ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ESTUDIO Y PROPUESTA DE SOLUCIONES DE VOIP EN UNA RED INALÁMBRICA WIFI AD HOC"

TESIS DE GRADO

Previo a la obtención del Título de:

MAGISTER EN TELECOMUNICACIONES

Presentado por:

CHRISTIAN ALBERTO COJITAMBO TERÁN

Guayaquil – Ecuador

2015

AGRADECIMIENTOS

A Dios, por haberme brindado esta vida, en este tiempo y en este lugar.

A mi Director Álvaro Suárez por sus recomendaciones, seguimiento, apoyo y amistad brindada en el tiempo de supervisión de este trabajo.

A la Administración del Parque Lago por haberme facilitado el acceso a las instalaciones para realizar las pruebas de campo.

DEDICATORIA

Dedico este trabajo a mi esposa María Luisa, por haber aceptado esta experiencia de tomar una maestría, compartiendo juntos esta etapa académica.

A mi familia, mi papi, mi mami, mi ñaño, por el apoyo y ánimo brindado en el proceso de ejecución de este trabajo.

TRIBUNAL DE SUSTENTACIÓN

Sara Ríos, M.Sc.

Sub-Decano FIEC

Álvaro Suárez Sarmiento, Ph.D.

Director de Tesis

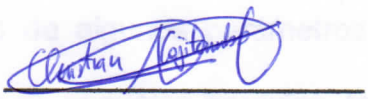
Boris Ramos, Ph.D.

Vocal Principal

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

(Art. 12 del Reglamento de Graduación de la ESPOL)



CHRISTIAN ALBERTO COJITAMBO TERÁN

RESUMEN

Hemos desarrollado este trabajo de Tesis como requisito de graduación previo a la obtención del título de Magíster en Telecomunicaciones, luego de haber cursado la Maestría en Telecomunicaciones dictada por la ESPOL, en su primera promoción. En esta Tesis hemos realizado un estudio descriptivo bibliográfico y de campo de las diferentes problemáticas inherentes a las redes inalámbricas, en específico las redes que utilizan el estándar IEEE 802.11, bajo un escenario específico, controlando una de las variables, la distancia entre los agentes de usuarios desde un metro hasta 30 metros, en saltos de un metro y estableciendo llamadas VoIP, durante el curso de ellas se realizaron mediciones de algunos parámetros como por ejemplo, jitter medio, jitter máximo, tasa de paquetes perdidos, tasa de bits por segundo, e indicadores de calidad de señal como RSSI y nivel de ruido. Posterior a la medición, se analizaron sus resultados y se calculó el coeficiente de determinación estadístico, el cual mide el porcentaje de influencia de una variable sobre otras, además se usó un modelo de regresión lineal entre las variables que se aproximan a una distribución normal, para esta comprobación se usó la prueba de Kolmogorov-Smirnov para una muestra.

Finalmente, se analizaron los resultados obtenidos, y se concluyó cuáles variables mostraron un alto coeficiente de determinación, comparándolos con estudios anteriores.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO

3G	3rd Generation
3GPP2	3rd Generation Partnership Project 2
ACK	ACKnowledgement
ADPCM	Adaptive Differential Pulse Code Modulation
AIFS	Arbitration InterFrame Space
AODV	Ad hoc On-demand Distance Vector
AP	Access Point
APP	APPlication
BRI	Basic Rate Interface
BSS	Basic Service Set
CAPEX	CAPital Expenditure
CDR	Call Detail Recording
CE	Community Edition
CEL	Channel Event Logging
CELP	Code Excited Linear Predictive
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CW	Contention Window
DCF	Distributed Coordination Function
DIFS	DCF InterFrame Space
DS	Distribution System
DSDV	Destination-Sequenced Distance Vector
DSSS	Direct Sequence Spread Spectrum

DTMF	Dual Tone Multifrequency
EIFS	Extended InterFrame Space
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
FHSS	Frequency Hopping Spread Spectrum
GSM	Global System for Mobile communications
HDLC	High-level Data Link Control
HTTP	Hypertext Transfer Protocol
IAX	Inter-Asterisk eXchange
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFS	InterFrame Space
ISM	Industrial, Scientific and Medical
ITU	International Telecommunications Union
LAN/MAN	Local Area Network/Metropolitan Area Network
LLC	Logical Link Control
LPC	Linear Prediction Coding
LTE	Long Term Evolution
MAC	Medium Access Control
MCU	Multipoint Control Unit
MELP	Mixed-excitation Linear Prediction
MG	Media Gateway
MGC	Media Gateway Controller

MIT	Massachusetts Institute of Technology
MKI	Master Key Identifier
MMUSIC	Multiparty Multimedia Session Control
MOS	Mean Opinion Score
NAV	Network Allocation Vector
NGN	Next Generation Network
NVP	Network Voice Protocol
OPEX	OPerational Expenditure
OSI	Open System Interconnection
PAMS	Perceptual Analysis Measurement System
PBX	Private Branch eXchange
PC	Personal Computer
PCF	Point Coordination Function
PCM	Pulse Code Modulation
PESQ	Perceptual Evaluation of Speech Quality
PIFS	PCF InterFrame Space
PLCP	Physical Layer Convergence Protocol
PLR	Packet Loss Rate
PMD	Physical Medium Dependent
PPP	Point-to-Point Protocol
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
PSQM	Perceptual Speech Quality System
PT	Payload Type

QoS	Quality of Service
RIFS	Reduced InterFrame Space
RR	Receiver Report
RSSI	Received Signal Strength Indicator
RTCP	Real-time Transfer Control Protocol
RTS/CTS	Request-To-Send/Clear-To-Send
SCTP	Stream Control Transmission Protocol
SDES	Source DEScription
SIFS	Short InterFrame Space
SIP	Session Initiation Protocol
SS7	Signalling System No. 7
SSID	Service Set IDentifier
SR	Sender Report
SRTP	Secure Real-time Transport Protocol
UA	User Agent
UDP	User Datagram Protocol
URI	Uniform Resource Indicators
VoIP	Voice over IP
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Access Network

INTRODUCCIÓN

Este trabajo de investigación es una tesis de carácter bibliográfico realizada con el objetivo de investigar y explorar los factores que según estudios realizados indican que inciden en las llamadas sobre la tecnología VoIP, y evidenciar en un escenario práctico los problemas presentados en las comunicaciones de VoIP en redes inalámbricas del estándar *Instituto de Ingenieros Eléctricos y Electrónicos* (*IEEE*, del inglés *Institute of Electrical and Electronics Engineers*) 802.11 en modo Ad Hoc, hemos tomado medidas de los valores obtenidos en algunos de los parámetros de calidad de servicio con el propósito de contribuir a la extensa investigación que se desarrolla en este temática.

En el capítulo 1, exponemos la descripción, justificaciones, objetivos tanto principales como específicos, la metodología por la cual obtuvimos los resultados mostrados.

En el capítulo 2, abarcamos el marco teórico correspondiente a la descripción avanzada del estándar IEEE 802.11 y el detalle del control del acceso al medio, topologías estandarizadas, así como la problemática presentada en el entorno estudiado en esta Tesis.

En el capítulo 3, describimos teóricamente la historia de la VoIP, su evolución, el proceso que toma la voz analógica hasta convertirse en señales

digitales, protocolos de control, señalización y tecnologías utilizadas en la actualidad.

El capítulo 4, explica los detalles y características del escenario levantado para la ejecución de las pruebas y la medición de los diferentes parámetros de QoS.

Finalmente, en el último capítulo se comparten los resultados, los cálculos realizados y se comprueba con evidencia estadística correlaciones entre algunas variables.

CAPÍTULO 1

1. MARCO REFERENCIAL

En el presente capítulo describimos las características del presente trabajo de investigación, y exponemos su alcance y aporte.

1.1 DESCRIPCION DE VOIP EN REDES WiFi AD HOC

Según el documento de *forecast* desarrollado y publicado por el fabricante Cisco sobre el Índice de Previsión Visual [1], con corte a Octubre del 2014, el tráfico de datos de dispositivos móviles era de 3% del tráfico *Internet Protocol* (*IP*) a nivel global en el año 2013, y al 2018 se espera que sea el 12%, esto muestra un nivel creciente en el uso de teléfonos inteligentes y tabletas, el mismo documento muestra que las tabletas al año 2018 habrían tenido un crecimiento del 5% en comparación con el 2013 y los teléfonos inteligentes aumentarán de un 14% al 19% en el 2018 dentro del total de dispositivos conectados, es común que estos dispositivos posean receptores y transmisores del estándar IEEE 802.11, coloquialmente conocido como

Wireless Fidelity (*WiFi*). Dicho documento revela el incremento en el uso de estos equipos en nuestra realidad habitual, por lo que se espera que la demanda en servicios, aplicaciones y disponibilidad sigan la misma tendencia de crecimiento.

El estándar IEEE 802.11 define modos de conexión entre los dispositivos terminales. Uno de estos modos se denomina *Ad Hoc*. Las redes *Ad Hoc* se definen para tener una duración de conexión temporal corta, y estar formadas dinámicamente de manera arbitraria por una colección de terminales según la necesidad [2]. Son una alternativa de conexión entre dispositivos móviles bajo los cuales no se proyecta un esquema jerárquico sino un trabajo cooperativo entre ellos, a través de una auto-organización que permite crear una red móvil ajustable a los requisitos de ancho de banda y energía. Estas redes permiten comunicar tráfico de voz, datos y videos entre varios terminales a través de varios enlaces diferentes simultáneamente (comparado con el otro modo de conexión denominado infraestructura).

El presente trabajo de investigación consiste en un estudio bibliográfico de las características, aplicaciones, topologías, tipos de protocolos y algoritmos usados en *WiFi* en modo *Ad Hoc* y su impacto sobre los servicios de *Voz sobre IP* (*VoIP*, del inglés *Voice over IP*). El servicio de voz es uno de los tipos de tráfico más sensibles a los problemas inherentes a las redes inalámbricas. Por tal motivo, realizamos un análisis de los problemas

presentados al realizar la comunicación de voz sobre WiFi y los inconvenientes que se añaden en el establecimiento de una llamada de VoIP en una comunicación de modo Ad Hoc en un escenario definido y controlado. En ese escenario observamos y medimos algunos parámetros de *Calidad de Servicio* (*QoS*, del inglés *Quality of Service*).

1.2 JUSTIFICACIÓN

Se proyectan las redes Ad Hoc como un esquema potencial de desarrollo en base al crecimiento de sistemas y dispositivos móviles a gran escala. Esta investigación ha servido de base técnica para futuras investigaciones sobre las aplicaciones VoIP en redes WiFi en modo Ad Hoc, su adaptabilidad y convergencia con esta tecnología de acceso, proporcionando a los investigadores una visión global sobre las *redes* WiFi Ad Hoc, describiendo sus ventajas y desventajas, para que en base a dichos parámetros se investigue o desarrolle posibles soluciones a las problemáticas presentadas en el trayecto del crecimiento de la tecnología y sus demandas derivadas. Adicionalmente, el estudio de campo permite técnica y experimentalmente identificar los factores positivos y negativos que intervienen en la comunicación de VoIP sobre WiFi Ad Hoc y valorar su correlación entre ellos.

1.3 OBJETIVOS

El objetivo principal de este trabajo de investigación es precisar y medir la problemática de VoIP sobre IEEE 802.11 en modo Ad Hoc.

Los objetivos específicos son:

1. Distinguir las diferentes topologías en una red implementada a través del estándar IEEE 802.11, determinar las características y funcionalidades de las redes WiFi en modo Ad Hoc, detallar las características y funcionalidades de la tecnología WiFi sobre redes Ad Hoc.
2. Conocer sobre la VoIP, conceptos básicos, códec de voz y protocolos de señalización, y estudiar las características y exigencia del tráfico de VoIP sobre redes WiFi en modo Ad Hoc.
3. Analizar los factores que intervienen para deteriorar el servicio de llamadas VoIP sobre redes WiFi en modo Ad Hoc bajo un ambiente controlado.
4. Fortalecer los conocimientos adquiridos de VoIP en la Maestría de Telecomunicaciones.

1.4 METODOLOGÍA

La parte descriptiva del presente trabajo se ha desarrollado bajo investigación bibliográfica, documental, y recopilación de información mediante tesis de maestría, de doctorados, patentes, documentos de revistas científicas disponibles en la Web, documentos técnicos expedidos por entes

regulatorios internacionales y trabajos de investigación para enmarcar los aspectos relevantes de las redes bajo estándar IEEE 802.11 y en particular el establecimiento de redes bajo la topología Ad Hoc, sus características y funcionalidad, métricas de QoS, en conjunto con los conceptos de VoIP y su despliegue en la realidad actual.

La segunda etapa estuvo comprendida por un protocolo de pruebas realizadas con terminales que establecieron una comunicación Ad Hoc y ejecutamos una aplicación de VoIP por medio de una plataforma de libre uso, llamada Trixbox, con el fin de crear un ambiente de llamadas VoIP entrantes y salientes. Bajo este escenario, se midieron parámetros de QoS para el tráfico de voz y se analizó su comportamiento. La variable controlada dentro del escenario fue la distancia entre terminales, fue aumentando constantemente, como efecto variaron algunos parámetros de la comunicación Ad Hoc que fueron tomados como métricas, se ejecutaron llamadas a fin de registrar las variaciones en los resultados obtenidos y analizarlos. El objetivo final fue el estudio de la problemática de la VoIP en WiFi en modo Ad Hoc y paralelamente experimentar con software adecuado para hacer pruebas prácticas sobre este tipo de redes. La versión de IP usado fue la 4 (*IPv4*) por ser la que más se utiliza en la actualidad.

1.5 RESULTADOS ESPERADOS

En este trabajo se han realizado cuatro contribuciones importantes a la investigación de VoIP sobre redes WiFi en modo Ad Hoc, las cuales se redactan en los siguientes puntos:

1. Un estudio técnico descriptivo sobre WiFi Ad Hoc que sirva como base para futuras investigaciones y desarrollos técnicos a fin de cubrir toda la gama de limitaciones y características de este tipo de redes para su futuro despliegue a gran escala.
2. Obtención de parámetros de QoS que denoten degradación del servicio al ser medidas en llamadas establecidas sobre redes WiFi en modo Ad Hoc debido a la carencia de mecanismos robustos de soporte.
3. Disminución de la eficiencia en comparación con valores obtenidos en topologías cableadas implementadas.
4. Establecer correlación entre parámetros de QoS y el rendimiento de la aplicación VoIP ejecutada en modo Ad Hoc.

1.6 ELEMENTOS DIFERENCIADORES E INNOVADORES

El estudio de las comunicaciones sobre VoIP en redes Ad Hoc ha dado muchos resultados en el pasado reciente; pero todavía es un campo de investigación en el que se deben llevar a cabo muchos estudios con el objetivo de modelizar el comportamiento de los parámetros de QoS en este tipo de redes, son muchos los factores que pueden afectar el comportamiento y mientras más estudios se realicen en diferentes escenarios, se aporta mayor conocimiento.

En esta Tesis nos esforzamos por aportar a este campo de investigación en base a los siguientes ítems:

- Fortalecer y apoyar los estudios técnicos previos sobre redes WiFi Ad Hoc, su alcance y limitaciones en la VoIP.
- Determinar, en campo experimental, con la ayuda de herramientas gratuitas y disponibles en la Web, el rendimiento de aplicaciones de tiempo real como VoIP, sobre Trixbox en redes WiFi Ad Hoc para poder conocer en detalle su comportamiento y rendimiento en escenarios controlados.
- Aportar al modelamiento de variables, correlacionando el comportamiento entre los diferentes parámetros presentes en la comunicación Ad Hoc mediante el estándar IEEE 802.11.

Esto permite exponer las limitaciones actuales y poder plantear futuras investigaciones para superar dichos parámetros adversos, además de concluir las limitaciones y la problemática que envuelve a la tecnología WiFi Ad Hoc.

CAPÍTULO 2

2. TECNOLOGÍA WIFI CON TECNOLOGÍA AD HOC

En este capítulo detallamos los fundamentos teóricos de las tecnologías y problemáticas del presente proyecto.

