicación entre dispositivos, de acuerdo con el informe de Visual Networking Index de Cisco, el tráfico IP a nivel mundial se ha triplicado, lo que además ha implicado un incremento en el número de dispositivos por habitante, en consecuencia, se espera que para 2020 se tenga 3.4 dispositivos por habitante (Kibernum,2017), este crecimiento acelerado de las redes IP y requerimientos de los usuarios, ha generado que se incremente el desarrollo de técnicas avanzadas para la digitalización de la voz y sobre este llevar cierto control sobre el protocolo IP e incluso tener una priorización de tráfico, a causa de estos desarrollos, se crearon nuevos estándares que permitan garantizar ciertas métricas y calidad en estos tipos de servicio, con esta evolución de nuevas técnicas y estándares se logró obtener la nueva tecnología que hoy se conoce como VoIP.

VoIP (Voice over IP) esta tecnología hace posible que una señal de voz digitalizada, a manera de paquetes viaje por medio de Internet utilizando el protocolo IP, con esta tecnología es posible unir dos mundos que estuvieron distantes desde hace mucho tiempo que son los datos y la transmisión de voz, por tanto, VoIP es una tecnología y no un servicio, sin embargo, comúnmente se utiliza este término para referirse al servicio de telefonía IP que es un servicio que integra aplicaciones de VoIP y agrega servicios de valor agregado de la telefonía tradicional como numeración, identificación de llamadas, llamadas en espera, facturación, etc.

Justificación

La telefonía IP se ha convertido en una revolución a nivel mundial, tan rápida e importante como la masificación de los PCs. Según estadísticas, su éxito radica en el gran abanico de posibilidades de comunicación que propone a los usuarios, superando las funcionalidades de la telefonía tradicional y ofreciendo menores costos. Para Renán Pérez, Gerente División Comercial de Belltech, "la telefonía IP es un tremendo negocio, una industria que está creciendo a tasas tan aceleradas como la que tuvieron los PCs en sus años de gloria" (Revista Gerencia, 2005). Sin ir más lejos, según datos aportados por Global Market Insights, en el 2017 se estimó que hay cerca de 1 billón de usuarios VOIP a nivel mundial y se espera que para 2021 lleguen a ser 3 billones de usuarios, por estas razones en 2018 se tenía un mercado de 20 billones de dólares y se espera que hasta 2025 el mercado aumente a 55 billones (Bhutani, 2019).

En el Ecuador en 2020 existen 2.444.414 abonados de telefonía fija a comparación del 2015 donde se tenían 2.494.274, esto indica que cerca de 50.000 usuarios han dejado la telefonía fija tradicional. Este sector de las telecomunicaciones ha tenido un desarrollo asimétrico, debido a que la demanda de la telefonía fija ha sufrido una especie de estancamiento año tras año, mientras que la oferta y la demanda de la telefonía IP se manifiesta en una continua evolución y desarrollo como consecuencia de los innumerables cambios tecnológicos y de acceso a la información. En la ciudad de Quito este mercado no ha sido explotado completamente, por tanto, existen varias oportunidades para desarrollar aplicaciones para diferentes áreas empresariales, comerciales, domesticas, entre otras, por consiguiente, este proyecto tiene como finalidad ofrecer un servicio más eficiente, que además permita reducir costos de implementación de centrales telefónicas digitales, mejorar la calidad del servicio brindado, y entregar una

mejor experiencia de estos sistemas al usuario, para que con esto a futuro se puedan desarrollar nuevas y destacadas aplicaciones.

La inseguridad en la actualidad es un problema urbano, este problema reside en que los crecimientos de delitos en urbes tienen consecuencias directas con la generación subjetiva de miedo e inseguridad en la población, esto tiene consecuencias directas en la población por las lesiones, daños, pérdidas y gastos públicos y privados para la prevención de este crimen. Según la Encuesta de Victimización y Percepción de Inseguridad (INEC,2011), 4 de cada 100 hogares ha sido víctima de robo a la vivienda, esto sin contar con los delitos que no son denunciados, sin embargo, la percepción de las personas es mucho mayor al de las cifras indicadas siendo así que en Pichincha un 53.4% de personas consideran que su barrio es inseguro, en las áreas residenciales varios de estos delitos son a causa de suplantación de identidades como hacerse pasar por familiares, amigos, visitantes, repartidores entre otros de ahí que, en muchas áreas residenciales se opten por sistemas de seguridad como: cámaras de circuitos cerrados, cercas eléctricas, entre otros, estas soluciones al tener que adquirir una gran cantidad de nuevo equipamiento hace que el costo sea muy elevado, además, de añadir costos extra por servicios adicionales como el de una alarma comunitaria, por consiguiente, este proyecto busca no solo dar una alternativa para estas áreas residenciales, también se busca ofrecer un sistema eficiente y con costos mucho más reducidos al utilizar la nueva tecnología que brinda la telefonía IP y la implementación de una PBX VOIP virtual.

Alcance

Este proyecto tiene como objetivo recopilar información y estado del arte sobre la implementación de centrales virtuales IP, protocolos de señalización, protocolos de transporte de voz, protocolos de plataforma IP, protocolos de control, mantenimiento, gestión integrada, técnicas de QoS [Quality of Service], herramientas de análisis y medición, estimación de densidad de tráfico y densidad de usuarios.

Por otro lado, el presente proyecto tiene como finalidad implementar un sistema de control de acceso y perifoneo mediante un servidor virtual para áreas residenciales, para el cual mediante encuestas se determinarán parámetros como la densidad de tráfico y hora pico, para definir los requerimientos mínimos del sistema a implementar, sobre el cual se realizará un análisis bajo los parámetros de QoS y mediante herramientas de monitoreo de llamadas VoIP [Voice over IP].

A esto se sumará el análisis de sonorización dado que se debe garantizar la mayor inteligibilidad posible, por tanto, se debe determinar las zonas en las cuales se deberán instalar los altavoces IP y realizar un diseño que permita cubrir la mayor área posible dentro de la zona residencial, para posteriormente implementar el sistema de perifoneo.

Objetivos

Objetivo General

Desarrollar e implementar un sistema que permita realizar el control de acceso e integración de los servicios de alarmas comunitarias para usuarios de áreas residenciales basados en VoIP.

Objetivos Específicos

- Estudio del estado del arte sobre la implementación de centrales virtuales VoIP y servicios provistos por alarmas comunitarias.

- Implementar un sistema de perifoneo mediante altavoces IP integrados a la central virtual.
- Configuración y evaluación de protocolos de seguridad para la central virtual IP.
- Evaluar el desempeño y funcionamiento del sistema VoIP considerando configuraciones de QoS.
- Implementación de la página web para la creación y tarifación del servicio VoIP.
- Elaborar un manual de usuario para la instalación y uso del Softphone de software libre para S.O. de Android y iOS.

Capítulo II

Fundamento Teórico

Introducción.

Este capítulo tiene como objetivo dar una introducción a los conceptos básicos de VoIP y la telefonía IP [Internet Protocol], su historia, protocolos de seguridad, protocolos de señalización, entre otros, además, dar a conocer técnicas de QoS, herramientas de monitoreo entre otros aspectos relacionados a la telefonía IP.

Se presentarán conceptos sobre centrales telefónicas virtuales VoIP tanto de código abierto como propietario, comparaciones con centrales físicas y con la telefonía tradicional, además de sus ventajas y desventajas.

Para finalizar se mostrarán conceptos sobre sistemas de acceso, perifoneo, sonorización, haciendo énfasis en los tipos de parlantes IP y Softphone que existen, también, el estado del arte de los sistemas de seguridad sobre IP.

Telefonía Tradicional (PSTN)

En el inicio de las comunicaciones, estas se basaban en la idea de tener un teléfono a cada extremo, así se formaba un circuito en el cual el usuario que descolgara primero el teléfono iniciaba la conversación, entonces, no había ningún tipo de marcación, por esto, se necesita un enlace físico para cada circuito de este tipo y a estos circuitos se les dio el nombre de ring down, hacer estos enlaces físicos por cliente implicaría tener un sin número de cables, por esto, se envió un cable físico por cliente hacia un switch aquí existían operadores que realizaban la conmutación hacia el destino, sin embargo, la red creció de manera exponencial , así que se crearon los conceptos de llamada telefónica y conmutador telefónico, lo que ya permitía dar una identificación a cada usuario y conmuntar automáticamente el proceso de la llamada hacia su destino, en la

actualidad la PSTN es una de las redes más grandes en todo el mundo, la PSTN consta de el transmisor, la conmutación y señalización y el receptor, ese es su esquema básico de funcionamiento.

En definitiva, la PSTN [Public Switched Telephone Network] es un conjunto de dispositivos físicos que permiten brindar el servicio de comunicación telefónica, permitiendo comunicar a dos individuos, para lo cual la red debe tener aparatos, medios y recursos adecuados con el fin de garantizar la calidad de la comunicación en la misma, por eso se incorporan funciones de conmutación, señalización y transmisión. De esta manera el proceso de conmutación se encarga de la identificación y conexión de los usuarios o abonados durante el trayecto de la llamada mientras que la función de señalización interpreta las señales de control y supervisión que son necesarias para la conmutación, y por último la transmisión es el proceso mediante el mensaje del usuario o abonado con sus respectivas señales de control son transmitidas por el medio o canal (Méndez, 2005). Todas estas funciones tienen funcionamientos muchos más complejos cada que se profundiza en cada uno de ellos, pero el objetivo es dar una referencia del funcionamiento global de cada una de ellas.

Historia de la telefonía IP

En síntesis, la telefonía IP es una tecnología que permite realizar y recibir llamadas utilizando el Internet, esta tecnología ha tenido un crecimiento imparable desde los años 2000, su origen se remonta a la red ARPANET en 1969, esta red es el comienzo del internet, el protocolo de transmisión de voz en la red ARPANET fue el RFC 741. VoIP fue creado por Danny Cohen y tenía como objetivo la transmisión de voz en tiempo real, en alta calidad, posteriormente en 1995 aparece el primer teléfono, este permitía que un usuario de internet llamara a otro usuario, este teléfono se conectaba a un altavoz, micrófono y un modem para su funcionamiento, este fue desarrollado por VOLCATEC y

se lo llamaba “InternetPhone”, acto seguido en 1997 se presentaron los primeros PBX software los cuales utilizaban el protocolo H323, este protocolo ofrecía voz y video mediante VoIP, pero, este servicio era de mala calidad porque el ancho de banda en esa época era limitado (EVOLUCIÓN DE LA TELEFONÍA IP timeline., 1973).

Hasta cierto punto en estos años la limitante principal era el ancho de banda, sin embargo, en 1998 comienza una evolución en las redes de banda ancha, con la alta demanda estas redes comienzan a progresar con mejores prestaciones y VoIP comienza a tomar posicionamiento en el mercado de las telecomunicaciones, apareciendo empresas dedicadas a VoIP, en este mismo año aparecen los primeros ATA [Analog Telephony Adapter] y Gateway, mediante estos dispositivos se hacía posible la comunicación entre un computador y la PSTN, con estos nuevos desarrollos se hace necesario un estándar y con esto aparece el protocolo SIP [Session Initiation Protocol], SIP es un protocolo de señalización que se utiliza en la telefonía IP, se presentó la segunda versión con un cambio significativo, permitiendo llamadas full-duplex, luego en 1999 Cisco y Microsoft lanzaron cada uno un servicio de telefonía, después, en el 2000 Microsoft crea Messenger y en este mismo año Mark Spencer creo Asterisk que era un centralita VoIP que distribuyo de manera gratuita, es decir esta es de código abierto hasta hoy en día (EVOLUCIÓN DE LA TELEFONÍA IP., 1973).

Estructura de una red VoIP

Mediante el desarrollo de la tecnología se iban añadiendo nuevos elementos a la PSTN, incluso se añadían computadoras con integración a esta red, lo que permitía tener nuevas funcionalidades, como identificador de llamadas, desplegar información sobre la pantalla acerca de la llamada y muchos otros servicios de valor agregado como datos de consumo de minutos entre otros, todos estos servicios que se podían conseguir

con nuevas tecnologías han ido desplazando la red de circuitos conmutados y pasando a una red de conmutación de paquetes.

VoIP maneja la misma estructura que el Internet, formado en un modelo OSI [Open Systems Interconnection] y pasando por las diferentes capaz del modelo de interconexión, estas capas se describen en la Figura 1.

Figura 1

Capa del modelo OSI

En la capa de transporte se utiliza el Protocolo RTP [Real-time Transfer Protocol) este utiliza datagramas del tipo UDP [User Datagram Protocol] sobre IP, se ha elegido este protocolo para VoIP, ya que se necesita asegurar lo que se conoce como transmisión en tiempo real, lo cual por las características de TCP [Transmission Control Protocol] no se consigue, por ello UDP es ideal, esto porque es un protocolo que no está orientado a la conexión, para hablar de tiempo real se sigue una recomendación de la ITU-T [International Telecommunication Union] que indica que el tiempo de retardo máximo de ida y vuelta debe ser de máximo 300 ms y un jitter no mayor a 50 ms, de modo similar, estos mismos retrasos existen en un red IP, ya que son retraso ocasionados por

diferentes factores como : Retardo de transmisión, Retardo de Procesamiento y Retardo de propagación (Méndez, 2005).

De manera general una PBX utiliza troncales que son enlaces que permiten unir una central con otra y mantener una comunicación. Actualmente los enlaces digitales más comúnmente utilizados son E1 y T1, estos enlaces digitales utilizan cierto número de canales para señalización, control y transmisión de datos, hay que considerar que cada canal tiene una capacidad de 64 kbps, en Ecuador los tipos de enlaces más utilizados son los E1 debido a que este es un estándar Europeo y las primeras centrales analógicas implementadas fueron con equipos Europeos, por ende también la ley de comprensión más usual es la ley a (a-law), a manera de resumen se presenta la Tabla 1, que representa un resumen del número de canales para tráfico y control y la velocidad tanto en troncales E1 como T1.

Tabla 1

Tabla Resumen troncales E1 / T1

	Número canales		Velocidad en Mbps		Número de canales		Velocidad en Mbps
	Canales de control	Canales de datos			Canales de control	Canales de datos	
T1		24	1.544	E1	2	30	2.048
T2	2	96	6.312	E2	12	120	8.448
T3	27	672	44.736	E3	57	480	34.368
T4	252	4032	274.176	E4	256	1920	139.264

Cabe recalcar que la Tabla 1 es solo un resumen de un modo de operación

de las troncales, ya que también se pueden utilizar bits de señalización sobre cada canal y se tendrían el total de canales para el transporte de los datos, sin embargo, esto depende netamente de la aplicación que se requiera ya que cada una de las configuraciones tiene sus ventajas y desventajas y dependerá del criterio del diseñador de la red.

Diferencias entre VoIP y Telefonía IP

De manera general una PBX utiliza troncales que son enlaces que permiten unir una central con otra y mantener una comunicación. Actualmente los enlaces digitales más comúnmente utilizados son E1 y T1, estos enlaces digitales utilizan cierto número de canales para señalización, control y transmisión de datos, hay que considerar que cada canal tiene una capacidad de 64 kbps, en Ecuador los tipos de enlaces más utilizados son los E1 debido a que este es un estándar Europeo y las primeras centrales analógicas implementadas fueron con equipos Europeos, por ende también la ley de comprensión más usual es la ley a (a-law), a manera de resumen se presenta la Tabla 1, que representa un resumen del número de canales para tráfico y control y la velocidad tanto en troncales E1 como T1.

VoIP como se menciona en secciones anteriores es un conjunto de normas, elementos o recursos que hacen posible el envío de señales mediante el protocolo IP, por esto, podemos deducir que VoIP es la tecnología en si, por ende, no es un servicio, en cambio, la Telefonía IP es un servicio que integra aplicaciones de VoIP y a estas les añade otros servicios o prestaciones de valor agregado que son parte de la telefonía tradicional como la facturación, contestadora automática entre otros, en definitiva, la telefonía IP utiliza VoIP para establecer la comunicación a través de paquetes de datos y brinda el servicio telefónico como tal al público, además se rige a la recomendación de la UIT E.164 para asignar a cada país un código numérico.

Estándar VoIP

El primer protocolo utilizado en VoIP fue el H.323 y este fue definido en 1996, este estándar describe una agrupación de especificaciones para el transporte de servicios multimedia, H.323 posee ciertas características principales que fueron los fundamentos del VoIP, estas son: Este estándar es independiente del tipo de red, esto quiere decir que no se especifica ningún protocolo específico para la red, posee interoperabilidad entre diferentes fabricantes ya que este es el propósito de un estándar, este estándar permite realizar multiconferencias proporcionando una robusta arquitectura y mucho más flexible, H323 permite gestionar el ancho de banda, permitiendo limitar el total de conexiones simultaneas y de esta forma controlar en tráfico de la red, también, se puede implementar tanto en software como hardware, soporta multicast y proporciona seguridad en base a H.235, además, proporciona un enlace a la red de telefonía tradicional.

Protocolos

Un protocolo es un conjunto de reglas que conforman un lenguaje utilizado por diferentes entidades o dispositivos para realizar una comunicación o una conexión, este protocolo es de vital importancia ya que en base a este se define la eficacia, complejidad, interoperabilidad entre otros aspectos de la comunicación entre diferentes dispositivos. En la telefonía IP se utiliza actualmente una variedad de protocolos, pero el más común es el protocolo SIP, existen otros como el H.323 e incluso protocolos propietarios como los que usan Cisco y Skype para sus equipos, algunos de los protocolos más utilizados son los siguientes:

Tabla 2

Protocolos VoIP

PROTOCOLO	DESCRIPCIÓN
H.323	Este fue el primer protocolo definido para VoIP por la ITU-T
SIP	El protocolo más utilizado actualmente, este fue definido por la IETF
Megaco (H.248)	Es un protocolo de control entre entidades y fue definido conjuntamente entre ITU-T y IETF.
Skinny	Es un protocolo propietario, propiedad de CISCO
MiNet	Es un protocolo propietario, propiedad de MINTEL
Cornet-IP	Es un protocolo propietario, propiedad de SIEMENS
IAX	Este es un protocolo que permite la comunicación entre centrales Asterisk actualmente fue remplazado con IAX2.
Skype	Es un protocolo propietario peer to peer, utilizado por Skype
IAX2	Es un protocolo para la comunicación entre centrales Asterisk que remplazo a IAX
Jingle	Es un protocolo utilizado por la tecnología JABBER

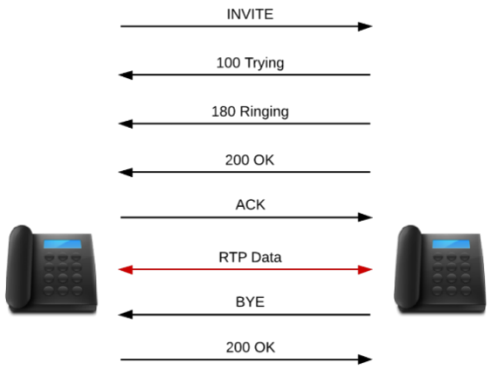
SIP

El protocolo SIP, es decir, un protocolo de inicio de sesiones, fue desarrollado por el IETF [Internet Engineering Task Force], este tiene el objetivo de ser un estándar para la iniciación, modificación y finalización de sesiones, donde se ven inmersos ciertos elementos multimedia como la voz, el video, la mensajería instantánea, juegos en línea y realidad virtual, tiene ciertas similitudes con HTTP y SMTP, ya que SIP estaba diseñado con el propósito de convertir a la telefonía IP en un servicio más del Internet, ya para el

año 2000 SIP fue aceptado como un protocolo de señalización en 3GPP [3rd Generation Partnership Project] y actualmente es uno de los protocolos de señalización para VoIP.

Figura 2

Sesión de llamada SIP entre dos teléfonos



Nota: En la figura se puede ver como se da el proceso para establecer una llama a través del protocolo SIP, (Calle Espinoza 2017).

En la Figura 2 se observa la secuencia en una sesión de llamada establecida por SIP, en primer lugar el teléfono A desde donde se realiza la llamada envía un INVITE, luego, el teléfono B envía un Trying y posteriormente empieza a sonar (Ringing), una vez que el teléfono B se levanta se envía una respuesta OK, que quiere decir que está disponible, posteriormente el teléfono A responde con un ACK de confirmación para iniciar la llamada, en este punto la comunicación se establece y todos los datos se envía vía RTP mientras se mantenga la conversación, pero una vez, se cuelga el teléfono se envía una solicitud BYE para terminar la comunicación y el otro teléfono responde con un mensaje de confirmación OK, esta es la forma más simple de ver cómo funciona el protocolo SIP, para entender de mejor manera cómo funcionan cada uno de estas peticiones y respuestas, se describe cada uno en la Tabla 3.

Tabla 3

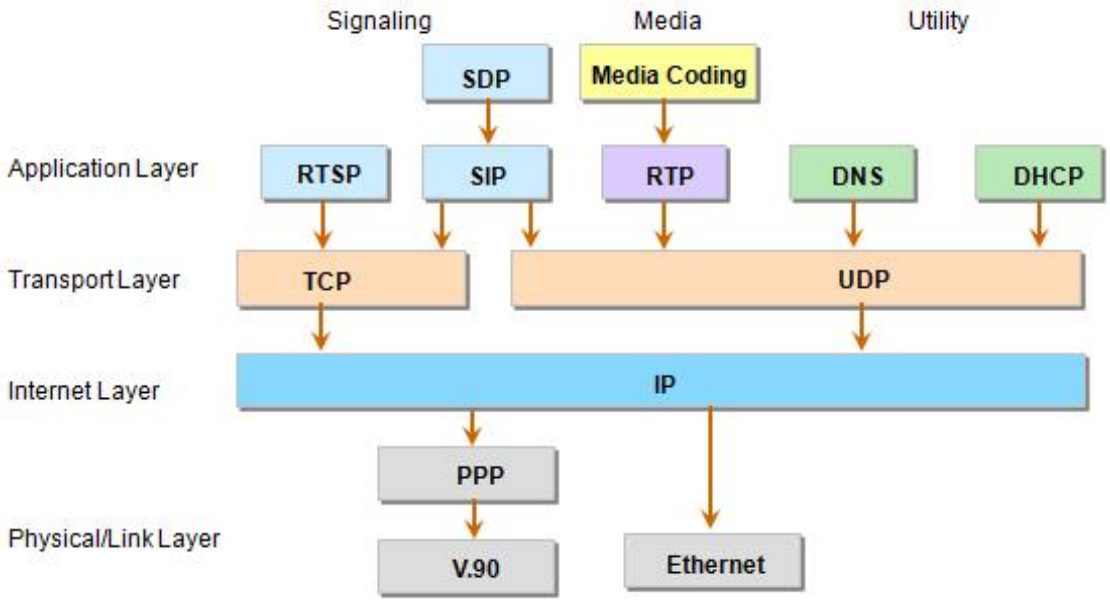
Respuestas y peticiones SIP

Mensajes	Descripción
INVITE	Permite invitar un usuario para participar en una sesión o para modificar parámetros en una sesión ya existente.
TRYING	Envía una respuesta que indica que la solicitud está siendo procesada y posteriormente detendrá el temporizador de retransmisión SIP.
RINGING	La terminal que recibe el INVITE intenta alertar al usuario que tiene una llamada.
OK	Indica que la solicitud se ha realizado correctamente.
ACK	Confirma el establecimiento de una sesión
BYE	Indica la terminación de una sesión.

SIP de manera general no funciona solo, sino, que es un conjunto de otros protocolos que lo complementan como son el SDP [Session Description Protocol], este se encarga de describir el contenido multimedia de la sesión, como direcciones IP, puertos que se utilizan, codecs de audio y video entre otros, también, se complementa con RTP este en sí, es el verdadero protocolo que se encarga del transporte de los datos y de manera general se encarga de determinar la ubicación de los usuarios, establecer, modificar y terminar sesiones multipartitas entre usuarios.

Figura 3

SIP en modelo TCP/IP



Nota: En la figura se puede observar las capas que componen el modelo TCP/IP , (Hanumesh, 2013).

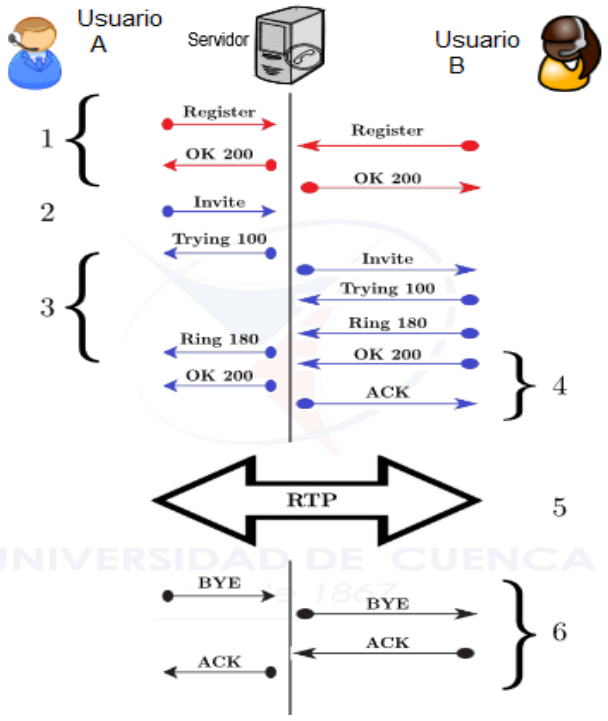
En el modelo TCP/IP como se observa en la Figura 3, SIP se encuentra en la capa de aplicación, ya que su objetivo es aportar con un conjunto de funciones de procesamiento de llamadas y otros aspectos que ya están presentes en la PSTN, por ello se tienen funciones típicas como son el tono de ocupado, otra característica de SIP es que fue diseñado por IETF es decir está más asociado a una comunidad IP y no a la industria de telecomunicaciones como se piensa, sin embargo, SIP ha tomado mayor importancia y se podría decir que suplanto a H.323 de la ITU-T, sin embargo, esto no es del todo cierto ya que, SIP y H323 pueden trabajar de manera conjunta, aunque en la

actualidad son pocos los dispositivos que trabajan con H.323 y por eso ha ido quedando de lado.

SIP permite establecer una sesión multimedia entre dos o varios usuarios, esto mediante un puerto que de manera general viene por defecto en el puerto 5060 y como se observa en la Figura 3, SIP puede trabajar sobre TCP o UDP, así puede recibir peticiones de los clientes SIP por cualquiera de estos dos protocolos, un ejemplo mucho más claro de los mensajes SIP entre dos usuarios se observa en la Figura 4.

Figura 4

Mensajes SIP en una comunicación entre dos usuarios.



Nota: En la figura se observa a mayor detalle una sesión de una llamada mediante SIP, (Calle Espinoza, 2017).

RTP

RTP se publicó en 1996 en el estándar RFC1886 que define tanto a RTP como RTCP que son protocolos suplementarios utilizados en SIP para usarlos para el transporte de datos en tiempo real, RTP es el protocolo encargado de añadirle a los paquetes UDP el número de secuencia, la marca de tiempo y la identificación del tipo de carga útil, este protocolo se encuentra en la capa de aplicación y se utiliza bajo el protocolo UDP, siendo así que una vez que UDP recibe los paquetes este se los entrega RTP detectando cualquier problema que pudiera ocurrir la perdida de paquetes o un cambio en el orden de llegada de los mismo, este protocolo no corrige estos errores si no que le informa de ellos a aplicaciones o protocolos de capas superiores para que puedan tomar medidas sobre los errores.

RTP utiliza números de puerto par comprendidos entre 1025 y 655535, pero, su puerto por defecto es el 5004, acabe recalcar que cuando una sesión RTP se inicia también se inicia una sesión RTCP, RTP tiene un propósito claro y este es el de proporcionar un medio uniforme de transmisión de datos sometidos a limitaciones de tiempo real, en base a este objetivo RTP permite identificar el tipo de información que se transporta, añadir marcadores temporales para identificar el instante en que se transmitió el paquete y una aplicación VoIP pueda ordenarla en caso de un cambio en el orden de llegada, incluye un número de secuencia a los paquetes de información para detectar perdidas de paquetes, aun así, RTP no garantiza que la entrega de paquetes en el destino, ni tampoco, puede reservar recursos o controlar la calidad del servicio.

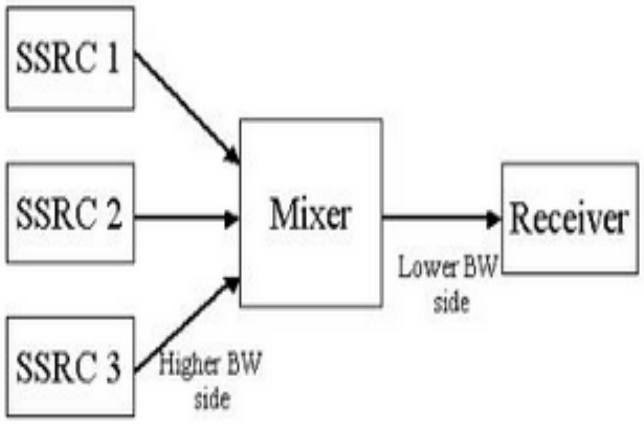
RTP tiene una especificación importante y es que permite identificar el códec que se está utilizando en el origen, sin embargo, considerando que, los participantes en una comunicación puede que no dispongan de los mismos codecs, RTP tiene en cuenta la

posibilidad de que existan aplicaciones intermedias que lleven a cabo las comunicaciones, para esto se pueden utilizar:

• Mezclador (Mixer): Esta aplicación recibe flujos de datos de varias fuentes denominadas SSRC's [Synchronization Sources Identifier], se modifica el formato y posteriormente se reenvía un único flujo de datos, en resumen, el mixer se comporta como una fuente particular SSRC que reagrupa los datos de varias otras fuentes SSRCs y se convierten en CSRC [Contributing Source Identifier] que es un paquete que contiene todos los flujos transformados.