2.1 INTRODUCCIÓN A LA TECNOLOGÍA WIFI

La tecnología WiFi en la actualidad es una manera coloquial para nombrar o definir al estándar emitido por el *IEEE 802.11*, que se enmarca en la denominada *Red de Área Local Inalámbrica* (*WLAN*, del inglés *Wireless Local Access Network*). Sin embargo, se debe considerar que WiFi es una marca de certificación de dispositivos otorgada por la organización de empresas fabricantes de tecnología y servicios Wi-Fi Alliance [3] a los equipos que son compatibles con dicho estándar [4]. Desde el año 1999 y hasta el año 2003 era llamada *Alianza de Compatibilidad de Ethernet Inalámbrico* (*WECA*, del inglés *Wireless Ethernet Compatibility Alliance*).

A pesar del continuo incremento en la tasa de transferencia por medio de las nuevas tecnologías de acceso en las redes celulares móviles, debido al costo moderado de los planes móviles celulares y dado que no se ofrecen planes ilimitados por parte de los operadores, el ancho de banda necesario para ciertas aplicaciones y para la nueva era tecnológica llamada “El Internet de las cosas” aún sigue siendo escaso. El uso de WiFi aún tiene un rol primordial dentro del ámbito de las redes inalámbricas, manejando el mayor porcentaje del *tráfico offload móvil* (tráfico que originalmente fue enviado por medio de redes móviles celulares), una muestra del actual uso masivo de *WiFi*, es el lanzamiento en enero del año 2014 [5], el estándar IEEE 802.11ac, el cual es la última versión del estándar IEEE 802.11, que aumenta la tasa de transferencia a 1Gbps y usa el rango de las frecuencias de 5 GHz.

La Tabla 1 [6] registra en orden cronológico algunos de los principales estándares revisados, liberados y aprobados por el IEEE 802.11 y que son los más populares a nivel comercial, los implementados a gran escala por los fabricantes de tecnología.

Tabla 1: Estándares WLAN

Revisión del Estándar	Enmienda	Año de aprobación de enmienda	Frecuencia	Bit rate Máximo (teórico)
802.11-1997	802.11	1997	2,4 GHz	1-2 Mbps
802.11-1999	802.11a	1999	5 GHz	54 Mbps
802.11-1999	802.11b	1999	2.4 GHz	11 Mbps
802.11-1999	802.11g	2003	2.4 GHz	54 Mbps
802.11-2007	802.11n	2009	2.4 GHz o 5 GHz	600 Mbps
802.11-2012	802.11ac	2014	5 GHz	1 Gbps

Dentro de cada estándar existen más enmiendas que normalizan su funcionamiento, por ejemplo mejoras de rendimiento, implementación de nuevos protocolos de seguridad, habilitación de la operación en diferentes bandas, ofrecimiento de mayores tasas de transmisión; todos estos progresos son realizados gracias a la investigación de los grupos de trabajos formados por el comité de estándares *Red de Área Local/Red de Área Metropolitana*, (*LAN/MAN*, del inglés *Local Area Network/Metropolitan Area Network*) que son auspiciados por la Sociedad de Computación del IEEE. Las frecuencias usadas son las bandas de uso *Industrial, Científico y Médico* (*ISM*, del inglés *Industrial, Scientific and Medical*), que son bandas de frecuencias reservadas para aplicaciones dentro de estos campos pero sin fines comerciales.

El estándar IEEE 802.11 [6] define y describe las funciones, servicios, mecanismos requeridos para que un dispositivo pueda funcionar en un entorno de redes inalámbricas.

Nivel	Nombre	
7	Aplicación	
6	Presentación	
5	Sesión	
4	Transporte	
3	Red	
2	Enlace	Control de Enlace Lógico
		Control de Acceso al Medio
1	Física	

Figura 2.1. Modelo OSI, niveles y subniveles.

A nivel general, las especificaciones IEEE 802 se enfocan en los 2 niveles más bajos del *Modelo de Interconexión de Sistemas Abiertos*, (*OSI,* del inglés *Open System Interconnection*): el nivel físico y los 2 subniveles que pertenecen al nivel de Enlace de datos (*LLC*, del inglés *Logical Link Control*) y *Control de Acceso al Medio (MAC,* del inglés *Medium Access Control*) tal como nos muestra la figura 2.1.

El nivel físico del estándar 802.11 de similar manera se subdivide en dos subniveles llamados: *Protocolo de Convergencia del Nivel Físico* (*PLCP*, del inglés *Physical Layer Convergence Protocol*) y *Medio Físico Dependiente* (*PMD*, del inglés *Physical Medium Dependent*), el primero es el responsable de la entrega de los frames desde el medio inalámbrico hacia el subnivel MAC, mientras que el nivel PMD es el encargado de seleccionar la modulación a aplicarse sobre la señal.

Ethernet forma parte de las especificaciones IEEE 802 siendo una de las más prominentes, implementadas a nivel macro por la Industria de la

Telecomunicación, es la especificación IEEE 802.3, otros ejemplos que trabajan sobre este nivel del mencionado modelo son los protocolos: *Protocolo Punto a Punto* (*PPP*, del inglés *Point-to-Point Protocol*), *Control de Enlace de Datos de Alto Nivel* (*HDLC*, del inglés *High-Level Data Link Control*).

El nivel de Enlace de Datos es responsable entre el nivel físico, de otorgar el direccionamiento físico por medio de hardware, detección y manejo de errores, control de flujo de tramas.

El subnivel LLC provee servicios hacia los niveles superiores, establece y controla los enlaces lógicos, define un número de campos en la trama del nivel de enlace que permite a los protocolos de niveles superiores compartir un mismo enlace de datos físico.

Mientras que el subnivel MAC, es similar a la tecnología Ethernet en la que se utiliza el mecanismo de “escuchar antes de transmitir” para controlar y compartir el medio, típicamente usa reutilización espacial de los canales de transmisión para proveer comunicación simultánea. Fue diseñado para otorgar robustez y seguridad sobre el medio [7].

Específicamente los estándares IEEE 802.11 se definieron sobre el nivel Físico y el subnivel MAC del nivel de Enlace de Datos, dejando a un lado el subnivel LLC.

2.2 CONTROL DE ACCESO AL MEDIO

En escenarios en los que básicamente se comparte el canal por el cual se realizan varias conversaciones de forma simultánea entre diferentes dispositivos de comunicación se requiere un gestor para el MAC. Un gestor es un algoritmo definido que esquematiza el proceso de transmisión para que el porcentaje de interrupciones, cortes, o retrasos sean mínimos de tal forma que no afecten la integridad y disponibilidad de la información transferida. Esta función está determinada según el modelo OSI, por el subnivel MAC, ubicado en el nivel 2.

El medio inalámbrico es un entorno de transmisión saturado en el que varios dispositivos transmiten simultáneamente. El MAC es el responsable de brindar un intercambio de información eficaz, una de sus funciones principales es lograr una utilización eficiente del canal físico intentando establecer la mayor cantidad de conexiones posibles. Agrega la dirección MAC del terminal origen y el destino en cada de una de las tramas transmitidas. Define dos tipos de mecanismos o métodos de acceso para la transmisión de paquetes: *Función de Coordinación Distribuida*, (*DCF*, del inglés *Distributed Coordination Function*) y *Función de Coordinación Puntual* (*PCF*, del inglés *Point Coordination Function*), que se usa en el modo Ad Hoc. La técnica DCF está basada en 2 métodos: Método de Acceso Básico, que es una técnica de conversación de 2 vías y el método de acceso *solicitud-para-enviar y libre-para-enviar* (*RTS/CTS*, del inglés *Request-To-*

Send/Clear-To-Send) que en cambio se realiza por medio de 4 vías. Está basado en *Acceso Múltiple con Escucha de Portadora y Evitación de Colisión* (*CSMA/CA*, del inglés *Carrier Sense Multiple Access/Collision Avoidance*) y proporciona acceso asíncrono a la transmisión de datos de mejor esfuerzo [8]. La transmisión sobre el medio está controlada por el *espacio inter-trama* (*IFS*, del inglés *InterFrame Space*), que es el intervalo de tiempo entre cada trama transmitida. Existen definidos 6 diferentes IFS:

- *Espacio Inter-trama reducido* (*RIFS*, del inglés *Reduced Interframe Space*).
- *Espacio Inter-trama Corto* (*SIFS*, del inglés *Short InterFrame Space*).
- *Espacio Inter-trama del PCF* (*PIFS*, del inglés *PCF InterFrame Space*).
- *Espacio Inter-trama del DCF* (*DIFS*, del inglés *DCF InterFrame Space*).
- *Espacio Inter-trama de Arbitraje* (*AIFS*, del inglés *Arbitration InterFrame Space*).
- *Espacio Inter-trama Extendido* (*EIFS*, del inglés *Extended InterFrame Space*).

La transmisión de acuerdo al método básico se realiza en el caso de que el medio esté ocioso por un lapso mayor al DIFS, si el medio estuviera ocupado espera que ocurra un DIFS desocupado y seguidamente genera un valor aleatorio de retraso antes de transmitir, este es llamado período de *backoff*

(contención), el mencionado temporizador decrece a medida de que encuentra el canal libre y mantiene su valor cuando detecta ocupado el canal y se reanuda cuando el canal se muestra de nuevo en condiciones para permitir la transmisión. Esta transmisión se ejecuta siempre y cuando el *timer* (temporizador) de *backoff* llegue al valor cero. Una colisión ocurre cuando el *timer* de *backoff* de varios terminales llega a cero simultáneamente.

El valor del DIFS es dependiente del SIFS y del slot de tiempo, el temporizador de período SIFS a su vez es dependiente de variables establecidas por diferentes parámetros del nivel Físico y MAC.

La tabla 2 registra los valores del SIFS para las diferentes versiones del IEEE 802.11, los cuales fueron inferidos en la revisión 802.11-2012 [6].

La tabla 3 muestra los valores del intervalo DIFS para las versiones del IEEE 802.11, los cuales fueron inferidos de la revisión 802.11-2012 [6].

Tabla 2: Valores de intervalo SIFS

Revisión del Estándar	**Enmienda**	**SIFS (µs)**
802.11-1997	802.11-1997 (FHSS)	28
802.11-1997	802.11-1997 (DSSS)	10
802.11-1999	802.11b	10
802.11-1999	802.11a	16
802.11-1999	802.11g	10
802.11-2007	802.11n (2.4 GHz)	10
802.11-2007	802.11n (5 GHz)	16
802.11-2012	802.11ac	16

Tabla 3: Valores de intervalo DIFS

Revisión del Estándar	Enmienda	Slot de tiempo	DIFS (µs)
802.11-1997	802.11-1997 (FHSS)	50	128
802.11-1997	802.11-1997 (DSSS)	20	50
802.11-1999	802.11b	20	50
802.11-1999	802.11a	9	34
802.11-1999	802.11g	9 o 20	28 o 50
802.11-2007	802.11n (2.4 GHz)	9 o 20	28 o 50
802.11-2007	802.11n (5 GHz)	9	34
802.11-2012	802.11ac (5 GHz)	9	34

El temporizador de *backoff* se escoge aleatoriamente por medio de una distribución uniforme discreta entre los valores [0 y CW], siendo la *Ventana de contención* (*CW*, del inglés *Contention Window*) un valor que expresa su tamaño, y depende del número de transmisiones fallidas; en el primer intento el valor de *CW* se fija en el valor mínimo de la ventana de contención, después de cada transmisión fallida el valor de CW se duplica hasta llegar a un valor máximo de $(CW_{min} + 1)*(2^n - 1)$ donde n es el número de retransmisión. La ventana de contención por ejemplo para el IEEE 802.11b posee un valor mínimo de 31 *slots* (ranuras de tiempo) y un máximo de 1023 slots.

En el caso de realizarse la recepción de la trama con éxito, el terminal destino envía un *acuse de recibo inmediato* (*ACK*, del inglés *Acknowledgement*) después de un intervalo SIFS hacia el terminal fuente, es por esta razón que este método se lo conoce como de doble vía, si el

terminal origen no recibe el ACK indica que se ejecutó una transmisión fallida y ocurrieron pérdidas de paquetes, por lo que se programa una retransmisión, con el valor de la ventana de contención duplicado según lo explicado en las líneas anteriores.

En el método de acceso RTS/CTS se introduce un proceso adicional al método de acceso básico; cuando el temporizador de *backoff* llega a cero en lugar de proceder a ejecutar la transmisión, se realiza el envío de una trama RTS por parte del terminal transmisor, el terminal receptor responde con un trama CTS luego de transcurrir un intervalo SIFS, luego de que este intercambio se haya realizado exitosamente se procede con la transmisión de las tramas, debido a este intercambio adicional se lo conoce como el método de acceso de 4 vías. Las tramas RTS y CTS contienen un campo llamado *vector de asignación de red* (*NAV*, del inglés *Network Allocation Vector*) quien define el lapso de reserva del canal para la transmisión de la trama.

En el caso de que el mensaje a transmitir sea mucho más grande que el máximo tamaño de la trama para el estándar IEEE 802.11, se requiere la fragmentación antes de la transmisión. Los diferentes fragmentos se transmitirán con un SIFS de separación, por tanto, solo el primer fragmento es el que debe ejecutar el proceso de monitoreo del canal para lograr el acceso.

2.3 TOPOLOGÍAS DE INTERCONEXIÓN

En el estándar IEEE 802.11 se han definido dos modos de acuerdo a la operación: modo infraestructura y el modo Ad Hoc, esta clasificación va de la mano con los tipos de *Conjuntos de Servicios Básicos* (*BSS*, del inglés *Basic Service Set*) que es el bloque mínimo de comunicación en el estándar IEEE 802.11, que son dos: *Conjunto de Servicios Básicos Independientes* (*IBSS*, del inglés *Independent Basic Service Set*), llamado Ad Hoc y Conjunto de Servicios Básicos de Infraestructura, llamado infraestructura.

El estado de los campos *To DS* y *From DS* del encabezado de la trama MAC indica si una trama está destinada hacia un *sistema de distribución* (*DS*, del inglés *Distribution System*) o en un sistema de distribución. Cuando se lleva a cabo una transmisión en modo Infraestructura se requiere que las tramas sean enviadas hacia un *Punto de Acceso* (*AP*, del inglés *Access Point*), por lo que el campo *To DS* debe estar encendido y el campo *From DS* apagado o en el caso de que sea una transmisión desde el AP, el estado de los bits debe ser inverso. Mientras que cuando se realiza una transmisión en modo Ad Hoc ambos campos deben estar a cero.

2.3.1 Infraestructura

El modo infraestructura posee la característica de requerir la asociación a un AP para obtener los servicios de la red, y toda comunicación con el resto de terminales se realiza a través del AP.

En este modo se pueden establecer conexiones con otros terminales que se encuentren bajo la misma cobertura del AP y también puede establecerse comunicación con terminales que se encuentren bajo el control de diferentes puntos de acceso. Los AP deben estar conectados a un sistema de distribución, este esquema es llamado *Conjunto de Servicios Extendido* (*ESS*, del inglés *Extended Service Set*). Cada ESS posee un identificador llamado *Identificador de Conjunto de Servicios* (*SSID*, del inglés *Service Set Identifier*).

2.3.2 Ad Hoc

Modo también denominado IBSS, carece de AP, basta con estar dentro del mismo área de cobertura del otro terminal para lograr establecer una comunicación punto a punto. Los terminales pueden estar en movimiento y son capaces de conectarse dinámicamente de forma arbitraria, pero posee las siguientes desventajas: los terminales deben permanecer de manera fija en el canal en el cual se estableció la conexión, requieren de mayor consumo de energía, y la mayoría de dispositivos móviles no soportan este modo de

funcionamiento, al menos los que poseen sistemas operativos basados en Android e iOS [9]. Sin embargo es posible ejecutar aplicaciones sobre dispositivos que sean desarrollados exclusivamente para esta función.

En este trabajo de investigación analizamos las soluciones a los problemas generados en aplicaciones de VoIP bajo este tipo de topología.

2.4 PROBLEMÁTICA DE LAS TECNOLOGÍAS AD HOC

En esta sección abordamos todos los problemas surgidos en la comunicación por medio del estándar IEEE 802.11, que al usar el medio inalámbrico es menos confiable que los medios cableados y a su vez conlleva una serie de limitantes en los escenarios establecidos bajo este medio.

Uno de los principales inconvenientes en el medio inalámbrico y que producen degradación del servicio es el hecho de ser un medio compartido por otros terminales que se encuentran comunicándose bajo la misma frecuencia.

El primer problema que tomamos en cuenta es el llamado Terminal oculto.