Figura 5

Funcionamiento de un Mixer

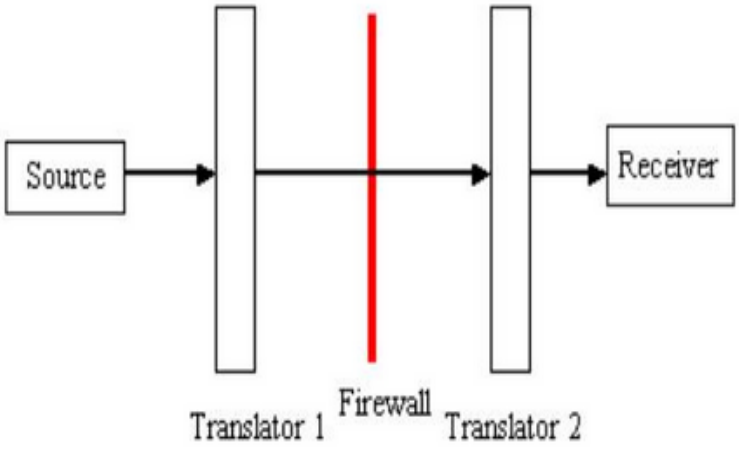


Nota: En la figura se observa un diagrama de bloques de un mixer, (Carrington, 2014).

• Traductor (Translator): Esta aplicación realiza una conversión de sistema de codificación, esta transmite paquetes RTP, pero al contrario del mezclador no cambia el identificador del SSRC, el traductor permite cambiar la codificación de un dato, por ejemplo, si se necesita conectar un terminal A que es compatible con u-law con otro que sea compatible con G.711 se necesita utilizar un traductor.

Figura 6

Funcionamiento de un traductor



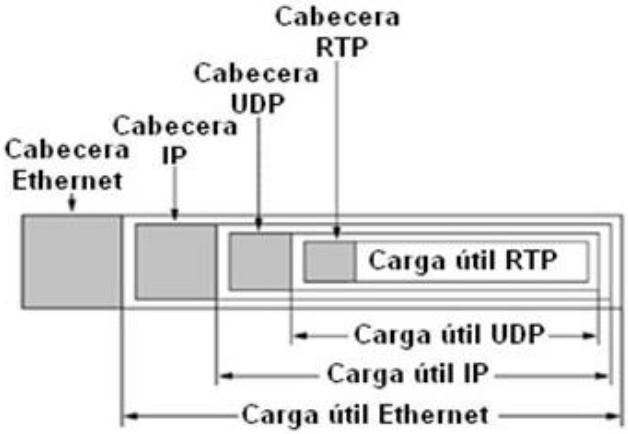
Nota: En la figura se observa un diagrama de bloques de un traductor, (Carrington, 2014).

Cabecera RTP

En síntesis, RTP transporta paquetes de datos como señales de audio o video codificados, cada uno de estos paquetes contiene una cabecera RTP (header), se debe considerar que estos paquetes RTP deben pasar por el protocolo UDP el cual le añade otra cabecera, la cabecera RTP está constituida por 12 octetos y a esta cabecera le procede el “payload” que representa la carga útil, para tener una idea más clara sobre la estructura de las cabeceras que se van agregando en un paquete se observa la estructura en la Figura 7.

Figura 7

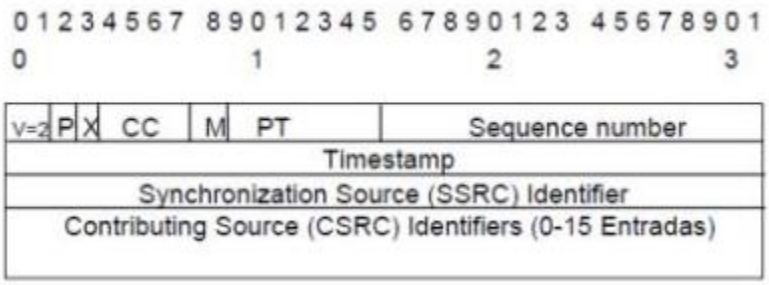
Estructura de un paquete Ethernet considerando RTP



Nota: En la figura se puede observar las el contenido de un paquete(García Montoya, 2014).

Figura 8

Cabecera del paquete RTP



Nota: En la figura se puede observar las cabeceras de RTP, (García Montoya, 2014).

RTCP

RTCP [Real-time Control Transport Protocol), este protocolo se encarga de informar sobre la calidad de recepción de los paquetes y la identidad de los usuarios o interlocutores, este definido en el estándar RFC 3350, este protocolo trabaja en conjunto con RTP, RTCP se utiliza para enviar paquetes de control a los participantes de una llamada, esto para proveer una retroalimentación sobre la calidad de servicio que brinda RTP.

RTCP utiliza número de puertos impares comprendidos entre 1025 y 655535, su puerto por defecto es el 5005, cabe recalcar que al iniciarse una sesión RTP se inicia también una RTCP y este ocupa el puerto inmediatamente superior al que esté utilizando RTP, de esta manera RTCP transporta las estadísticas e información, en forma de conteo de paquetes y tiempo de regreso, esta es información útil para una aplicación VoIP , ya que en base a esta información puede controlar parámetros como QoS o definir el mejor códec para utilizar en la comunicación, también puede transportar información básica de los usuarios o participantes de una sesión y lo hace en base distintos paquetes que se muestran en la Tabla 4.

Tabla 4

Paquetes RTCP

TIPO	NOMBRE	DESCRIPCION	RFC
192	FIR	Full intra/frame request	RFC2032
193	NACK	Negative acknowledgement	RFC2032
200	SR	Sender report	RFC3551
201	RR	Receiver report	RFC3551
202	SDES	Source description	RFC3551

TIPO	NOMBRE	DESCRIPCION	RFC
203	BYE	Goodbye	RFC3551
204	APP	Aplication-defined	RFC3551
205	RTPFB	Generic RTP feedback	
206	PSFB	Payload-specific	
207	XR	Extended report	RFC3611

Estos paquetes transportan información básica que es de utilidad para aplicaciones en capas superiores, los principales o más utilizados son:

• **SR** (Sender Report): Este paquete contiene las estadísticas de transmisión y recepción para todos los usuarios que son emisores en la sesión.

• **RR** (Receiver Report): Este paquete contiene las estadísticas de transmisión y recepción para todos los usuarios que son receptores en la sesión.

• **SDES** (Source Description): Describe las características de la fuente como el nombre (Caller ID), email, teléfono, entre otros.

• **BYE**: Este paquete le indica a una estación el fin de su participación en una sesión.

• **APP**: Este paquete es un paquete especifico por cada aplicación, se puede considerar como un identificador para cada aplicación.

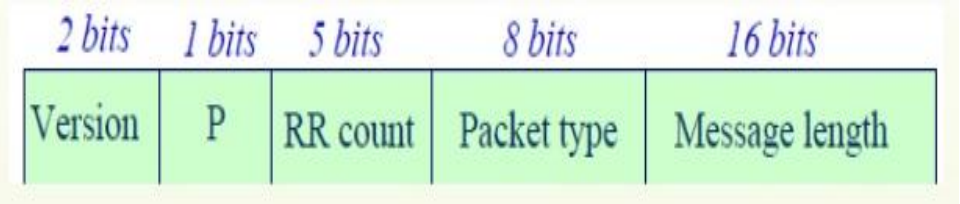
Cabecera RTCP

En definitiva, RTCP se utiliza para un intercambio de información que sirve para el control, esta información puede ser, el número de paquetes perdidos, jitter, retardo, codecs, entre otros, toda esta información se obtiene de todos los participantes en la

sesión, algo a diferenciar es que RTCP también incluye la información del CNAME [Canonical name] este es un ID único para cada participante de la sesión, de manera general varios paquetes RTCP son encapsulados en un solo datagrama UDP esto con el objetivo de disminuir el problema de sobrecarga por las cabeceras, se debe considerar que cada tipo de paquete tendrá una estructura diferente pero una cabecera común esta se detalla en la Figura 9.

Figura 9

Cabecera común RTCP

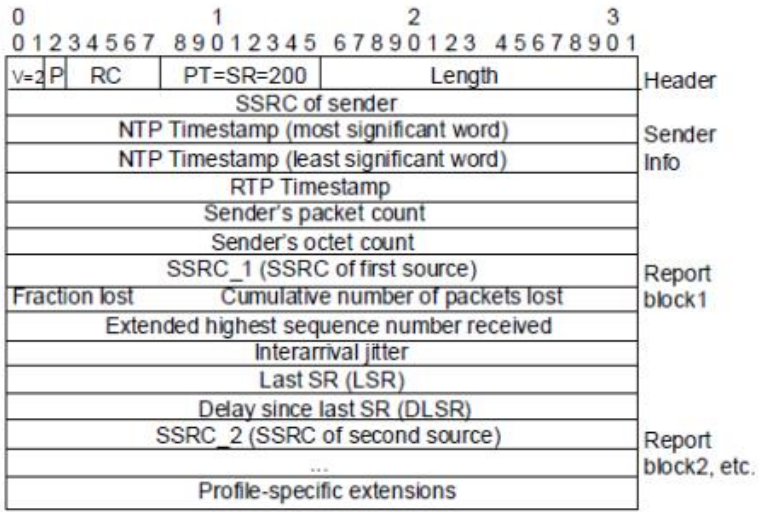


Nota: En la figura se observa a detalle el número de bits que compone la cabecera RTCP, (Guerra, 2013).

Una vez en claro que cada paquete tendrá una cabecera común se detalla a continuación, la estructura de los paquetes a los que comúnmente se les da mayor importancia, estos son los paquetes SR, RR, SDES, BYE y APP, estos se detallan desde la Figura 10 hasta la Figura 14.

Figura 10

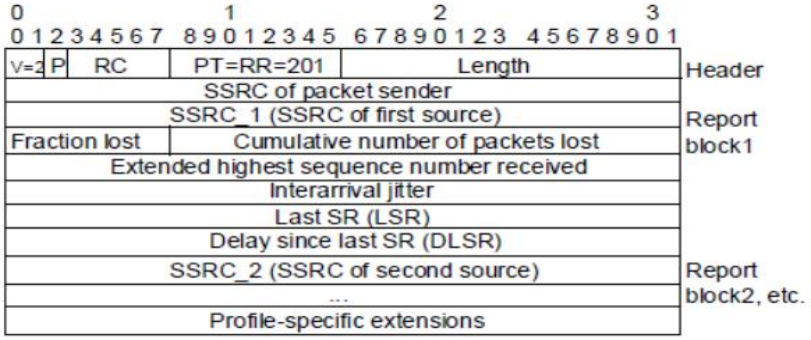
Paquete sender report



Nota: En la figura se observa a detalle la cabecera sender report (EFORT, 2011).

Figura 11

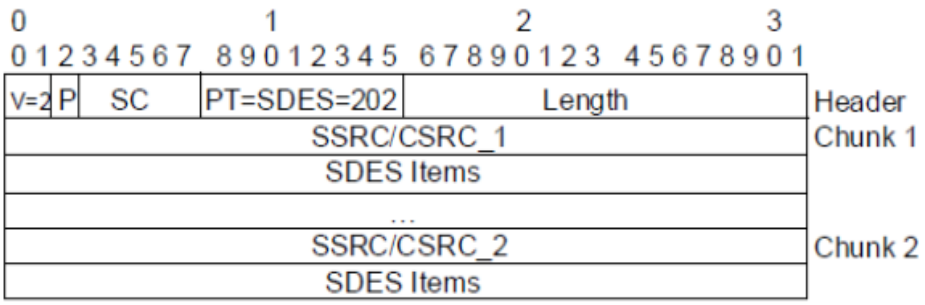
Paquete Receiver report



Nota: En la figura se observa a detalle la cabecera receiver report (EFORT, 2011).

Figura 12

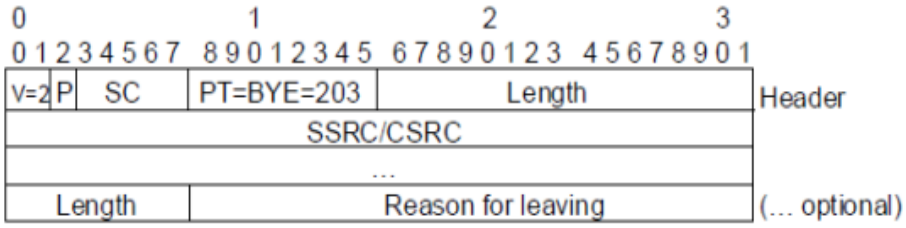
Paquete source description



Nota: En la figura se observa a detalle la cabecera source description (EFORT, 2011).

Figura 13

Cabecera del paquete BYE

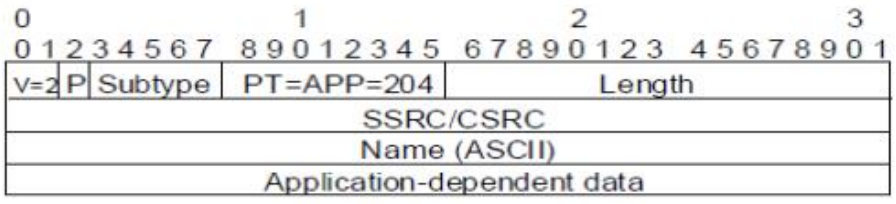


Nota:

En la figura se observa a detalle la cabecera paquete BYE (EFORT, 2011).

Figura 14

Cabecera de paquete APP



Nota: En la figura se observa a detalle la cabecera paquete APP (EFORT, 2011).

SRTP

SRTP [Secure Real-time Transport Protocol], es una extensión de RTP que su finalidad es adherir funciones de seguridad, como confidencialidad, autenticación de mensaje, integridad, en si este protocolo fue desarrollado para las comunicaciones VoIP y se define en el IETF RFC 3711.

Aun cuando existen una gran cantidad de protocolos de señalización (por ejemplo, SIP , H.323, Skinny) y una gran cantidad de mecanismos de intercambio de claves (por ejemplo, MIKEY, SDESCRIPTIONS, ZRTP), SRTP se considera uno de los mecanismos estándar para proteger los medios en tiempo real (voz y video) en aplicaciones multimedia. Asimismo, se encarga de proteger los paquetes RTP, proporciona protección para los mensajes RTCP. El protocolo RTCP se utiliza principalmente para proporcionar retroalimentación de QoS (por ejemplo, retraso de ida y vuelta, bytes y paquetes enviados) a los puntos finales participantes de una sesión. Los mensajes RTCP se transmiten por separado de los mensajes RTP, utilizan puertos separados para cada uno de los protocolos. Entonces, tanto RTP como RTCP deben protegerse durante una sesión multimedia. Si RTCP se deja sin protección, un atacante puede manipular los mensajes RTCP entre los participantes y causar interrupciones en el servicio o puede realizar un análisis de tráfico con la ayuda de un software diseñado para esto mismo (por ejemplo, Wireshark) (Takanen, 2007).

Los encargados de diseñar el protocolo SRTP se enfocaron en que se realice una protección adecuada para las transmisiones de datos, pero además de esto mantuvieron las propiedades claves para admitir tanto redes cableadas como redes inalámbricas en donde puedan existir limitaciones en el ancho de banda.

Algunas de las propiedades resaltadas son las siguientes (Takanen, 2007).:

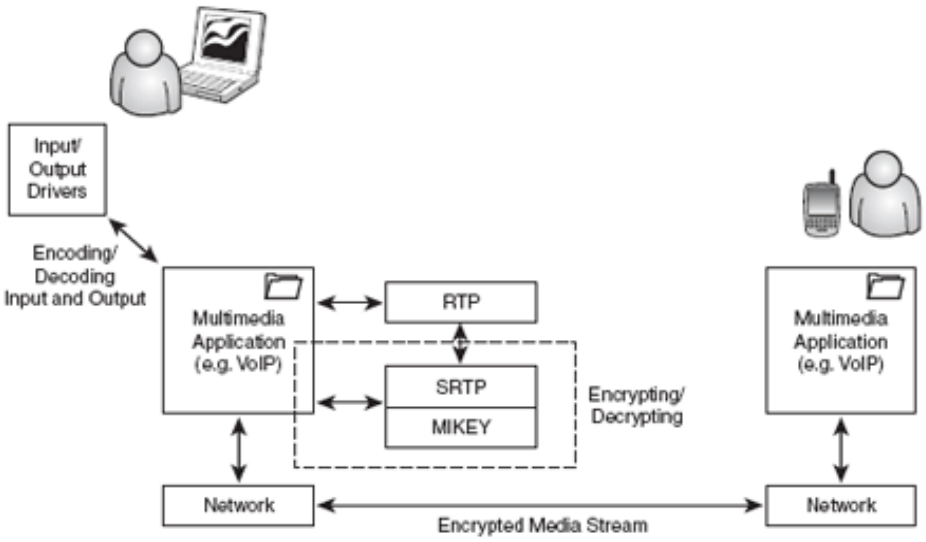
- Facultad de agregar nuevas modificaciones criptográficas.
- Mantener un bajo ancho de banda y bajo costo computacional.
- Conservador en el tamaño del código de implementación. Esto es de gran utilidad para dispositivos con memoria limitada (por ejemplo, teléfonos celulares).

Cabecera SRTP

Para aplicar el protocolo SRTP se tiene que convertir los paquetes RTP en paquetes SRTP antes de que dichos paquetes vayan a ser enviados por la red. De igual manera para realizar el descifrado de estos paquetes ser realiza el proceso inverso. La Figura 15 muestra este proceso.

Figura 15

Codificación y decodificación del protocolo SRTP

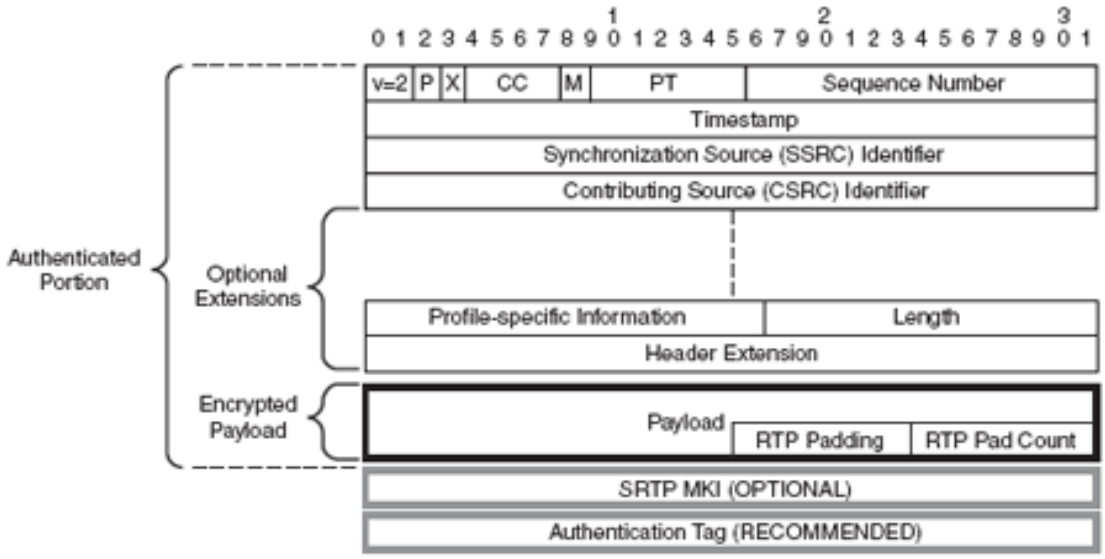


Nota: En la figura se puede ver el proceso de codificación y decodificación del protocolo SRTP, (Takanen, 2020).

Otra característica importante del protocolo SRTP es que además de proporcionar cifrado de datos, SRTP admite la autenticación de mensajes y la integridad del paquete RTP. Para la realización de autenticación de mensaje se utilizar un algoritmo predeterminado que es el SHA-1 que tiene una longitud de clave de 160 bits. El código de autenticación de mensaje (MAC) se produce al calcular un hash de todo el mensaje RTP, incluidos los encabezados RTP y la carga útil cifrada, y colocando el valor resultante en el encabezado de la etiqueta de autenticación, como se muestra en la Figura 16 (Takanen, 2007).

Figura 16

Cabecera SRTP



Nota: En la figura se puede observar a detalle todo lo que compone la cabecera SRTP, (Takanen, 2020).

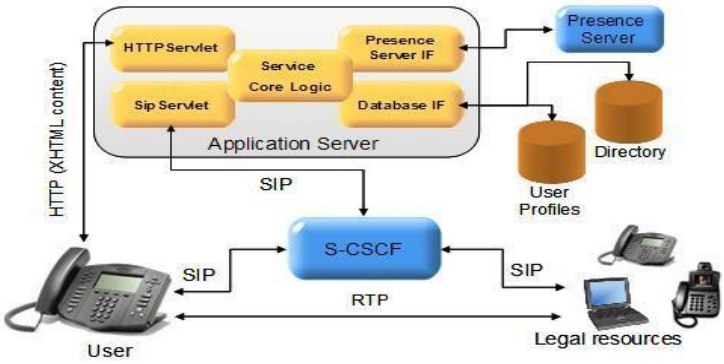
En la Figura 16 se observar que la cabecera SRTP es muy similar a la cabecera RTP con la excepción de que está compuesto de dos encabezados adicionales: el MKI [Master Key Identifier] y la etiqueta de autenticación. El MKI es implementado para el mecanismo de gestión de claves (por ejemplo, MIKEY), y su presencia en implementaciones de acuerdo con el estándar SRTP (RFC 3711) es opcional. El MKI se puede utilizar para volver a escribir o para identificar la clave maestra de la que se derivaron las claves de sesión para que la aplicación las utilice para descifrar o verificar la autenticidad de la carga útil SRTP asociada. El mecanismo de intercambio de claves genera y gestiona el valor de este campo durante toda la vida de la sesión. El uso del encabezado de la etiqueta de autenticación es importante y proporciona protección contra ataques de reproducción de mensajes (Takanen, 2007).

Arquitectura VoIP

En la Tabla 3 se definieron las Respuestas y peticiones SIP que se establecen en una sesión, en la Figura 17, se observa a más detalle toda la estructura que esta implica, ya que al enviarse la petición de INVITE, lo que se hace en primera instancia es dirigirse a la base de datos, luego se comprueba si el perfil del usuario existe y posteriormente se busca de igual manera al otro participante de la sesión, es decir se busca el perfil de usuario para cada participante y que cada participante se encuentre registrado en el directorio, de esta manera se puede continuar con el proceso para establecer la sesión.

Figura 17

Arquitectura VoIP



Nota: En la figura se observa la estructura de la arquitectura VoIP, (EFORT, 2011).

Aquí se definen tres partes fundamentales para esta estructura que son los equipos terminales, los Gatekeepers y los Gateway, cada uno de ellos cumple una función específica, siendo así que el equipo terminal son todos los sustitutos a los teléfonos actuales, estos puedes ser implementados tanto en hardware como en software, existen una gran variedad de estos y se la vera más a profundidad en secciones posteriores.

Los Gatekeepers es el núcleo del funcionamiento de VoIP y se lo podría considerar como un sustituto a las centrales actuales, en la actualidad se implementan en software y de estas existen una gran variedad de posibilidades, dependiendo si se desea utilizar una de estas centrales de código abierto como lo es Asterisk, FreePBX, Isabell, entre otros o de software propietario como 3CX, Cisco, etc. Se debe tomar en cuenta que todo el tráfico de las comunicaciones pasara por el Gatekeepers.

Los Gateway por otro lado es un elemento que permite crear un enlace con la red telefónica tradicional o PSTN, en esta se debe configurar una troncal que servirá para la

comunicación y mediante la cual el proceso de conmutación será transparente para el usuario, para ello se utilizan tarjetas FXS y FXO.

Terminales IP

Los terminales IP hacen referencia al dispositivo que utiliza el usuario final, este puede ser implementado tanto en hardware como en software, en hardware existe una amplia variedad de teléfonos IP con diferentes características que van desde solo el audio hasta el pantallas y cámaras para el video, estos teléfonos están diseñado de manera general para trabajar con el protocolo SIP para tener interoperabilidad entre dispositivos de diferentes marcas, las marcas que predominan en estos dispositivos son Cisco, Fanvil, Grandstream, Htek, Polycom, Avaya, entre otros, de manera similar existen los Softphones que es un software el cual está orientado a la comunicación y permite realizar llamadas a través de VoIP, para esto se instala el software sobre un dispositivo que puede ser desde un teléfono celular hasta una PC o laptop, existen una gran variedad de Softphone disponibles en el mercado, desde gratuitos hasta propietarios, algunos de estos son Zoiper, 3CX, Linphone, Acrobit, Groundwire, Bria, Cisco Jabber, entre otros.

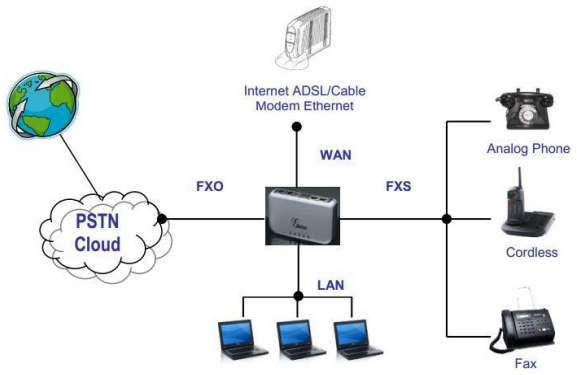
Gateways y adaptadores analógicos

Estos dispositivos son normalmente conocidos como ATA, este dispositivo convierte señales analógicas hacia un protocolo IP para utilizar con VoIP, por ello estos dispositivos se utilizan para conectar un dispositivo o teléfono convencional y así convertirlo en un dispositivo IP, es decir un teléfono IP que pueda funcionar con VoIP, para realizar esto se utilizan puertos FXO y FXS. FXO [Foreing Exchange Office] es el encargado de comunicar la red IP con la PSTN, es decir realiza el cambio de la señal analógica a paquetes de datos, en cambio, FXS [Foreing Exchange Station] es la encargada de conectar los teléfonos análogos o tradicionales a un computador, Central IP o Servidor IP, así el teléfono análogo ya puede recibir y realizar llamadas, es decir se

vuelve un teléfono Mixto ya que funciona como un teléfono IP pero con la singularidad que puede usar la también la línea convencional, un ejemplo de estos Gateway es el HT503 de Grandstream, la conexión se muestra en la Figura 18 (Sangoma Technologies Corporation, 2020).

Figura 18

Ejemplo de Conexión de un ATA



Nota: En la figura se observa un ejemplo práctico de la conexión de un dispositivo ATA, (Sangoma Technologies Corporation, 2020).

Tipos de PBX

La central telefónica o PBX [Private Branch Exchange] se puede definir como un equipo que permite gestionar llamadas telefónicas internas en una empresa, pero, que además permite compartir las líneas de acceso a la PSTN entre varios usuarios con el objetivo de realizar y recibir llamadas hacia y desde el exterior, en la actualidad existen varios tipos de PBX, que son:

- PBX Analógicas o Convencionales
- PBX Virtual
- PBX Hibrida

Cada una de estas centrales o PBX, poseen ventajas y desventajas una sobre otra y la elección de cual utilizar dependerá de la aplicación y el diseñador, en este documento haremos hincapié solo en la PBX Virtual, ya que es una centralita de bajos costos y una capacidad moderada que permitirá cumplir con los objetivos planteados al inicio del documento.

PBX Virtual o Cloud PBX es un servicio dirigido a empresas, esta tiene funciones similares a un PBX tradicional pero alojado en la nube, otra diferencia es que una PBX tradicional está limitada por su máximo número de líneas, en cambio una PBX Virtual permite una mayor escalabilidad, ya que se pueden crear o disminuir muchas extensiones y troncales de manera sencilla, lo que lo hace que se adapte a las necesidades del cliente, además es mucho menos complejo la creación de estas extensiones y troncales a comparación de una PBX tradicional. Algunas de sus ventajas son que las extensiones pueden ser utilizadas en cualquier parte del mundo, además, el cliente no requiere hacer ningún tipo de instalación o comprar costosos aparatos, por otra parte, se ofrecen servicios como, Grupos de marcado, Buzón de voz, IVR, Reportes de llamadas, entre otros. (Campanella, 2017).

En el mercado actualmente existe una gran variedad de PBX Virtuales, incluso en nuestro País CNT ofrece una central de este tipo, otras empresas internacionales muy reconocidas que ofrecen estas centrales virtuales son 8x8, Nextiva, RingCentral, 3CX, entre otras, estas son empresas que ofrecen el servicio de telefonía IP como tal y los costos pueden variar dependiendo el número de extensiones, pero también existen plataformas de código abierto que tienen la misma funcionalidad y pueden ser implementadas para diversas aplicaciones, algunos ejemplos de estas son Asterisk, FreeSwitch, FreePBX, Issabel, VitalPBX, etc.

Asterisk

Asterisk es una plataforma de código abierto y su principal funcionalidad es crear aplicaciones de comunicaciones. Asterisk se puede instalar sobre cualquier plataforma de servidor con sistema operativo Linux (GNU Linux), además puede convertir una computadora común en un servidor de comunicaciones o instalarse en un servidor virtual. Asterisk impulsa sistemas IP PBX, servidores de conferencias y otras soluciones personalizadas. Esta plataforma es utilizada por pequeñas, medianas y grandes empresas, centros de llamadas, operadores y agencias gubernamentales en todo el mundo. Cabe recalca que Asterisk es gratuito y está patrocinado por Sangoma.

En la actualidad, hay más de un millón de sistemas de comunicaciones basados en Asterisk en uso en más de 170 países. Asterisk es utilizado por casi toda la lista de clientes de Fortune 1000. Con mayor frecuencia implementado por integradores y desarrolladores de sistemas, Asterisk puede convertirse en la base de un sistema telefónico empresarial completo, o utilizarse para mejorar o ampliar un sistema existente, o para cerrar una brecha entre sistemas (Asterisk, 2020).

Asterisk entrega todas las operatividades de las grandes centralitas propietarias (IVR, buzones de voz, etc.), además presenta ciertos medios y servicios no aprovechables en la mayoría de ellos (extensiones remotas, grabación de llamadas).

FreeSwitch

FreeSwitch es una plataforma de código abierto con la funcionalidad de crear aplicaciones de comunicaciones. FreeSwitch funciona a través de una biblioteca que envía un ejecutable, inicia el núcleo del sistema y configura las diversas labores definidas por los módulos. FreeSwitch es una aplicación de telefonía PBX, tiene muchas características similares a Asterisk, pero con la ventaja que es capaz de manejar miles

de llamadas simultáneas. FreeSwitch puede interconectarse con el mundo exterior y escalar a cualquier tamaño.

FreeSwitch hace viable la construcción de un Softphone, además se pude elaborar un sistema PBX, un interruptor de software o una interfaz con otros sistemas PBX de código abierto como OpenPBX.org, Bayonne, Yate o Asterisk. Asimismo, se puede emplear para construir una plataforma de conmutación de VoIP (Voice over IP) que agrupa varias tecnologías como SIP (usando la biblioteca Nokia Sofia), H.323, SCCP, LDAP, Zeroconf, XMPP / Jingle, etc (Voip-info.org, 2020).