2.4.1 Terminal oculto

El problema de terminal oculto es bien conocido y tiene gran incidencia en los escenarios que usan redes inalámbricas. Se presenta en un escenario en el que participan al menos 3 terminales de comunicación, donde 2 terminales, A y B, pueden comunicarse con un tercer terminal C que se encuentra espacialmente intermedio, se lo puede representar como un AP, los dos primeros terminales no pueden comunicarse entre ellos por estar fuera de cobertura mutua, si la comunicación realizada desde el terminal A hacia el terminal C se realiza por medio del método de acceso DCF, este monitorea el medio para ejecutar la transmisión, al ver el canal libre procede a ejecutar la transmisión pero debido a que no es capaz de detectar la comunicación desde el terminal B hacia el C, el resultado es la presencia de colisiones en el medio y el número de retransmisiones pueden llegar a ser indeterminadas; esto aplica al tráfico enviado desde los terminales A y B hacia el terminal C. Este problema replicado en un ambiente con una cantidad mayor de terminales afectaría el rendimiento, y el retraso de transmisiones, al tener el terminal fuente realizando reenvíos de tramas constantemente, produce un consumo de energía adicional. Algunos estudios [10] mencionan que más del 40% de los paquetes transmitidos se pierden debido al problema del terminal oculto, volviéndose mucho más crítico en el caso de aumentar el número de terminales en la red.

Los canales de transmisión de los terminales no están protegidos contra señales externas, existen métodos que mitigan los negativos efectos del terminal oculto, se han segmentado estos mecanismos dentro de 3 categorías [10]:

- Mecanismos de negociación, donde el terminal receptor y emisor envían paquetes de control para reservar el canal.
- Mecanismos de tono ocupado, donde el terminal receptor enciende un tono de ocupado y los otros terminales detectan este estado, por lo tanto no inician nuevas transmisiones, de esta manera el terminal receptor no recibirá tramas adicionales que provoquen colisiones.
- Mecanismo de administración de caminos, donde se implementan protocolos de encaminamiento con el objetivo de buscar el mejor camino libre de colisiones.

Adicionalmente, un problema similar al explicado es el terminal expuesto. Éste ocurre cuando un terminal transmisor está impedido de transmitir, debido al mecanismo de acceso por la interferencia de un segundo terminal transmisor. Consideremos 4 terminales, A, B, C y D; los terminales A y D son terminales receptores y los terminales B y C son terminales transmisores, donde los terminales A y D están fuera de cobertura mutuamente, mientras que los terminales B y C se encuentra mutuamente bajo cobertura, asumiendo que se encuentra ejecutando una transmisión por parte del

terminal B hacia el terminal A, el terminal C es impedido de realizar una transmisión hacia el terminal D dado a que el mecanismo de acceso detecta una interferencia con la transmisión del terminal B, en este caso se está impidiendo una transmisión que se ejecutaría correctamente.

2.4.2 Cobertura

En una red Ad Hoc, cada terminal tiene una máxima potencia de transmisión para lograr comunicarse con el resto de terminales que se encuentre dentro de su alcance, esta cobertura es fija y no dinámica.

En el caso de que dos terminales no se encuentren dentro de su radio de cobertura, tratan de comunicarse a través de terminales intermedios que encaminan hacia el terminal destino, ejecutando una transmisión de varios saltos, esto conlleva que cada terminal actúe como un dispositivo de encaminamiento independiente.

La cobertura está ligada directamente proporcional a la potencia de transmisión de los terminales, ya sean terminales o puntos de acceso, por lo tanto el consumo de energía se ve afectado según sean las características de cobertura del terminal.

El problema de la cobertura tiene un rol importante y crítico debido al factor de movilidad inherente a las aplicaciones de los entornos contemporáneos.

2.4.3 Movimiento de terminal

Los terminales de una red Ad Hoc, no poseen la conexión a un AP, no tienen elementos de red de infraestructura fija, los terminales pueden ser usados en cualquier lugar, en cualquier momento, al tener la capacidad de movilidad proporcionan versatilidad a la red y al contenido que se puede ofrecer por medio de la misma. Esta característica de movilidad intrínseca de las redes Ad Hoc hace que las limite en su potencia de transmisión y por ende en su rango de cobertura.

Se han desarrollado modelos de movilidad de usuarios, por ejemplo, en el caso de conexiones realizadas por medio de Ad Hoc entre terminales que sean portátiles, se espera una frecuencia de movilidad menor que a usuarios conectados desde teléfonos móviles.

2.4.4 Interferencias de canal

El estándar IEEE 802.11 utiliza frecuencias no licenciadas, las cuales forman parte de ISM, dichas frecuencias son usadas por diversos dispositivos que no usan el estándar IEEE 802.11 como por ejemplo: teléfonos inalámbricos, dispositivos *Bluetooth*, hornos microondas, fuentes de iluminación de baja energía *RF*. La interferencia ocurre cuando dos señales de radio se transmiten en la misma frecuencia al mismo tiempo; si ambas señales tienen potencias relativas y similares, la interferencia es mutua, en el caso de que

una de las señales sea mucho mayor, esta es la que interferiría a la señal más débil. De acuerdo a estudios [11] realizados de los efectos de la interferencia entre dos terminales en modo Ad Hoc, esto afecta a la cantidad de bits transmitidos, el tiempo de respuesta de subida, y aumento de paquetes perdidos y retransmisiones de tramas.

2.4.5 Paquetes perdidos

Los paquetes perdidos en una red Ad Hoc son los paquetes de información enviados por el terminal A que no fueron recibidos por el terminal B, y en el sentido recíproco, los paquetes respondidos desde el terminal B que no alcanzaron a llegar al terminal A, pueden ser medidos en un sentido o en el sentido completo de la comunicación. Este comportamiento se debe a los efectos de la diversa problemática mostrada en la comunicación de las redes Ad Hoc, a esto debe sumarse los inconvenientes presentados en una red inalámbrica. Esto causa que los servicios provistos en una red Ad Hoc se noten degradados en una comunicación donde se presente pérdidas de paquetes y según sea el servicio, sea más o menos sensible a la percepción humana. Se pueden establecer índices como tasas de paquetes perdidos o tasas de paquetes de recepción de paquetes que sirven para establecer un parámetro de calidad de los enlaces Ad Hoc.

2.4.6 Rendimiento

El rendimiento de una red es la suma del rendimiento por terminal de cada uno que pertenece a la red. El rendimiento por terminal se denomina al tiempo promedio del número de bits que puede ser transmitido por cada terminal a su destino [12]. La disminución del rendimiento en una red es un efecto que es producido por la presencia de elementos que causan que las comunicaciones de una red inalámbrica no se establezcan de una manera idónea, como por ejemplo el factor de movilidad de los usuarios de la red, los obstáculos que producen atenuaciones en las señales, las interferencias por señales externas, entre otros.

2.5 ARQUITECTURAS DE RED

En esta sección especificamos las características y funciones de algunas arquitecturas implementadas comúnmente en el estándar IEEE 802.11 y en general en las comunicaciones inalámbricas, entre las cuales se destacan: modo anclaje de red, modo *mesh* (malla).

2.5.1 Anclaje de red

Debido a la expansión de las redes telefónicas móviles y aunque la penetración de Internet está en continuo aumento, existen lugares y

ocasiones en los cuales no se posee y es necesaria una conexión WiFi ya sea para una conexión hacia Internet o para cualquier otro uso. De acuerdo a los datos recogidos en el estudio realizado por Rahmati, Ahmad [13] en Estados Unidos, las personas pasan las horas del día en lugares con un 99% de probabilidad que tenga señal de red celular móvil, mientras que un 49% de señal de red WiFi, este dato puede ser usado para predecir de semejante manera, aunque no con esos mismos valores, en nuestros países la penetración de estas diferentes redes móviles, por lo que la solución más común es realizar una conexión inalámbrica entre un teléfono móvil con un plan de datos disponible, y el dispositivo requerido de la conexión, esto se denomina anclaje de red o *tethering*. Una conexión IEEE 802.11 con anclaje de red se lleva a cabo cuando un dispositivo que posea la interfaz apropiada se conecta a un teléfono móvil usando WiFi, este modo de arquitectura no está limitado a conexiones inalámbricas.

En este tipo de arquitectura se emplea el teléfono celular como un PA móvil, utilizando sus interfaces *Global System for Mobile Communications* (*GSM*), Tercera Generación (*3G*) o *Long Term Evolution* (*LTE*) para brindar el servicio. El tethering es una característica inherente del sistema operativo del teléfono móvil, no del hardware del teléfono móvil. Al establecer una red bajo estas características aumenta la potencia eléctrica consumida por el teléfono móvil, provocando que su tiempo de disponibilidad de energía proporcionada por la batería disminuya, comparado con WiFi, las redes celulares requieren

menos energía para permanecer conectado, pero necesita una energía mucho mayor por transferencia de MB [13]. Según las pruebas realizadas en el trabajo de investigación de Jung, Kyoung-Hak, se demuestra con valores concretos en algunos modelos de teléfonos móviles, que el uso del anclaje de red, disminuye el tiempo de energía proporcionada por la batería [14] considerablemente.

2.5.2 Mesh

La topología mesh aplica a una red en modo infraestructura, posee la característica de conectar a todos los terminales pertenecientes a la red entre sí, los terminales extremos pueden llegar a tener una sola conexión. Esto ayuda a evitar el inconveniente de tener conectividad dedicada hacia el servidor central, y hace admisible que los fallos de un enlace no afecte la operación de la red: es una opción viable para redes con gran densidad de terminales. Además, al tener que usar varios terminales para llegar al terminal destino usa menor potencia en la transmisión y puede llegar a transmitir mayor cantidad de bits por segundo. Un reto para esta topología es el encaminamiento, debe poseer un protocolo eficaz asignando las métricas correctas para lograr un encaminamiento eficiente entre todos los caminos disponibles para llegar de un terminal a otro, el protocolo escogido asigna el tamaño de la escalabilidad de la red. El hecho de tener varios caminos con

gran cantidad de saltos entre terminales, produce una limitante a nivel de latencia, este tipo de topología está diseñado para transmitir servicios que sean tolerables a la latencia.

El rendimiento de la red es también limitado, esta capacidad es inversamente proporcional a la cantidad de saltos que posea el camino entre los terminales.

CAPÍTULO 3

3. VoIP

VoIP es uno de los ejes fundamentales del presente estudio, por tal motivo a continuación conoceremos con detalles su historia, características y protocolos asociados.

3.1 GENERALIDADES DE LA TELEFONÍA

En este apartado se señala la evolución, las características del proceso llevado a cabo en la prestación del servicio de Telefonía y en general los requerimientos que se presentan en la Telefonía en general.

3.1.1 Evolución Histórica de la Telefonía

Desde la antigüedad, el hombre se ha ingeniado y ha desarrollado diferentes formas de comunicación como parte de su necesidad imperante de establecer relaciones y contactos con su comunidad. Desde sus inicios

existieron formas rústicas de comunicación como las señales de humo o los mensajeros que recorrían largas distancias a pie, que tenían un solo fin: transmitir un mensaje. El descubrimiento de la electricidad ayudó a que nuevas formas de comunicación se generen. A mediados del siglo XIX, el italoamericano Antonio Meucci, inventó el teletrófono que era capaz de transmitir la voz humana utilizando corriente continua, instrumento que posteriormente fue denominado “teléfono”.

La invención del teléfono marcó una nueva era para las comunicaciones a nivel mundial y estableció el origen de las telecomunicaciones, paulatinamente surgieron más inventos alrededor de él que disminuían las distancias y los tiempos además de incrementar la calidad en la comunicación; el envío de mensajes sin cables, llamadas automática entre los abonados sin intervención de operadoras, disminución de costos lo que ocasionó mayor facilidad en el acceso, evolución de los terminales telefónicos, el micrófono, marcación por pulsos, marcación por tonos, servicios suplementarios y el gran despliegue de la red de telefonía fija hasta los hogares, convergencia en redes digitales de conmutación por paquetes. La conmutación asistida por computadores conllevó la implementación de la señalización, con el fin de declarar los parámetros de establecimiento, liberación y control de las llamadas; la señalización se establece entre centrales y entre centrales y abonados.

Inicialmente las clásicas líneas *Red Telefónica Básica* (*RTB*) tenían asignadas una numeración única, estas numeraciones variaban dentro de un rango otorgado por el ente regulatorio al operador. Estas líneas físicamente llegaban al hogar por medio de un par de hilos cobre que estaban conectados a la central telefónica del operador, que se conocía como bucle de abonado. Cada central ofrecía una determinada cobertura dependiendo del cableado de planta externa instalado. La red interna del operador consistía en comunicar todas las centrales entre sí, además de interconectarse a otros operadores, inicialmente las conmutaciones eran mecánicas por medio de un operador humano, luego fueron reemplazadas por conmutaciones de tipo electro-mecánico. Con este cambio tecnológico, entró en funcionamiento la capacidad de conmutación, y empezaron a llamarse *Red Telefónica Conmutada* (*RTC*) o *Red Pública Telefónica Conmutada* (*PSTN*, del inglés *Public Switched Telephone Network*). La digitalización de la trasmisión de voz y señalización empezó con la implementación de la *Red Digital de Servicios Integrados* (RDSI) pese a mantener a líneas analógicas del abonado. Esta Red brindaba a los usuarios servicios suplementarios como identificación del número llamante, desvío de llamadas, además de ofrecer una telecomunicación más integral, soportando el envío de datos, imágenes y texto por el mismo par de cobre. Los primeros tipos de señalización se establecieron de modo “en banda”, aquellas que utilizaban frecuencias del canal telefónico, posteriormente se implementaron

señalizaciones “fuera de banda", las cuales mantienen el canal de voz libre y usa espectro complementario para el envío de las señales de control.

3.1.2 Características de la telefonía convencional

En los países en vía de desarrollo, las redes de telefonía convencional usan tecnología PSTN. Esta red posee la particularidad de que si se establece la llamada, el canal queda reservado y garantizado hasta que sea liberado por alguno de los extremos. Sus elementos que caracterizan al servicio de telefonía son:

- *Transmisor y receptor*. Usualmente en los dispositivos transmisores, parte de la señalización es el tipo de marcación. La comúnmente usada es la de *Tono Dual de Multifrecuencia* (*DTMF*, del inglés *Dual Tone Multifrequency*), por medio de *dial pads* que son matrices de pulsadores donde se encuentran los caracteres numéricos y especiales.
- *Medio de transmisión*. Está dado por la red de planta externa que tenga implementada la operadora telefónica.
- *Conmutación*. Realizada por las centrales que forman parte de la red de planta interna del operador. La PSTN establece una red jerárquica que consta de al menos de 3 tipos de centrales: Nodo de Intercambio Local (se encuentran en el extremo de la jerarquía brindando servicios

directamente a los usuarios), Nodo de Tránsito (brindan la interconexión hacia nodos que manejan gran tráfico, por ejemplo interconexiones internacionales o regionales) y Nodo Tándem (ofrecen conectividad entre las centrales de Intercambio Local y los nodos de Tránsito).

- *Señalización*. Conformada por señales que ayudan al control de las llamadas, tales como: señales de marcación como los tonos DTMF, peticiones de establecimiento, señales de supervisión, señales de estado de ocupado y de llamada, señales de timbrado. La señalización utilizada en las redes PSTN, se ha estandarizado, es el *Sistema de Señalización por canal común No.* 7 (*SS7*, del inglés *Signalling System No. 7*), es un sistema fuera de banda y clasificado como señalización de canal común, dado que utiliza un único canal para transportar la señalización de todos los canales de voz, para mayores detalles la *Unión Internacional de Telecomunicaciones* (*ITU*, del inglés *International Telecommunications Union*) ha normado la suite de protocolos SS7 por medio de recomendaciones disponibles públicamente.
- *Plan de numeración*. Cada usuario del servicio de telefonía de un operador posee un identificador único, llamado número telefónico; dentro de las redes de telefonía es esencial mantener un orden y estructura en la asignación de los números telefónicos, la ITU lo ha

regulado por medio de la recomendación E.164 [15] a nivel nacional, regional e internacional, dejando al libre albedrío y organización de la numeración dentro de un país a sus entes regulatorios correspondientes; por lo general es basado en prefijos.