FreePBX

FreePBX es una plataforma de código abierto que ofrece a las organizaciones una central que funciona mediante IP, todas las características están disponible gratuitamente solo es cuestión de descargar y proceder a instalar todos los elementos necesarios para la construcción y el correcto funcionamiento del sistema telefónico.

FreePBX, es una plataforma que está patrocinado y desarrollado por Sangoma y una sólida comunidad global. Una de las características principales de FreePBX es que consta de una interfaz gráfica, es decir, esto facilita al usuario la creación o configuración de las extensiones, buzón de voz, IVR, ect. FreePBX ofrece la forma más sencilla posible de instalar y configurar un sistema telefónico de código abierto basado en Asterisk en un servidor o entorno virtual.

FreePBX está estrechamente integrado con una tienda de mercado en línea que ofrece funciones adicionales para mejorar la funcionalidad y ayudar a escalar su implementación (FreePBX, 2020).

Issabel

Issabel, nació en 2016 de la mano de la comunidad de Asterisk para evitar la pérdida de los avances realizados durante años con Elastix, su predecesor (Issabel, 2020).

Issabel es una plataforma de código abierto con la finalidad de dar un servicio de telefonía IP y comunicaciones asociadas basadas en la plataforma de Asterisk, se puede montar tanto en un servidor virtual o convertir una computadora común en un servidor incluyendo las siguientes funcionalidades: correo electrónico, fax, PBX IP, mensajería instantánea, video conferencia, centro de llamadas y funciones colaborativas.

Uno de los principales objetivos de Issabel es crear una herramienta que pueda unificar todas las características de un PBX propietaria y así integral todas las comunicaciones de la empresa en su plataforma.

El software Issabel es una de las plataformas de comunicaciones más completas existentes en la actualidad, y aporta una serie de importantes beneficios a la empresa (Issabel, 2020).

VitalPBX

VitalPBX es una plataforma de código abierto con la finalidad de dar un servicio de telefonía y comunicaciones para pequeñas, medianas y grandes empresas. VitalPBX es una plataforma completa que se puede instalar en el hardware físico del sitio o como una aplicación alojada, es decir, se puede instalar en una computadora común para que actúe como servidor o instalar en un servidor virtual.

VitalPBX actúa como la interfaz de capa superior para la base de Linux y luego Asterisk (uno de los kits de herramientas de comunicación más populares del mundo).

Por esta razón, VitalPBX es la interfaz gráfica de usuario entre usted y el complejo mundo de las comunicaciones modernas (VitalPBX, 2020).

Elección de la plataforma de desarrollo

Es indispensable determinar la mejor plataforma de desarrollo del proyecto y que este estudio sirva como guía para cualquier persona que se adentre con la tecnología VoIP. Tanto Asterisk,FreeSwitch, FreePBX, Issabel y Vital PBX son plataformas de grandes capacidades, que sin tener inconvenientes se puede crear un servicio de telefonía de alta fidelidad y funcionalidad para pequeñas, medias y grandes empresas o urbanizaciones dependiendo del aplicativo que se le vaya a dar. Todas estas plataformas mencionadas anteriormente presentan ventajas y desventajas propias de los desarrolladores, de la cual para su elección se analizó tomando en cuenta la experiencia con las plataformas, investigaciones anteriores y el cumplimiento de los objetivos.

Una vez que se ha investigado las ventajas y desventajas de las plataformas ya mencionadas, se ha elegido trabajar con la plataforma de Asterisk, ya que está construido por desarrolladores para desarrolladores, es decir, para desarrollar aplicaciones y soluciones con Asterisk se necesitará conocimientos prácticos de Linux, redes, telefonía, etc.

Otro punto importante por el cual se escogió la plataforma de Asterisk es porque dicha plataforma está compuesta por varias funciones y las más destacadas son las siguientes: grabación de llamada, identificación de llamada, llamada en espera, IVR flexible y configurable, email, notificaciones push, entre otras, pero el punto clave aquí es que a diferencia de las anteriores plataformas mencionadas (FreeSwitch, FreePBX, Issabel, Vital PBX) con Asterisk se tiene un mayor control en las funciones mencionas ya que Asterisk está construido por desarrolladores para desarrolladores, y las otras plataformas ya están definidas, entonces se pierde un poco el control de dichas funciones.

Asimismo, las plataformas FreeSwitch, FreePBX, Issabel, Vital PBX requieren un mayor procesamiento y requerimientos en la nube (por ejemplo, mayor memoria RAM, más disco duro, mayor ancho de banda), es decir, son plataformas mucho más pesadas. Además, existe problemas a nivel de aplicación, es decir, en varios softphone no son soportadas estas plataformas.

Códecs

En todo transceptor de comunicaciones, un codificador/decodificar es un elemento básico para la transmisión eficiente de datos, este codificador/decodificador posee la capacidad de convertir una señal analógica en un flujo digital mediante técnicas de codificación, en cambio, el decodificador realiza el proceso inverso, además el codificador o códec utiliza códigos de longitud variable para reducir los símbolos al mínimo, de esta manera representa la información transmitida de manera comprimida, de manera similar, el decodificar utiliza la misma técnica pero de manera inversa para obtener el mensaje original, todo esto tiene un propósito general que es la eficiencia, ya que con estas técnicas se puede reducir el consumo de recursos, como por ejemplo el ancho de banda, tiempo de procesamiento, entre otros.

En síntesis, se busca utilizar un codificador/decodificador para optimizar un sistema de comunicación, sin embargo, en la telefonía esto tiene otras consideraciones, porque, se debe garantizar la inteligibilidad de la señal de audio, lo que se puede traducir a la calidad y fidelidad de la señal para que esta sea inteligible en el destino, todo esto dependerá del codificador/decodificador y sus características, sus principales característica a ser tomadas en cuenta son las tasas de transmisión y retardos, sin embargo existe un factor importante y es la frecuencia en la que trabaja o funciona cada uno de estos codificadores/decodificadores, existiendo tres clasificaciones que se muestran en la Tabla 5.

Tabla 5

Clasificación de los códecs de acuerdo a su frecuencia de trabajo

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

En la Tabla 5 se muestran los tipos de códec clasificados por su frecuencia de funcionamiento siendo estos, NarrowBand (NB), WideBand (WB), SuperWideBand(SWB) y FullBand(FB), de manera general los códecs más utilizados son los de banda angosta , ya que estos comprenden la frecuencia de la voz por ende son de amplio interés para la telefonía, sin embargo existen otros códecs de Banda ancha WideBand o Banda SuperAncha SuperWideBand que son utilizados para, video, video conferencias, audio de alta calidad entre otros, en Tablas 6 a 9, se muestra un resumen de los diferentes códecs de acuerdo a su clasificación en base a la frecuencia.

Tabla 6

Códecs de Banda angosta (NB)

Códec	**Nombre**	**Tasa de bit (Kbps)**	**Retardo (ms)**	**Comentarios**
G.711	PCM: Pulse Code Modulation	64 / 56	0,125	Utiliza dos posibles leyes de compresión: μ-law y A-law

Códec	Nombre	Tasa de bit (Kbps)	Retardo (ms)	Comentarios
G.723.1	Hybrid MPC-MLQ and ACELP	6,3 / 5,3	37,5	Desarrollado inicialmente para videoconferencias en la PSTN. Se utiliza actualmente en VoIP
G.728	LD-CELP: LowDelay Code Excited Linear Prediction	40 / 16 / 12,8 / 9,6	1,25	Diseñado para aplicaciones DCME (Digital Circuit Multiplex Encoding)
G.729	CS-ACELP: Conjugate Structure Algebraic Codebook Excited Linear Prediction	11,8 / 8 / 6,4	15	Ampliamente utilizado en aplicaciones de VoIP, a 8 KHz
AMR	Adaptative Multi Rate	12,2 a 4,75	20	Utilizado en redes celulares GSM
iLBC	internet Low Bitrate Códec	15,2 / 13,33	20 / 30	Utilizado en VoIP por su robustez ante pérdida de paquetes

Nota: La tabla muestra las características de los códecs de banda angosta, (Joskowicz, 2015).

Tabla 7

Códecs de banda ancha (WB)

Códec	Nombre	Tasa de bit (Kbps)	Retardo (ms)	Comentarios
G.722	Sub-band ADPCM	64 / 56 / 48	3	Originalmente creado para audio y videoconferencias. Actualmente utilizado en servicios de telefonía de banda ancha en VoIP
G.722.1	Transform Coder	32 / 24	40	Usado en audio y videoconferencias
G.711.1	WideBand G.711	96 / 80 / 64	11,875	Amplía el ancho de banda del códec G.711, optimizando su uso para VoIP
G.729.1	WideBand G.729	8 a 32	49	Amplía el ancho de banda del códec G.729, optimizando su uso para VoIP con audio de alta calidad
G.722.2	AMR-WB	23,85 a 6,6	25,8375	Estándar en común con 3GPP
GSM	-	13	22,5	Alta relación de compresión, es gratuito y se usa en muchas plataformas.

Nota: La tabla muestra las características de los códecs de banda ancha, (Joskowicz, 2015).

Tabla 8

Códecs de super banda ancha (SWB)

Códec	Nombre	Tasa de bit (Kbps)	Retardo (ms)	Comentarios
G.711.1 SWB	G.711.1 Superwideband	128 a 96	12,8125	Extensión interoperable con G711 y G711.1
G.722 SWB	G.722 Superwideband	96 / 80 / 64	12,3125	Extensión interoperable con G.722
G.722.1C	Anexo C de G.722.1	48 / 32 / 24	40	Optimizado para su uso en tiempo real
SILK	SILK	8 a 24	25	Utilizado por Skype

Nota: La tabla muestra las características de los códecs de super banda ancha,

(Joskowicz, 2015).

Tabla 9

Códecs de banda completa

Códec	Nombre	Tasa de bit (Kbps)	Retardo (ms)	Comentarios
G.719	Low-complexity, full-band	32 a 128	40	Primer códec fullband estandarizado por la ITU-T
Opus	Opus	6 a 510	Hasta 60	Incorpora tecnología de SKYPERFC 6716 (propuesta en set 2012)

Nota: La tabla muestra las características de los códecs de banda completa,

(Joskowicz, 2015).

Valores de medición

En la sección anterior se especificó una de las características principales de los codificadores/decodificadores que se presento es la inteligibilidad de la señal de voz y video en cuanto a la comunicación, gracias a las características propias de cada uno de los códecs cada uno afecta de cierta manera a la señal ya sea por una alta compresión, un alto retardo entre otros factores, por ello es necesario tener una medida práctica para indicar esta calidad, para ello existen tres formas o medidas prácticas que son CoS, RFactor y MOS [Means Opinion Score] (VoiceHost Limited, 2020).

Class of Service (CoS): Este mide el porcentaje de los paquetes que llegan a ambos extremos de la conversación, es decir, de forma ideal se esperaría que lleguen el 100% de los paquetes, por lo que se esperan valores porcentuales, como COS=100%, COS=95%, etc.

R-Factor: Esta es una medida que se obtiene a partir de métricas como la latencia, retardo, perdida de paquetes, todo esto en base a la recomendación de la ITU-T G.107, este valor R es de gran ayuda para evaluar de manera sencilla y rápida la calidad de una llamada VoIP y se mide en valores de 0 a 100, siendo 0 el peor valor y 100 el mejor, de manera práctica estos valores suelen oscilar entre 50 y 90.

MOS: De manera similar a el factor R, se basa en medir los valores de paquetes perdidos, jitter, retardo, pero genera un valor promedio entre 1 y 5, siendo 1 el peor y 5 el mejor, esta medida es la más utiliza para tener una idea la calidad de la llamada mediante VoIP.

Es importante entender que estas mediciones de las llamadas VoIP son principalmente más objetivas, por lo que se calculan en base al rendimiento de la red IP, sin embargo, la implementación es abierta a la interpretación del software o fabricante del

equipo, para ello existen diferentes herramientas de monitoreo VoIP tanto de paga como de software libre.

Tabla 10

R-Factor y MOS

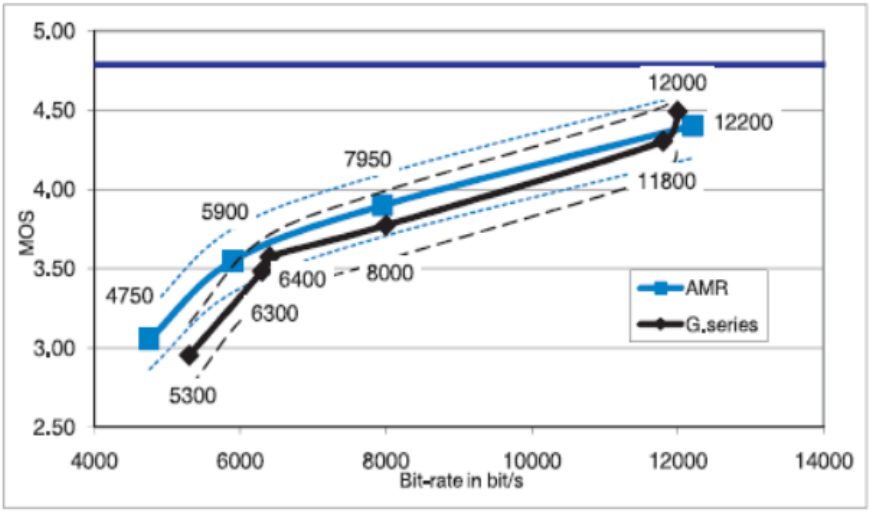
MOS	R-Factor	Quality	Deterioro
5	90-100	Excelente	Imperceptible
4	80-90	Bueno	Perceptible pero no molesta
3	70-80	Normal	Ligeramente molesta
2	50-70	Pobre	Molesta
1	<50	Malo	Muy molesta

Nota: La tabla muestra los valores correspondientes para las mediciones en base a MOS, (VoiceHost Limited, 2020).

En definitiva, estas medidas son una manera sencilla y efectiva para tener una idea de la calidad y experiencia que tuvo o tendrá un usuario en una llamada a través de VoIP, todo esto tiene un factor clave que son los códecs, por ello se debe tener un criterio de lo que el servicio o servicios a implementar con VoIP va a ofrecer, para tener una idea más clara de estas medidas, en las Figuras 19 a la 21, aquí se observan comparaciones entre códecs, NW, BW y SWB.

Figura 19

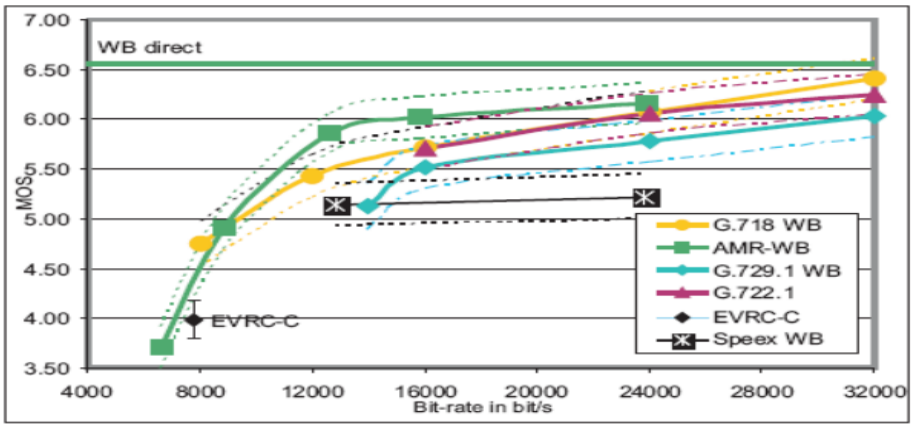
Comparación de códecs de banda angosta en base a MOS



Nota: La figura muestra una comparación del MOS entre códecs, (Barrera, 2012).

Figura 20

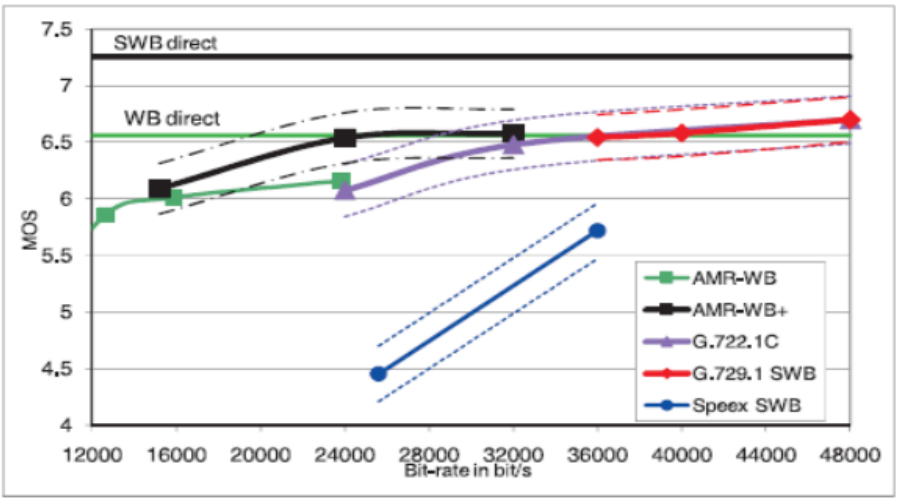
Comparación de códecs de banda ancha en base a MOS



Nota: La figura muestra una comparación del MOS entre diferentes códecs, (Barrera, 2012).

Figura 21

Comparación de códecs de super banda ancha en base a MOS



Nota: La figura muestra una comparación del MOS entre códecs de banda super ancha, (Barrera, 2012).

Cloud-Hosting

El alojamiento en la nube o conocido como Cloud Hosting, es un servicio en el cuál uno o varios servidores virtuales son utilizados de manera remota, esto con el fin de crear una aplicación, sitios web, entre otros, todos estos servicios tienen la ventaja que pueden ser accedidos desde cualquier parte del mundo mediante Internet, estos servidores tienen grandes ventajas en cuenta a disponibilidad y escalabilidad, este servicio de manera general se cobra por la demanda del mismo es decir en base a las capacidades que se requieren para la aplicación, como, Memoria RAM, Capacidad de Procesamiento, Tasa de transferencia, servidores de propósito general o dedicados, etc.

Existen múltiples ventajas que proporciona el alojamiento en la nube, las principales son la escalabilidad, ya que si se requiere de una mayor capacidad, espacio

de almacenamiento u otro requerimiento se puede realizar este redimensionamiento de manera sencilla, además, posee un control de costos ya que se define un monto mensual dependiendo las necesidades, por otro lado su manejo es sencillo y de manera remota, por lo que se pueden agregar o eliminar recursos de manera fácil, finalmente, existen un sin número de empresas o Clouds que ofrecen este servicio, pero las más conocidas y con mejores prestaciones costo beneficio son (Guajardo, 2020) :

- Amazon AWS
- Cloudways
- Digital Ocean
- Google Cloud

Asterisk

Introducción

Hoy en día sin lugar a dudas se puede afirmar que el mundo de las comunicaciones ha cambiado radicalmente, ya que al inicio solo se disponía de la telefonía fija, pero al transcurso del tiempo esto ha ido avanzando y ahora tenemos telefonía móvil, telefonía IP, etc.

Todo este gran avance de la telefonía IP comenzó cuando un joven (Mark Spencer) se lanzó al mundo empresarial e implemento una empresa para dar soporte en temas relacionados con Linux, a la que la llamo Linux Support Services. Entonces el objetivo principal de Mark Spencer fue proporcionar un servicio las 24 horas al día, para poder atender estas inquietudes cualquier persona podría llamar, dejar un mensaje y su solicitud se la atendería lo antes posible. La idea que tuvo Mark Spencer resulto en la utilización de un sistema telefónico, que a la final el precio a pagar era demasiado alto,

entonces le vino una idea que era la de programar una PBX desde cero y ahí es donde nació Asterisk.

Asterisk fue creado en el año de 1999 para ese año la utilización de dicho software fue un cambio radical para las comunicaciones, ya que existían PBX, pero eran basadas en hardware y Asterisk era una solución basada en software, entonces tenía ciertas particularidades como ofrecer una mayor flexibilidad y escalabilidad.

Para ese año era un gran avance realizar llamadas mediante el internet, entonces para que Asterisk sea un producto completo le faltaba interaccionar con líneas analógicas y digitales (PSTN), en este punto se encontró con el proyecto Zapata Telephony. En este sentido Asterisk fue capaz de unir ambos mundos: la telefonía tradicional y la tecnología VoIP.

El secreto del éxito de Asterisk es que esta desarrollado mediante software libre, entonces contrasta el mundo de las PBX tradicionales ya que es un mundo totalmente cerrado. Asimismo, esto llevo a que Asterisk se propague rápidamente y capte todo tipo de público como las pequeñas, medias y grandes empresas que basan su modelo de negocio en dicha plataforma (López & Montoya, 2008).

Definición

Asterisk es una plataforma de código abierto desarrollado para construir aplicaciones relacionados con la comunicación (central telefónica). Entre las principales características de Asterisk se puede crear sistemas de telefonía IP, servidores de conferencia, Gateways VoIP y diferentes soluciones personalizadas, que en un tiempo atrás se las obtenía realizando una gran inversión para poder obtener y acceder a todas las funcionales de dichos sistemas.

Asterisk es un estupendo instrumento al momento de crear una central PBX, ya que al utilizar sus múltiples módulos y múltiples funciones se logra crear un sistema de comunicaciones integral.

Principales características de Asterisk

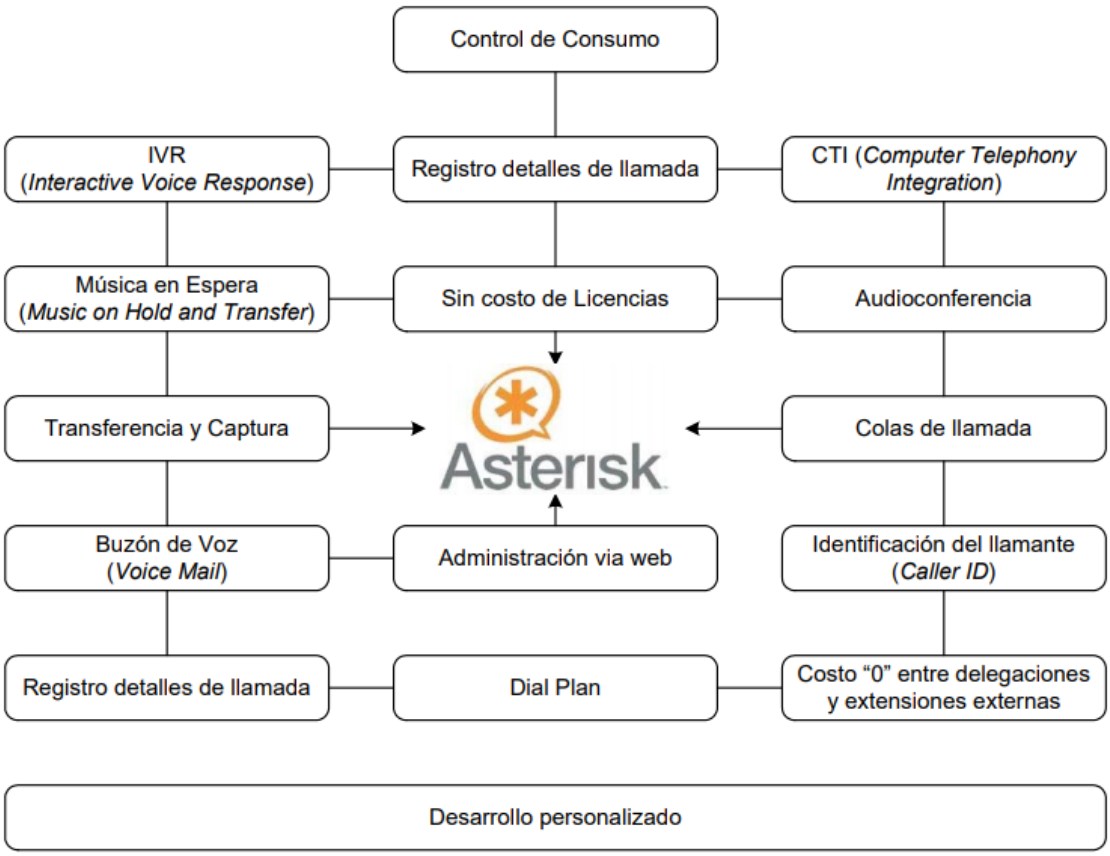
Asterisk cuenta con varias particularidades que nos facilita la creación de un sistema de comunicaciones y las características más relevantes son las siguientes (Masip, 2019):

- **Escalable y flexible**: esto es debido a que la plataforma está desarrollada para que su funcionamiento sea mediante módulos, entonces cada desarrollador puede manipular y personalizar según sus necesidades, y a medida que vayan creciendo pueden ir aumentando la cantidad de usuarios e ir agregando mayores funcionalidades a su sistema.
- **Integración con la PSTN**: esta es una característica bastante sobresaliente ya que es compatible con la telefonía tradicional y la telefonía IP, es decir, es una central mixta.
- **Soporta una variedad de códecs (audio, video):** G.711, G.722, G.723, G.729, GSM, Opus, VP8, H.264, ILBC.
- **Soporta todo tipo de protocolos**: SIP, IAX2 [Inter-Asterisk eXchange], H.323, Skinny, MGCP [Media Gateway Control Protocol].

En la Figura 22 se muestra las características de Asterisk.

Figura 22

Características de una central Asterisk



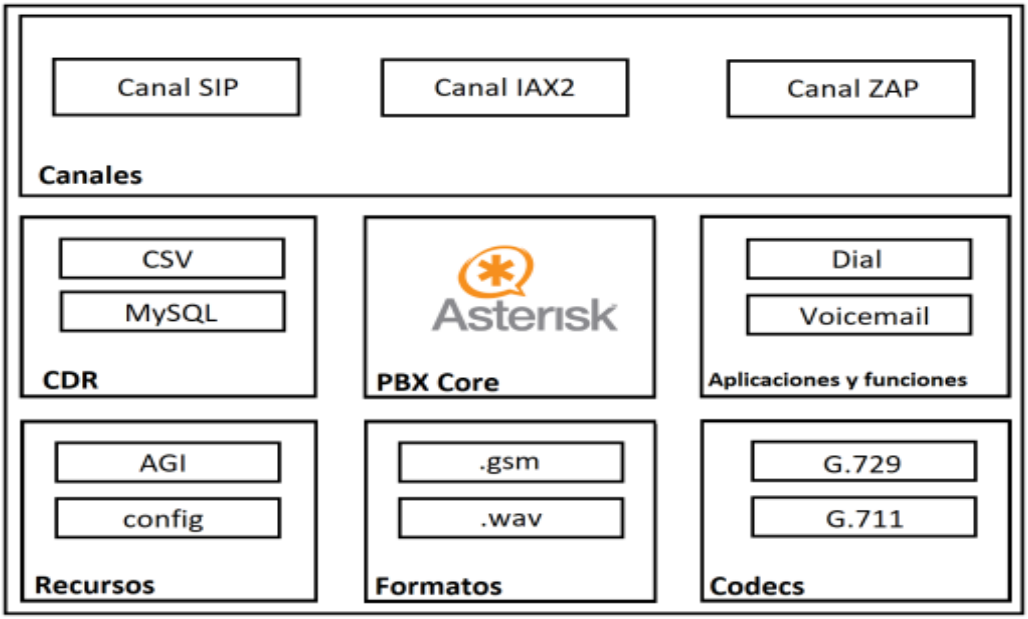
Nota: La figura muestra una serie de componentes que posee y son de utilidad en una central Asterisk, (Vaca, 2008).

Arquitectura

En la Figura 23 se observa que Asterisk fue desarrollado mediante módulos, donde cada usuario puede seleccionar los módulos que mejor se adapten a su diseño.

Figura 23

Estructura modular de Asterisk



Nota: La figura muestra los módulos que están integrados en Asterisk, los cuales tiene una función definida, (López & Montoya, 2008).

Se puede observar en la Figura 23 que dicha arquitectura se divide en 7 módulos, donde el usuario elegirá los módulos que mejor se adapten a su diseño y así irá armando su sistema de comunicación. A continuación, se detalla cada módulo (López & Montoya, 2008).:

- **Core**: Como su nombre lo indica se trata del núcleo de Asterisk y su función es permitir la carga de cada módulo.

- **Canales**: Este módulo se refiere a los diferentes protocolos que soporta la plataforma Asterisk. El protocolo IAX2 utiliza el módulo chan_iax, el protocolo SIP chan_sip y para canales análogos/digitales se utiliza chan_zap.

- **CDR**: Este módulo es el encargado de realizar todo el registro telefónico (por ejemplo, número de extensión, duración de la llamada, fuente de la llamada, destino de la llamada, etc). Además, es compatible con el formato CSV, MySQL, etc.

- **Aplicaciones y Funciones**: Este módulo nos permite aportar con varias herramientas al momento de realizar la configuración de la plataforma Asterisk.

- **Recursos**: Este módulo va de la mano con el módulo Core ya que le aporta con otras funcionalidades (por ejemplo, música en espera, lectura de los ficheros de configuración, etc).

- **Formatos**: Este módulo se encarga de manejar diferentes ficheros con diferentes formatos es decir permite que Asterisk maneje varios formatos (por ejemplo, alaw, mp3, gsm, etc.)

- **Códecs**: Este módulo nos ayuda en la codificación y decodificación de la información, ya sea esta audio o video.

Zabbix

Zabbix es un sistema que integra varias soluciones de monitoreo, nos ayuda a llevar un mejor control de servidores, servicios de red, máquinas virtuales, base de datos, backups, entre otros. Las principales características son las siguientes (Zabbix, 2020):

- El panel de control nos ayuda a mostrar los diferentes datos (por ejemplo, el número de llamadas realizadas en un día), los diferentes problemas que puedan darse en el servidor, los gráficos favoritos mostrados en primera plana, el estado del sistema entre otras vistas. Además, se puede realizar un filtro para que solo muestre los datos que realmente le interese al usuario.

- Muestra notificaciones de aviso cuando existe algún tipo de problema (por ejemplo, que el almacenamiento del servidor está totalmente lleno), envía un aviso al panel de control con el error que se ha producido.
- Nos proporciona recopilación de datos que se los puede visualizar mediante gráficas que son muy interactivas y se los puede observar desde el panel de control. También se puede especificar el período de tiempo en el cual se quiere visualizar los datos, con la ayuda de la herramienta calendario.
- Se puede crear acciones internas para que Zabbix nos notifique que acciona acabamos de ejecutar, esto se lo puede anexar con SMTP para que llegue un correo electrónico al administrador de la cuenta.

No-IP

No-IP ofrece varios servicios los cuales son: Dominios, DNS [Domain Name System], monitoreo de la red, correo electrónico, entre otros. El servicio de DNS dinámico se lo puede adquirir tanto de manera gratuita como pagada. El DNS gratuito tiene las siguientes características (No-IP, 2020):

- Permite como máximo 3 nombres de host.
- La cantidad de dominios son limitados.
- Para seguir utilizando el dominio gratuito sin que los administradores de No-IP lo eliminen se debe confirman cada treinta días que aún se lo está utilizando.

Fail2ban

Es un sistema de prevención de intrusos, esta aplicación es realizada a través del software Python y su objetivo principal es la de bloquear boots o conexiones remotas que

intentan ingresar a nuestro sistema mediante la fuerza bruta, es decir, ingresando claves aleatorias hasta lograr adivinarla. Los ataques de fuerza bruta consumen un gran ancho de banda que se lo podría dedicar a tareas útiles. El funcionamiento de Fail2ban es buscar en los registros (logs) de los programas que se haya decidido aplicar la penalización. Entre las penalizaciones tenemos (León, 2020):

- Bloquear la aplicación que ha fallado en un puerto en específico.
- Bloquear la aplicación en todos los puertos.
- Las penalizaciones son definidas por el administrador que pueden ser minuto, horas o incluso días.

Además, se le permite al usuario una cierta cantidad de intentos para poder ingresar, si supera esta cantidad de intentos automáticamente el usuario queda bloqueado con las condiciones definidas por el administrador. Incluso se puede levantar la penalización si el usuario que intento ingresar se equivocó al ingresar las credenciales, entonces mediante el CLI se le puede desbloquear.

Capítulo III

Análisis, Diseño e Implementación del Sistema

Introducción

En este capítulo se desea presentar el enfoque que se consideró para realizar el diseño en base a los diferentes requerimientos, tanto técnicos como de los usuarios, posteriormente con estos requerimientos se realizará una investigación para lograr elegir de una manera eficiente los equipos y software necesario que cumplan con dichos requerimientos, por añadidura, una vez que se planteó la elección del software y equipos necesarios se procedió con la configuración del software e implementación del sistema,

en las zonas que de acuerdo al diseño y requerimientos que fueron levantados para cumplir los requerimientos de los beneficiarios.

Definición de los escenarios

Se busca implementar un sistema de acceso y alarma comunitaria basado en una PBX virtual para áreas residenciales. De forma general los dispositivos necesarios al ser una PBX virtual son los teléfonos celulares de cada residente y el servidor que provea el servicio de Cloud-Hosting.

Para el primer escenario lo que se busca es la implementación del sistema de acceso en la garita de control de la urbanización San Francisco del Rancho para lo cual fue necesario instalar un Softphone en el celular de cada usuario, de esta manera, cuando lleguen personas externas el guardia podrá comunicarse con el residente de la casa correspondiente mediante una llamada o videollamada.

Por otra parte, para la alarma será necesario un dispositivo, por lo cual debe ser considerado que el dispositivo pueda funcionar en el ambiente exterior de la Ciudad de Quito, de manera más concreta en la urbanización San Francisco del Rancho ubicada en Sangolquí, este dispositivo se ubicó en una zona estratégica donde se tienen límites con otras urbanizaciones o zonas residenciales por lo cual estará a la intemperie y es necesario considerar los cambios bruscos de clima, además, que puede ser objeto de actos vandálicos, por lo cual debe ser adaptado en un poste a una altura adecuada, también, se debe tomar en cuenta que no debe tener un exceso de potencia para no molestar a las residencias más cercanas al dispositivo y que el mismo no presente anomalías para un correcto funcionamiento.

La urbanización San Francisco del Rancho cuenta con un total de 37 Hectáreas, que se distribuyen en 5 sectores (Ver Anexo 1), donde se encuentran un total de 557

lotes, se consideró que en una casa promedio se cuentan con 4 personas que forman el núcleo familiar, siendo un total estimado de 2228 personas que viven en esta urbanización, de las cuales se consideró que al menos la mitad utilizaría el sistema, puesto que, muchas personas no siempre se encuentran en sus hogares debido a que deben salir por diferentes necesidades o situaciones labores , siendo un total aproximado de usuarios de 1114 personas.

Requerimientos de la Urbanización

Para comenzar, se establecieron diferentes reuniones con el presidente, administradora, diferentes miembros de la junta directiva y personal de seguridad de la Urbanización San Francisco del Rancho, en los cuales se trataron diferentes temas entre estos están las necesidades que tenían en ese momento en la urbanización, los problemas más frecuentes, las zonas más vulnerables y el número de personas que participaron en el plan piloto, en consecuencia, surgieron los siguientes requerimientos.

- Instalación del sistema de control de acceso en la garita para visitantes
- Instalación y socialización del Softphone en los dispositivos móviles de los usuarios.
- El sistema de control de acceso debe contar con audio y video .
- Instalación del sistema de alarma y perifoneo.
- Desarrollo de una página Web para visualizar el registro de llamadas.
- Los avisos realizados por guardianía mediante perifoneo puedan ser escuchados por todos los usuarios, dichos avisos pueden ser realizados en tiempo o real o estar pregrabados.

- Instalación del parlante en una zona específica donde se tenían la mayor cantidad de inconvenientes.
- Activación de una alarma comunitaria mediante la marcación de un numero definido en el Dialplan (Ver Anexo 2).

Análisis de la propuesta de diseño e implementación

El sistema tiene como propósito controlar el acceso y alarma en un área residencial, para ello se debe considerar principalmente aspectos, como códecs, ancho de banda, sonorización entre otros, en primera instancia se necesita conocer el ancho de banda requerido para con ello elegir un plan adecuado en el Cloud-Hosting y posteriormente realizar un estudio de sonorización de acuerdo a las zonas del área residencial.

Sistema de monitoreo y control de acceso

El sistema de control de acceso, se basará en la implementación de un servidor de Telefonía IP que estará alojado en la nube y que deberá funcionar de la siguiente manera, en el área residencial, en este caso la urbanización San Francisco del Rancho ubicada en Sangolquí, la cual cuenta con una garita de acceso, en la cual se dispondrá de un dispositivo móvil, en el momento que una persona solicite el ingreso el guardia encargado solicitara el número de casa y llamara a través del dispositivo móvil marcando el número de casa “###” (mismo que es de 3 cifras), una vez establecida la llamada se comunicara con un residente de la vivienda y podrá negar o autorizar la entrada de la persona en cuestión, además de ser necesario se podrá activar el video para la verificación visual.

Sistema de monitoreo y control de acceso

En cuanto al sistema de alarma y perifoneo, se instalará un parlante en una zona estratégica, en el cual se podrán reproducir mensajes pregrabados o dar anuncios en vivo mediante un dispositivo móvil, también, se podrá activar una alarma en caso de una emergencia marcando un número establecido en el Dial plan (Ver Anexo 2).

Análisis de implementación del sistema de control de acceso en contraste con los requerimientos de los usuarios

Análisis para la elección del plan de alojamiento del Servidor de Telefonía

Para la elección correcta de un plan del Cloud-Hosting o servidor como se lo llamará en adelante, se basa principalmente en parámetros como son Cuota de transferencia, Número de CPU, Capacidad de Almacenamiento, Memoria RAM, por ello primero se determinará el ancho de banda necesario, en este caso se implementara un prototipo a un total de 30 personas de un total aproximado de 1114 personas, considerando que el tiempo de duración medio de una llamada es de 2.5 minutos, con estos datos se calculará la intensidad de tráfico en base a la siguiente ecuación.

$$I = \frac{\#Usuarios \cdot t}{HoraCargada} \quad (1)$$

$$I = \frac{30\ usuarios\ \cdot 2.5\ \frac{min}{usuarios}}{60\ min} = 1{,}25\ [Er] \quad (2)$$

De manera general se considera una probabilidad de bloqueo para una aplicación VoIP entre 0.5% hasta un 1%, para nuestro caso se utilizará el 1% y se calculará el número de canales en base a la tabla de Erlang B (Academia, 2021).

$$PB(I = 1{,}25\ ;C = ?) = 1\%$$

$$C = 5$$

Una vez obtenido el número de canales se analiza los codecs disponibles y mostrados en las Tablas 6 a 9, con esto se han elegido los codecs GSM, G711 para el audio y VP8 para el video.

GSM

$$v_{tx} = 5 \cdot 2 \cdot 13kbps = 0{,}13\ Mbps$$

Se debe calcular el RBR que es el número de bits que se van a transmitir por segundo, con el propósito de garantizar que el medio que va a realizar la transmisión pueda soportar toda esta cantidad de información, esto se lo realiza con la ecuación número 3 y para lo cual se considerara una eficiencia de un 55%, de manera análoga este proceso se debe realizar con cada uno de los códecs.

$$RBR = \frac{\eta}{E_f} \tag{3}$$

$$RBR = \frac{0{,}13\ Mbps}{55\%} = 0.24\ Mbps \tag{4}$$

G711

$$v_{tx} = 5 \cdot 2 \cdot 64kbps = 0{,}64\ Mbps$$

$$RBR = \frac{\eta}{E_f}$$

$$RBR = \frac{0{,}64\ Mbps}{55\%} = 1{,}16\ Mbps \tag{5}$$

VP8

VP8 [Video Compression Format] es un códec de video de código abierto y desarrollado por Google, el cual tiene una tasa de bit aproximada de 490kbps para una calidad de video media (A. Mazhar, 2016).

$$v_{tx} = 5 \cdot 2 \cdot 490kbps = 4{,}9\ Mbps$$

$$RBR = \frac{\eta}{E_f}$$

$$RBR = \frac{4{,}9\ Mbps}{55\%} = 8.91\ Mbps \quad (6)$$

Se debe tomar en cuenta el peor escenario posible, el cual sería que todas las llamadas utilicen video, en este caso y para el propósito del sistema no se consideran llamadas simultaneas, pero si varias llamadas al día por usuario, por lo que se elige un plan de 1 TB de transferencia mensual, lo cual con una distribución equitativa para un mes de 30 días equivale a 33,33 GB al día, por lo que es una capacidad ideal para cumplir con los requerimientos, además considerando las capacidades básicas que necesita Asterisk para un correcto funcionamiento, siendo una capacidad mínima de memoria 1 GB RAM, 1 CPU, 2GB almacenamiento, se decidió utilizar Digital Ocean como servidor, el cual presenta los planes de la Figura 24.

Figura 24

Planes de los Droplets disponibles en Digital Ocean.

Como se observa en la Figura 24, se disponen de diferentes planes, para nuestro propósito el plan de $5, será suficiente, sin embargo, se eligió un plan de $10 mensuales, ya que pueden existir otros aspectos que no se consideran como la posible asignación de más extensiones, usuarios, entre otros, por lo cual este plan será suficientemente capaz de cumplir con requerimientos posteriores en caso de que estos surjan.

Software

Una vez comprendido el diseño y la solución del sistema, se realizará la elección de los elementos del sistema. Por consiguiente, se presenta un análisis de los requerimientos técnicos para el funcionamiento del sistema.

Al momento de realizar el control de acceso desde la guardianía, el guardia realizará una llamada desde su teléfono móvil (celular), marcando el número de casa que la persona externa vaya a visitar, esto se lo puede realizar mediante una llamada telefónica o una videollamada. Para realizar la llamada mediante el teléfono móvil es necesario tener instalado un Softphone.

Existen una gran cantidad de Softphone, gratuitos como pagados y entre los más utilizados están los siguientes:

- Acrobits Groundwire
- Linphone
- SessionTalk SIP Softphone
- Softphone
- Zoiper

Acrobits Groundwire

Acrobits Groundwire es una aplicación VoIP gratuita, está disponible solo para dispositivos móviles (Android, iOS). Fue diseñada específicamente para usuarios móviles, es decir, para usuarios activos de smartphones. La principal característica de esta aplicación es que cuenta con la opción de notificaciones push, también, si se desea personalizar la aplicación se pueden contactar con los administradores para adquirir una licencia premium, esto nos permitirá realizar cambios, aumentar o quitar funcionalidades, teniendo en cuenta que cada funcionalidad tendrá un costo adicional (Acrobits, 2020).

Linphone

Linphone es una aplicación VoIP gratuita, la cual es gratuita y está disponible tanto para ordenadores (Linux, Windows, Mac) como dispositivos móviles (Android, iOS). La característica principal es que este softphone es de código abierto, entonces los usuarios o clientes tienen la libertad para modificar dicha aplicación (Linphone, 2020).

SessionTalk SIP

SessionTalk SIP es una aplicación VoIP gratuita que está disponible solo para dispositivos móviles (Android, iOS). Es una aplicación fácil de usar y configurar, tiene

varias opciones bastante intuitivas para acceder de manera rápida a todas las funcionalidades que nos proporciona dicho softphone *(Central IP, 2020)*.

Softphone

Softphone es una aplicación VoIP gratuita disponible tanto para ordenadores (Windows, Mac) y dispositivos móviles (Android, iOS). Su principal característica es que fue diseñada para un nivel empresarial y se le pude sacar el máximo de provecho a sus llamativas funcionalidades, por ejemplo, compartir pantalla, administración de contactos, entre otros *(Central IP, 2020)*.

Zoiper

Zoiper es un softphone VoIP gratuito, es compatibles tanto con ordenadores (Windows, Mac) como para dispositivos móviles (Android, iOS). Además, cuenta con un alto grado de encriptación, para los usuarios que necesiten tener un mayor nivel de seguridad (Bancos, Cobros bancarios, etc) *(Central IP, 2020)*.

Elección del softphone

Es necesario seleccionar la mejor plataforma del desarrollo del proyecto y que este estudio sirva como guía para cualquier persona que se adentre con la tecnológica VoIP.

Todos los softphone anteriormente mencionados presentan ventajas como desventajas propias de los desarrolladores, entonces para la elección del softphone a utilizar se realizará un cuadro comparativo para así seleccionar la aplicación que más se ajuste a nuestros objetivos. En la Tabla 11 se observa una comparativa de los diferentes softphone a utilizar:

Tabla 11

Comparaciones de los diferentes softphone

Softphone Características	Linphone	Zoiper	Softphone	Acrobits Groundwire	SessionTalk SIP
Notificaciones Push				X	
Video llamada	X	X	X	X	X
Transferencia de llamada	X	X	X	X	X
Open Source	X				
Encriptación SRTP	X	X	X	X	X
Integración de contactos	X	X	X	X	X
Registro simultaneo de múltiples cuentas	X		X	X	
Contestación automática	X	X		X	

Nota: En la tabla se muestran las especificaciones de los diferentes softphone que se utilizó para realizar las pruebas de funcionamiento.

En la Tabla 11 se observa que el softphone que mayores características tiene son “Linphone” y “Acrobits Groundwire”, sin embargo, se realizó las pruebas con cuatro softphone con el objetivo de evaluar las diferentes características, siendo estos: “Linphone”, “Zoiper”, “SessionTalk SIP” y “Acrobits Groundwire”.

Para realizar la elección correcta del softphone a utilizar se realizó una encuesta a los moradores de la urbanización San Francisco del Rancho que estaban dentro del plan piloto. Se les instalo los siguientes softphone: “Linphone”, “Zoiper”, “SessionTalk SIP” y “Acrobits Groundwire”. En el Anexo 3 se puede observar la encuesta realizada a los moradores de la urbanización San Francisco, para así seleccionar el softphone que más se adapte a sus necesidades.

Con los comentarios obtenidos a través de la encuesta realizada (Ver Anexo 3) se hizo un análisis de cada softphone para así seleccionar el que mejor se adapte a las necesidades. A continuación, se muestra el análisis realizado:

- Acrobits Groundwire, utiliza un ancho de banda mínimo para establecer la llamada, cabe destacar que nunca hubo desconexión, la voz y el video tienen una calidad aceptable ya que los códecs utilizados son GSM para audio y VP8 para video. Es preciso señalar que la principal característica de la aplicación es que trabaja con notificaciones push, por lo tanto, se realiza consultas desde el servidor hacia el usuario para notificarle que le está ingresando una llamada sin la necesidad que la aplicación esté funcionando en segundo plano, estas notificaciones nos ayudan a alertar o despertar al celular. Las notificaciones push definitivamente fue de mucha ayuda para los celulares iOS, ya que los desarrolladores de dichos dispositivos no nos permiten tener aplicaciones en segundo plano, de tal forma que Acrobits Groundwire es una aplicación diseñada específicamente para usuarios móviles, por lo tanto, cumple con los objetivos planteados.

En la Figura 25 se observa el logo de “Acrobits Groundwire”.

Figura 25

Logo "Acrobits Groundwire

Nota: En la figura se muestra el logo de Acrobits Groundwire, (Vittles, 2020).

Análisis de implementación del sistema de Alarma Comunitaria contraste con los requerimientos de los usuarios.

Análisis de Sonorización

Es necesario analizar y diseñar la sonorización, para la elección adecuada de los equipos y tomar en consideración la salud auditiva del o los individuos que puedan estar o verse afectados por este entorno, por tanto, se requiere obtener cierto perfil de la zona, además, es de vital importancia conocer que en el Distrito Metropolitano de Quito y otros municipios se presentó la ordenanza N° 146 que tiene como objetivo establecer los valores máximos permitidos de ruido que son 65dB durante el día y 55dB por la noche (Avila, 2016).

Hay que considerar ciertos aspectos como la velocidad del sonido que es 356 m/s, también a una temperatura de 22 °C se tiene 1 atmosfera de presión, este valor puede variar dependiendo diversas condiciones, temperatura, humedad, presión, entre otros. Hay que tener en cuenta que el rango de frecuencia que puede percibir el oído humano es de 20Hz hasta 20kHz, de manera general, el sonido varía en función del tiempo y se ve influenciado por los siguientes parámetros:

- Velocidad (v)
- Longitud de onda (λ)
- Periodo (T)
- Amplitud (A)
- Frecuencia (f)

Es necesario tomar en cuenta dos unidades importantes, la primera los decibelios (dB) que expresa una relación entre dos potencias sean acústicas o eléctricas, esta unidad no tiene dimensiones es decir es adimensional. Por otra parte, el SPL [Nivel de Presión Sonora] permite expresar la magnitud de un campo sonoro, se debe tener una referencia y para ello nos basamos en la Figura 26, donde se expresa varios SPL y sus ejemplos para asimilar su magnitud. (Isbert, 1998)

Figura 26

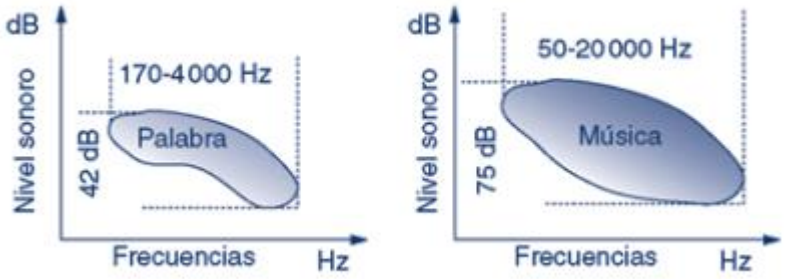
Niveles de presión Sonora

Nota: En la figura se muestra los niveles de presión sonora el denominado SPL (Carramolino, 2007).

Es necesario tomar en cuenta que el sonido o los sonidos no solo varían en frecuencia si no en intensidad, esta intensidad estará determinada por la fuente del sonido a la que se le denomina dinámica de los sonidos y comprende 40dB para la voz y 70dB para la música.

Figura 27

Dinámica de los sonidos



Nota: En la figura se muestra la dinámica de los sonidos, es decir, el nivel sonoro respecto de la frecuencia, (Carramolino, 2007).

En nuestro caso es importante determinar estas dos características la voz para el tema de perifoneo y la música para la activación de las alarmas, para ello la Tabla 12 indica un resumen de ciertos tipos de voz con su respectivo nivel sonoro en referencia a un metro de distancia del hablante.

Tabla 12

Niveles acústicos aproximados de la voz referente a 1 metro de distancia del hablante.

Voz	Nivel sonoro [dB]
Susurro	25
Conversación	30-55
Orador	60
Arenga	75
Grito	80

Nota: En la figura se muestra la dinámica de los sonidos, es decir, el nivel sonoro respecto de la frecuencia, (Carramolino, 2007).

Por otro lado, en la música es bien conocida que existe una infinidad de instrumentos con los que se pueden generar diferentes sonidos, estos dependen fundamentalmente del rango de frecuencias que es capaz de abarcar el instrumento y es tan amplia como el rango de frecuencias que detecta nuestro oído, en la Tabla 13 se indica un ejemplo de alguno de estos instrumentos.

Tabla 13

Rango de frecuencia y niveles sonoros de algunos instrumentos .

Voz	Rango de frecuencias	Nivel sonoro [dB]
Piano	27 Hz a 3 kHz	64
Flauta	250 Hz a 2.5 kHz	49
Órgano	16 Hz a 5 kHz	72
Orquesta	30 Hz a 16 kHz	95

Nota: En la tabla se muestra el rango de frecuencias y niveles sonoros de ciertos instrumentos, (Carramolino, 2007).

Un punto que es esencial a tomar en consideración ya que siempre está presente, es el ruido, debido a que diariamente nos vemos rodeados de sonido como aullidos, ladridos, motores, entre otros, en la Tabla 14 se muestra algunos ejemplos de Ruido con su determinada frecuencia y nivel Sonoro. Sin embargo, es importante tomar en cuenta

que el ruido también depende de las condiciones ambientales de una zona específica y de la persona que lo percibe.

Tabla 14

Ejemplos de Ruido con sus determinados niveles de frecuencia y nivel sonoro.

Ruido	Rango de frecuencias	Nivel sonoro [dB]
Tráfico	100 Hz a 3 kHz	77-88
Reactor	20 Hz a 4 kHz	110
Impresora	300 Hz a 5 kHz	55

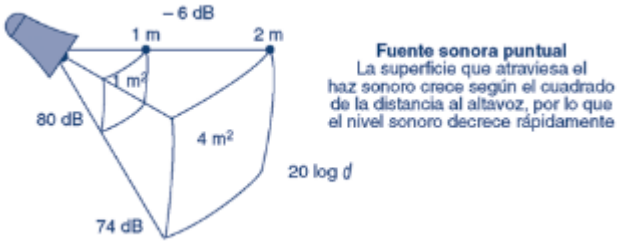
Nota: En la tabla se muestra los ejemplos de ruido con sus determinados niveles de frecuencia y el nivel sonoro (Carramolino, 2007).

Con todas las características mencionadas es importante considerar que la propagación del sonido se emite de una fuente sonora puntual y se propaga en forma de ondas esféricas a una velocidad de 340 [m/s], cuyo centro es el origen (Carramolino, 2007). No obstante, este concepto es el ideal ya que no siempre las fuentes son puntuales o todas las ondas se propagan de manera esférica, algunas pueden ser cilíndricas, cónicas, etc., por estas razones es importante conocer la atenuación que tendrá la onda sonora.

Si nos alejamos de la fuente sonora el sonido se atenúa de manera gradual, a razón de -6 dB en una fuente puntual y de -3 dB en una fuente lineal al duplicar la distancia, de esta manera en nuestro caso al utilizarse fuentes puntuales debemos considerar -6 dB de atenuación cada que se duplique la distancia, un ejemplo de esto se observa en la Figura 28.

Figura 28

Atenuación de una fuente puntual



Nota: En la figura se muestra la atenuación de una fuente puntual. La superficie que atraviesa el haz sonoro según el cuadrado de la distancia al altavoz, (Carramolino, 2007).

Debido a que el parlante será instalado en una zona externa es necesario considerar que existe una afectación debido a los agentes atmosféricos como viento, temperatura, etc. Estos influyen cuando en el recorrido de la onda sonora, la Tabla 15 muestra algunos valores de atenuación de una onda sonora por la absorción de aire, también, es necesario considera que como es una zona exterior el viento y la temperatura tendrán un gran efecto ya que de manera general en horas de la mañana el sonido se propaga hacia arriba ya que el aire caliente está cerca de la tierra y el aire frío por encima, al contrario, en horas nocturnas se invierten las condiciones y el sonido se propaga hacia abajo, por otra parte se recomienda que al estar en exterior la inclinación del parlante sea con una inclinación hacia abajo esto con el propósito de disminuir la atenuación (Carramolino, 2007).

Tabla 15

Atenuación del sonido en base a diferentes frecuencias

Frecuencias [Hz]	Atenuación [dB/100 m]
100	0.02
500	0.2
1000	0.6
5000	3
10000	10

Nota: En la tabla se muestra valores de la atenuación del sonido en base a diferentes frecuencias, (Carramolino, 2007).

Conociendo estos datos técnicos y diferentes fenómenos y características, se pueden obtener ciertas características necesarias, puesto que el parlante se colocará en un poste de alumbrado público, según la normativa de la Empresa Eléctrica Quito S.A. en el 2017, los postes decorativos tendrán una altura de 6 metros y los postes normales una altura de 15 metros (Varela, 2017).

Figura 29

Zona seleccionada para la instalación del parlante IP

Nota: En la figura se muestra la zona que fue seleccionada para instalar el parlante con sus respectivas dimensiones.

En la Figura 29 se observa la zona donde se va a instalar el parlante, esta zona fue elegida al momento de levantar los requerimientos de la urbanización, ya que en esta zona se presentan algunos problemas debido a que colinda con otras dos urbes diferentes, por lo cual es necesario tener un mayor control, por otra parte, al instalarse un solo dispositivo este será considerado como una fuente puntual, por lo que será necesario calcular un SPL adecuado en base a la atenuación, para ello la ecuación indicada para una fuente puntual es la Ecuación 7 (Carramolino, 2007):

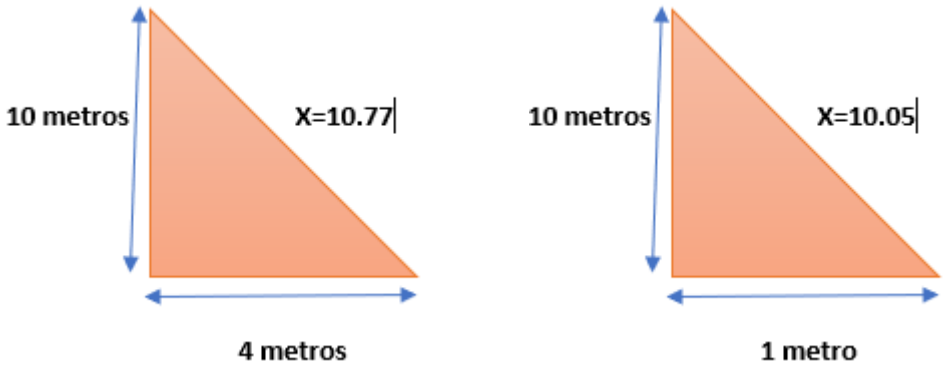
$$At = 20\log(d) \qquad (7)$$

En este caso la distancia más larga estará dada en base al teorema de Pitágoras ya que se tiene dos dimensiones que fueron medidas la altura y el largo de la calzada por donde pasan los peatones, para esto se consideran dos casos el primero el caso más alejado cuando se está a 4 metros del parlante y el segundo caso donde se encuentre a

una distancia de 1 metro es decir al borde de la vereda aproximadamente estas distancias se aprecian en la Figura 30.

Figura 30

Cálculo de la distancia en base a triángulos para obtener la atenuación del parlante



Nota: En la figura se muestra cómo se realizó el cálculo de la distancia en base a triángulos para lograr obtener la atenuación del parlante.

$$At = 20\log(d)$$

$$Caso\ I$$

$$At = 20\log(10.77) = 20.64\ dB$$

$$Caso\ II$$

$$At = 20\log(10.05) = 20.04\ dB$$

Con todos los datos presentados se elige una atenuación de 20.64 dB que sería la peor atenuación de acuerdo a la frecuencia correspondiente a la voz, además, se debe considerar la atenuación en base a la Tabla 14, de acuerdo a la frecuencia de la voz se elige 3 dB, se busca obtener un SPL mínimo de 95 dB, para esto se utiliza la Ecuación 8, obteniendo

$$SPL \geq 95dB \quad (8)$$

$$SPL - 20.64 - 3 \geq 95dB$$

$$SPL \geq 95dB + 20.64dB + 3dB$$

$$SPL \geq 118.64\ dB$$

Por tanto, en base a los cálculos y parámetros planteados se necesita un parlante que tenga un mínimo SPL de 118.64 dB considerando las peores condiciones posibles, esto ayudara a tener un sonido claro en el área estimada para el uso del parlante.

Hardware

Para realizar el perifoneo el guardia realizará una llamada desde su teléfono móvil (celular) a través de la aplicación “Acrobits Groundwire”, marcará el número de extensión al cual está configurado en el Dial Plan y el parlante para poder dar avisos a los moradores de la urbanización. En el mercado existen varias soluciones para realizar el perifoneo mediante IP. Se realizará una comparación entre las soluciones más llamativas para elegir la solución que cumpla con los objetivos planteados.

Evaluación del sistema de Perifoneo

KNTECH

KNTECH es una empresa ubicada en China en la ciudad de Hong-Kong especializada en la tecnología VoIP. La empresa tiene a su disposición algunos tipos de altavoces IP que funcionan mediante el protocolo SIP, los cuales son los siguientes:

- KNSIPSP-L8-30W
- KNSIPSP-L7-7W
- KNSIPSP-T-L9-7W

Las especificaciones de cada parlante se muestran en la Tabla 16.

Tabla 16

Especificaciones de parlantes IP

Modelo **Características**	**KNSIPSP-L7-7W**	**KNSIPSP-L8-30W**	**KNSIPSP_T-L9-7W**
Potencia	7 W	30 W	7 W
Dimensión (W*H*D)	150*80*270 mm	150*80*270 mm	240*156 mm
Protocolo	SIP RFC 3261	SIP RFC 3261	SIP RFC 3261
Alimentación	PoE	110 V – 230 V AC	PoE
Máximo SPL	>95 dB	>95 dB	>92 dB
Respuesta de frecuencia	280 Hz – 12.5 kHz	280 Hz – 12.5 kHz	280 Hz – 12.5 kHz
Compresión de audio	G.711 G.723 G.726 G.729	G.711 G.723 G.726 G.729	G.711 G.723 G.726 G.729
Grado de protección	IP66	IP66	--

Figura 31

Parlantes IP de KNTECH

Nota: En la Figura se puede observar los altavoces IP (KNTECH, 2021).