3.1.3 Funcionamiento de telefonía actual

Los sistemas de telefonía tradicional requerían solventar las limitantes tecnológicas propias de la PSTN, éstas se dieron a notar ante la demanda de los servicios de datos, video y sobre todo acceso a Internet. El siguiente nivel de "evolución" estandarizado por las operadoras telefónicas fueron las *Redes de Próxima Generación* (*NGN*, del inglés *Next Generation Network*), estas redes son basadas en la conmutación de paquetes, permiten la integración y convergencia de servicios y aplicaciones adicionales debido a su mayor capacidad para transportar bytes de información, permitiendo a los operadores extender su cartera de clientes y recaudar mayor cantidad de ingresos, disminuyen también sus gastos en *Inversiones en bienes de capitales* (*CAPEX*, del inglés *CAPital EXpenditure*) y sus *gastos de operación* (*OPEX*, del inglés *OPerational Expenditure*), al tener una red brindando múltiples servicios y no múltiples arquitecturas por cada servicio. Las redes NGN es lo más común en la actualidad para brindar servicios de telefonía.

La red NGN posee una arquitectura horizontal que consta de 4 niveles: servicios de red, control, medio y acceso; en este tipo de redes de conmutación por paquetes es requerido el uso de políticas de QoS debido a que no se establece un canal por cada conexión. El transporte de la información es por paquetes que deberán compartir el medio y deberán ser priorizados los paquetes de voz ante los paquetes de datos o Internet; en el caso de redes saturadas con políticas de QoS no tan afinadas aumenta la probabilidad de degradación del servicio más sensible a latencias. La NGN fue diseñada con el propósito de ofrecer movilidad a sus clientes independientemente de la plataforma de Acceso que el operador oferte. Tiene la capacidad de ofrecer QoS de extremo a extremo.

La UIT-T resume sus características en la definición presentada en la recomendación Y.2001 aprobada en el año 2004: "*Es una red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la QoS, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a proveedores de servicios y/o servicios de su elección. Se soporta movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios*" [16].

Al igual que su antecesora, NGN maneja una arquitectura de protocolos en los diferentes niveles del modelo OSI.

Aparece un elemento importante en la transmisión de voz por redes de conmutación de paquetes, es el *Softswitch*, este equipo tiene como función la integración por medio de interfaces hacia la antigua tecnología PSTN con los componentes de la arquitectura NGN, las funcionalidades del Softswitch varía según el fabricantes, pero se puede resumir que es una plataforma de conmutación basada en software que proporciona las funciones de control y conexión de llamadas, traducción de números telefónicos y encaminamiento. [17].

3.2 DESCRIPCIÓN DE LA VoIP

Debido a las migraciones realizadas por parte de los operadores hacia redes de conmutación por paquetes, cualquiera de los nuevos servicios que podrían ofrecer sería empaquetado sobre IP, sin excepción de la voz. Este entorno dio inicio a la tecnología mediante la cual la voz humana se empaqueta y transporta por redes de conmutación por paquetes IP, llamada *VoIP,* este término constituye además una amplia cantidad de servicios de valor añadido.

3.2.1 Historia y principios básicos de la VoIP

No es posible establecer un inventor de la VoIP, la transmisión de la voz humana empaquetada en IP se dio gracias a un entorno que estuvo listo y disponible a los usuarios gracias a múltiples desarrollos en las redes de los operadores telefónicos y la normalización por los entes reguladores, pero era necesario un terminal o software que lo permitiera. A nivel académico se realizaron pruebas exitosas entre laboratorios de la Universidad del Sur de California y el *Instituto Tecnológico de Massachusetts* (*MIT*, del inglés *Massachusetts Institute of Technology*) en el año de 1976, usando dos de los protocolos desarrollados años atrás, TCP y el *Protocolo de Voz en la Red* (*NVP*, del inglés *Network Voice Protocol*) [18].

La empresa *VocalTec* lanzó comercialmente el primer producto de VoIP, llamado *Internetphone*, en febrero de 1995. Se trataba de un software que permitía realizar llamadas entre 2 *computadores personales* (*PC*, del inglés *Personal Computer*), utilizando sus micrófonos, parlantes y tarjetas de sonido. Empleó el protocolo H.323, codificando y comprimiendo la señal de voz y empleando la misma configuración en ambos PC [19]. Este producto no fue muy exitoso debido a la limitante del ancho de banda disponible hacia los usuarios. Este hecho marcó un hito comercial y posteriormente las empresas desarrollaron diversas soluciones dedicadas a la comunicación PC-teléfono y teléfono-teléfono.

Al ser un servicio basado en IP, la VoIP se estableció como un servicio de comunicación integrador, que además de voz, podía incorporar servicios de mensajería instantánea, servicios suplementarios e inclusive transmisión de video. En caso de establecerse la llamada vía Internet el usuario se independiza de la limitante de cobertura ofrecida por el operador, se flexibiliza al poder comunicarse mediante NGN con usuarios de plataformas de telefonía tradicional y móvil, eximiéndose de cancelar al operador las tarifas de interconexión; el servicio de VoIP necesariamente no se realiza por medio de Internet, se puede establecer por medio de un enlace de transmisión de datos, permitiendo minimizar los costos para el segmento empresarial estableciendo redes VoIP corporativas. Otra capacidad de la tecnología VoIP es la portabilidad, no es requerido tener una ubicación fija, basta tener una conexión y el usuario efectuaría las llamadas, siendo transparente su punto de nexo.

Así como heredan sus beneficios, heredan las vulnerabilidades de las redes de conmutación de paquetes y falta de QoS para servicios en tiempo real (sensibles a la pérdida de paquetes, latencia o jitter). La congestión podría afectar al servicio. Un mal diseño del *COdificador-DECodificador* (*CODEC*) incide en la degradación del servicio. Existe una elevada probabilidad de ataques de denegación de servicio, suplantación de identidad, entre otros afecten a la disponibilidad, confiabilidad y confidencialidad de los datos. La dependencia de energía por parte de los elementos empleados para el

establecimiento de una llamada VoIP, la PC, el encaminador, el *modulador-demodulador* (*modem*) requiere del consumo constante de energía eléctrica.

De manera general, para establecer una llamada de VoIP es requerido contar los siguientes elementos disponibles:

- *Software*: módulo de procesamiento de voz, detección de ruidos y de tonos, entre otros.
- *Hardware*: tarjetas de audio, PC, módems, gateways de voz.
- Protocolos de señalización y de negociación de los requisitos de QoS de la llamada (negociación de códecs o transcodificación para un correcto establecimiento de la llamada).

3.2.2 Funcionamiento de los sistemas de VoIP

En resumen los pasos para comunicar la voz en un sistema de VoIP son:

- *Digitalización*: la entrada de audio analógico debe ser capturada por un dispositivo que haga su conversión a su formato digital. Es la etapa de muestreo y cuantificación. El muestreo se basa en el teorema de *Nyquist* y la cuantificación o cuantización es la representación digital de las amplitudes tomadas durante el muestreo. Mientras mayor sea la cantidad de bits mayor sería la exactitud. A mayor exactitud, más uso de los recursos computacionales se haría.

- *Compresión*: es un proceso basado en software que minimiza el ancho de banda utilizada durante la comunicación según el códec seleccionado o negociado.
- *Paquetización*: para comunicar en redes de paquetes conmutados es requerido colocar los flujos de las muestras digitalizadas de voz en paquetes IP, tomando en cuenta que cada paquete IP tiene su encabezado propio.
- Dentro del campo de investigación de la VoIP existen muchos retos para seguir perfeccionando el procesamiento de la señal a transmitirse, algunos de los campos que están en continuo desarrollo son: la cancelación de ecos, compresión de la voz, reducción de ruido de retorno, monitoreo de la calidad de la voz transmitida, sensibilidad al retraso de paquetes, sensibilidad a la pérdida de paquetes, sensibilidad a una constante variación del jitter.

3.3 PROCESO DE DIGITALIZACIÓN DE LA VOZ

El proceso de digitalización consta de los siguientes pasos: muestreo, cuantificación, y codificación.

Muestreo

El muestreo es la entrada al mundo digital, su objetivo es la toma continua de valores instantáneos en los flujos analógicos del audio fuente, este proceso debe ser realizado cada cierto lapso, con una frecuencia definida.

En el año de 1928 Harry Nyquist elaboró una conjetura basada en el trabajo previo de E.T. Whittaker, año 1915, no relacionados aún con muestreo, el primero en relacionar el muestreo con la comunicación fue V.A. Kotelnikov en el año de 1933, finalmente en el año de 1949 Claude E. Shannon basado en los 3 trabajos anteriormente mencionados [20] publicó un artículo revolucionario donde enunció el teorema de muestreo que indica que si una señal variante en el tiempo posee una frecuencia máxima, la señal puede recuperarse perfectamente muestreándola a una tasa igual a dos veces su frecuencia máxima, también llamada frecuencia de Nyquist, que es habitualmente conocido como el teorema de Shannon-Nyquist.

Para esta tesis se toma en cuenta el teorema de Nyquist, pese a que actualmente existen estudios donde se han diseñado nuevas arquitecturas y esquemas para convertidores analógico a digital, que permiten muestrear señales con eficacia mediante frecuencias menores a la de Nyquist [21].

Cuantificación

El proceso de cuantificación convierte los valores continuos de las amplitudes muestreadas en valores discretos, para obtenerlos es necesario definir el número de intervalos requeridos, con esto se dimensiona el número de bits que se usarán para representar las amplitudes de la señal. Es el primer paso en generar pérdida de información, mientras mayor sea la resolución en el proceso de cuantificación, menor sería la pérdida de datos en la reconstrucción de la señal original. Este es el conocido error de cuantificación; por ejemplo, en el caso de utilizar 8 bits para digitalizar los datos, tendríamos 256 intervalos disponibles para representar las amplitudes. Si alguna amplitud se presentara en el intermedio de un intervalo, ocurriría pérdida de señal redondeando el valor al inmediato inferior o superior, si la cantidad de bits aumentara, los intervalos de cuantización aumentan, pero la magnitud de cada intervalo se reduce, reduciendo la pérdida de información en este paso.

Para este paso se podría optimizar implementando detectores de ruido inactivo o detectores de actividad de voz, esto informaría cuando la entrada de audio sea nula, tiene el objetivo de minimizar tráfico al suprimir la señal cuando no se estén enviando señales de voz. Sin esto, el proceso de cuantificación sería aplicado al ruido de entrada, aumentando consumo de recursos innecesarios. Los tipos de cuantificación se pueden dividir en dos grandes grupos: uniforme y no uniforme.

Codificación

Este proceso se encarga de realizar la representación de los datos cuantizados para su transporte en el medio digital, transformación, compresión y organización en paquetes, parte de las fases finales realizadas por los codecs. No es posible ocupar todo el ancho disponible de un canal, por lo que es requerido limitar la transmisión de voz a una tasa específica, comprimiendo la señal, en este proceso se define la tasa de bits por segundo, el reto está en representar la voz con la máxima calidad posible, manteniendo la menor tasa de transmisión.

Los codecs que tomamos en cuenta en esta sección son los codificadores de voz y audio, estos deben ser robustos y capaces de manejar una alta probabilidad de que existan paquetes perdidos durante la transmisión.

Los principales atributos de un códec de voz son según Kleijn [22] son los siguientes:

- Tasa de bits.
- Calidad de voz subjetiva.
- Complejidad computacional y requerimientos de memoria.
- Retraso.
- Sensibilidad y robustez a los errores de canales.
- Ancho de banda de la señal.

Hay autores que indican tres técnicas de compresión de voz: compresión de la forma de onda, compresión paramétrica y compresión híbrida [23] [24].

La técnica de compresión de forma de onda es independiente de la señal de entrada, es más versátil, dado que se acopla para otros tipos de señales como audio y tiende a reformar la señal mucho más cercana a la señal original, posee un bajo proceso computacional, las tasas de bits otorgados por lo general van desde 16Kbps hasta 64Kbps. De acuerdo a Kleijn, [25] son codificadores que producen señales reconstruidas que convergen hacia la señal original reduciendo los errores de cuantización.

Algunos codecs que utilizan esta técnica de compresión son: *Modulación por impulsos codificados* (*PCM*, del inglés *Pulse Code Modulation*) y *Modulación Adaptativa Diferencial por impulsos codificados* (*ADPCM*, del inglés *Adaptive Differential Pulse Code Modulation*).

La técnica de compresión paramétrica, obtienen los parámetros de la voz, con esto emulan el comportamiento del audio, y los mismos parámetros son utilizados en el proceso de síntesis de la voz, esto consume gran cantidad de procesamiento. De acuerdo a Kleijn, [25] son codificadores que producen señales reconstruidas que no convergen hacia la señal original reduciendo los errores de cuantización.

Existen tres clases de codecs de compresión paramétrica:

- Codificadores de voz basada en predicción lineal.
- Codificadores de transformada sinusoidal.
- Codificadores de interpolación de forma de onda.

Los códecs de *Codificación de Predicción Lineal* (*LPC*, del inglés *Linear Prediction Coding*), comúnmente produce tasas de transmisión entre 1.2 y 4.8 Kbps, aproximadamente, por un lado se logra una alta capacidad de compresión pero tiene la desventaja de que la calidad del audio no es idónea, tiene un aspecto robotizado, un ejemplo es el códec de *Predicción Lineal Mixto por Excitación* (*MELP*, del inglés *Mixed-excitation Linear Prediction*).

Por último, la técnica de compresión híbrida, agrupa las ventajas de los dos anteriores métodos, utilizando tanto la codificación de forma de onda y la paramétrica en momentos diferentes, generan tasas de bits fijas o variables, entre cinco y 32 Kbps. Es un códec adaptivo que puede cambiar su técnica de codificación de acuerdo a la señal fuente. Un ejemplo de códec híbrido es el códec *Predicción Lineal por Excitación por Código* (*CELP*, del inglés *Code Excited Linear Predictive*). Otra métrica de clasificación de codecs, es por la banda de frecuencia en la cual opera, existen de codecs de banda estrecha para frecuencias hasta 4000Hz y codecs de banda ancha para señales de hasta 7000Hz.

El empaquetado es el último paso: la voz está lista para su transporte digital, además de portar la voz, el paquete consta de un encabezado de tamaño fijo que adiciona bits en la transmisión ya sea en bajo *TCP* o el *Protocolo de Datagrama de Usuario* (*UDP*, del inglés *User Datagram Protocol*)

La elección del códec adecuado, es un reto, se debe tener un conocimiento amplio de las limitantes de la red a utilizar, del uso que se va a dar de la señal transmitida, la calidad requerida, el hardware utilizado, con el fin de evaluar las características en cada atributo del códec y dentro de toda la gama de métodos y clases seleccionarlo óptimamente.

3.4 CODECS USADOS EN VoIP

Luego de haber visto la variedad de tipos, clasificaciones y métodos de compresión de señales que existen, es notorio que no todos los codificadores desarrollados, se acoplan para una idónea transmisión de audio y voz.

El sector de Normalización de las Telecomunicaciones de la UIT, la UIT-T, dentro de sus recomendaciones de la serie G, llamada *Sistemas y Medios de Transmisión, Sistemas y Redes Digitales*, en la subserie G.700-G.799 correspondiente a *Equipos Terminales Digitales*, en el rango desde G.710 hasta G.729 que se los conoce como Codificación de voz y señales de audio, establece los codecs estandarizados para la codificación de señales de audio

y voz humana. En la Tabla 4 se enlistan todas las recomendaciones presentadas por este ente.

Tabla 4. Recomendaciones UIT-T codecs de voz.

Recomendación UIT-T	Año de última versión
G.711	1988
G.711.0	2009
G.711.1	2012
G.712	2001
G.718	2008
G.719	2008
G.720	1995
G.720.1	2010
G.722	2012
G.722.1	2005
G.722.2	2003
G.723.1	2006
G.724	1988
G.725	1988
G.726	1990
G.727	1990
G.728	2012
G.729	2012
G.729.1	2006

La UIT-T comparte públicamente las recomendaciones, a excepción de las que se encuentran en desarrollo por parte de los grupos de trabajo, son accesibles a través del portal web de la institución y pueden ser descargadas, varía su disponibilidad en varios idiomas. En el caso de usarse con fines de negocio, es requerido el pago de una licencia, estas recomendaciones son desarrolladas por lo general por personal de

investigación de universidades, en conjunto con fabricantes interesados en mejorar el desempeño de los codecs. Existen otras instituciones que norman codecs de voz o audio, como por ejemplo el *Instituto Europeo de Normas de Telecomunicaciones* (*ETSI*, del inglés *European Telecommunications Standards Institute*), el *Proyecto Asociación de Tercera Generación 2* (*3GPP2*, del inglés *3rd Generation Partnership Project 2*).

Según [26] los codecs más populares son: G.711, G.726, G.728, G.729, G723.1, iLBC.

La ITU-T, dentro de sus recomendaciones de la serie P, que corresponde a la calidad de transmisión telefónica, instalaciones telefónicas y redes locales, ha desarrollado la recomendación P.862 (02/2001) titulada: *Evaluación de la calidad vocal por percepción*: un método objetivo para la evaluación de la calidad vocal de extremo a extremo de redes telefónicas de banda estrecha y codecs vocales [27]. Esta recomendación describe un método objetivo conocido como *Evaluación de la Calidad Vocal por Percepción* (*PESQ*, del inglés *Perceptual Evaluation of Speech Quality*) que mide los efectos del ruido y la distorsión de voz unidireccionales sobre la calidad vocal, mientras que otros parámetros de degradación, como eco, retraso no son evaluados por este método [28]. Este es uno de tantos métodos que se han desarrollado para evaluar codecs de voz, se realizó un estudio que se presentó en una reunión del *Grupo de Trabajo de Ingeniería de Internet* (*IETF*, del inglés *Internet Engineering Task Force*) efectuada en Marzo del

año 2010, donde el fabricante Broadcom usó este parámetro de medición para realizar una comparación entre varios codecs de banda estrecha [29]. Existen otros modelos de medición, tantos objetivos como subjetivos, como por ejemplo: *Medición Perceptual de la calidad* de voz (*PSQM*, del inglés *Perceptual Speech Quality Measure*), *Sistema de Medición de Análisis Perceptual* (*PAMS*, del inglés *Perceptual Analysis Measurement System*), el modelo E, *Puntuación de la Opinión Media* (*MOS*, del inglés *Mean Opinion Score*).

Podemos inferir que es muy relativo concluir que algún códec es mejor que otro, es un proceso complejo de evaluación que se debe realizar con precaución estimando cada variable dentro del entorno único que se vaya ejecutar la aplicación y escogiendo el método de evaluación apropiado al contexto.

3.5 PROTOCOLOS DE SEÑALIZACIÓN

Los protocolos de señalización han tenido un desarrollo desde la época en la cual su uso único uso era en redes telefónicas basadas en conmutación de circuitos. En Internet se requiere de igual manera, realizar el control de las llamadas VoIP establecidas ya sea entre redes netamente IP o llamadas establecidas hacia usuarios tradicionales conectados a PSTN. El objetivo de la señalización se mantiene tal cual en una llamada convencional, el

establecimiento, control y liberación de las llamadas, en el caso de llamadas en tiempo real la supervisión de la habilitación o no de una aplicación en uso es realizada por la señalización. Al realizar una llamada por medio de Internet, entran nuevas funciones que deben ser cumplidas por los protocolos de señalización, son las siguientes:

- Traducción de nombres y ubicación del usuario.
- Establecimiento de la sesión.
- Negociación de la sesión.
- Gestión de los participantes de las llamadas.

Existen una gran cantidad de protocolos se señalización para la VoIP, tomamos en cuenta los establecidos por los entes regulatorios más comúnmente usados que son el *Protocolo de Inicio de Sesión* (*SIP*, del inglés *Session Initiation Protocol*), H.323 y el *Protocolo de Intercambio entre-Asterisk* (*IAX*, del inglés *Inter-Asterisk eXchange*).

SIP

En el año de 1996 la IETF creó el grupo de trabajo *Control de sesión multimedia y multiparticipante* (*MMUSIC*, del inglés *Multiparty Multimedia Session Control*), tres años posteriores, en 1999, fue establecido como estándar, como la recomendación RFC 2543, un protocolo que opera en el nivel de aplicación llamado SIP, finalmente el grupo de trabajo SIP en el año 2002 publicó el RFC 3261.

SIP heredó la estructura del *Protocolo de Transferencia de Hipertexto* (*HTTP*, del inglés *Hypertext Transfer Protocol*), utiliza conversaciones basadas en peticiones y respuestas en un esquema cliente-servidor, fue diseñado para ser independiente del protocolo asignado en el nivel de transporte, opera bajo UDP, TCP y el *Protocolo de Transporte de Control de Flujo* (*SCTP*, del inglés *Stream Control Transmission Protocol*) [30], aunque debido a su naturaleza de transmitir por medio de Internet, comúnmente utiliza UDP. Es capaz de establecer sesiones entre dos participantes, conferencias con múltiples participantes y hasta en modo de multidifusión, transmitiendo además de voz, datos y video, generando una comunicación completamente multimedia a través de Internet. SIP es un protocolo de señalización, de control, luego de haberse establecido la sesión, la transferencia de paquetes multimedia entre los participantes es responsabilidad del *Protocolo de Tiempo Real* (RTP, del inglés *Real-time Transport Protocol*).

SIP ayuda en 5 elementos funcionales para el establecimiento y terminación de comunicaciones multimedia [31]:

- Localización de usuarios.
- Disponibilidad de usuarios.
- Intercambio y negociación de capacidades de los terminales.
- Establecimiento de sesión.
- Mantenimiento de sesión.

Los componentes de la arquitectura SIP son los siguientes:

- *Agente*: pueden ser Agente de Usuario o Agente Servidor.
- *Servidor*: se clasifican dentro de cuatro tipos: Proxy, Redireccionador, Registrador y Localizador.
- *Gateway* (pasarela): es la interfaz hacia redes que utilizan diferentes protocolos de señalización.

Los equipos terminales en SIP son conocidos como *Agente de Usuario* (*UA*, del inglés *User Agent*), pueden tomar dos roles que son: Agente de Usuario Cliente y Agente de Usuario Servidor, las peticiones y respuestas se intercambian entre ellos, estos roles son temporales, en un escenario práctico un mismo terminal puede actuar como un agente de usuario cliente cuando emite una petición y luego cuando reciba una respuesta actúa como servidor. Las respuestas generadas en una comunicación SIP se encuentran codificadas según el formato utilizado en el protocolo HTTP versión 1.1, SIP añadió una nueva clase de respuestas, la familia 6xx correspondiente a fallas globales [32].

En una llamada, SIP utiliza para localizar al cliente o terminal un *Indicador Uniforme de Recursos* (*URI*, del inglés *Uniform Resource Indicators*), que puede ser un correo electrónico, un usuario, un número telefónico, o hasta un grupo dentro de una organización, deben contener la suficiente información como para iniciar y mantener la sesión establecida entre los recursos [31].

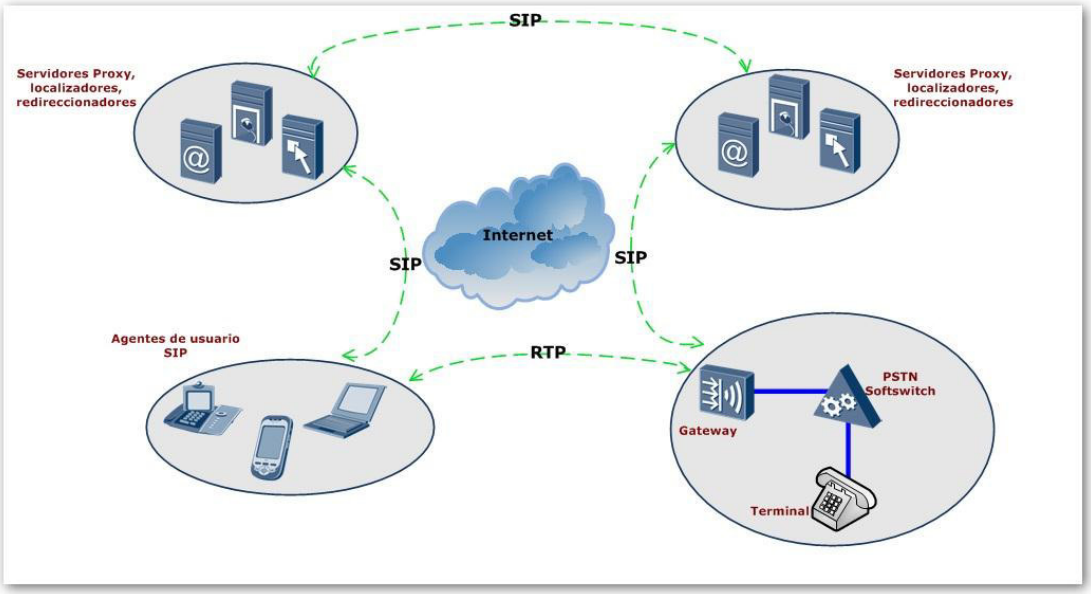


Figura 3.1. Arquitectura del protocolo SIP.

En la Figura 3.1 se muestran los flujos de la comunicación entre los distintos elementos que conforman la arquitectura SIP y su interacción con la PSTN.

H.323

La UIT es responsable de su desarrollo, las normalizaciones de la familia H corresponden a Sistemas Audiovisuales y Multimedia, el rango desde H.300 hasta H.349 norma los Sistemas y Equipos terminales para servicios audiovisuales, en el año de 1996 fue lanzada la primera versión del protocolo H.323 por la UIT, el nombre oficial de la recomendación es: Sistemas de comunicación multimedia basados en paquetes, la versión que se encuentra en vigor es la versión 6 aprobada en el año 2009 [33].

H.323 es una recomendación que establece una suite de protocolos y todos los componentes de un entorno H.323 que son usados para proveer comunicación de audio, opcionalmente datos y video, manteniendo una independencia de la topología de red usada, no es un protocolo de comunicación.

Los elementos que conforman un entorno H.323 son:

- *Terminal*: elemento final de red que permiten la comunicación en tiempo real. Deben soportar los siguientes protocolos de manera mandatoria *H.245*, *Q.931*, Registration Admission and Status (RAS) y RTP.
- *Pasarela*: está compuesta por *Controlador de Pasarelas de datos Multimedia* (*MGC*, del inglés *Media Gateway Controller*) o *Pasarelas de datos Multimedia* (*MG*, del inglés *Media Gateway*). El MGC se encarga de la señalización y el MG de la señales de audio, voz, video en el caso que aplique. Es la interfaz que realiza la traducción entre diferentes formatos de transmisión.
- *Gatekeeper*: administra el control de admisión y resolución de nombres, además de realizar control de ancho de banda. Es un elemento opcional.

- *Elemento de borde*: realiza funciones similares al gatekeeper, guarda la información de caminos de todos los gatekeepers pertenecientes a un dominio o zona administrativa específica.
- *Unidad de Control Multipunto* (*MCU*, del inglés *Multipoint Control Unit*): Ayudan a la gestión de las multiconferencias.

En la Figura 3.2 se muestra la arquitectura de protocolos y recomendaciones establecidos bajo esta recomendación.

En la Figura 3.3 se adjunta la estructura básica de la recomendación H.323, se puede apreciar los terminales son los puntos finales de red que permiten comunicaciones simultáneas, H.323 permite la interacción entre PSTN y las redes basadas en conmutación de paquetes, gracias al elemento Gateway que realiza la "traducción" para el establecimiento y mantenimiento de la llamada, se aprecian los demás elementos que conforman el entorno H.323.

<table>
<tr><td colspan="9">Aplicaciones Multimedia, Interfaz de usuario.</td></tr>
<tr><td colspan="3">Aplicaciones de Datos</td><td colspan="3">Control del Medio</td><td colspan="3">Control del terminal y gestión</td></tr>
<tr><td>V.150</td><td>T.120</td><td>T.38</td><td>Audio Codecs G.711 G.723.1 G.729</td><td>Video Codecs H.261 H.263 H.264</td><td>RTCP</td><td>H.225.0 Call Signalling</td><td>H.245</td><td>H.225.0 RAS</td></tr>
<tr><td>UDP</td><td>TCP</td><td>TCP/UDP</td><td colspan="3">UDP</td><td>TCP/UDP</td><td>TCP</td><td>UDP</td></tr>
<tr><td colspan="9">IP</td></tr>
</table>

Figura 3.2. Pila de protocolos de la recomendación UIT-T H.323.

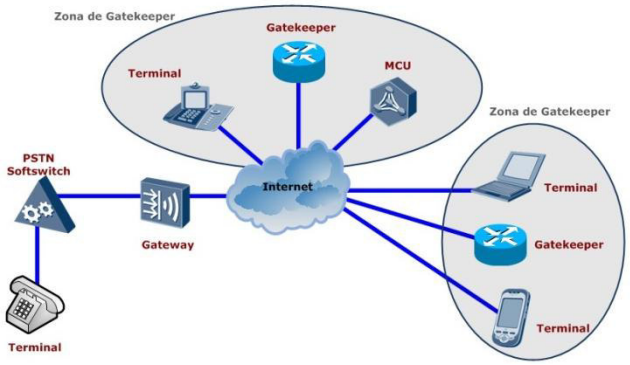


Figura 3.3. Estructura de la recomendación H.323.

IAX

Protocolo binario de código abierto más conocido como IAX2, el cual fue desarrollado por la comunidad Digium. Se puede encontrar un detalle de sus características y funcionalidades en el RFC 5456 [34], establecido desde el año 2010, a pesar de que no sea considerado un estándar, el objetivo de la publicación es netamente informativa. El aplicativo Asterisk, el cual es un *Central Telefónica Privada* (*PBX*, del inglés *Private Branch eXchange*) soporta de origen este protocolo.

IAX2 es útil para establecer una comunicación entre servidor-servidor o cliente-servidor; es considerado un protocolo robusto y de mejor rendimiento. A pesar de su utilidad para cualquier tipo de tráfico multimedia, su diseño contempla un mayor desempeño y menor uso de ancho de banda [35]. Utiliza el puerto 4569 para el transporte de los datos de voz y la señalización, a diferencia de SIP, esto permite un mejor control para administradores de red

y mejor funcionalidad sobre redes cortafuegos (*firewall*) o *Network Address Translation* (*NAT*) habilitado.

Para comprender la estructura de IAX2 y su funcionamiento, se deben conocer los tipos de mensajes disponibles para el intercambio de información. Cada mensaje está clasificado en base a la unidad básica utilizada denominada *frame* (cuadro), entre ellos tenemos los:

- *Full Frame*: utilizados para el envío de información de señalización y control de manera confiable, es decir el terminal transmisor del mensaje espera recibir un acuse de recibo confirmando la recepción del Full frame enviado.
- *Mini Frame*: transportan los paquetes de voz de manera no confiable cuando una llamada está establecida. Este tipo de mensaje tiene este nombre por el tamaño de su cabecera el cual es de 4 B de longitud a diferencia de un Full frame que es de 12 B.
- *Meta Frame*: mensajes más robustos y clasificados en dos tipos en base a su propósito: *Meta Video Frame* (transporte de video de forma similar que los Mini Frame) y Meta Trunk frame (útiles para condensar en un mismo frame varios flujos de datos para el envío de información entre servidores de una troncal).

3.6 RTP y RTCP

Son protocolos estándares descritos en el RFC 3550 expedido por la IETF. RTP, es el protocolo encargado de la transferencia de información en tiempo real sobre redes poco confiables como Internet. *Protocolo de Control de Transporte en Tiempo Real* (*RTCP*, del inglés *Real-time Transfer Control Protocol*) se encarga de verificar la QoS de los datos que son enviados por el RTP, es decir monitorea los parámetros de envío de paquetes. Ambos esquemas trabajan de forma paralela sobre la red, utilizan puertos contiguos en el rango del 1025 al 65535, por defecto los puertos 5004 y 5005 son los activados a menos que el usuario final cambie tal definición, además se desenvuelven en ambientes unidifusión (*unicast*) y muldidifusión (*multicast*) sin inconvenientes [36].

La versatilidad y adaptabilidad de estos protocolos han determinado su crecimiento y expansión hacia nuevas aplicaciones y desarrollos de todo tipo. En su concepción se maneja un esquema abierto, de tal forma que se pueda ir adaptando a las necesidades del desarrollador y el objetivo de la aplicación final.

El formato fijo del encabezado establecido para RTP es el descrito en la figura 3.4, el cual está compuesto por la versión del RTP utilizada (V), bits banderas como las utilizada en el campo relleno (P), extensión del encabezado (X) o el marcador (M) que indica eventos de interés. El contador

de orígenes o fuentes participantes (CC) trabaja directamente con el campo CSRC y están activados cuando funcionan un mezclador intermedio, esto es, se recibe un flujo desde varios fuentes y se genera una sola salida.