KNTECH es una empresa ubicada en China en la ciudad de Hong-Kong especializada en la tecnología VoIP. La empresa tiene a su disposición algunos tipos de altavoces IP que funcionan mediante el protocolo SIP, los cuales son los siguientes:

CINETO

CINETO es una empresa ubicada en Ecuador en la ciudad de Quito especializada en soporte de soluciones hoteleras, Wifi y telefonía IP. La empresa tiene a su disposición algunos tipos de parlantes IP que funcionan mediante el protocolo SIP, los cuales son los siguientes:

- Altoparlante bocina IP
- Parlante de pared IP

- Parlante de techo IP

Las especificaciones de cada parlante se muestran en la Tabla 17.

Tabla 17

Especificaciones de parlantes IP .

Modelo **Características**	**Altoparlante bocina IP**	**Parlante de pared IP**	**Parlante de techo IP**
Potencia	20 W	20W	10W
Dimensión (W*H*D)	390*370 mm	350*500*200 mm	210*120 mm
Protocolo	SIP-RTP, RFC 3261	SIP-RTP, RFC 3261	SIP-RTP, RFC 3261
Alimentación	PoE	PoE	PoE
Máximo SPL	92 dB	88 dB	85 dB
Respuesta de frecuencia	250 Hz – 10 kHz	250 Hz – 10 kHz	250 Hz – 10 kHz
Compresión de audio	G.711 PCM (U-Law, A-Law)	G.711 PCM (U-Law, A-Law)	G.711 PCM (U-Law, A-Law)
Grado de protección	IP66	IP66	--

Figura 32

Parlantes IP de CINETO .

Nota: En la Figura se puede observar los altavoces IP (CINETO, 2021).

EMACS

EMACS es una empresa ubicada en España en la ciudad de Madrid especializada en sistemas de seguridad, sistemas contra incendios y Smart Cities (electrónica, sistemas informáticos, perifoneo, etc). La empresa tiene a su disposición una interfaz de audio IP/SIP para megafonía e intercomunicación.

Tabla 18

Especificaciones de la interfaz OPTIMUS IA-20SIP .

Modelo **Características**	**IA-20SIP**
Alimentación	PoE
Salida de audio	Directa para altavoz (8 ohm, 2 W)

Modelo **Características**	**IA-20SIP**
Indicadores	Alimentación, llamada y nivel de audio
Entrada de audio con nivel seleccionable	AUX / MIC
Modo de funcionamiento	Emisor, receptor o bidireccional
Configuración de parámetros	Mediante servidor WEB
Salidas de audio	AUX (0 dB) / MIC (-60 dB)

Nota: En la Tabla 18 se puede observar las características de la interfaz OPTIMUS IA-20SIP.

Figura 33

Equipo IA-20SIP.

Nota: En la Figura se puede observar el equipo IA-20SIP.

CISER SYSTEM

CISER SYSTEM es una empresa ubicada en España en la ciudad de Madrid especializada en intercomunicación, telefonía, asistencia y seguridad. La empresa tiene a su disposición un sistema de megafonía para difusión de avisos en entornos 100% IP. La empresa tiene a su disposición varias soluciones que funcionan mediante IP, los cuales son los siguientes:

- Bocina IP MIP-650
- Altavoz de techo MIP-660
- Altavoz de pared MIP-670
- Gateway Megafonía IP MIP-381
- Gateway Megafonía IP con amplificación MIP-3840

En la Tabla 19 se puede observar las características de los altavoces IP.

Tabla 19

Especificaciones de los altavoces IP .

Modelo **Características**	**Bocina IP MIP-650**	**Altavoz de techo MIP-660**	**Altavoz de pared MIP-670**
Potencia	20 W	6 W	20 W
Dimensión (W*H*D)	280*200*280 mm	198*166*110 mm	270*150*195 mm

Modelo Características	Bocina IP MIP-650	Altavoz de techo MIP-660	Altavoz de pared MIP-670
Protocolo	SIP (RFC 2543, RFC 3261)	SIP (RFC 2543, RFC 3261)	SIP (RFC 2543, RFC 3261)
Alimentación	PoE	PoE	PoE
Máximo SPL	92 dB	--	85 dB
Respuesta de frecuencia	300 Hz – 10 kHz	300 Hz – 10 kHz	300 Hz – 10 kHz
Compresión de audio	G.711, G.726, G.722, G.729	G.711, G.726, G.722, G.729	G.711, G.726, G.722, G.729
Grado de protección	IP60	--	IP55

Figura 34

Altavoces IP de CYSER SYSTEM .

Nota: En la Figura se puede observar los altavoces IP (CYSER SYSTEM, 2021).

Tabla 20

Especificaciones de los Gateway megafonía IP .

Modelo **Características**	**Gateway Megafonía IP MIP-381**	**Gateway Megafonía IP con amplificación MIP-3840**
Potencia	--	40W
Conector de Audio	3.5 mm	3.5 mm
Protocolo	SIP (RFC 2543, RFC 3261)	SIP (RFC 2543, RFC 3261)
Alimentación	110-240V – 12V/1A	110-240V – 24V/2A
Direccionamiento	1 Puerto RJ45 10/100 Mbps	1 Puerto RJ45 10/100 Mbps
Dimensión (W*H*D)	170*145*40 mm	170*145*40 mm
Compresión de audio	G.711, G.726, G.722, G.729	G.711, G.726, G.722, G.729
Configuración	Vía Web browser	Vía Web browser

Nota: En la Tabla se puede observar las características de los Gateway megafonía IP.

Figura 35

Gateway megafonía IP

Nota: En la Figura se puede observar el equipo Gateway megafonía IP (MIP-381, MIP-3840).

Elección del dispositivo de sonorización IP

A continuación, se procede a seleccionar el dispositivo IP que nos ayudará a realizar el perifoneo. Cabe destacar que, de todas las opciones mostradas con anterioridad, las que mejor se adaptan a nuestros objetivos son los siguientes:

- KNSIPSP-L8-30W
- Altoparlante bocina IP
- IA-20SIP
- Bocina IP MIP-650
- MIP-3840

Es necesario realizar un estimado de los precios de cada dispositivo IP, hay que tener en cuenta que los costos que se mostraran a continuación no incluyen el precio de

envió e importación, ya que tres de las cuatro soluciones propuestas son desarrolladas por empresas que se encuentran ubicadas en el continente europeo o asiático.

Tabla 21

Valor estimado de los dispositivos IP.

Equipo	Empresa	Precio
KNSIPSP-L8-30W	KNTECH (China)	$220.00
Altoparlante bocina IP	Cineto (Ecuador)	$470.40
IA-20SIP	EMACS (Madrid)	$689.85
Bocina IP MIP-650	Ciser System (Madrid)	$205.64
MIP-3840	Ciser System (Madrid)	$436.21

En la Tabla 21 se puede observar el valor estimado de los dispositivos IP, obviamente estos precios de los equipos no incluyen el precio del envío e importación. Es necesario resaltar que para los dispositivos IA-20SIP y MIP-3840 trabajan a la par con un software propietario desarrollado por cada empresa, por esa razón el valor aumentará por cada parlante que se conecte a estos equipos. Por consiguiente, los valores de los equipos son bastantes altos, entonces se decidió trabajar con una solución más económica que es la que se presenta a continuación.

TV-BOX Tx3 Mini

Un TV-Box es un dispositivo que cuenta con un sistema operativo Android, es de tamaño reducido, es importante destacar que contiene varias características y

funcionalidades por el motivo que trabaja con la tienda de “Play Store”, “Google Play”, entre otras. Por ese motivo se puede instalar cualquier aplicación que esté disponible en dichas tiendas. Así mismo consta de varios tipos de puertos y conectores (Tarjeta microSD, USB, Wifi, Ethernet, etc), interfaces de audio y video (HDMI, AV), entre otras características.

Figura 36

TV-BOX Tx3 Mini

Nota: En la Figura 36 se puede observar el TV-BOX.

TV-BOX Tx3 Mini se adapta perfectamente a nuestras necesidades, por consiguiente, se instaló la aplicación “Acrobits Groundwire”. Conviene enfatizar que a través de la interface de audio AV se puede conectar cualquier tipo de parlante o altavoz, sea este pasivo o activo mediante un acoplamiento. Además, cabe destacar que el precio del equipo no supera los $40.

Altavoz HN-30P

En la sección 3.6.1 se realizó un estudio de sonorización con la intención de conocer las características mínimas que debe tener el altavoz o parlante para realizar el perifoneo. El altavoz que cumple con todos los requisitos es el HN-30P. Conviene destacar que el precio del equipo no supera los $75.

Tabla 22

Especificaciones del altavoz HN-30P.

Características	**HN-30P**
Potencia	30 W
Sensibilidad	105 dB
Máximo SPL	120 dB
Respuesta en frecuencia	350Hz – 8 KHz
Alimentación	110 V / 70 V, 8 Ω
Peso	2.30 Kg
Color	Gris blanco
Dimensión (W*H)	292*246 mm
Grado de protección	IP67

Nota: En la Tabla 22 se observa las especificaciones del altavoz.

Figura 37

Altavoz HN-30P

Nota: En la Figura se puede observar el altavoz HN-30P, (Lucky Tone, 2016).

Amplificador BT-309A

En la subsección 3.6.2.4 se eligió el altavoz HN-30P para realizar el perifoneo, sin embargo, el altavoz HN-30P es un dispositivo pasivo. Por ese motivo es necesario tener una etapa de amplificación. Por lo tanto, se ha elegido el amplificador BT-309A. Conviene destacar que el precio del equipo no supera los 50$.

Tabla 23

Especificaciones del amplificador BT-309A.

Características	**BT-309A**
Potencia	50 WRMS
Entrada de audio	RCA
Interfaces	AUX, USB, MIC
Respuesta en frecuencia	20Hz – 20 KHz

Características	BT-309A
Alimentación	110 V / 220 V, 8 Ω
Resistencia de carga	4 Ω, 8 Ω, 16 Ω
Material	Metal
Dimensión (W*H*D)	200*200*55 mm

Nota: En la Tabla se observa las especificaciones del amplificador.

Figura 38

Amplificador BT-309A

Nota: En la Figura se puede observar el amplificador BT-309ª, (*Banggood, 2021).*

A modo de cierre, cabe destacar que el precio de los tres equipos (TV-BOX Tx3 Mini, Altavoz HN-30P, Amplificador BT-309A) no superan el valor de $165, por otra parte, como se observa en las Tablas 22 y 23 este dispositivo cumple con los requerimientos establecidos de potencia que fue de 30 Watts. Además, el Altavoz HN-30P tiene una protección IP67 que le permite tener cobertura para ambientes externos y este cumple con el nivel del SPL que se determinó en la sección 3.6.1 con la ayuda de la Ecuación 8,

por último, el equipo de amplificación no cuenta con protecciones para exteriores por lo cual fue necesario utilizar una caja protectora para este propósito, por ende, sin lugar a dudas esta solución es la que mejor se adecuado a las necesidades y requerimientos planteados por los moradores de la urbanización San Francisco del Rancho.

Implementación del sistema

A continuación, se detallará una clara explicación de cómo se realizó la configuración, diseño e implementación del sistema. Empezaremos explicando el diseño del software, desde como instalar Asterisk a través del CLI, la configuración el archivo sip.conf, cómo crear las extensiones para cada usuario, es decir, mediante el archivo extensions.conf, también abarcaremos la configuración del archivo voicemail.conf, y la configuración del Email. Además, mostraremos como se realizó la configuración de la base de datos, la configuración del servidor Zabbix y la del No-IP. Una vez finalizada la configuración del software comenzaremos a explicar los elementos, y equipos involucrados para el diseño del hardware.

Diseño de software

A continuación, se muestra cómo se realizó el diseño del software, se ha divido la configuración en partes, para así tener una mejor comprensión y facilidad al momento de leer y entender el código implementado.

Instalación de Asterisk

Para la instalación de la plataforma Asterisk es necesario realizar los siguientes pasos:

1. apt-get update
2. apt-get install asterisk

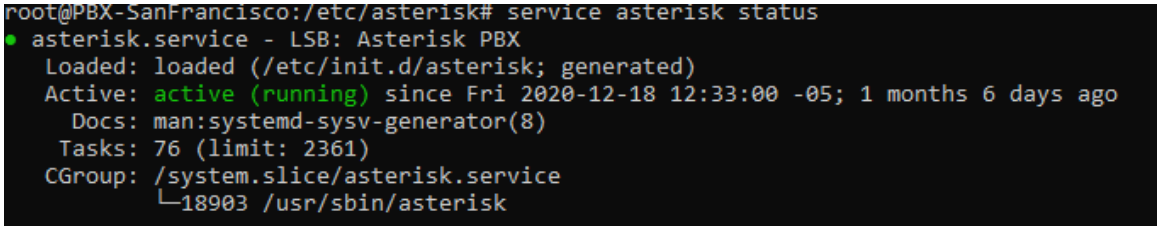
Una vez colocados los dos comandos mostrados en la parte superior, empezará la instalación del software Asterisk.

Para verificar si Asterisk está funcionando correctamente se coloca en la línea de comandos lo siguiente:

3. service asterisk status

Figura 39

Estado de la plataforma Asterisk activado



Nota: En la Figura se observa el estado de Asterisk, que en este caso ya se encuentra activo.

Sip.conf

Es importante destacar que el archivo “sip.conf” se utiliza para configurar todo lo relacionado con el protocolo SIP. Comienza con una sección [general], que es la que contiene las configuraciones por defecto, entonces se utilizó una plantilla creada por nosotros con el nombre [usuario], en donde se definen parámetros personalizados con el fin de modificar, optimizar y facilitar la creación de usuarios. La plantilla utilizada es la que se muestra a continuación:

[usuario](!)

type=friend

host=dynamic

qualify=5000

nat=yes

canreinvite=no

dtmfmode=RFC2833

allow=vp8, ulaw, alaw, gsm

videosupport=yes

context=teléfonos

A continuación, se detalla que función tiene cada parámetro:

- Type: se puede elegir entre “user”, “peer”, friend y su función es autenticar llamadas entrantes, llamadas salientes y en ambas direcciones (bidireccional) respectivamente.
- Host: su función es realizar la autentificación IP que puede ser estática o dinámica.
- Qualify: su función es enviar una petición cada cierto tiempo y verificar que dispositivos siguen conectados y cuáles no.
- Nat: Fuerza a Asterisk a ignorar el campo información de contacto y usar la información de la dirección que vienen los paquetes.
- Dtmfmode: se puede elegir entre “in-band”, “RFC2833”, “auto”, “info” y su funcionalidad es la transmisión de tonos de audio, de la misma manera que el habla.
- Allow: su función es activar los diferentes códecs a utilizar.
- Videosupport: su función es habilitar el video.

- Context: Indica el contexto con el cual estará asociado los usuarios.

Una vez creada la plantilla se tienen definidos todos los parámetros necesarios para una cuenta SIP, a excepción de dos el username y la clave, ya que estas son únicas para cada usuario, entonces en base a un dial-plan (Ver Anexo 2) que se acordó con la administradora de la urbanización se procedió a crear treinta cuentas SIP. A continuación, se observa cómo crear una cuenta SIP:

[extensión](contexto)

username: “Nombre del usuario”

secret= “Clave”

Cabe recalcar que las letras en cursiva son los parámetros que se editan para cada usuario que se vaya a registrar. A continuación, se detalla que función tiene cada parámetro:

[extensión]: Numero de extensión del usuario.

contexto: Contexto con el cual estará asociado los usuarios.

username: Nombre del usuario, es de suma importancia ya que este parámetro se lo utiliza al momento de registrarse en el softphone.

secret: Clave para registrar la cuenta en el softphone.

Es preciso señalar que para la configuracion de todas las cuentas SIP se sigue la misma estructura. En el Anexo 4 se observa la configuración realizada en el archivo sip.conf.

Extensions.conf

Otro archivo de suma importancia es el archivo “extensions.conf” se lo puede considerar como el más importante de Asterisk debido a que se define el dial-plan para cada usuario. En el Anexo 5 se observa la configuración del archivo extensions.conf.

A continuación, se detalla cómo crear una extensión:

exten => extensión,prioridad,Dial(SIP/extensión,tiempo)

exten => extensión,prioridad,VoiceMail(extensión@default)

A continuación, se detalla que función tiene cada parámetro:

extensión: Número de extensión.

prioridad: El número uno es la prioridad más alta.

SIP/extensión: Se conecta con el archivo sip.conf busca la extensión y obtiene todos sus parámetros.

tiempo: Tiempo máximo para responder la llamada, si no se contesta la llamada pasa a la siguiente prioridad.

VoiceMail: Se conecta con el buzón de voz.

Es preciso señalar que para la configuración de todo el dial-plan se sigue la misma estructura.

- Configuraciones especiales

En definitiva, se pueden considerar las configuraciones realizadas en los ítems superiores, son las configuraciones básicas que se realiza en una central IP. Para cumplir con los objetivos propuestos han sido necesarias otras funciones o configuraciones

especiales, para así poder satisfacer la mayor cantidad de necesidades que tienen los moradores de la urbanización San Francisco, siendo estas las siguientes:

- Activación de una alarma comunitaria.
- Avisos realizados por la guardianía, a través del perifoneo, puedan ser escuchados por todos los moradores.
- Activación de parlantes individuales o grupales.

Activación de una alarma comunitaria.

Una de las necesidades de los moradores de la urbanización San Francisco, fue la activación de una alarma comunitaria de manera remota, para poder cumplir con este requerimiento se creó una extensión para que cualquier usuario pueda activar la alarma cuando suceda un evento inesperado, en el Anexo 2 se puede observar el número de extensión que se les otorgo. A continuación, se muestra la función que se utilizó para solventar esta necesidad con éxito:

exten =>extensión,prioridad,Set(TIMEOUT(absolute)=tiempo)

exten =>extensión,prioridad,Dial(SIP/extension,tTaA(“dirección”))

extensión: Número de extensión

prioridad: El número 1 es la prioridad más alta.

tiempo: Tiempo máximo que estará activada la alarma

dirección: Ubicación donde se almacenó el archivo pregrabado.

El primer comando nos ayuda para la finalización de la llamada, es decir, si la persona que activo la alarma no cuelga la llamada automáticamente después de un tiempo “X” finaliza la llamada, del mismo modo la sirena dejará de sonar.

El segundo comando nos permite seleccionar el archivo de audio a reproducir.

Avisos realizados por la guardianía, a través del perifoneo puedan ser escuchados por todos los moradores.

Otra necesidad que tenían los administradores de la urbanización San Francisco del Rancho, era la de dar avisos a los moradores de algún tema en particular o comunicarle de algún evento o noticia que este por realizarse, entonces para disminuir la cantidad de parlantes a ser colocados, se optó por realizar una llamada en tiempo real a la extensión en la cual se encuentre el parlante (Ver Anexo 2) y una vez se haya realizado el aviso y se finalice la llamada automáticamente la grabación se envié a sus correos electrónicos. Entonces se reduce la cantidad de parlantes a colocar y si por alguna razón algún habitante no se encuentre en su hogar, el podrá escuchar el perifoneo que realizó la guardianía y estará al tanto de los eventos sucedidos en su urbanización mientras él no se encontraba. A continuación, se muestra la función que se utilizó para enviar la llamada grabada en tiempo real a los correos electrónicos:

exten => extensión,prioridad,GoSub(contexto,start,prioridad(${EXTEN}))

extensión: Número de extensión.

prioridad: El número 1 es la prioridad más alta.

contexto: Contexto con el cual estará asociado los usuarios.

En el archivo “extensions.conf” se utilizó la función GoSub que permite ejecutar un bloque específico (contexto o sección) del plan de marcación, en este caso salta a un contexto “X” con el parámetro start, que nos ayuda activar la función una vez ingresada al contexto.

El contexto “X” se muestra a continuación:

[contexto]

exten => start,prioridad,MixMonitor(dirección)

exten => start,prioridad,Dial(SIP/${ARG1},tiempo)

exten => h,prioridad,System(bash dirección)

dirección: Ubicación donde se almacenó el archivo grabado.

prioridad: El número 1 es la prioridad más alta.

tiempo: Tiempo máximo para responder la llamada, si no se contesta la llamada pasa a la siguiente prioridad.

Se utilizó la función MixMonitor que nos permite empezar a grabar la llamada y nos permite configurar la dirección en donde se va a guardar el archivo y el nombre con el cual se guardará el archivo, la segunda línea hace referencia al establecimiento de llamada mediante el protocolo SIP con un tiempo de respuesta máximo de “X” segundos, sino se responde la llamada saltará a la siguiente prioridad, la tercera línea utiliza la función System que su función es comunicarse con un script, ya que ahí fue donde se realizó la configuración del mensaje que se enviará a los residentes y es la mostrada a continuación:

rm “dirección/nombre-del-archivo.mp3”

read -t 3 -rsp

ffmpeg -i “dirección/nombre-del-archivo.wav”-acodec mp3 “dirección/nombre-del-archivo.mp3”

sleep 10s

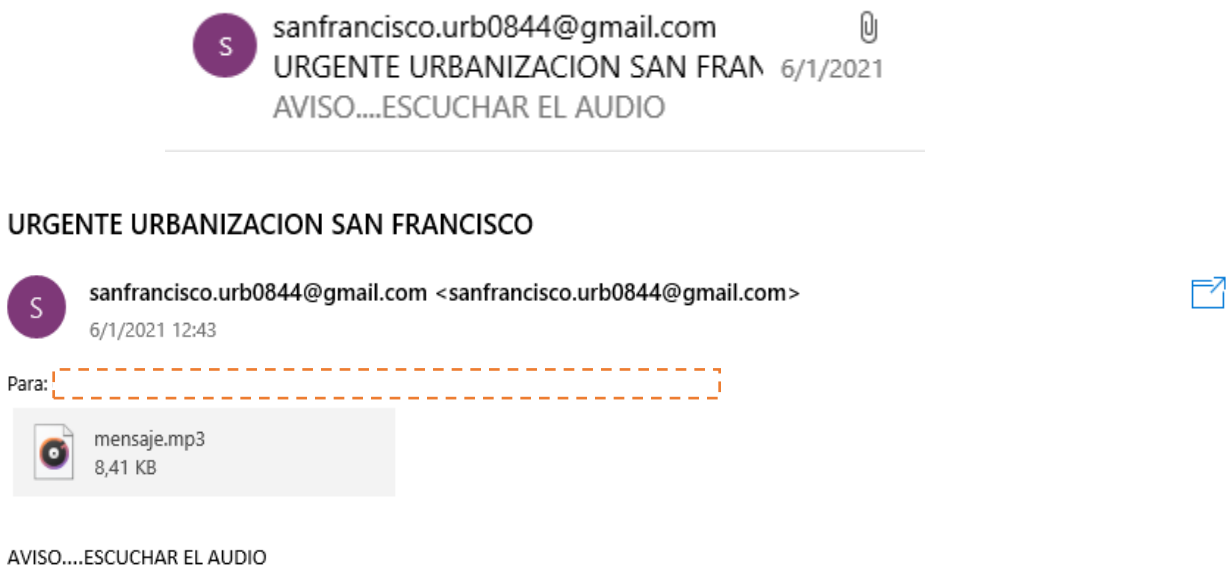
sudo echo "AVISO....ESCUCHAR EL AUDIO" | s-nail -a /var/spool/asterisk/monitor/mensaje.mp3 -s "URGENTE URBANIZACION SAN FRANCISCO" usuario1@dominio.com, usuario2@dominio.com, usuario3@dominio.com

rm “dirección/nombre-del-archivo.mp3”

En el script se configuró de la siguiente manera: cada vez que se grabe una llamada la grabación anterior se borrara automáticamente, luego que se cuelga la llamada y se espera un tiempo de 3 segundo para la sincronización del archivo a la ruta especificada, además se realizó la transformación del archivo .wav a .mp3 y se realizó la configuración del encabezado y asunto del email. En el Anexo 6 se observa la configuración realizada en el script. En la Figura 40 se muestra el email que les llega a los moradores de la urbanización:

Figura 40

Correo recibido



Activación de parlantes individuales o grupales

Otra necesidad que querían solventar los administradores de la urbanización San Francisco del Rancho era que la activación de parlantes se pueda activar uno, dos o tres parlantes a la vez o activarlos todos a la vez, entonces se utilizó la siguiente función:

exten => extensión,1,Page(SIP/extensión&SIP/extensión)

Se utilizo la función Page para realizar la activación de varios parlantes a la vez, marcando a una extensión definida en el dial-plan (Ver Anexo 2). Se realizaron las pruebas con varios parlantes, pero por ser un plan piloto se instaló un solo parlante por cuestiones netamente académicas y financieras.

Voicemail.conf

Por último, la configuración del voicemail.conf es bastante sencilla y permite configurar el buzón de voz de manera general como claves, correo de voz entre otros parámetros, a continuación, se muestra la configuración realizada:

extensión => clave, Nombre de usuario, usuario1@dominio.com

extensión: El número de extensión del usuario

clave: La clave para ingresar al voicemail

Los parámetros extensión y clave son los requeridos por el buzón de voz, ya que si son incorrectos no podrá ingresar a escuchar los mensajes almacenados. En el Anexo 7 se puede observar la configuración realizada en el archivo voicemail.conf. Así mismo, el Anexo 2 muestra el dial-plan para acceder al buzón de voz.

E-mail

Para la configuración del correo electrónico nos ayudamos del servidor EXIM4 siguiendo los pasos que se muestra a continuación:

1.- Asegurarse que Exim4 está instalado:

apt-get install exim4 exim4-config

2.- Una vez que esté instalado, aparecerá una pantalla de configuración, si el paquete ya estaba

instalado se empezará en el paso 2. Si no aparece, se puede acceder a ella en cualquier momento ejecutando el comando:

dpkg-reconfigure exim4-config

3.- Se selección la opción “el correo se envía mediante un smarthost; se recibe a través de SMTP o fetchmail”.

4.- Escribir el nombre del dominio del correo a utilizar (Gmail, Outlook, etc).

5.- En la dirección IP escribir “127.0.0.1”.

6.- Seleccionar aceptar.

7.- En la dirección IP del smarthost saliente escribir “smtp.gmail.com::587”.

8.- Seleccionar NO.

9.- Seleccionar NO.

10.- Seleccionar Aceptar.

11.- En el caso de que aparezca más mensajes seleccionamos las opciones por defecto que nos muestra el sistema.

A continuación, se edita el archivo “/etc/exim4/passed.client”, dentro del archivo se incluye los datos del correo que se encargará de enviar los correos por defecto de la siguiente manera:

smtp.gmail.com:usuario1@dominio.com:contraseña

12.- Ya configurada la cuenta de Gmail, se debe especificar nuevamente que utilizará el puerto 587 para realizar el envío, entonces se edita el archivo:

/etc/exim4/conf.d/transport/30_exim4-config_remote_smtp_smarthost

13.- Buscar la línea “hosts_try_auth” y arriba de esa línea añadimos lo siguiente:

port=587

14.- Y listo, lo último que queda es recargar la configuración con el comando:

update-exim4.conf

En este caso se utilizó gmail por lo cual el puerto correspondiente es el 587, además es necesario dar permisos a aplicaciones poco seguras en gmail directamente para que se puedan enviar los correos sin problema, luego de estos pasos, el correo electrónico estará configurado correctamente, entonces cuando se realice el perifoneo o no pueda responder el residente la llamada, la grabación le llegará tanto a su buzón de voz como a su correo electrónico.

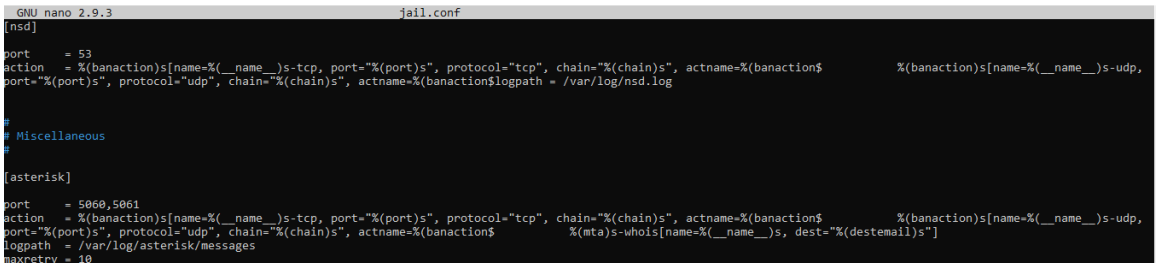
Fail2Ban

Una vez se realiza toda la configuración de Asterisk de acuerdo al Dialplan y los diferentes parámetros planteados, se debe tener en cuenta la seguridad de la nube, para lo cual en primer lugar se habilita el firewall que por defecto en Ubuntu es UFW, aquí se bloquearan de manera general todos los puertos al habilitar ufw con el comando “sudo ufw enable”, posteriormente es necesario conocer los puertos que se van a utilizar para los diferentes servicios como el puerto 80 para http, 5060 para Asterisk, entre otros, y estos se habilitaran con el siguiente comando “sudo ufw allow 8000/tcp” , de esta manera se activaran todos los puertos necesarios.

Por otro lado, es importante considerar que hay diferentes ataques que se realizan a este tipo de servicios en especial ataques de denegación de servicios, por lo cual, es necesario contar con una herramienta como Fail2ban que su principal función como se planteó anterior mente es detectar y bloquear intrusos, para lo cual primero ejecutamos el comando “apt-get install fail2ban”, una vez instalado es necesario con figurar el archivo “jail.conf” ubicado en “/etc/fail2ban/jail.conf”, en este archivo se debe configurar los puertos a ser escuchados, en este caso 5060 y 5061 para Asterisk como se observa en la Figura 41.

Figura 41

Configuración de Asterisk en Fail2ban en el archivo jail.conf



En la Figura 41 los principales parámetros a configurar son port, action, logpath y maxretry, cada uno de estos parámetros tiene que ser configurado adecuadamente, donde:

Port: Puertos a ser escuchados.

Action: Las acciones que se tomaran cuando se acceda de manera incorrecta al servicio, en este caso se añaden las acciones de baneo.

Logpath: ruta o dirección donde se guardarán los mensajes correspondientes a las acciones tomadas.

Maxretry: Número máximo de intentos para acceder al servicio a través del puerto configurado.