El campo que determina el tipo de dato a transportar por RTP es el tipo de carga útil (*PT*, del inglés *Payload Type*). En la tabla 5 se registran los tipos definidos en el estándar RFC 1890. El número de secuencia y la marca de tiempo son campos que llevan casi todos los tipos de paquetes, el primero determina el orden de llegada al destino y el segundo el sello de tiempo colocado por el terminal origen del paquete.

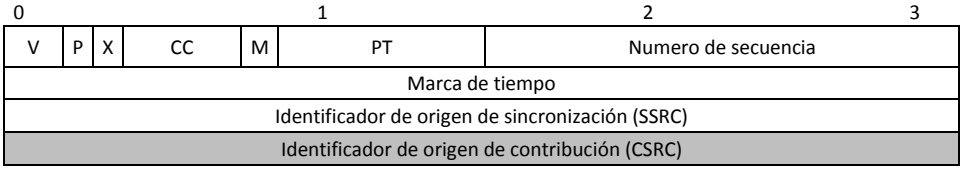


Figura 3.4. Formato del paquete RTP.

Tabla 5. Tipos de carga útil

PT	Codificación	Audio/Video (A/V)	Clock Rate (Hz)	Canales (audio)
0	PCMU	A	8000	1
1	1016	A	8000	1
2	G721	A	8000	1
3	GSM	A	8000	1
4	unassigned	A	8000	1
5	DVI4	A	8000	1
6	DVI4	A	16000	1
7	LPC	A	8000	1
8	PCMA	A	8000	1
9	G722	A	8000	1
10	L16	A	44100	2
11	L16	A	44100	1
12	unassigned	A		
13	unassigned	A		
14	MPA	A	90000	(see text)
15	G728	A	8000	1
16--23	unassigned	A		
24	unassigned	V		
25	CelB	V	90000	
26	JPEG	V	90000	
27	unassigned	V		
28	nv	V	90000	
29	unassigned	V		
30	unassigned	V		
31	H261	V	90000	
32	MPV	V	90000	
33	MP2T	AV	90000	
34--71	unassigned	?		
72--76	reserved	N/A	N/A	N/A
77--95	unassigned	?		
96--127	dynamic	?		

El RTCP no transporta ningún tipo de dato, únicamente información de control, estadísticas o compendio del estado de la red y la calidad del servicio, esa es su función principal. Adicionalmente es empleado para el registro de los nombres canónicos de las fuentes que pueden ser perdidos

por los receptores por alguna falla o novedad en el sistema o red, notifica el número de participantes en el flujo de datos y/o información adicional de los participantes. A nivel de formato de los paquetes, tenemos cinco tipos de paquetes de control que detallaremos a continuación:

- *Informe del remitente* (*SR*, del inglés *Sender Report*).
- *Informe del receptor* (*RR*, del inglés *Receiver Report*).
- *Paquete de descripción de la fuente* (*SDES*, del inglés *Source Description*).
- BYE.
- Definidas por la *aplicación* (*APP*, del inglés *Application*).

El formato de cada uno de los tipos de paquetes está definido en [37].

A nivel de seguridad podemos encontrar el RFC 3711 [38] denominado *Protocolo de Transporte Seguro en Tiempo Real* (*SRTP*, del inglés *Secure Real-time Transport Protocol*), el cual es una extensión del perfil definido en el RFC 3551 que aporta confidencialidad a la carga útil de los paquetes RTP y RTCP e integridad a ambos de forma completa, trabajando tanto en ambientes unicast como multicast sin incrementar costo computacionales, consumo de ancho de banda y adaptable a mejoras futuras independiente de los niveles inferiores del modelo OSI. Según un estudio de la Universidad de Slovak de Tecnología se registra que el impacto de la aplicación de SRTP sobre la calidad de llamadas en mínimo [39].

El SRTP aumenta en el formato convencional de RTP dos campos que permiten agregar aspectos seguros, estos son el *Identificador Clave Master* (*MKI*, del inglés *Master Key Identifier*) y la etiqueta de autenticación. Este perfil puede ser utilizado con ambas características deshabilitadas, únicamente es mandatorio la autenticación en paquetes RCTP.

Otro concepto relevante que maneja RTP en su funcionamiento son los traductores y mezcladores, conocidos como "sistemas intermedios" que permiten la interacción entre dos escenarios diferentes en los niveles del modelo OSI y que no limitan al protocolo en su funcionamiento. Por ejemplo, el envío de paquetes IPv4 hacia destinos IPv6 necesita de un sistema que conozca varios idiomas y sea interlocutor entre ambos, a estos sistemas se los denomina traductores. En el caso de conferencias con participantes que gozan de un ancho de banda holgado para manejo de audio y video y participantes enganchados remotamente por una línea telefónica, necesitan un sistema que permita acoplarse a ambos participantes, se les denomina mezcladores. Los traductores no alteran la composición del paquete en su mayoría, el flujo de entrada es enviado a la salida con algunas pequeñas actualizaciones como la codificación o la marca de tiempo, a diferencia de los mezcladores los cuales reciben varios flujos de entrada y crean un propio flujo de salida actualizando los parámetros de origen y el campo CC y CSRC para no perder el rastro de los contribuyentes del flujo. Se muestra el formato del paquete RTP en la figura 3.5.

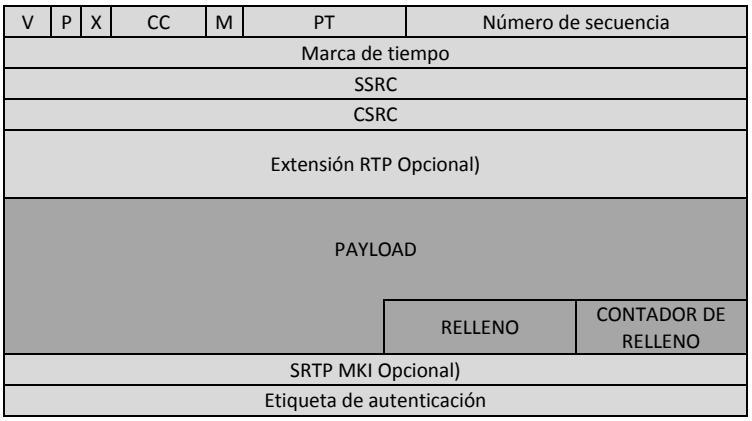


Figura 3.5. Formato de paquete RTP.

3.7 Tecnologías comerciales para VoIP

En este apartado se describen algunos modelos tomados comercialmente para el desarrollo de aplicaciones VoIP.

3.7.1 Modelo Servidor-cliente

La arquitectura cliente-servidor es un esquema que permite especializar al hardware y/o software en las tareas asignadas con mayor eficacia y eficiencia logrando un despliegue más ágil a la hora de mantenimientos y/o actualizaciones. Se pueden utilizar un matiz de formas sobre esta arquitectura hasta encontrar el equilibrio deseado entre los dos componentes cliente y servidor, es decir proyectar un equipo robusto con altas capacidades de almacenamiento y procesamiento de datos como servidor y limitar al cliente a ser la interfaz gráfica amigable hacia el usuario final o

podemos visualizar una aplicación cliente más robusta que maneja la lógica de la presentación, aplicación y el servidor sea el repositorio de datos. El equilibrio y alcance de cada componente lo determina la lógica del negocio que deseamos aplicar.

El cliente es la entidad física o lógica destinada a interactuar directamente con el usuario, su interfaz permite recoger los requerimientos del cliente, validarlos superficialmente, procesarlos y realizar los requerimientos necesarios al servidor, obtener los datos resultantes y presentarlos de forma comprensible para el usuario final. El servidor es la entidad física o lógica destinada a interactuar con múltiples clientes de forma simultánea quienes envían sus requisitos, estos los procesan, los validan, verifican permisos y emiten los resultados en formato científico, son quienes almacenan la información, registran los cambios, actualizan la base de datos, mantienen los perfiles y los permisos por cada uno de ellos.

En VoIP podemos encontrar fácilmente el despliegue de esta arquitectura. Existen servidores centralizados separados geográficamente con millones de usuarios en todo el Mundo como por ejemplo tenemos a Skype, un software privado, el cual utiliza este esquema para autenticación y manejo de perfiles de usuarios. La aplicación cliente es ejecutada por el usuario final, al generar una llamada se dispara una petición TCP a servidores de autenticación registrados alrededor del mundo y los cuales autorizan o deniegan dicha llamada de acuerdo al perfil de cada usuario. A nivel de código abierto

tenemos a Asterisk y su interfaz gráfica Trixbox, el cual nos permite integrar como clientes a softphone o equipos que hablen protocolos estándar desarrollados de forma independiente. Esta es una de las ventajas del esquema cliente servidor, es independiente de la plataforma que ejecuta en cada uno permitiendo abaratar costos, gran despliegue de la red y los servicios a ofrecer.

3.7.2 Asterisk (Trixbox)

Asterisk es una plataforma de telefonía de código abierto originario de Linux que actúa como un PBX orientado a medianas y grandes empresas. Fue desarrollada por Mark Spencer en 1999 la cual tuvo una gran acogida en el mercado dado que las soluciones de telefonía propietarias de aquella época eran altamente costosas e implicaba comprar toda la línea de productos compatibles. Cuando apareció Asterisk vieron una gran oportunidad en el desarrollo y fortalecimiento de la aplicación, atrajo comunidades de desarrolladores para ampliar sus funcionalidades y corregir errores de codificación, además fabricantes de software se alinearon a la metodología de Asterisk para desarrollar aplicaciones compatibles con dicha aplicación.

Este PBX maneja la arquitectura cliente-servidor siendo Asterisk la plataforma servidor que permite las conexiones de diversos tipos de terminales, privados o de código abierto, que utilizan los códecs y protocolos

habilitados como son IAX2, SIP, H323, MGCP y a nivel de códecs tenemos a G711a, G711u, G729, GSM, entre otros. La gama es amplia dando plena libertad al usuario final escogerla bajo sus propios gustos y necesidades.

Otra de sus principales funcionalidades es la interacción con las demás tecnologías existente como por ejemplo, mediante el uso de tarjetería adicional se puede conectar a la PSTN tradicional, establecer enlaces con tecnología de *Interfaces de Servicio Básico* (*BRI*, del inglés *Basic Rate Interface*), e *Interfaces de Servicio Primario* (*PRI*, del inglés *Primary Rate Interface*), enganchar líneas analógicas, permitiendo interactuar y adaptarse sin ningún inconveniente a la infraestructura existente o a las limitaciones o necesidades del negocio. Asterisk actúa como puerta de enlace de los terminales conectados permitiendo la salida hacia la red conmutada local pero adicionalmente gozar de todas las funcionalidades adicionales que provee VoIP. Actualmente está siendo portado a sistemas operativos de Windows y Mac OS.

La ingeniería de Asterisk es modular, está compuesto por diferentes módulos con funcionalidades específicas, entre estas tenemos:

- *Grabación detallada de las llamadas* (*CDR*, del inglés *Call Detail Recording*).
- *Registros de eventos del canal* (*CEL*, del inglés *Channel Event Logging*).

- Drivers de canales.
- Traductores de codecs.
- Intérpretes de formato.
- Funciones del Plan de Marcado.
- Módulos de sonidos, ADDONS.

En el libro Asterisk: The Definitive Guide podemos encontrar el manual paso a paso para la instalación y configuración de la central telefónica para todo tipo de necesidades. Según estudios realizados en [40] [41] se verifica el comportamiento de Asterisk y su rendimiento en medianas y fácil adaptación al negocio a nivel de medianas y grandes empresas.

3.8 CARACTERÍSTICAS Y LIMITACIONES DE LA VOIP EN WIFI AD HOC

Como se mencionó anteriormente, la VoIP es un método de enviar paquetes de voz sobre redes de datos en tiempo real y dado que todo sistema en tiempo real exige limites estrechos a parámetros tales como latencia, jitter, pérdida de paquetes y genera un considerable consumo de ancho de banda con el objetivo de brindar un resultado satisfactorio a la experiencia del usuario final. Proveer QoS sobre redes Ad Hoc es una tarea compleja por las características propias de esta tecnología. Los modelos tradicionales no generan el resultado deseado porque se debe considerar además de los parámetros antes mencionados, otras variables como la densidad de

terminales, la movilidad constante de cada uno de ellos, la capacidad de procesamiento y almacenamiento, el ancho de banda limitado, el consumo de energía y el desenvolvimiento autónomo de los terminales, esto es, no contar con una administración centralizada. Estos factores generan más variables independientes dentro de un análisis de calidad de servicio. Las redes WiFi Ad Hoc, heredan las limitaciones de una red WiFi añadiendo la movilidad y dinamismo característico de las redes Ad Hoc.

Para redes Ad Hoc, el protocolo de encaminamiento utilizado influye directamente en el tiempo de llegada de los paquetes a su destino. Para protocolos de encaminamiento reactivo, el descubrimiento de terminales y vecindades necesarias para generar una tabla de rutas inicia cuando el terminal requiere enviar un paquete, de esta manera conserva los recursos de la red y del dispositivo, pero de forma contraria, es alto el impacto en el tiempo de respuesta con respecto a los demás tipo de protocolos disponibles. Un protocolo proactivo genera de forma anticipada la tabla de encaminamiento y mantiene contacto constante con los terminales vecinos disminuyendo el tiempo de respuesta para la llegada de un paquete a su destino pero de igual forma, genera un impacto en la conservación de los recursos. Según el estudio realizado [42], el protocolo de encaminamiento proactivo denominado OLSR denota un mejor rendimiento a nivel de tiempo de llegada de paquetes probado desde diferentes escenarios y utilizando diversos codecs. Además podemos revisar las pruebas realizadas en [43]

entre los protocolos denominados reactivos, *Vector Distancia Bajo Demanda Ad Hoc* (*AODV*, del inglés *Ad hoc On-Demand Distance Vector*) y *Vector Distancia de Destino Secuenciado* (*DSDV*, del inglés *Destination-Sequenced Distance Vector*), más un protocolo proactivo, OLSR, se comparan los comportamientos de cada uno en diversos escenarios de pruebas y se concluye que mientras menor sea el número de saltos entre origen y destino, aumenta la calidad de servicio provista por los distintos protocolos pero a diferentes escalas, esta conclusión está respaldada por el estudio realizado en [44]. El número de saltos está íntimamente ligado al retraso entre paquetes.

A nivel de paquetes perdidos, se observa que a mayor densidad de terminales, disminuye el porcentaje de paquetes perdidos; esto es fácilmente deducibles dado que la probabilidad de encontrar un camino viable hacia un destino en particular sin provocar interrupción es mayor cuando existe mayor vecindad y cooperación entre terminales.

Dado que las redes Ad Hoc están sujetas a la disponibilidad de terminales cercanos para establecer una red de forma dinámica, esto limita el ancho de banda disponible, el tiempo de presencia de un terminal, el protocolo de encaminamiento capaz de soportar los constantes cambios del entorno, por lo que la transferencia de voz se vuelve vulnerable a todos los constantes cambios que está sujeta la red.

CAPÍTULO 4

4. ANÁLISIS DE CAMPO

En este capítulo damos a conocer los detalles de la implementación del escenario, que tuvo como propósito la ejecución de pruebas de diagnóstico de varios parámetros de QoS, donde se efectuaron mediciones antes y durante la realización de llamadas VoIP. También se especifica las herramientas utilizadas, características del hardware, software y demás.

4.1 ESCENARIO DE TRABAJO

El escenario fue constituido por 2 terminales, que establecieron una comunicación IBSS, es decir, en modo Ad Hoc utilizando el estándar IEEE 802.11. Los terminales fueron dos laptops: un computador marca Hp ProBook 4440s y una portátil marca Samsung NP470RSE-K01UB.

Se buscó un lugar que cuente con nula densidad de redes WiFi, se identificó en primera instancia a las afueras de la ciudad, las canchas de uso múltiple del complejo deportivo de la *Escuela Superior Politécnica del Litoral*

(*ESPOL*), sus coordenadas son 2°09'13.4" Latitud Sur y 79°57'34.3" Longitud Oeste (-2.153715, -79.959539), pero se notó que la incidencia de redes inalámbricas en las frecuencia de 2.4GHz no era la deseada, por lo que se amplió la búsqueda a lugares más remotos dentro de la ciudad de Guayaquil, localizando el lugar ideal para las mediciones en las instalaciones del Parque Lago, parque público administrado por la Empresa Pública de Parques Urbanos y Espacios Públicos, sus coordenadas son: (-2.2258477, -80.0964494), en el área de parqueadero se detectó una incidencia nula de redes inalámbricas que usen las frecuencias que usa el estándar IEEE 802.11.

Las pruebas se realizaron en horas de la mañana, desde las 09h00 hasta las 17h00, con clima soleado y nublado, con una temperatura promedio de 29ºC, durante varios días debido a la gran cantidad de muestras tomadas.

En la laptop Samsung, se virtualizó un servidor Asterisk, era necesario que el servidor tenga conectividad IP, la tarjeta de red de la máquina virtual fue configurada en modo bridge con el objetivo de extender la red local y que se encuentre en la misma red LAN que la laptop, en este mismo equipo se levantó un softphone que tenía asignado una de las 2 extensiones configuradas sobre el servidor, ambas extensiones trabajaron sobre el protocolo SIP. La otra extensión fue configurada en un softphone que se encontraba instalado en la laptop marca HP.

A continuación se expone el direccionamiento IP utilizado en las laptops en el escenario, se utilizó direccionamiento IP versión 4, estático, privado, clase C.

En la laptop Samsung fue creada una red inalámbrica en modo Ad Hoc utilizando el estándar IEEE 802.11, se usó el SSID “Ad Hoc Tesis”. La laptop HP establecía la conexión hacia esta red. Se usó el protocolo de cifrado *Privacidad Equivalente a Cableado* (*WEP*, del inglés *Wired Equivalent Privacy*).

Durante las pruebas se deshabilitó el firewall del antivirus de cada laptop, además del firewall que viene por defecto en el sistema operativo Windows, los usuarios de ambos terminales poseían el rol de administrador.

Las configuraciones de las extensiones en el servidor fueron realizadas de tal manera de que el flujo RTP sea establecido entre los agentes de usuario sin necesidad de que se transmita o direccione a través del servidor, tal como se aprecia en la figura 4.1, por defecto el tráfico RTP se realiza a través del servidor SIP, gracias a este cambio los flujos RTP entre las extensiones fluctuaron por medio de la conexión inalámbrica en modo Ad Hoc establecida.

Tabla 6. Direccionamiento red Ad Hoc.

Terminal	Dirección IP	Máscara de red	Extensión SIP
Servidor Asterisk	192.168.1.100	255.255.255.0	N/A
Laptop Samsung	192.168.1.101	255.255.255.0	101
Laptop HP	192.168.1.102	255.255.255.0	102

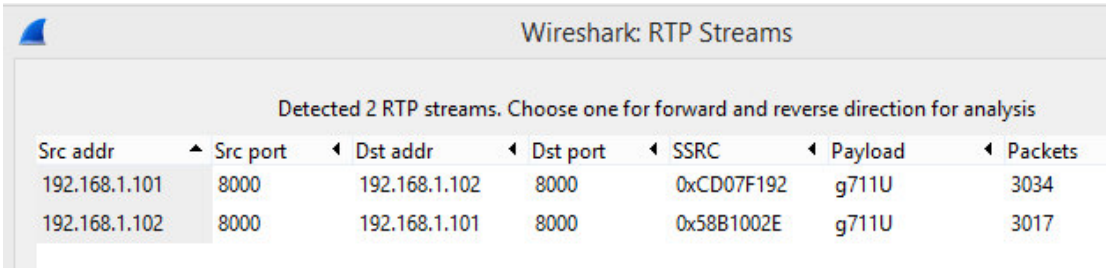


Figura 4.1. Flujos RTP entre los agentes de usuario.

En cada laptop se instaló un softphone y se ejecutaron llamadas de voz entre las extensiones, la marcación fue realizada desde la extensión 102 hacia la extensión 101, al establecerse la llamada se reprodujo un archivo de audio en formato *WAV*, que contenía una conversación entre dos personas, se configuró el software reproductor de audio en modo repetición de forma que el archivo *.wav* fuera reproducido de manera cíclica, la duración del archivo de audio fue de 53 segundos, la llamada se mantuvo establecida por 60 segundos en promedio. El códec negociado entre ambos terminales fue el G.711, tipo *u-law* en todos los casos.

Mientras estuvo establecida la llamada fueron ejecutados varios programas con el objetivo de registrar el comportamiento de ciertos parámetros de QoS y poder modelar una relación entre ellos. Las laptops fueron colocadas inicialmente a una distancia de 1 m, se encontraban sobre una superficie plana a una altura de 45 cm del nivel del suelo de concreto, la distancia de separación entre las laptops fue aumentando en intervalos de un metro hasta llegar a 30 m, en cada intervalo se realizaron tres mediciones, con el fin de

establecer un promedio para cada distancia. Para aplicaciones Ad Hoc la distancia máxima que tomamos es suficiente, luego de cada movimiento de terminal se ejecutaba la desconexión de la red y la conexión en cada distancia de medición. El lugar donde se ejecutaron las pruebas se encontraba sin cubierta y en campo libre para evitar el efecto rebote de la señal inalámbrica Ad Hoc que se transmitió.

El terminal móvil fue la laptop HP, el terminal Samsung se mantuvo fijo, la llamada y las mediciones no se realizaron inmediatamente después de haber movido el terminal, esperamos alrededor de 30 segundos para realizar la llamada. Mediante el software Acrylic Wi-Fi Professional en la laptop HP se tomaron los paquetes beacon del protocolo IEEE 802.11, los cuales fueron analizados con el fin de obtener datos requeridos como SNR, RSSI, cantidad de señales que compartían el mismo canal que ocupaba la señal en estudio.

En referencia a la energía, ambos computadores portátiles funcionaron con la energía provista por la batería, y con toma de corriente continua.

En la figura 4.2 se muestra el esquema del escenario implementado.

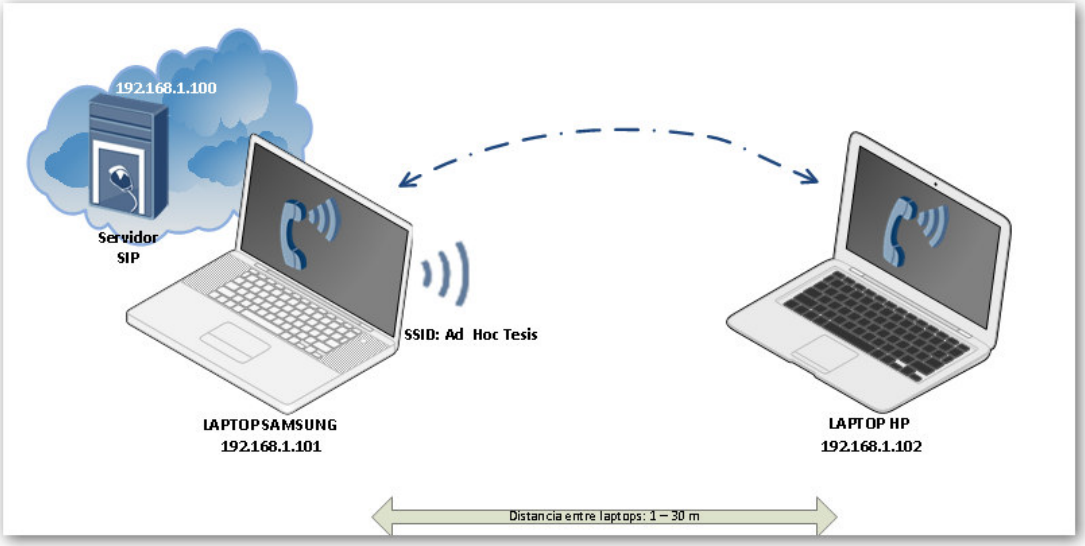


Figura 4.2. Esquema de conexión.

Se realizó exactamente el mismo estudio, con las mismas herramientas y software, en un ambiente con interferencia, en este lugar no teníamos control de las señales que ofrecían interferencia, el lugar escogido fue el parque principal de la Ciudadela Ceibos Norte, lugar netamente residencial. Las mediciones fueron realizadas en horas de la noche, con una temperatura cercana a los 25 grados centígrados, con clima despejado. En cada distancia fueron tomadas 3 muestras de las variables con el fin de obtener el promedio por cada distancia entre los ordenadores.

En el desarrollo del capítulo se detallan los valores tomados, los parámetros de calidad medidos.

Los detalles serán profundizados en los siguientes apartados.

4.2 HERRAMIENTAS UTILIZADAS

Las herramientas utilizadas para la ejecución de las pruebas y para la medición de los parámetros de QoS están divididas en tangibles e intangibles, dentro de los tangibles se encuentra el hardware y los intangibles fueron programas, aplicaciones que se instalaron en ambos computadores utilizados para el escenario.

4.1.1 Hardware

Esta sección consiste básicamente en el detalle del hardware usado en los terminales que sirven de usuario. Los terminales elegidos fueron laptops, a continuación detallamos las características de ambas laptops utilizadas durante las pruebas.

Las características principales de la laptop HP, modelo ProBook 4440s las compartimos en la Tabla 7.

Las especificaciones técnicas de la tarjeta inalámbrica propia de la laptop HP las indicamos en la Tabla 8, el modelo es AR9485 del fabricante Atheros, desde el año 2011 Atheros fue comprado por Qualcomm.

Tabla 7. Características de Hardware de laptop HP ProBook 4440s.

Procesador	Intel® Core™ i5-3210M CPU 2.50GHz
Memoria RAM	4 GB

La dirección MAC de la tarjeta AR9485 instalada en la Laptop es 74E5.434D.2202.

La segunda laptop marca Samsung, modelo NP470RSE-K01UB tiene las características que se muestran en la Tabla 9.

Este computador tiene integrada una tarjeta inalámbrica, marca Intel Centrino, modelo Advanced-N 6235, cuyas características se muestran detalladas en la tabla 10.

Tabla 8. Características de tarjeta Atheros AR9485.

ATHEROS AR9485	
Operación	Opera en la frecuencia 2400 MHz
Soporte para Estándares	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, 802.11d, 802.11g
Velocidad de Señal	11n: Hasta 150Mbps (dinámico) 11g: hasta 54Mbps (dinámico) 11b: hasta 11Mbps (dinámico)
Modulación	OFDM with BPSK, QPSK, 16 QAM, 64 QAM; DBPSK, DQPSK, CCK
Modos Inalámbricos	Infraestructura, Ad Hoc
Seguridad Inalámbrica	Compatible con AES, TKIP, WEP
Tecnología de Modulación	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM

Tabla 9. Características de Samsung NP470RSE-K01UB.

Procesador	Intel® Core™ i5-3230 CPU 2.60GHz
Memoria RAM	6 GB

Tabla 10. Tarjeta Intel Centrino, modelo Advanced-N 6235.

Intel® Centrino® Advanced-N 6235	
Operación	Opera en las frecuencias 2.4Ghz y 5Ghz.
Rendimiento	300Mbps de velocidad con doble flujo.
Diversidad	Sistema diseñado con dos antenas
Sistemas Operativos	Microsoft Windows 7,8 y Linux
Wi-Fi Alliance	Wi-Fi certificado para 802.11a, 802.11b, 802.11g, 802.11n, WMM, WPA2 y WPS.
Soporte para Estándares	802.11a, 802.11b, 802.11g, 802.11n, 802.11d, 802.11e, 802.11i, 802.11h
Modos Inalámbricos	Modo infraestructura y SoftAP, Ad Hoc
Autenticación	WPA and WPA2, 802.1X (EAP-TLS, TTLS, PEAP, LEAP, EAP-FAST), EAP-SIM, EAP-AKA
Protocolo de autenticación	PAP, CHAP, TLS, GTC, MS-CHAP*, MS-CHAPv2
Cifrado	64-bit and 128-bit WEP, AES-CCMP, TKIP

La dirección MAC de la tarjeta Intel instalada en el computador Samsung es B4B6.76B9.52F3.

4.1.2 Software

A continuación describimos los programas utilizados y las configuraciones aplicadas para el establecimiento del escenario, posteriormente serán descritos los programas usados para las mediciones de los parámetros de QoS.

Virtualbox

Software de virtualización disponible en su versión 4.2.12 r84980, fue instalado en la laptop Samsung con el objetivo de virtualizar el servidor Trixbox que explicamos más adelante. El procedimiento de instalación se encuentra descrito en el Anexo A.4.

La máquina virtual levantada requiere tener total conectividad hacia la laptop Samsung para poder establecer la comunicación hacia el servidor, en pro de lograr esto se habilitó el adaptador de red inalámbrico en modo puente, con esto se logra expandir la red LAN establecida en la tarjeta de red de laptop Samsung, para las demás configuraciones se tomaron los parámetros por defecto.

Trixbox

Es una distribución del sistema operativo Linux utilizado como sistema telefónico VOIP basado en la PBX Asterisk, hemos usado su Edición de Comunidad (CE, del inglés Community Edition) versión 2.8.0.4, en la máquina virtual fue establecido como disco de arranque la imagen del sistema operativo Trixbox. El proceso de instalación se encuentra detallado en el Anexo A.5.

Por defecto el servidor viene por defecto configurado una dirección IP, clase A. En el servidor se realizó la configuración de la dirección IP estática,

modificando el archivo *ifcfg-eth0,* ubicado en la ruta /etc/sysconfig/network-scripts, fue asignada la dirección IP 192.168.1.100, con máscara de red 255.255.255.0, al ejecutar este proceso es requerido el reinicio del servicio de red del servidor, mediante el comando *service network restart*. La configuración de las extensiones fue realizada ingresando por medio de un navegador de internet hacia el siguiente url: http://192.168.1.100/admin, se asignó la extensión 101 a la laptop Samsung y la extensión 102 a la laptop HP. Se configuraron dos extensiones SIP, las configuraciones fueron realizadas de modo que el tráfico RTP sea establecido entre los agentes de usuario sin necesidad de que llegue a través del servidor, esto se realizó cambiando el parámetro *canreinvite* a *yes* en cada una de las extensiones. Tomar en cuenta que es posible realizar esta configuración dado que en el escenario no tenemos la limitante de tener alguna extensión detrás de una dirección IP nateada, todas pertenecen a la misma red local, el parámetro *nat* fue configurado en *no*, adicionalmente en el parámetro *dtmfmode* fue configurado con el valor *info* en ambas extensiones, los valores de los demás parámetros de configuración fueron tomados por defecto.

Zoiper

Cliente VoIP multiplataforma, en su versión 3.9.32144 se puede configurar como cliente SIP, IAX o XMPP. Las instrucciones para la instalación se encuentran descritas en el Anexo A.6.

Para nuestro objetivo fue usado como cliente SIP, toda la configuración por defecto fue utilizada, el puerto SIP usado por esta aplicación fue el 5060, mientras que para el RTP fue usado el 8000. En las opciones de audio fue configurado para que la entrada de audio sea el sistema de mezcla estéreo propio de Windows, desactivando el micrófono externo de las laptops, el objetivo es que el archivo de audio reproducido sea tomado como entrada de audio y sea constante en todas las pruebas realizadas.

A continuación se detallan los programas utilizados para la medición de los diferentes parámetros de VoIP y QoS.

Iperf

Iperf es un programa desarrollado con el objetivo de realizar mediciones de rendimiento de ancho de banda utilizando en el nivel de transporte ya sea el protocolo TCP o UDP. Se han desarrollado otros programas en base al iperf, como son el jperf y el kperf, que tiene una interfaz más amigable con el usuario [45]. El manual de instalación de Iperf se encuentra en el Anexo A.2.

En este trabajo hemos utilizado la versión 3.0.11, con el objetivo de medir la capacidad del volumen de información neto que se puede transmitir por medio del enlace Ad Hoc establecido entre ambas laptops. Esta medición se la realizó luego de establecer el enlace en cada distancia, antes de ejecutar la llamada entre softphones. El listado de las opciones para la línea de comando a ejecutar está disponible en la página oficial del programa [45], a

continuación se especificarán las opciones usadas en las mediciones realizadas en esta Tesis.