De la misma forma es necesario configurar el archivo “jail.local”, ubicado en la misma dirección, “/etc/fail2ban/jail.local”, aquí se establecen diferentes parámetros como el tiempo de baneo, la configuración utilizada se observa en la Figura 42.

Figura 42

Configuración de Asterisk en Fail2ban en el archivo jail.local

```
[sshd]
bantime = 10m
maxretry = 5
findtime = 5m
#ignoreip= 181.113.100.143
[asterisk]
ignoreip= 181.199.52.222
enabled  = true
port     = 5060,5061
action   = %(banaction)s[name=%(__name__)s-tcp, port="%(port)s", protocol="tcp", chain="%(chain)s", actname=%(banaction)s-tcp]
           %(banaction)s[name=%(__name__)s-udp, port="%(port)s", protocol="udp", chain="%(chain)s", actname=%(banaction)s-udp]
           %(mta)s-whois[name=%(__name__)s, dest="%(destemail)s"]
logpath  = /var/log/asterisk/messages
maxretry = 10
bantime = 12h
findtime = 1200
```

Aquí se configuraron algunos parámetros al inicio como el número máximo de intentos en 10 y el tiempo de baneo en 1h, sin embargo, una vez realizada las pruebas y registrados los usuarios, esto se cambió a 3 y 12 horas respectivamente, donde:

Ignoreip: Se asigna una IP la cual no va a ser tomada en cuenta pese a cualquier acción.

Enabled: Se activa o desactiva el monitoreo de este servicio.

Port: Puerto/s que van a estar monitoreados para la detección y bloqueo de intrusos, estos deben ser los configurados en el servicio que se desea monitorear.

Action: Las acciones que se tomaran cuando se acceda de manera incorrecta al servicio, en este caso se añaden las acciones de baneo.

Logpath: ruta o dirección donde se guardarán los mensajes correspondientes a las acciones tomadas.

Maxretry: Número máximo de intentos para acceder al servicio a través del puerto configurado.

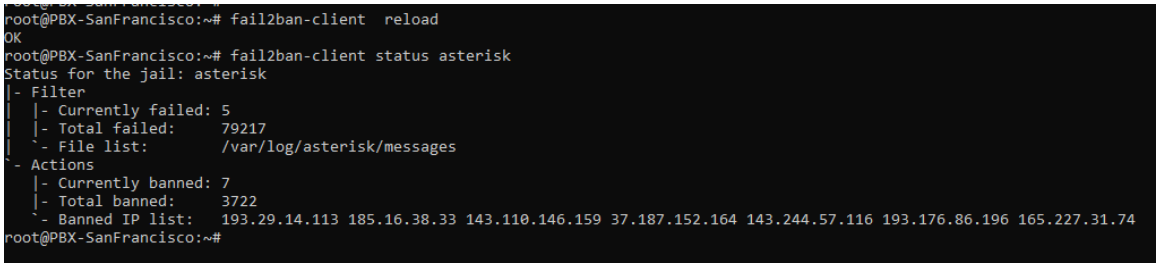
Findtime: Cantidad de tiempo entre intentos de inicio de sesión, antes de que se elimine el host.

Bantime: Cantidad de tiempo en que la IP permanecerá prohibida.

Una vez realizada todas las configuraciones en los archivos, para confirmar que este servicio IDPS esté funcionando correctamente debemos ejecutar el comando “fail2ban-client status <nombre del servicio>”, aquí obtendremos como respuesta el estatus, el filtro aplicado, con el número total de IP que fueron bloqueadas y las que actualmente están bloqueadas, esto se puede observar en la Figura 43.

Figura 43

Estado de la herramienta Fail2ban para el servicio de Asterisk



MariaDB

Es necesario tener una base de datos para poder tener un registro de las llamadas entrantes y salientes, además, de ser necesario esto permitirá realizar un cobro si fuera el caso, para ello se eligió MariaDB, ya que, desde hace unos años, MySQL ha sido poco a poco desplazada por MariaDB y teniendo como característica especial que está

desarrollado bajo una licencia GPL y está basado en MySQL, por esto, se ha comenzado utilizar más MariaDB, para la instalación se necesitan las siguientes líneas de comando:

“apt get install mariadb mariadb-server mariadb-devel -y”

“sudo service mariadb start”

Posteriormente se ejecuta “mysql_secure_installation”, esto permite establecer ciertos niveles de seguridad en el servido MariaDB, las preguntas fueron configuradas de la siguiente manera:

Change the root password? [Y/n] n

Remove anonymous users? [Y/n] y

Disallow root login remotely? [Y/n] n

Remove test database and access to it? [Y/n] y

Reload privilege tables now? [Y/n] y

Ahora es necesario crear la base de datos y la tabla donde se guardará los datos de las llamadas para ello debemos crear la base de datos, usuario, tabla, dar una estructura a la tabla y permisos de usuario, lo cual haremos con los siguientes comandos:

“mysql -u <usuario> -p <contraeña>”

“create database asteriskcdr;”

“use asteriskcdr”

“CREATE TABLE cdr (

calldate datetime NOT NULL default '0000-00-00 00:00:00',

clid varchar(80) NOT NULL default '',

src varchar(80) NOT NULL default '',

dst varchar(80) NOT NULL default '',

dcontext varchar(80) NOT NULL default '',

channel varchar(80) NOT NULL default '',

dstchannel varchar(80) NOT NULL default '',

lastapp varchar(80) NOT NULL default '',

lastdata varchar(80) NOT NULL default '',

duration int(11) NOT NULL default '0',

billsec int(11) NOT NULL default '0',

disposition varchar(45) NOT NULL default '',

amaflags int(11) NOT NULL default '0',

accountcode varchar(20) NOT NULL default '',

peeraccount varchar(20) NOT NULL default '',

uniqueid varchar(32) NOT NULL default '',

linkedid varchar(80) NOT NULL default '',

userfield varchar(255) NOT NULL default '',

KEY callerid (clid)

);”

“GRANT ALL PRIVILEGES ON <nombre de la tabla>.* TO '<usuario>'@'%'

IDENTIFIED BY '<contraseña>';”

También es necesario instalar un driver importante que es el ODBC, para realizar esto es necesario descargar el driver de la siguiente dirección web, https://dev.mysql.com/get/Downloads/Connector-ODBC/8.0/mysql-connector-odbc-8.0.15-linux-ubuntu18.04-x86-64bit.tar.gz , de este link se obtendrá un archivo zip con el driver, así, con este archivo, se siguen los siguientes pasos:

“sudo tar zxvf mysql-connector-odbc-8.0.15-linux-ubuntu18.04-x86-64bit.tar.gz”

“cd mysql-connector-odbc-8.0.15-linux-ubuntu18.04-x86-64bit/”

“sudo cp bin/* /usr/local/bin”

“sudo cp lib/* /usr/local/lib”

“sudo myodbc-installer -a -d -n "MySQL ODBC 8.0 Driver" -t "Driver=/usr/local/lib/libmyodbc8w.so "”

“sudo myodbc-installer -a -d -n "MySQL ODBC 8.0" -t "Driver=/usr/local/lib/libmyodbc8a.so"”

Luego será necesario configurar los parámetros del driver ODBC para ello es necesario ir al archivo “/etc/odbc.ini”, en este archivo es necesario establecer los parámetros para realizar la conexión con la base de datos que generara Asterisk

[Nombre de la tabla]

Description = MySQL connection to 'asterisk' database

Driver = MySQL ODBC 8.0 Driver

Database = nombre de la tabla

Server = servidor ejemplo localhost o 192.168.0.1

User = Usuario

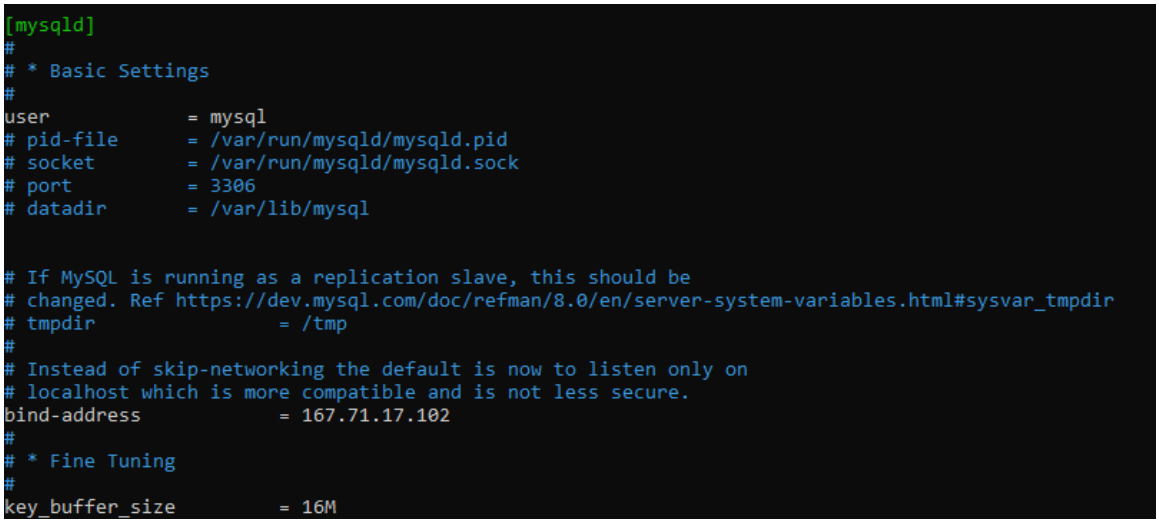
Password = Clave del usuario

Port = puerto de la base de datos por lo general por defecto 3306

En nuestro caso, era necesario acceder a la base de datos de manera remota, por lo cual se debe configurar el archivo en la siguiente ruta “/etc/mysql/mariadb.conf.d/50-server.cnf”, aquí se busca la opción de blind-addres y se la cambia por la dirección IP donde se aloja la base de datos como se observa en la Figura 44.

Figura 44

Configuración para acceso remoto de la base de datos



Una vez configurados todos los parámetros en la base de datos y el driver ODBC, se procede a conectarlo con Asterisk, primero configuraremos el archivo “/etc/odbcinst.ini”, este debe estar configurado como en la Figura 45.

Figura 45

Configuración del archivo odbcinst.ini

```
[MySQL ODBC 8.0 Driver]
Description     = ODBC for MySQL
Driver=/usr/local/lib/libmyodbc8w.so
#UsageCount=1
FileUsage       = 1
Pooling         = Yes
CPTimeout       = 120
[MySQL ODBC 8.0]
#Description     = ODBC for MySQL
Driver=/usr/local/lib/libmyodbc8a.so
#UsageCount=1
FileUsage       = 1
Pooling         = Yes
CPTimeout       = 120
```

Posteriormente se debe configurar o crear el archivo “/etc/odbc.ini”, en este archivo se colocan los siguientes parámetros: servidor, usuario, clave entre otros y debe configurarse como se observa en la Figura 46.

Figura 46

Configuración del archivo odbc.ini

```
[asteriskcdr]
Description = MySQL connection to 'asterisk' database
Driver = MySQL ODBC 8.0 Driver
Database = asteriskcdr
Server = localhost
User = ******
Password = *****
Port = 3306
#Socket = /var/lib/mysql/mysql.sock
```

Para finalizar las configuraciones se debe realizar la configuración en Asterisk para que utilice ODBC y mediante este se conecte a la base de datos, para esto debemos modificar dos archivos en las siguientes rutas, “/etc/asterisk/res_odbc.conf” y “/etc/asterisk/cdr_adaptive_odbc.conf”, cabe mencionar que el archivo CDR por defecto guarda todos los parámetros como duración de una llamada, los números de los

participantes entre otros, estos son generados cada que se realiza una llamada, con esto en mente las configuraciones que se deben agregar se observan en las Figuras 47 y 48.

Figura 47

Configuración del archivo res_odbc.conf

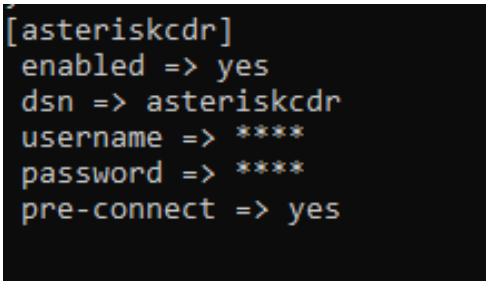
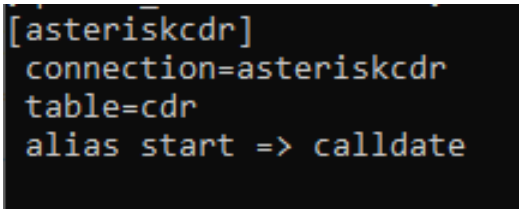


Figura 48

Configuración del archivo cdr_adaptive_odbc.conf



Por último, se debe considerar que en este caso las configuraciones se hicieron de acuerdo a las necesidades planteadas, por lo cual se pueden realizar cambios para acoplarlas de acuerdo a un requerimiento determinado, además, en el Anexo 8 se puede observar de manera gráfica la tabla accedida desde Excel mediante un complemento de SQL.

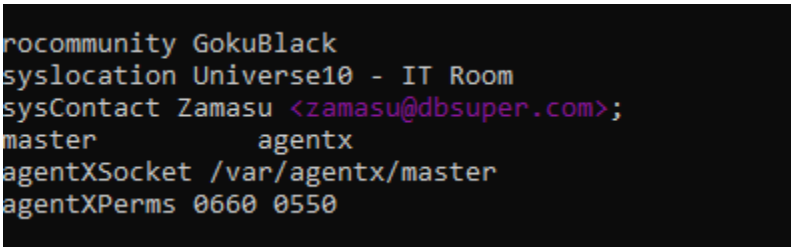
Zabbix

En el capítulo 2 se mencionó los beneficios y características de Zabbix, para instalar esta herramienta de monitoreo se debe instalar primero SNMP y configurar sus diferentes parámetros, esto mediante el comando “apt-get install snmp snmpd snmp-

mibs-downloader", luego, se debe editar el archivo "/etc/snmp/snmpd.conf", este debe tener solo la configuración que se observa en la Figura 49.

Figura 49

Configuración del archivo snmpd.conf

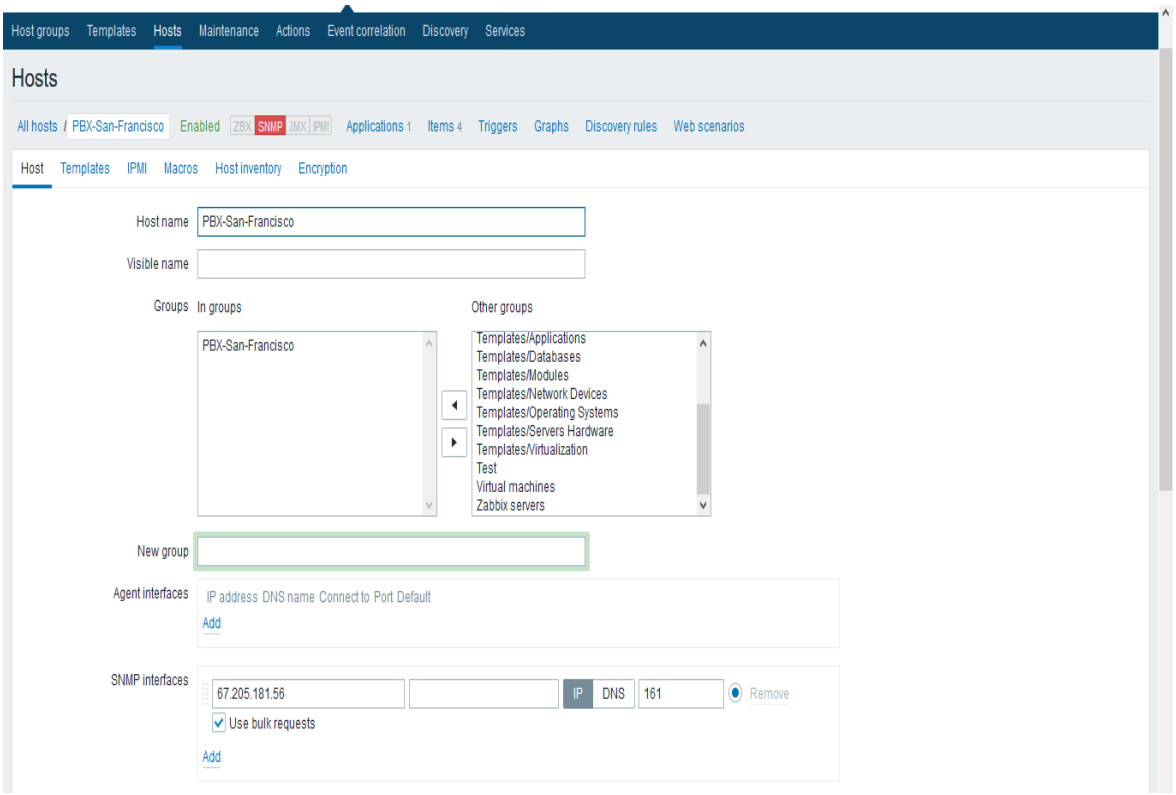


Posteriormente es necesario habilitar las opciones "subagent=yes" y "enabled=yes" en Asterisk, estos parámetros se configuran en el archivo "/etc/asterisk/res_snmp.conf", también , es necesario dirigirnos al directorio "cd /usr/share/snmp/mibs" y crear el archivo "ASTERISK-MIB.txt" que contendrá lo que indica los desarrolladores en el siguiente link "https://wiki.asterisk.org/wiki/display/AST/Asterisk+MIB+Definitions", así mismo, en este directorio se debe crear el archivo "DIGIUM-ASTERISK.txt" su contenido de manera similar está definido en el enlace "https://wiki.asterisk.org/wiki/display/AST/Digium+MIB+Definitions".

Una vez realizadas las configuraciones para la instalación, no dirigimos al navegador y con la Ip "X.X.X.X/zabbix", se accede a la plataforma Zabbix, nos dirigimos a "Configuration" y luego a "Host" para crear un nuevo Host que va a ser monitoreado, esto se puede observar en la Figura 50.

Figura 50

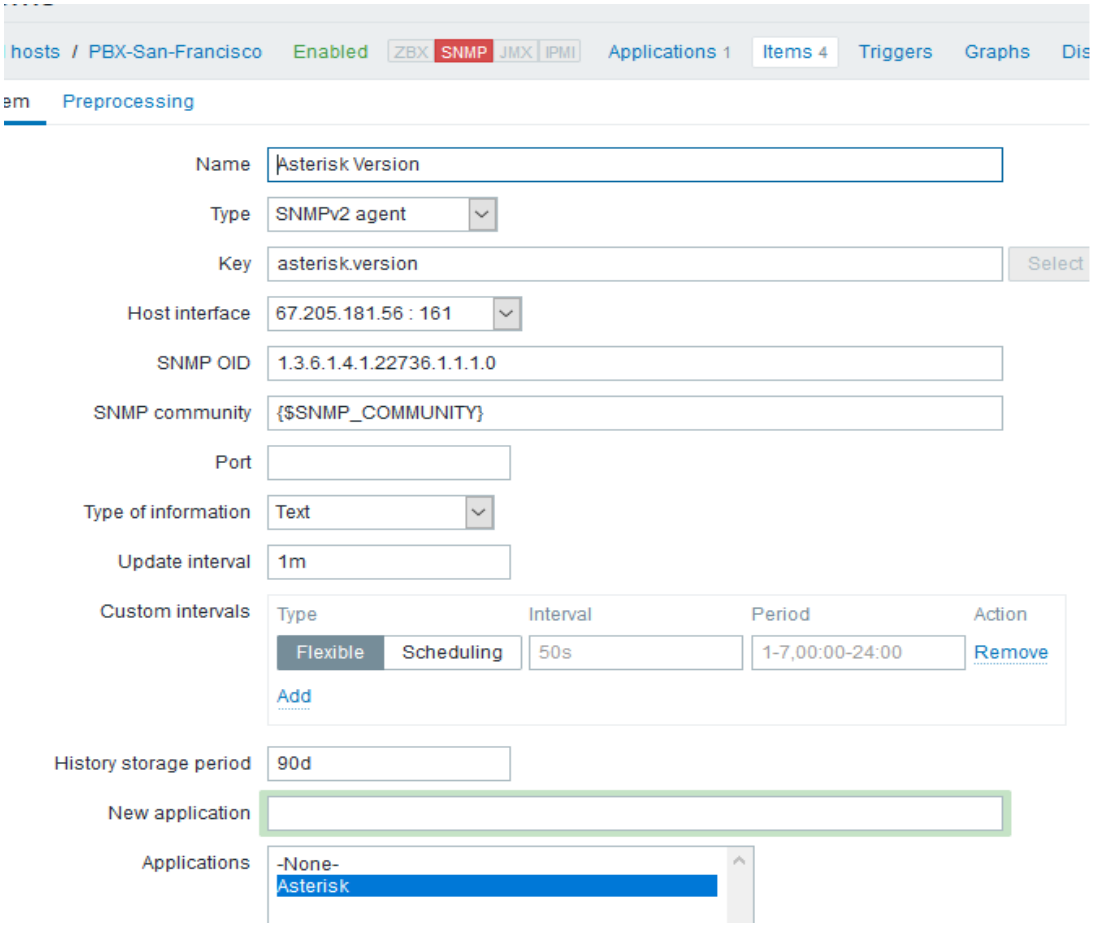
Configuración del Host en Zabbix



Para finalizar se deben crear un macro con aplicaciones que se utilizarán para monitorear Asterisk, es necesario tener en cuenta que cada aplicación cuenta con varios ítems y cada una de estos se encarga de algo diferente, un ejemplo de la configuración de un ítem en aplicación, este ítem llamado Asterisk versión tiene como función verificar la versión o cambios en la versión de Asterisk, esto se puede observar en la Figura 51.

Figura 51

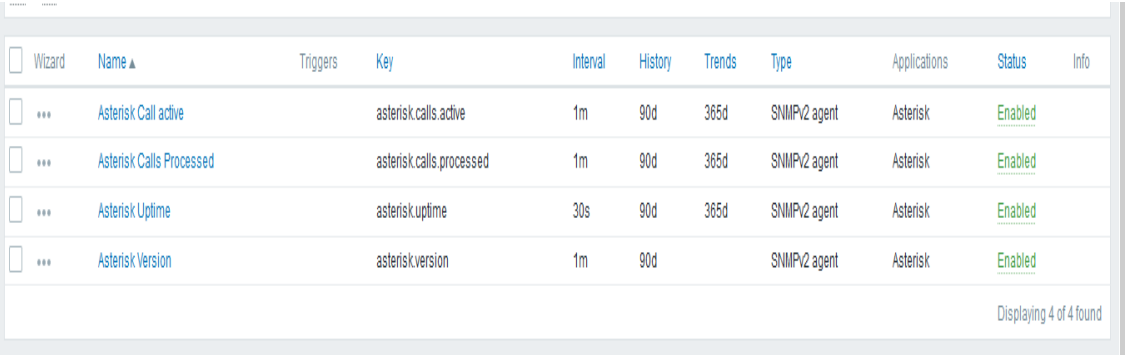
Creación y configuración de una aplicación en Zabbix



De la misma manera que se configura el ítem que se observa en la Figura 51, es posible crear otros, en este caso se crearon 4 ítems, uno para monitorear una llamada que se encuentre ejecutándose, este ítem tiene el nombre “Asterisk Call Active”, otro ítem que se creó con el propósito de obtener todas las llamadas que han sido establecidas, cuyo nombre es “Asterisk Call Processed” y un último ítem “Asterisk Uptime” que tiene la finalidad de verificar el tiempo activo de Asterisk, todas estas ítem se pueden observar en la Figura 52.

Figura 52

Aplicaciones creadas en Zabbix para el monitoreo de Asterisk



Wizard	Name ▲	Triggers	Key	Interval	History	Trends	Type	Applications	Status	Info
•••	Asterisk Call active		asterisk.calls.active	1m	90d	365d	SNMPv2 agent	Asterisk	Enabled	
•••	Asterisk Calls Processed		asterisk.calls.processed	1m	90d	365d	SNMPv2 agent	Asterisk	Enabled	
•••	Asterisk Uptime		asterisk.uptime	30s	90d	365d	SNMPv2 agent	Asterisk	Enabled	
•••	Asterisk Version		asterisk.version	1m	90d		SNMPv2 agent	Asterisk	Enabled	

Displaying 4 of 4 found

Página Web

Con el propósito principal de cumplir uno de los objetivos de la tesis y necesario para los administradores de la urbanización San Francisco del Rancho, ya que en la página web se podrá visualizar los registros de las llamadas realizadas, por tanto, se otorgará, un usuario y contraseña para acceder a esta función, la página web fue diseña mediante HTML y PHP, obteniendo la página como se muestra en la Figura 53, que se encuentra en el siguiente enlace “urbsanfrancisco.ddns.net”.

Figura 53

Vista de la página Web urbanización San Francisco

En la Figura 53 se puede visualizar la estructura de la página web, esta cuenta en la página principal con varia información sobre la urbanización como las áreas verdes, sistemas de seguridad, puntos de control, servicios de guardianía entre otros, esto con el fin de brindar información sobre la propia urbanización, luego, se puede ver en la parte superior varios ítems , en estos están “ACERCA DE NOSOTROS” que muestra la misión y visión de la urbanización, también cuenta con una pestaña de “INFORMACIÓN“ donde se encuentran preguntas frecuentes sobre la urbanización como donde están ubicados entre otras, además cuenta con una “CARTELERA” tipo blog para subir noticias o

información importante para los residentes y finalmente contiene un “LOGIN” en este solo pueden acceder los administradores con un usuario y contraseña, todo esto se observa en las Figuras 53 a 57.

Figura 54

Vista de la pestaña Acerca de nosotros de la página web

Figura 55

Vista de la pestaña información de la página web

Figura 56

Vista de la pestaña cartelera de la página web

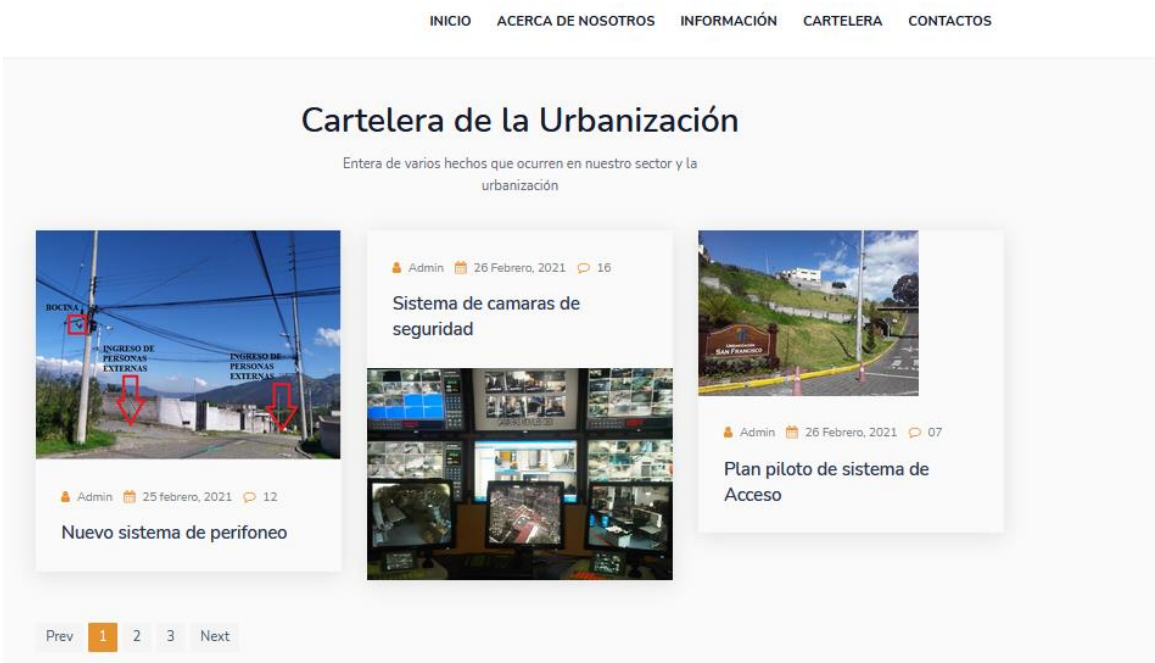
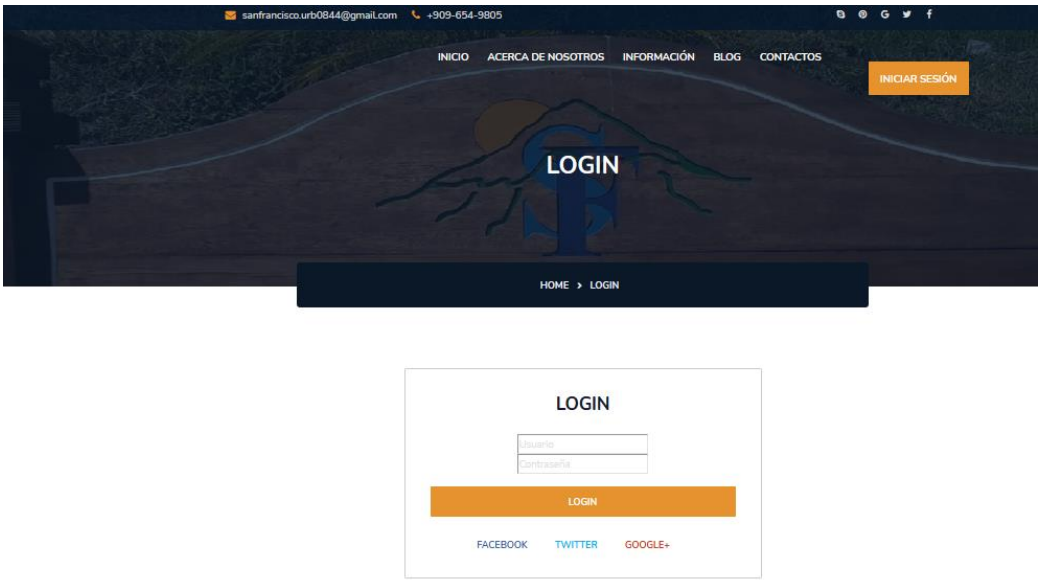


Figura 57

Vista de la pestaña login de la página web



Como se observa en la Figura 57 en esta pestaña de login es necesario ingresar un usuario y contraseña que será solo de uso de los administradores y este les permitirá acceder a un registro de llamadas como se observa en la Figura 58, este registro contiene todas las llamadas realizadas por medio de la centralita VoIP, se tienen 4 columnas las cuales son: “Salientes” esta muestra el origen de la llamada, es decir quien origino la llamada, “Destino” esta columna muestra el número de destino de la llamada, luego las columnas “Start” y “End” muestran las fechas y las horas de inicio y fin respectivamente de cada llamada, además, cada columna tiene un buscador para facilitar la búsqueda de un registro en específico o un buscador general que hará la búsqueda en todo el registro, esto con la finalidad de facilitar su uso al usuario.

Figura 58

Vista del registro de llamadas de la página Web

Diseño de Hardware

El diseño del hardware es tan importante como el diseño del software. En la sección 3.6.2.2 se realizó una descripción de los dispositivos a ser utilizados para la respectiva implementación del hardware, por ese motivo, en esta sección únicamente se mostrará la interconexión de los equipos y los materiales utilizados para realizar dicha conexión. En la Tabla 24 se muestra los equipos y materiales utilizados para la implementación del sistema.

Tabla 24

Equipos y materiales utilizados para la implementación del sistema.

Descripción	Cantidad
Bocina HN-30P	1
TV BOX TX3 Mini	1
Amplificador 50 W (BT-309 A)	1
Cable de red (1 metro)	1
Cable gemelo (50 metros)	1
Cable auxiliar (1 metro)	1

Figura 59

Diagrama de bloques

Nota: En la figura se observa el diagrama de bloques de la implementación del sistema.

Capítulo IV

Análisis de resultados

Introducción

En este capítulo se presenta un análisis sobre los resultados obtenidos de todo el sistema implementado, es decir tanto del software y hardware utilizado, para esto se realizará una serie de análisis como en la instalación del dispositivo, costos, protocolos de seguridad y también un análisis sobre la calidad de servicio QoS, en consecuencia, se busca analizar el comportamiento del sistema y la experiencia del usuario frente al mismo, buscado que ambos tengan los mejores resultados posibles.

Análisis de la instalación

Tomando en consideración que la urbanización San Francisco del Rancho presento no solo una sino varias necesidades para la seguridad de sus moradores como son el control de acceso y la activación remonta de una alarma comunitaria para así disminuir y prevenir posibles hurtos, persuadir delincuentes, monitorear a las personas

extrañas que ingresan a la urbanización y/o residentes realizando actividades no adecuadas en los predios. Considerando todas estas necesidades se desarrolló un prototipo que nos permita cumplir con estos requerimientos. El dispositivo implementado fue modificado tanto en hardware como software para cumplir las necesidades de los moradores, por estas razones, se utilizó un software (Asterisk) alojado en la nube para realizar la comunicación con los Softphone (Groundwire) y la bocina, de esta manera se puede realizar las llamadas, avisos o activación de la bocina desde cualquier lugar en el que se encuentre con la única condición que el usuario que requiera acceso al sistema (telefonía y/o bocina) esté conectado al internet.

De esta manera se alcanza con el cumplimiento del objetivo principal, el cual fue “Desarrollar e implementar un sistema que permita realizar el control de acceso e integración de los servicios de alarmas comunitarias basado en VoIP para usuarios de áreas residenciales”, esto se logró mediante diferentes fases en las cuales se plantearon los objetivos específicos y cada uno de estas tuvo una metodología.

Para comenzar, el primer objetivo específico “Estudio del estado del arte sobre la implementación de centrales virtuales VoIP y servicios provistos por alarmas comunitarias”, este fue planteado con el propósito de considerar toda la tecnología existente para cumplir con las necesidades planteadas y elegir equipos tanto hardware como software que cumplan con los requerimientos y satisfagan estas necesidades como se pudo ver en la sección 3.3.

Por otra parte, el segundo objetivo “Implementar un sistema de perifoneo mediante altavoces IP integrados a la central virtual” fue planteado con el fin de dar avisos, alertas y advertencias tanto a los moradores como personas extrañas que encuentren en ciertas zonas. Para cumplir con dicho objetivo los materiales que se utilizaron se muestran en la Tabla 24. Para la elección del punto de instalación se tomó

en cuenta los requerimientos de la urbanización San Francisco del Rancho planteados en el punto 3.3 y el análisis de sonorización planteado en el punto 3.6.1, de esta manera se instaló el parlante en una zona apropiada, se colocó el parlante en un mástil que está sujeto a un poste a 10 metros de altura , esta altura es adecuada ya que así el parlante está situado en un punto de difícil acceso para los peatones, lo cual previene actos de vandalismo o robo , por otra parte la ubicación del parlante permite tener un acceso sencillo para su mantenimiento. Además, el parlante está localizado a una altura adecuada para que al momento de realizar el perifoneo o un aviso, el ruido no sea molesto ni para los transeúntes ni para las personas de las casas aledañas.

En la Figura 60 se muestra la instalación de la bocina, esta fue instalada en la zona donde existía la mayor cantidad de problemas, ya que en esta zona no existía un control para el acceso y mediante la bocina se pudo dar advertencias a las personas externas de la urbanización, por lo tanto, se cumplió con el objetivo planteado y mediante este se dio solución a la necesidad que tenían los moradores de la urbanización.

Figura 60

Instalación de la bocina

Figura 61

Ingreso de personas externas

Análisis de desempeño y funcionamiento del sistema considerando QoS

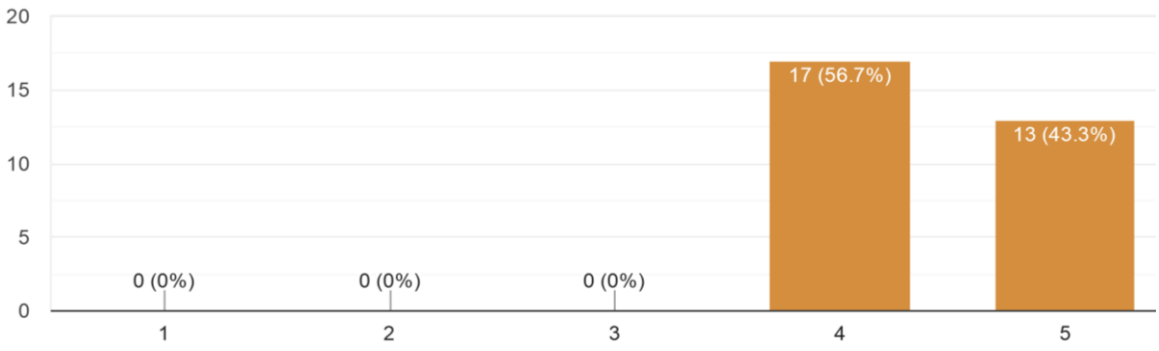
Una vez implementado el sistema, es necesario realizar una evaluación de la calidad del servicio para cumplir con el objetivo específico “Evaluar el desempeño y funcionamiento del sistema VoIP considerando configuraciones de QoS”, las configuraciones realizadas en el servidor se muestran en el Anexo 10, luego se realizó una evaluación en base al criterio de MOS (Means Opinion Score), para lo cual se aplicó una encuesta a los participantes del plan piloto. Además, se utilizó la plataforma VoIP Spear cuya función principal es el monitoreo de servicios IP, mediante estos dos métodos se logró obtener métricas del MOS en base a la Tabla 10.

A continuación, se realizará el análisis de los resultados de la encuesta de 10 preguntas empleada a 30 personas que fueron parte del plan piloto, estas personas llenaron la encuesta realizada en Google Form que se muestra en el Anexo 9. Por consiguiente, se ha elegido las preguntas más relevantes para realizar el análisis de las mismas.

- **Del 0 al 5 valore que tan satisfecho se siente con la calidad del sonido, siendo 0 muy malo y 5 excelente.**

Figura 62

Calidad de sonido

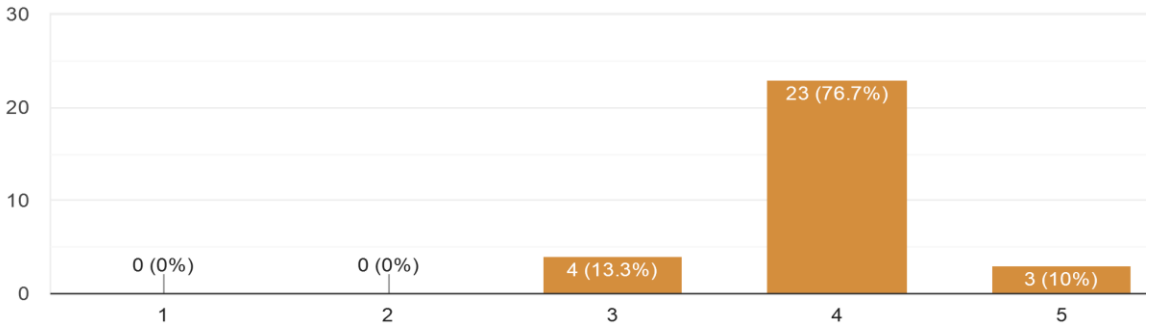


En la Figura 62 se muestra que la calidad de sonido está en el valor de 4 y 5, rigiéndonos a los valores de la Tabla 10, la calidad de sonido esta entre buena o excelente respectivamente. Por lo tanto, el deterioro de la señal es imperceptible o perceptible pero no molesta.

- **Del 0 al 5 valore que tan satisfecho se siente con la calidad del video, siendo 0 muy malo y 5 excelente.**

Figura 63

Calidad de video

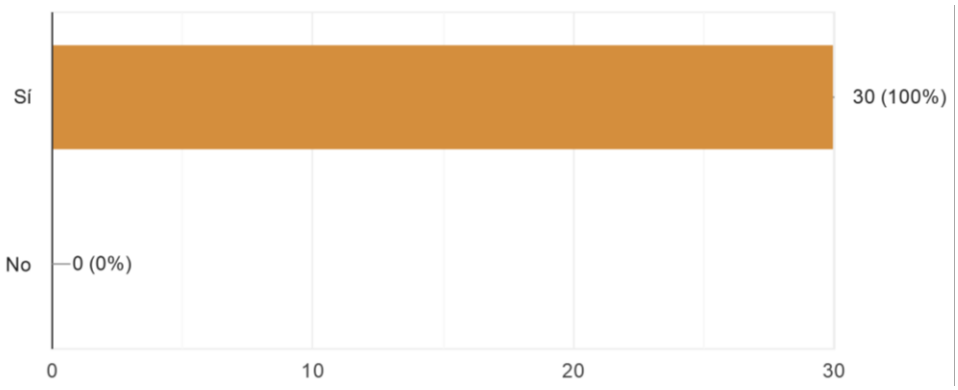


En la Figura 63 se muestra que la calidad de video está en el valor de 3, 4 y 5, rigiéndonos a los valores de la Tabla 10, la calidad del video esta entre el rango normal, buena o excelente respectivamente. La mayor cantidad de encuestados que son un total de 23 personas, sienten que la calidad de video es buena, por lo tanto, el deterioro de la señal es perceptible pero no molesta.

- **¿Cree usted que el sistema implementado ha ayudado a mejorar la seguridad de la urbanización?**

Figura 64

Seguridad de la urbanización

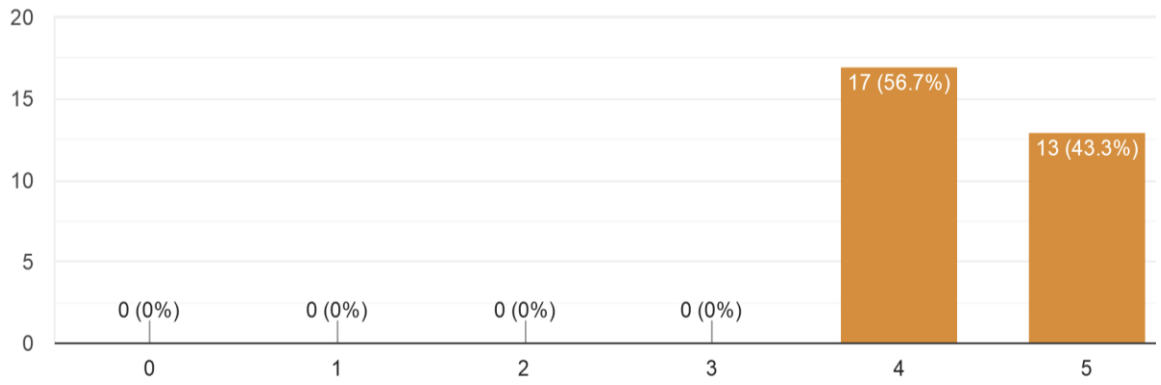


En la Figura 64 se muestra que las 30 personas encuestadas nos respondieron con un rotundo sí. Entonces según la perspectiva de las personas encuestadas el sistema implementado ha ayudado a mejorar la seguridad de la urbanización.

- **Del 0 al 5 valore que tan útil cree usted que es el sistema de perifoneo para realizar los avisos, siendo 0 nada útil y 5 muy útil.**

Figura 65

Perifoneo

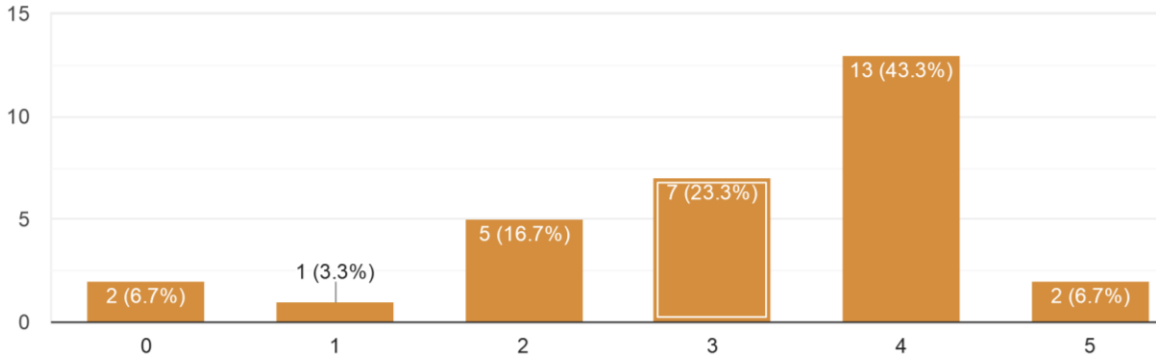


En la Figura 65 se muestra que tan útil es el sistema de perifoneo para realizar los avisos a los moradores de la urbanización, los encuestados respondieron con el valor de 4 y 5, rigiéndonos a los valores de la Tabla 10, el sistema de perifoneo tiene una perspectiva entre buena o excelente respectivamente.

- **Del 0 al 5 valore que tan difícil o complicado ha resultado para usted instalar el sistema, siendo 0 nada complicado y 5 muy complicado.**

Figura 66

Instalación del sistema (Softphone)

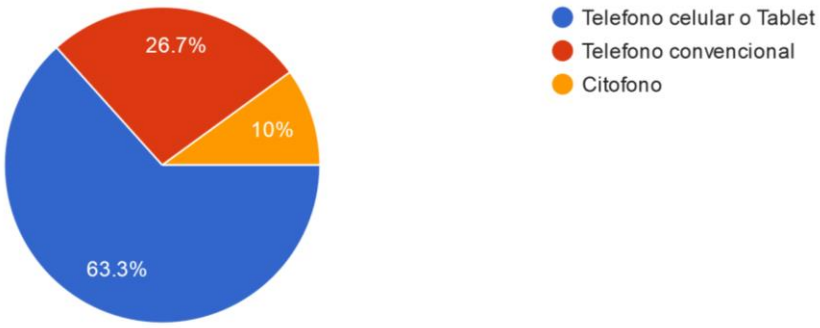


En la Figura 66 se muestra el nivel de dificultad que fue instalar el sistema. Los valores varían entre 0 y 5, en donde de las 30 personas encuestadas 13 de ellas respondieron con el valor de 4, es decir, se les complico la instalación y 2 personas nos respondieron con un valor de 5 lo que significa que fue muy complicado la instalación de dicho sistema, esto es debido a que las personas con las que trabajamos en el plan piloto en su mayorías son de 3era edad, entonces no estaban familiarizadas con la tecnología, así que se les ayudo con la realización de un manual para facilitarles la instalación. En el Anexo 11 se observa los manuales enviados a los moradores de la urbanización San Francisco. Sin embargo, aun así, algunas personas no pudieron instalar la aplicación de una manera exitosa, entonces se realizó varias reuniones en la casa comunal para que se acerquen las personas que no tuvieron éxito en la instalación y así poder ayudarles a tener el sistema funcionado correctamente.

- **¿Cuál de estos dispositivos preferiría usted utilizar o se sentiría más cómodo para usar el sistema?**

Figura 67

Preferencia de dispositivos para utilizar el sistema

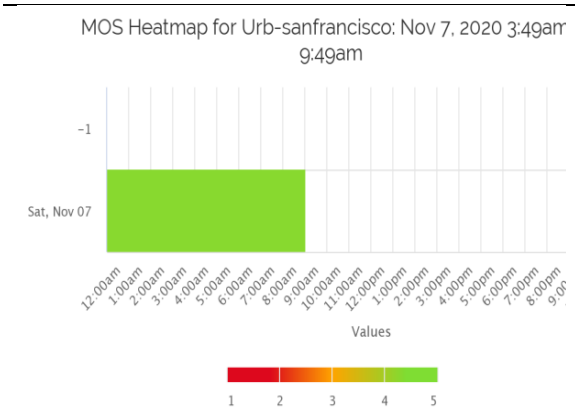


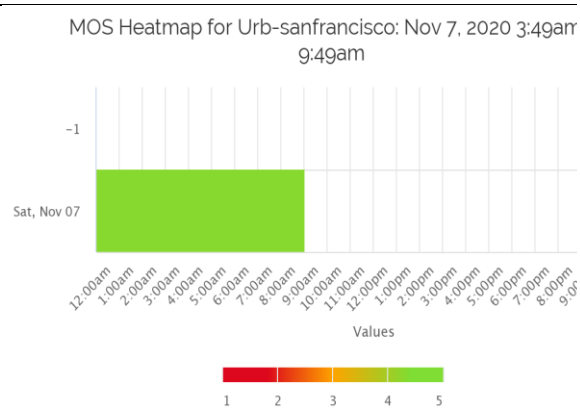
En la Figura 67 se muestra los tipos de dispositivos con los cuales se sentirían más cómodos los moradores de la urbanización San Francisco al momento de utilizar el sistema, entre los cuales 19 personas prefieren utilizar el celular, 8 personas se le facilitaría la utilización del sistema mediante un teléfono convencional y 3 personas les gustaría utilizar el sistema mediante un citófono.

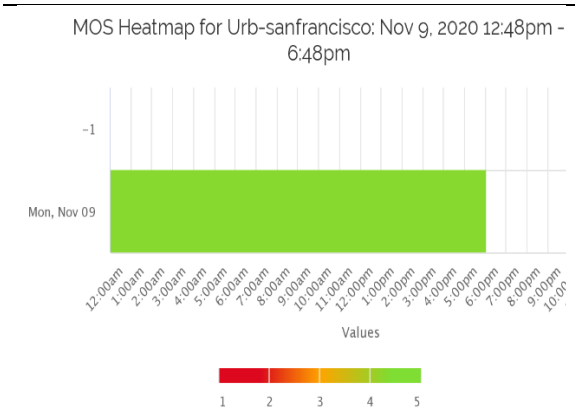
A continuación, se realizará el análisis de los resultados del MOS obtenidos mediante la plataforma VoIP Spear. En la Tabla 25 se muestra los diferentes valores del MOS obtenidos desde el mes de noviembre hasta el mes de febrero, en donde las imágenes nos muestran valores entre 4 y 5. Tomando como referencia la Tabla 10, la calidad de sonido y video esta entre buena o excelente respectivamente. Los valores mostrados del MOS por la plataforma VoIP Spear son bastante similares a los valores obtenidos de la encuesta realizada, por lo cual se concluye que en general el sistema implementado funciona correctamente y brinda al usuario una buena experiencia, cumpliendo con las expectativas de los usuarios.

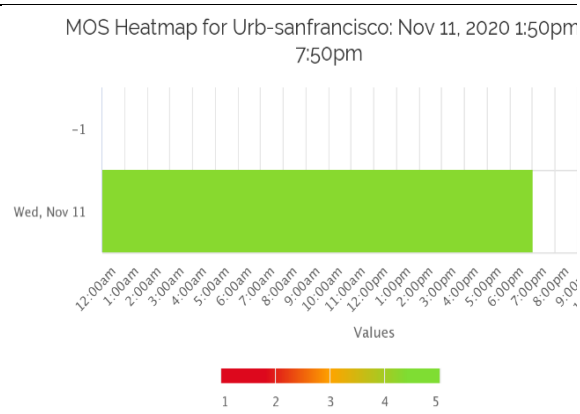
Tabla 25

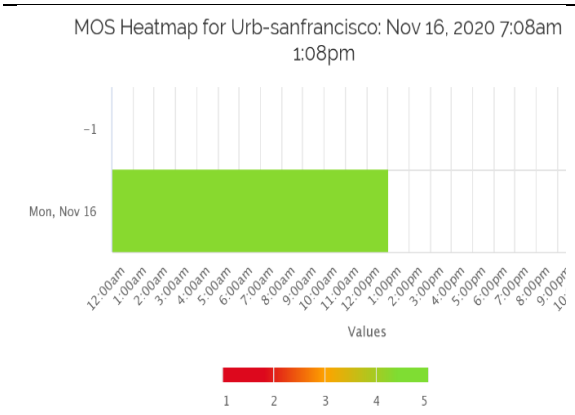
MOS obtenido de la plataforma VoIP Spear

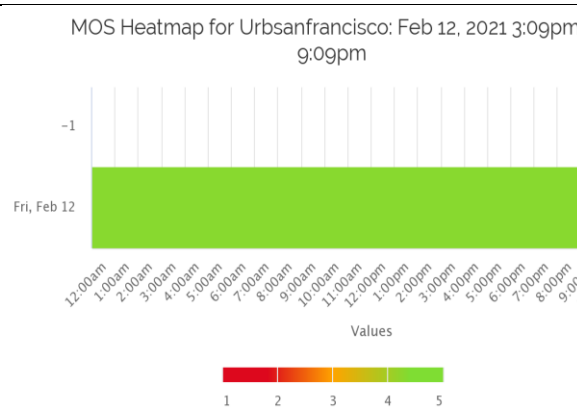








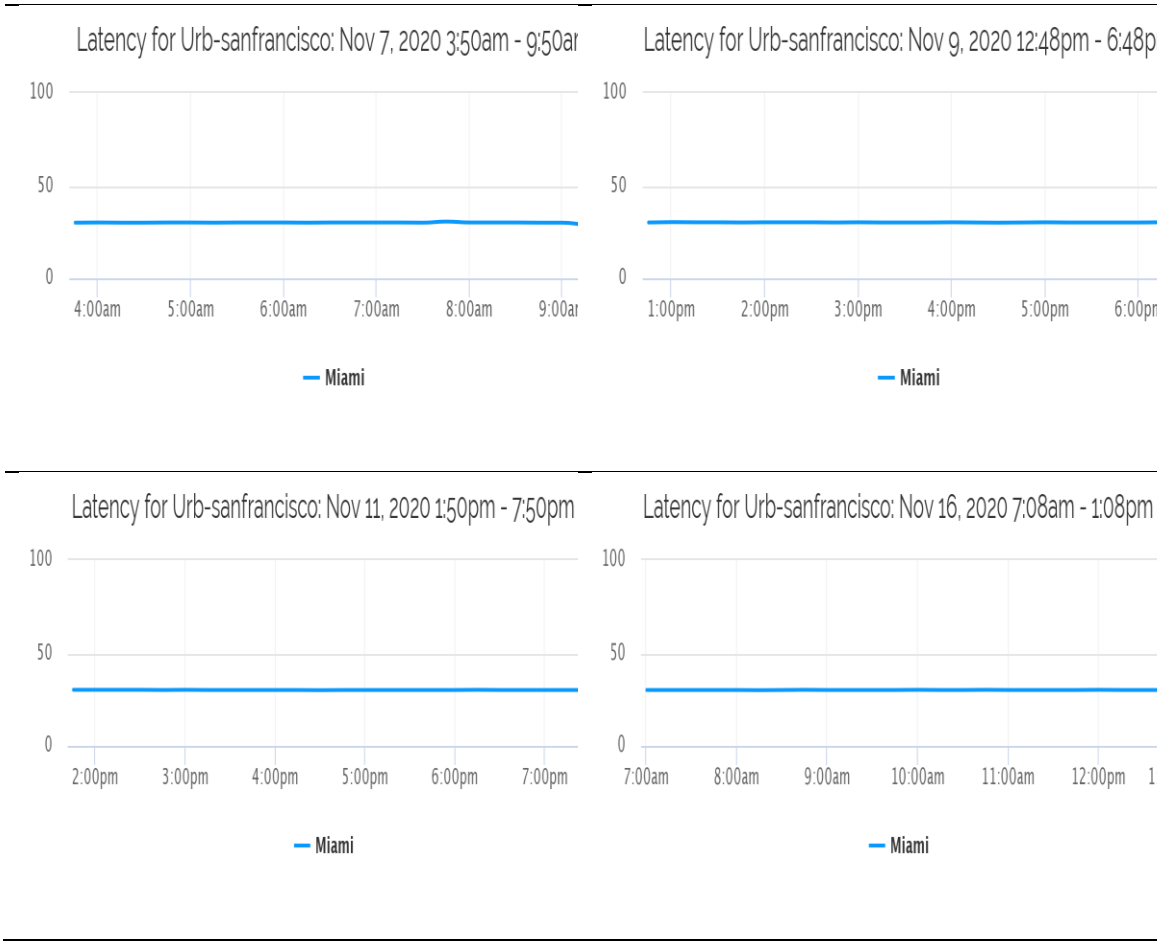


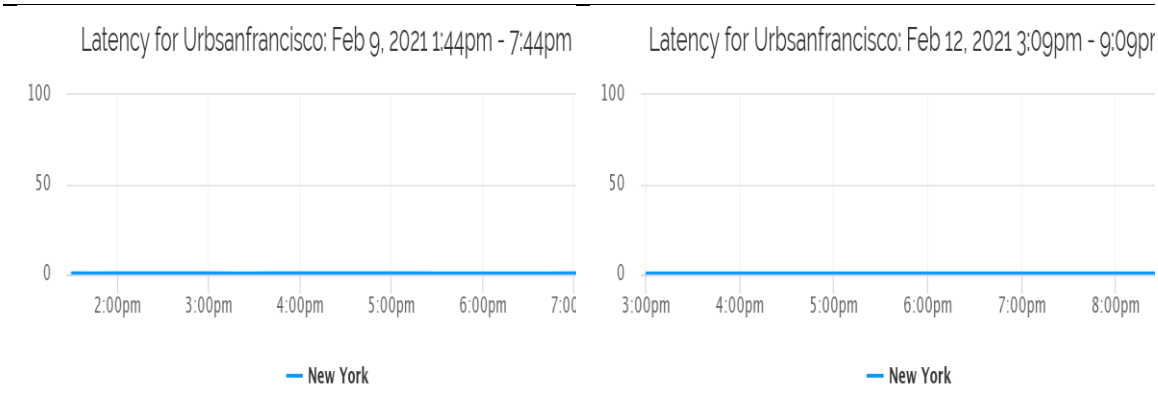


En la Tabla 26 se muestra los valores obtenidos de la latencia a través de la plataforma VoIP Spear, los valores mostrados son tomados desde el mes de noviembre hasta el mes de febrero, en donde se puede observar que la latencia es menor a 50 ms. La recomendación que nos da la ITU-T indica que la latencia máxima de ida y vuelta no debe ser máximo de 300 ms para no dificultar la interacción entre los usuarios, si la latencia es mayor a dicho valor es recomendable cerrar la llamada e iniciar de nuevo el proceso de conexión. Ya que la latencia es menor a 50 ms la interacción entre los usuarios se realizará sin ningún inconveniente.

Tabla 26

Latencia obtenida de la plataforma VoIP Spear.





En la Tabla 27 se muestra los parámetros de QoS tomados solo del mes de febrero mediante la plataforma VoIP Spear, en donde nos entrega los valores del MOS, paquetes perdidos, latencia y jitter. El valor del MOS esta con un valor mayor a 4 que tomando como referencia la Tabla 10 la calidad del MOS es buena. Los valores de la latencia, jitter están dentro de la recomendación establecidas por la ITU-T que indica que la latencia máxima de ida y vuelta no debe ser máximo de 300 ms y el jitter no debe ser mayor a 50 ms.

Tabla 27

Parámetros de QoS

New York	MOS	Packet Loss (%)	Latency Avg (ms)	Latency Min (ms)	Latency Max (ms)	Jitter (ms)
2021 1:30pm	4.3	0.0	0.7	0.5	1.7	0.3
2021 1:45pm	4.3	0.0	0.6	0.5	1.9	0.3
2021 2:00pm	4.3	0.0	0.7	0.5	3.2	0.3
2021 2:15pm	4.3	0.0	0.7	0.5	1.9	0.3

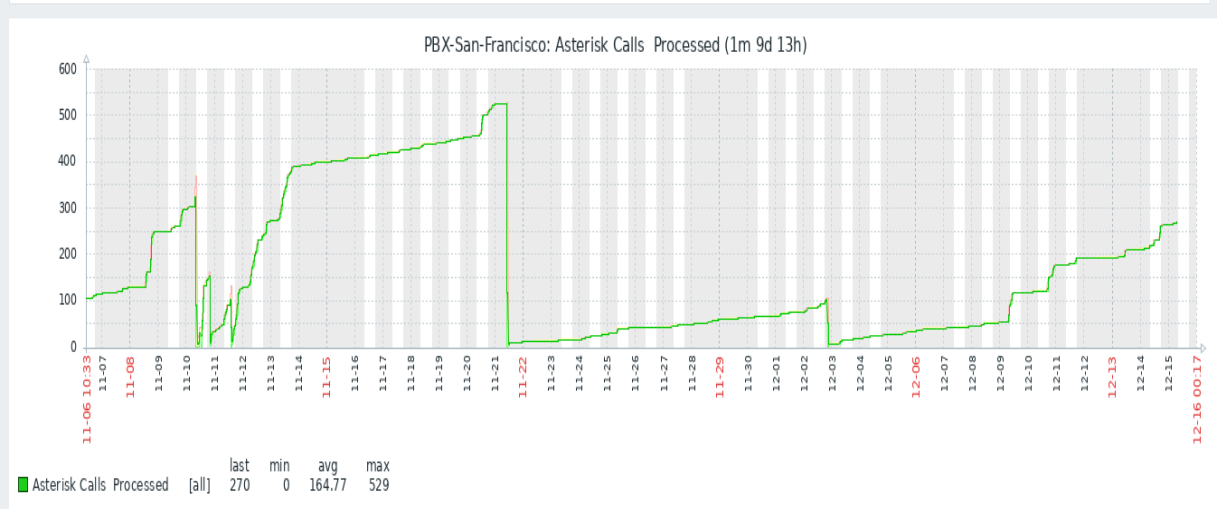
New York	MOS	Packet Loss (%)	Latency Avg (ms)	Latency Min (ms)	Latency Max (ms)	Jitter (ms)
2021 2:30pm	4.3	0.0	0.7	0.5	1.7	0.3
2021 2:45pm	4.3	0.0	0.7	0.5	1.7	0.3
2021 3:00pm	4.3	0.0	0.7	0.5	1.9	0.3
2021 3:15pm	4.3	0.0	0.6	0.5	4.6	0.4
2021 3:30pm	4.3	0.0	0.6	0.5	1.9	0.3
2021 3:45pm	4.3	0.0	0.7	0.5	25.4	0.6
2021 4:00pm	4.3	0.0	0.7	0.5	1.7	0.3
2021 4:15pm	4.3	0.0	0.7	0.5	1.9	0.3
2021 4:30pm	4.3	0.0	0.7	0.5	4.5	0.3
2021 4:45pm	4.3	0.0	0.7	0.5	2.3	0.3
2021 5:00pm	4.3	0.0	0.7	0.5	1.9	0.3
2021 5:15pm	4.3	0.0	0.7	0.5	3.9	0.3
2021 5:30pm	4.3	0.0	0.6	0.5	1.7	0.3
2021 5:45pm	4.3	0.0	0.6	0.5	1.7	0.3
2021 6:00pm	4.3	0.0	0.6	0.5	1.9	0.3
2021 6:15pm	4.3	0.0	0.6	0.5	1.7	0.3
2021 6:30pm	4.3	0.0	0.6	0.5	1.7	0.3

New York	MOS	Packet Loss (%)	Latency Avg (ms)	Latency Min (ms)	Latency Max (ms)	Jitter (ms)
2021 6:45pm	4.3	0.0	0.6	0.5	5.3	0.3
2021 7:00pm	4.3	0.0	0.7	0.5	1.7	0.3
2021 7:15pm	4.3	0.0	0.6	0.5	4.0	0.3
2021 7:30pm	4.3	0.0	0.7	0.5	4.5	0.3

Por último, se utilizó el software Zabbix para monitorear la cantidad de llamadas procesadas, esto con el fin de tener una idea del uso que se le dio al sistema en un tiempo determinado, en este caso se tiene una ventana de 1 mes 9 días y 13 horas, en este tiempo la máxima cantidad de llamadas procesadas fueron de 529 y se tuvo un promedio de 164.77 llamadas, esto se observa en la Figura 68.

Figura 68

Cantidad de llamadas procesadas por la centralita VoIP medidas a través de Zabbix



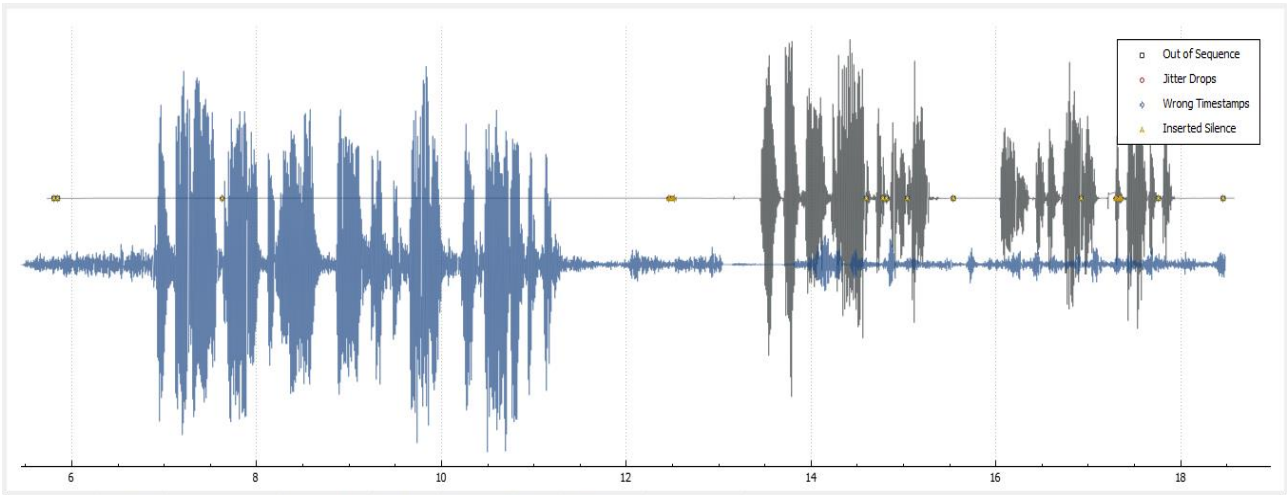
Análisis de protocolos de seguridad para la central virtual IP

Al tener ya en claro la perspectiva que tiene el usuario del sistema mediante el MOS, es importante analizar la seguridad del mismo, esto con el fin de garantizarle al usuario la seguridad en sus llamadas y a su vez cumplir con uno de los objetivos específicos “Configuración y evaluación de protocolos de seguridad para la central virtual IP”, en consecuencia, se utilizará el protocolo de seguridad SRTP definido en la sección 2.6, el mismo que fue configurado en el Softphone (Ver Anexo 11).

Para el análisis se utilizó el software de Wireshark y una tarjeta de red la cual se configuró en modo monitor para hacer la captura de los paquetes mientras se realizaba una llamada, con esto se obtuvieron dos graficas que se muestran en la Figura 69 y la Figura 70, en estas figuras se observa en color azul el enlace directo (fordware) y en color negro el enlace de retorno (reverse). Una vez establecida la llamada se utilizó la siguiente frase “Esta es una prueba de seguridad sin el protocolo SRTP”, para esta primera prueba no se configuro el protocolo de encriptación SRTP y como se puede observar en la Figura 69 las señales son visibles por lo cual el sistema es vulnerable, es decir cualquier atacante malicioso por el mismo método u otro, será capaz de acceder a los datos, por ellos es necesario establecer ciertos parámetros de seguridad, que se verán en las posteriores capturas, realizadas.

Figura 69

Captura de tráfico de la llamada sin el protocolo SRTP

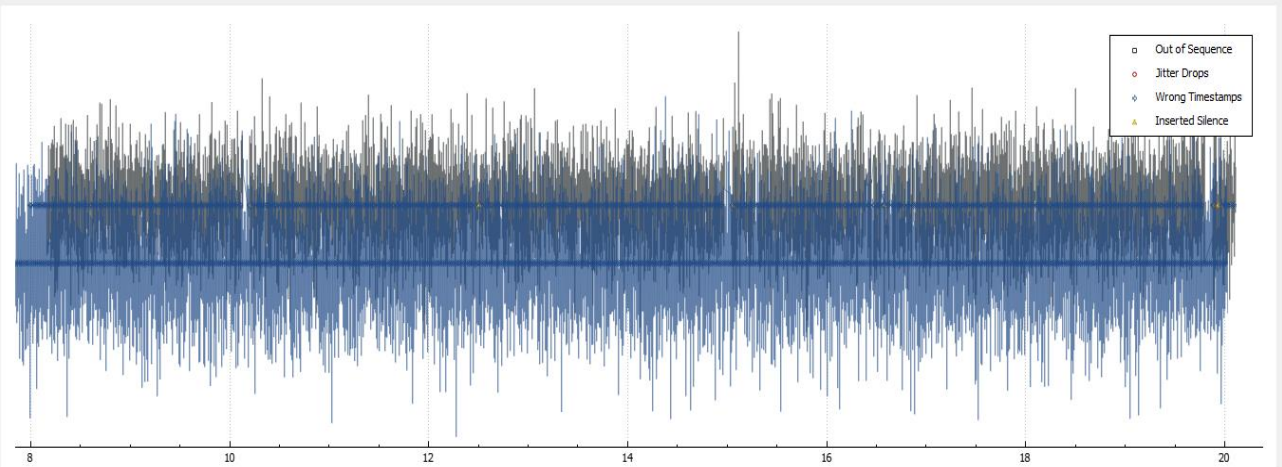


Source Address	Source Port	Destination Address	Destination Port	SSRC	Setup Frame	Packets	Time Span (s)	Sample Rate (Hz)	Payloads
161.35.2.23	12820	192.168.0.104	7078	0x0700b313	206	632	5.74 - 18.6 (12.8)	8000	g711A
192.168.0.104	7078	161.35.2.23	12820	0x598d11fc	394	655	5.38 - 18.5 (13.1)	8000	g711A

Posteriormente se configuró el protocolo SRTP y se utilizó la siguiente frase durante la llamada “Esta es una prueba de seguridad con el protocolo SRTP”, el resultado de la captura se aprecia en la Figura 70 y se observa como las señales son prácticamente irreconocibles ya que se insertan varias otras señales aleatorias dentro de cada una se las señales iniciales, de esta manera si un individuo trata de realizar una captura del tráfico de la red mediante una tarjeta de red no podrá obtener la conversación generada entre los usuarios.

Figura 70

Captura de tráfico de la llamada con el protocolo SRTP



Source Address	Source Port	Destination Address	Destination Port	SSRC	Setup Frame	Packets	Time Span (s)	Sample Rate (Hz)	Payloads
161.35.2.23	12102	192.168.0.104	7078	0x24e12fd4	236	605	7.97 - 20.1 (12.1)	8000	g711A
192.168.0.104	7078	161.35.2.23	12102	0xea21a33f	406	613	7.77 - 20 (12.2)	8000	g711A

Análisis de costos

El análisis de costos tiene como objetivo presentar los costos económicos que conlleva este proyecto en su etapa inicial para tener una base de los montos requeridos, además se busca establecer una comparativa referente a los costos de los elementos presentados en la Tabla 24.

En la Tabla 28 se muestra de manera detallada los costos finales para la implementación, como se puede observar esto concuerda con la Tabla 24, donde se hizo la elección del hardware y los diferentes elementos a utilizar.

Tabla 28

Costo del dispositivo implementado

Costos de implementación	Descripción	Cantidad	Costo unitario	Costo total
Costos de instalación	Cloud hosting	6 meses	$10	$60
	Cable # 12	100 metros	$0.15	$15
	Teléfono IP	1	$35	$35
	Accesorios		$1	$20
	Subtotal 1			**$130**
Costos del dispositivo	Amplificador	1	$50	$50
	Parlante	1	$72,80	$72,80
	TV Box	1	$40	$40
	Subtotal 2			**$162,80**
Total				**$292,80**

Finalmente, es importante destacar que los costos del dispositivo tienen un costo de $162,80, comparando este valor con los mostrados en la Tabla 21, ciertamente la solución mostrada en la Tabla 28 es mucho más económica. Además, la solución mostrada en la Tabla 28 presenta mayores beneficios, ya que es compatible con cualquier tipo de parlante y con cualquier amplificador comercial, de esta manera se puede ampliar el alcance de la sonorización.

Capítulo V

Conclusiones y recomendaciones

Conclusiones

En este capítulo se abordan los resultados del análisis de los datos obtenidos en las dieciséis pruebas realizadas para verificar el comportamiento del sistema propuesto. Estos resultados se concentraron en la respuesta del sistema a una cantidad de experimentos realizados con voluntarios que fueron ingresados en la base de datos, bajo ambientes controlados y variaciones previstas. Todo esto corresponde a información necesaria que valida o no el prototipo, además, se realizó una medición del gasto energético, para calcular el consumo de todo el sistema. Se analizó el porcentaje de acierto que tiene el sistema ante diferentes escenarios, en los cuales interfieren el nivel de luz y la incidencia de lunas de las gafas, así como la cantidad de energía que se está consumiendo durante los ensayos. Los objetivos a determinar fueron: si la arquitectura propuesta es eficiente, cumple su objetivo de reconocimiento facial y entrega una respuesta háptica adecuada para centrar al objetivo.

El aporte principal de este trabajo consiste en el diseño e implementación de un sistema que permite realizar el control de acceso e integración de los servicios de alarmas comunitarias basado en VoIP para los residentes de la urbanización San Francisco del Rancho ubicada en la provincia de Pichincha, cantón Rumiñahui, puesto que, hoy en día no se han desarrollado soluciones de este tipo con tecnología VoIP enfocadas a una serie de necesidades que presentan en la actualidad muchas áreas residenciales.

En esta tesis se evidencia el funcionamiento correcto del sistema mediante análisis y mediciones de diferentes parámetros como latencia, jitter, perdida de paquetes

y MOS, lo cual se muestra en el capítulo cuatro, para garantizar un funcionamiento adecuado es necesario establecer prioridad al tráfico de voz y video, por lo cual las configuraciones de QoS en el servidor son un punto importante, en consecuencia, los resultados obtenidos con estas configuraciones se muestran en el capítulo 4 en la Tabla 27, los valores mostrados fueron capturados mediante la plataforma VoIP Spear, donde se muestra que el tiempo de retardo es menor a 30 ms y el jitter menor a 1 ms, estos valores se encuentran dentro del rango establecidos por la ITU-T que indica que el tiempo de retardo máximo de ida y vuelta debe ser de máximo 300 ms y un jitter no mayor a 50 ms.

Otra conclusión que se deriva del presente trabajo de investigación que se presenta es que, no solo debe ser fundamental asegurar la calidad de las llamadas y el video, sino también asegurar la confidencialidad de las llamadas, por ende, es necesario configurar el protocolo SRTP mostrado en el capítulo cuatro, por medio del cual se obtiene un cifrado desde la fuente hasta el destino, por consiguiente, para comprobar el cifrado del tráfico se utilizó el software Wireshark y una tarjeta de red la cual se configuró en modo monitor para hacer la captura de los paquetes mientras se realizaba una llamada, este cifrado se puede observar esto se muestra en las Figuras 69-70 que se encuentran en el capítulo cuatro, de esta manera se garantiza la protección de la información confidencial de los usuarios.

En la última etapa de la implementación del sistema se logró integrar el altavoz IP, los puntos a considerar sobre instalación y elección de la zona, se muestran en el capítulo tres, donde a través de los requerimientos de los moradores de la urbanización San Francisco del Rancho se eligió la zona más conflictiva. Por otra parte, es importante tener en cuenta que, en áreas muy extensas, no es factible instalar una cantidad excesiva de parlantes para tratar de cubrir el área en su totalidad, por ello, es necesario buscar alternativas, así como, en nuestro caso fue la de enviar los mensajes del perifoneo al

correo electrónico y al buzón de voz, de esta manera el sistema es más eficiente, ya que estos avisos llegan a todos los usuarios y se utilizan la menor cantidad de parlantes posibles.

Cabe resaltar que, el software utilizado para que los usuarios se conecten a la centralita VoIP fue el softphone Groundwire. Se realizaron múltiples pruebas con diferentes Softphone, además se aplicó una encuesta a los usuarios cuyos resultados se muestran en el anexo 3 y de esta manera se logró determinar que el softphone Groundwire es el más adecuado, cuyas características y funcionalidades se muestran en el capítulo tres. Es especialmente importante señalar que, para la adecuada instalación del softphone se realizó una socialización con los moradores de la urbanización San Francisco del Rancho y a su vez se elaboró un manual de configuración como se muestra en el Anexo 11.

En base a este trabajo una de las conclusiones más importantes que se obtuvo fue sobre el costo de los equipos, ya que actualmente en el mercado existen varios dispositivos de un costo muy elevado o bastante limitados como se muestra en la Tabla 21 del capítulo 4, obteniendo un valor neto del sistema implementado en la urbanización San Francisco del Rancho menor a $300, que además, presenta mayores beneficios, ya que es compatible con cualquier tipo de parlante y con cualquier amplificador comercial, de esta manera se puede ampliar el alcance de la sonorización.

Finalmente, el cloud service que se utilizó para alojar la centralita VoIP fue Digital Ocean, esto debido a las características tanto técnicas como económicas que se muestran en el capítulo tres, esto permitió cumplir con ciertos requerimientos básicos que necesitó el sistema como es un ancho de banda aproximado de 10 Mbps cuando se realiza una videollamada y de 1 Mbps cuando se realiza solo llamada, estos valores hacen referencia al ancho de banda por usuario y son basados en los codecs VP8, GSM o G711. Además, una de las particularidades de la plataforma Digital Ocean es que nos

permite alojar un hosting, lo que permitió alojar una página web, en consecuencia, se realizó sobre esta la tarifación del servicio VoIP, es decir, se puede observar detalladamente diferente información sobre las llamadas como la duración, fecha, destino, esto se muestra en el capítulo tres.

Recomendaciones

A manera general es recomendable tener en cuenta que cuando se realiza un proyecto en el que se brinda un servicio hacia las personas, muchas de ellas no están familiarizadas con las nuevas tecnologías, por lo cual, para estas personas les resulta complicada la interacción con estos servicios o sistemas, debido a ello es indispensable realizar una socialización y capacitación del servicio o sistema.

Además, es de suma importancia tener en cuenta que cuando se realiza la instalación de un sistema de audio, se debe considerar que si la potencia es excesiva puede causar molestias a las personas que se encuentren cercanas al dispositivo, lo cual es desfavorable para el sistema e incluso puede llegar a tener implicaciones legales.

Por otro lado, al momento de instalar el sistema, pudimos darnos cuenta que para este tipo de soluciones el punto más importante es el personal de seguridad, ya que estas personas son las que, utilizarán constantemente el sistema, en consecuencia, es necesario ajustarse a sus necesidades, en nuestro caso para ello en lugar de utilizar un teléfono móvil se instaló adicionalmente un teléfono IP físico (fijo), para facilitar su trabajo.

Otro punto importante necesario de señalar es la realización de encuestas para medir el nivel de satisfacción de los usuarios, ya que es necesario evaluar los resultados que se obtuvieron mediante la realización del proyecto y así conocer la opinión del público.

Es de suma importancia realizar un mantenimiento del sistema de control de acceso y alarma comunitaria, debido a que el equipo está instalado al aire libre, entonces está sujeto a los diferentes cambios climáticos del medio ambiente, por ende, para alargar

la vida útil y el correcto desempeño del dispositivo es recomendable realizar este proceso cada cuatro o seis meses.

Una recomendación importante que se debe tener en cuenta es la seguridad tanto lógica como física del sistema, debido a que se debe ofrecer un sistema confiable y seguro lo que se traduce en protección de los usuarios y la seguridad del cloud service.

Conviene señalar que es necesario realizar una capacitación del uso adecuado del sistema de acceso y alarma comunitaria, enfocándose en el personal que lo vaya a utilizar (administración, guardias), debido a que estos usuarios estarán en constante utilización del sistema, en consecuencia, es necesario que ellos adquieran los conocimientos y habilidades necesarias para controlar y realizar un correcto, rápido y eficaz uso del sistema.

Trabajos futuros

Como continuación de este trabajo de tesis surgen varias líneas de investigación que quedan pendientes, todas estas ideas surgieron durante el desarrollo del proyecto y es posible continuar con estas ideas, utilizándolas para un trabajo futuro o por otra parte pueden ser de utilidad para otros investigadores.

- A continuación, se proponen algunas ideas que pueden desarrollarse en un futuro, como trabajos de investigación o para dar continuación y aportar con algunos desarrollos a este proyecto de tesis, estos posibles trabajos futuros que se proponen son:
- Desarrollar y elaborar un prototipo de un dispositivo IP que permita la conexión de una cuenta SIP en base a PJSUA y Rasberry Pi, ya que por medio de este controlador se pueden agregar nuevas funcionalidades, debido a sus puertos GPIO como son el control de energía, la activación o desactivación de un actuador, entre otros.

- Desarrollar una plataforma web para el dispositivo IP basado en el controlador Rasberry Pi planteado en el ítem anterior, que permita configurar los parámetros de las cuentas SIP como usuario, contraseña, codecs, etcétera.
- Analizar y desarrollar un softphone para dispositivos móviles que cuente con las características tradicionales (audio, video, seguridad) y también permita notificaciones push para los dispositivos, además de permitir generar códigos QR con las credenciales de cada usuario, con el fin de no depender de aplicaciones de terceros.
- Implementar un sistema centralizado para una zona residencial con varios dispositivos de perifoneo IP (parlantes) ubicados estratégicamente, los cuales se conecten mediante un radio enlace a un AP y este AP se conecte a una centralita VoIP alojada en la nube, esto con el fin de no depender de terceros y realizar un sistema independiente que pueda tener un fácil acceso para su mantenimiento y no molestar a los residentes.

Referencias

Revista Gerencia. (2005, agosto). Revista Gerencia - Telefoni-a IP: Cambio de paradigma en las

comunicaciones empresariales. http://www.emb.cl/gerencia.

http://www.emb.cl/gerencia/articulo.mvc?xid=2356&ni=telefonia-ip-cambio-de-paradigma-en-lascomunicaciones-empresariales

Bhutani, A. (2019, 12 abril). Voice over Internet Protocol (VoIP) Market Size By Type (Integrated Access/Session Initiation Protocol (SIP) Trunking, Managed IP PBX, Hosted IP PBX), By Access Type (Phone to Phone, Computer to Computer, Computer to Phone), By Call Type (International VoIP Calls, Domestic Calls), By Medium (Fixed, Mobile), By End-Use (Consumers, SMBs, Large Enterprises), By Application (IT & Telecom, BFSI, Healthcare, Government & Public Sector, Retail, Education, Hospitality), Industry Analysis Report, Regional Outlook, Growth Potential, Competitive Market Share & Forecast, 2019 - 2025. Global Market Insights, Inc.

https://www.gminsights.com/industry-analysis/voice-over-internet-protocol-voip-market

INEC. (2011). Encuesta de Victimización y Percepción de Inseguridad. Ecuador.

Kibernum. (2017, 23 junio). 2020, el año que se triplicará el tráfico IP y los dispositivos de los usuarios. Kibernum. https://www.kibernum.com/2017/06/23/2020-ano-se-triplicara-trafico-ip-los-dispositivos-los-usuarios/

EVOLUCIÓN DE LA TELEFONÍA IP. (1973, 7 mayo). Timetoast. https://www.timetoast.com/timelines/1519798

Méndez, C. (2005). Inbound para enlaces PSTN con VoIP. Universidad de las Américas Puebla.

Stallings, W. (2004). Comunicaciones Y Redes De Computadores (7.a ed.). Pearson Educación.

Calle Espinoza, E.M. (2017). Diseño e implementación de un adaptador para teléfono analógico de bajo costo. Universidad de Cuenca, Ecuador.

Hanumesh, P., & Profile, V. M. C. (2013, 10 julio). Set up your VOIP based SIP soft phone and know more about VOIP. techgeek-gig. https://techgeek-gig.blogspot.com/2013/07/voip.html

The Internet Society. (2002). RFC 3261. https://tools.ietf.org/html/rfc3261#page-269

Carrington, C. (2014, 6 septiembre). CSc 461/561 Multimedia Systems Part C: 1. RTP/RTCP - PowerPoint PPT Presentation [Diapositivas]. SlideServe. https://www.slideserve.com/carrington/csc-461-561-multimedia-systems-part-c-1-rtp-rtcp

García Montoya, Mario, León González, Nelia R., Marín Contreras, Víctor, & Yañez de la Rivera, René. (2014). Implementación de los protocolos de comunicación para VoIP: RTP/RTCP, sobre FPGAs de altera. Ingeniería Electrónica, Automática y Comunicaciones, 35(3), 39-47. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S181559282014000300004&lng=es&tlng=es

Guerra, E. (2013, 18 diciembre). RTCP (RTP control protocol). https://es.slideshare.net/. https://es.slideshare.net/EdgarGuerra1/rtcp-real-time-control

EFORT. 2011. RTP/RTCP. http://www.efort.com/media_pdf/RTP_ES_EFORT.pdf

Campanella, N. (08 de 09 de 2017). The Beginner's Guide to Virtual PBX. U.S.A.

Rengel, M., & Jimbo M. (2015). Diseño, construcción e implementación de un dispositivo de seguridad que permite la intercomunicación con audio y video entre dos puntos y la activación remota de elementos de seguridad. Universidad Politécnica Salesiana Sede Cuenca.

Joskowicsz, J. (2015). Digitalización y Codificación de Voz y Video, Instituto de Ingeniería Eléctrica, Uruguay. https://iie.fing.edu.uy/ense/asign/ccu/material/docs/Codificacion%20de%20voz%20y%20video%20(presentacion).pdf

VoiceHost Limited. (2020, 1 julio). Call Quality Defining using R-Factor and MOS | VoiceHost - UK VoIP Provider. https://www.voicehost.co.uk/. https://www.voicehost.co.uk/help/call-quality-r-factor-and-mos

Barrera, J. (2012). Ajuste Analítico del Rendimiento en la Multiplexación de Fuentes de VoIP con VAD. Universidad de Sevilla.

Sangoma Technologies Corporation. (2020, 30 noviembre). Analog Gateways. Sangoma. https://www.sangoma.com/voip-gateways/analog/

Asterisk. (2020, 19 agosto). Get Started. Open Source Communications Software | Asterisk Official Site. https://www.asterisk.org/get-started/

Voip-info.org. (2020, 13 enero). FreeSwitch. VoIP-Info. https://www.voip-info.org/freeswitch/

FreePBX. (2020, 29 mayo). Getting Started. FreePBX - Let Freedom Ring. https://www.freepbx.org/get-started/

Issabel. (2020, 20 enero). Issabel – Unified Communications Freedom. https://www.issabel.com/

VitalPBX. (2020, 5 diciembre). VitalPBX - Fastest growing PBX System based on asterisk. VitalPBX - Advanced PBX System. https://vitalpbx.org/

López, J. G., & Montoya, F. G. (2008). VoIP y Asterisk: redescubriendo la telefonía. Alianza Editorial.

Zabbix. (2020). Zabbix - The Enterprise-Class Open Source Network Monitoring Solution. https://www.zabbix.com/

NO-IP. (2020). Free Dynamic DNS - Managed DNS - Managed Email - Domain Registration - No-IP. https://www.noip.com/

León, M. (2019, 15 noviembre). Instalar y configurar Fail2ban para prevenir accesos no deseados al servidor. Blog de arsys.es. https://www.arsys.es/blog/instalar-fail2ban/

Aguilar, C. (2015). Análisis, Diseño e implementación de un sistema de VoIP para el hospital un canto a la vida. Universidad Politécnica Salesiana, 4.

Vaca, J. (2008). Diseño e implementación de un emulador de central telefónica IP utilizando el software de código abierto ASTERISK para la red de datos de la Facultad de Ingeniería Electrónica de la Escuela Politécnica del Ejército. Escuela Politécnica del Ejército.

MasIP. (2019, 5 junio). Asterisk: el software de código abierto para telefonía IP. Mas IP. https://www.masip.es/blog/asterisk-el-software-de-codigo-abierto/

A. Mazhar, A. (2016). Performance Evaluation of h.265/mpeg-hevc, vp9 and h.264/mpeg-avc Video Coding. The International journal of Multimedia & Its Applications, 8(1), 35-44. https://doi.org/10.5121/ijma.2016.8103

Takanen, P. T. (2007, 31 agosto). Creating new business opportunities with SRTP for VoIP. SearchITChannel. https://searchitchannel.techtarget.com/tip/Creating-new-business-opportunities-with-SRTP-for-VoIP

Guajardo, P. (2020, 20 agosto). Cloud Hosting: ¿qué es y cómo funciona un servidor en la nube? Rock Content. https://rockcontent.com/es/blog/cloud-hosting/

Groundwire for Android & iOS: The Best $10 You'll Ever Spend – Nerd Vittles. (2020, 26 octubre). Nerd Vittles. http://nerdvittles.com/?p=33573

J. (2020, 20 abril). Top 10 de Aplicaciones de Softphone en 2020. Central IP. https://www.centralip.cl/aplicaciones-softphone-2020/

Licensing & services | Linphone. (2020). Linphone. https://www.linphone.org/licensing-services

Acrobits. (2020, 18 junio). Acrobits SIP Client Apps for iOS & Android. Acrobits | Creators of Cloud Softphone and an Industry-Leading SDK. https://www.acrobits.net/sip-client-ios-android/

Sip speaker horn | KNTECH. (2021). KNTECH. https://www.koontech.com/sip-speaker-horn__475.html

Altoparlante Bocina Ip. (2021). Cineto. https://www.cineto.net/megafonia-ip/altoparlante-bocina-ip.html

Interfaz OPTIMUSTM IA-20SIP. (2021). EMACS. https://store.emacs.es/products/n300if

Gateway Megafonía IP Ciser MIP-381 - Onedirect. (2021). Ciser System. https://www.onedirect.es/productos/ciser-system/gateway-megafonia-ip-ciser-mip-381

HN-30P. (2016). Lucky Tone. http://www.lucky-tone.com/product_detail/92.html

Banggood.com. (2021). BT-309A 220V-240V DC12V Digital bluetooth Stereo Audio Home And Car Amplifier. www.banggood.com. https://www.banggood.com/BT-309A-220V-240V-DC12V-Digital-Bluetooth-Stereo-Audio-Home-And-Car-Amplifier-p 1358263.html?utm_source=google&utm_medium=cpc_ods&utm_campaign=arvin-led-sds-view-tritium&utm_content=arvin&gclid=CjwKCAiAxeX_BRASEiwAc1QdkSoHX4UYWkp8wvuUbqm49xjdcHCWK86xpw7PRp94BigKQuAZPH7eKRoC38wQAvD_BwE&cur_warehouse=CN

Avila, S. (2016). Atlas ambiental 2016, Quito sostenible. Isuu. https://issuu.com/fiorum/docs/atlas_ambiental_2015_primera_parte

Isbert, A. C. (1998). Diseño acústico de espacios arquitectónicos.Catalunya: Edicions UPC

Carramolino, J. C. (2007). Instalaciones singulares en viviendas y edificios. McGraw-Hill Education.

Varela, S (2017). Diseño Eléctrico Especificaciones Técnicas, MDMQ.

Dastanova, N. (2021, 27 febrero). Erlang B Traffic Table. Academia. https://www.academia.edu/25945139/Erlang_B_Traffic_Table