Se ejecutaron dos órdenes, la laptop Samsung fungió de servidor iperf, mientras que la laptop HP de cliente iperf; para mayor facilidad en el cliente iperf se configuró una ventana de línea comando con el fin de que ejecute el aplicativo *iperf* con el siguiente comando en el campo “Destino”:

C:\Windows\System32\cmd.exe /k iperf3.exe -c 192.168.1.101 -u -p 5001 -i 1 -V -b 54M -t 60 -O 1 -R > D:\iperfdemoPL.wordpad

Mientras que en el campo “Iniciar en:” se coloca la ruta donde se almacena el archivo .exe del iperf. A continuación en la figura 4.3 se muestra como se configuró la ventana de línea de comando usada en el cliente iperf

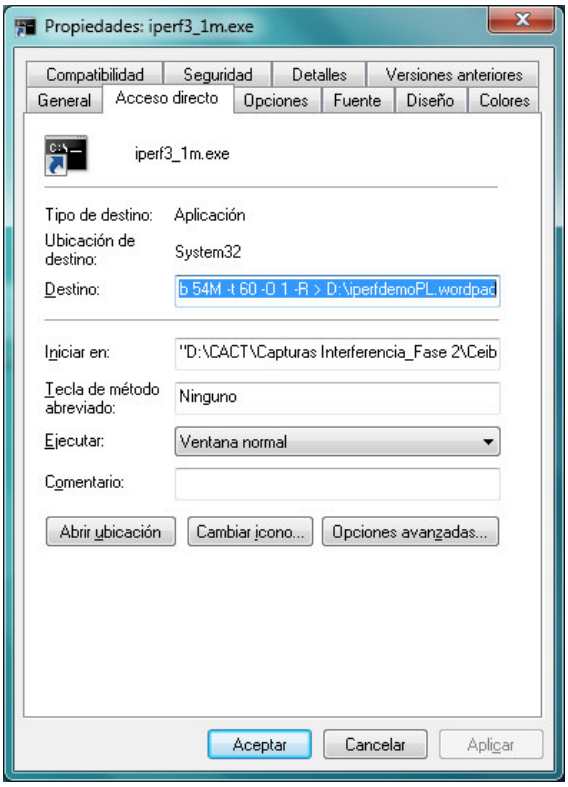


Figura 4.3. CMD Windows customizado.

A continuación se muestra el comando utilizado en el servidor iperf.

Servidor:

iperf – s –i 0 –V –p 5001

A continuación se describe cada opción ejecutada en cliente y servidor:

- -s: ejecución en modo servidor.
- -i: configura el intervalo periódico de tiempo en segundos para el reporte de jitter, ancho de banda.
- -p: el puerto que escucha el servidor, por defecto es el 5001.
- -c: ejecución en modo cliente (orden ejecutada en cliente).

- -b: ancho de banda UDP a enviar, en bps.
- -t: tiempo en segundos a transmitir.
- -V: modo verbose, para una salida de comando con más detalles.
- -O: Omite los primeros n segundos.
- -R: Ejecuta en modo reversa, (servidor envía, cliente recibe).

La ejecución tomó 60 segundos en cada prueba, al transcurrir este período se generó un reporte sumarizado de los parámetros medidos, que fue almacenado en una ruta del disco local de la laptop, se tomaron los valores de valor de ancho de banda, jitter, y datagramas perdidos y fueron tabulados. Luego de la ejecución de los comandos iperf se estableció la llamada VoIP, con el fin de evitar la ejecución de la llamada sobre un canal saturado.

Acrylic Wi-Fi Professional

Acrylic Wi-Fi Professional [46] es un programa analizador de redes que utilizan el estándar IEEE 802.11, identifica velocidades de transmisión, y optimiza los canales para obtener el mejor rendimiento.

En este trabajo de investigación hemos utilizado la versión 2.4.5652.32374, y hemos adquirido la licencia por un año para una PC, este programa fue instalado en la laptop cliente, con el fin de realizar un análisis detallado de las señales capturadas por el cliente y medir los diferentes parámetros sobre la red Ad Hoc levantada en la laptop servidor. Las instrucciones para la instalación se encuentran en el Anexo A.3.

Luego de iniciar el monitoreo de redes inalámbricas, el programa captura todos los paquetes "*beacon*" de las redes inalámbricas que se encuentran cubriendo la laptop cliente, luego estos paquetes fueron almacenados en un archivo con formato pcap. Los beacon son frames de administración que poseen toda la información referente a las redes inalámbricas 802.11, son transmitidos periódicamente en modo broadcast. Luego de la captura, salvamos el archivo, y analizamos todos los paquetes, filtramos 60 muestras y recogimos los datos, como RSSI, nivel de ruido, e interferencia en el canal, luego de exportar la data hacia un archivo con formato .xls.

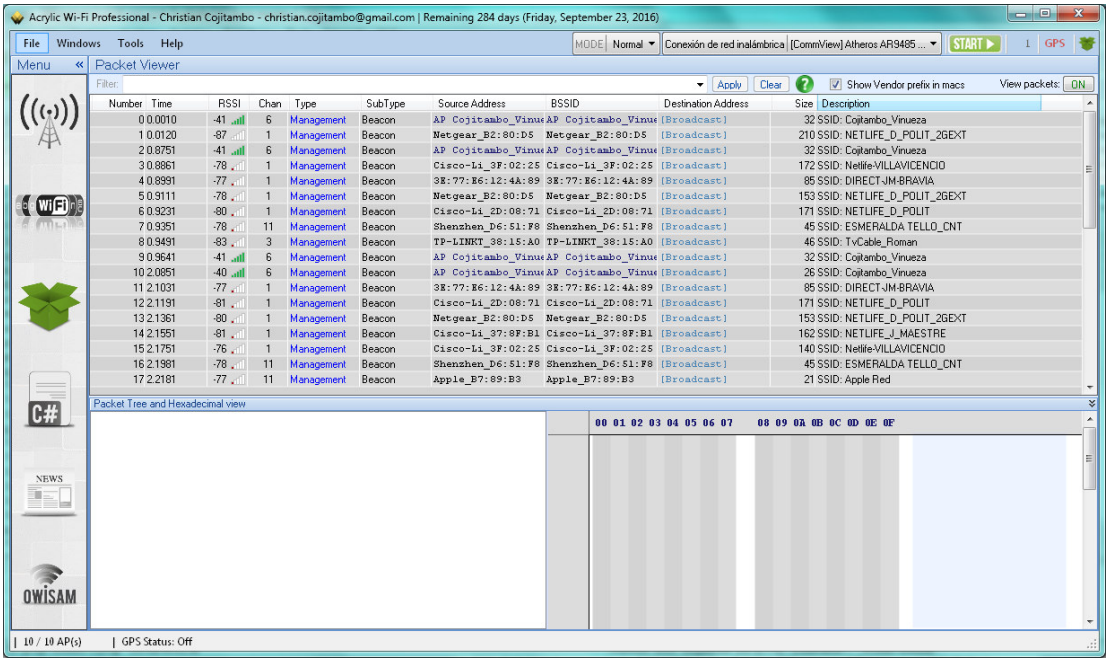


Figura 4.4. Captura de beacons, programa Acrylic Wi-Fi Professional.

Wireshark

Wireshark [47] es un programa multiplataforma que tiene la funcionalidad de analizar protocolos, tráficos de redes, estableciendo las tarjetas de red en modo promiscuo o no, puede examinar paquetes de más de 480 protocolos, aún es gratis. Para este trabajo hemos utilizado la versión 1.12.8 en ambas laptops. El procedimiento de instalación se encuentra descrito en el Anexo A.1.

Para este trabajo se realizó la captura en modo no promiscuo sin ningún filtro de todos los paquetes sobre la tarjeta inalámbrica que tenía establecida la conexión Ad Hoc. Luego de finalizar la llamada, se detiene la captura y se guarda el archivo de extensión .pcap.

Wireshark posee un módulo de análisis de llamadas VoIP disponible en la ruta Telephony – RTP – Show All Streams, SIP es uno de los protocolos soportados en esta función, se utilizó este módulo para el análisis de los flujos RTP de cada llamada, en ambos sentidos.

En la figura 4.5 es posible apreciar las estadísticas calculadas por Wireshark para cada flujo RTP encontrado en el archivo de captura.

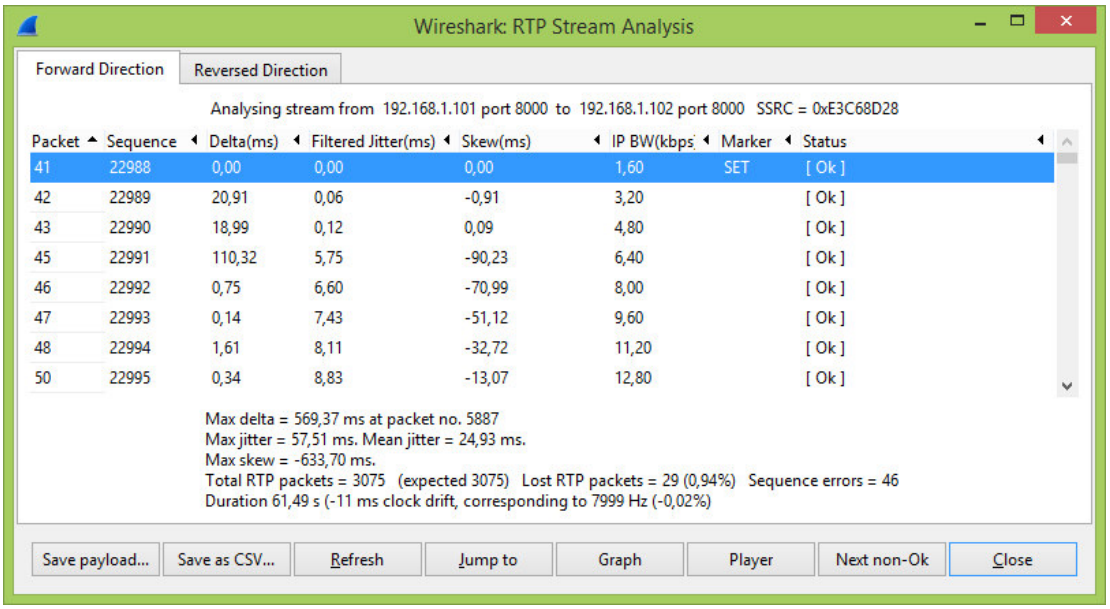


Figura 4.5. Análisis del flujo RTP mediante Wireshark.

4.2.1 MÉTRICAS EMPLEADAS

Durante la ejecución de las pruebas en el escenario establecido, se midieron algunos parámetros y métricas de QoS que fueron tomadas antes y durante la llamada VoIP con el objetivo de identificar si su comportamiento afecta o no el rendimiento o calidad de las llamadas ejecutadas, adicionalmente demostrar o no una correlación lineal entre varios de ellas, estos datos obtenidos se compararon con los mismas métricas tomadas en un escenario similar pero sin interferencia. A continuación se explica el proceso de la medición realizado en este trabajo experimental.

RSSI

Cada llamada fue realizada variando la distancia entre los agentes de usuario, las laptops, al variar la distancia varió el indicador de fuerza de la señal recibida (*RSSI*, del inglés *Received Signal Strength Indicator*); y se tomaron los valores de este parámetro. El RSSI es un parámetro especificado en el estándar IEEE 802.11, que toma valores entre 0 y un RSSI máximo que depende del fabricante del chipset inalámbrico, es una medida de energía de la señal observada en la antena.

Este parámetro fue medido en la laptop HP, era el terminal que se conectaba hacia la red Ad Hoc establecida en la laptop Samsung, la medición fue realizada gracias al programa Acrylic Wi-Fi Professional, con este programa se realizó una captura de todas las señales que brindaban cobertura en cada punto de medición, esta captura consistió en almacenar en un archivo con formato pcap, todos los frames beacons de todas las señales inalámbricas que usaban el protocolo IEEE 802.11, a este archivo posteriormente se ejecutaron y aplicaron filtros por medio del comando tshark que generaron archivos .csv, tabulando entre algunos otros más, los valores de RSSI; se seleccionaron 60 frames consecutivos como muestra en cada medición. El archivo .pcap generado presentó los resultados por medio del formato de cabecera radiotap, esta cabecera fue añadida por el programa Acrylic, en la figura 4.6, se aprecia uno de los archivos generados, con la cabecera añadida.

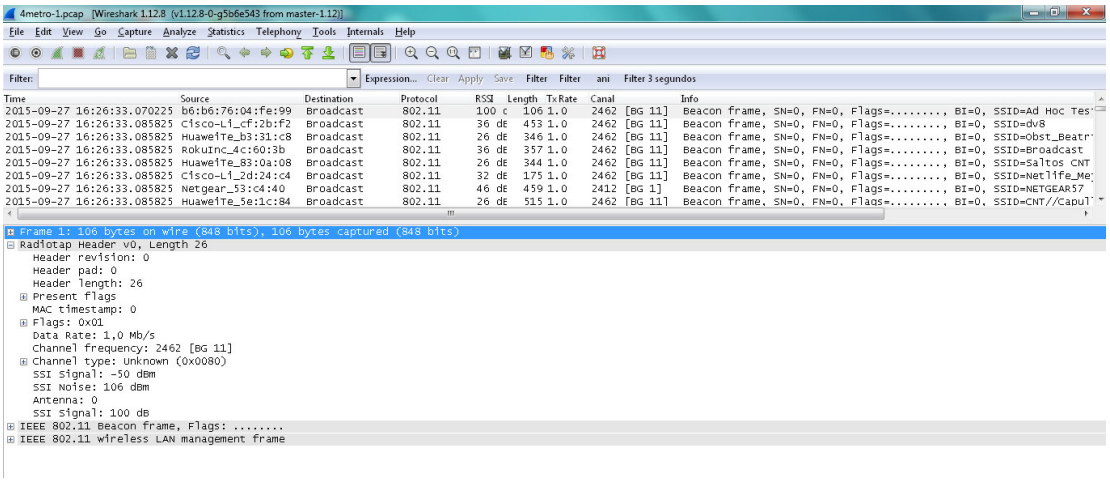


Figura 4.6. Cabecera radiotap en archivo pcap.

La cabecera radiotap posee información adicional dentro sus diferentes campos, el valor tomado como RSSI para este estudio es el campo radiotap.dbm_antsignal, la unidad utilizada por este campo es dBm.

El valor de RSSI es una medida de energía adimensional registrada en la antena receptora, medida establecida en el nivel físico y soporta hasta 256 valores empezando desde cero [48]. El rango de RSSI varía según sea el fabricante del chipset de la tarjeta de red inalámbrica, por ejemplo Cisco utiliza un valor máximo de 100, Atheros 60, para Intel se escaló el caso al fabricante pero no reveló dicha información.

El filtro aplicado usando el ejecutable tshark fue el siguiente:

tshark.exe -r D:pcap\1metro-3.pcap -Y "wlan_mgt.fixed.capabilities.ibss ==1" -T fields -e frame.time_relative -e wlan.sa -e wlan.da -e wlan_mgt.ssid -e wlan_mgt.fixed.capabilities.ibss -e wlan_mgt.ds.current_channel -e radiotap.channel.freq -e radiotap.db_antsignal -e radiotap.antenna -e radiotap.dbm_antnoise -e radiotap.dbm_antsignal -e radiotap.datarate -E header=y -E separator=";" > D:csvf\1metro-3.csv

Ruido

El SNR es la medida de la relación de la potencia de la señal con el nivel de ruido medido en la antena receptora en dBm.

En este trabajo ha sido el nivel ruido medido gracias a la aplicación Acrylic Wi-Fi Professional, mediante el método idéntico al aplicado para la medición del RSSI, mediante campos de la cabecera radiotap en la captura de beacons de las redes inalámbricas presentes.

El valor tomado como medida de SNR, según el programa Acrylic Wi-Fi Professional es el campo radiotap.db_antsignal, de idéntica manera el valor en cada medición fue tomado luego de aplicar la media aritmética a 60 muestras, se tomaron 3 mediciones por distancia. Esta variable está dada en unidades de decibelios.

Jitter

El jitter es la variación de la latencia entre paquetes recibidos, fue medido mediante el módulo de VoIP de la aplicación Wireshark. Durante la ejecución de la llamada se realizaron capturas mediante Wireshark, del archivo .pcapng generado se tomaron los valores de jitter medio y jitter máximo calculados en los flujos RTP, tanto desde extensión 101 hacia extensión 102 y viceversa, de cada distancia medición. Tuvimos disponible el valor de

medición de jitter medio y jitter máximo por punto medido, fue escogido el jitter medio como dato muestral para este estudio.

Paquetes perdidos

Fueron medidos en porcentaje, los paquetes perdidos sobre los paquetes transmitidos, tomando como referencia los paquetes que participaron en los flujos RTP, en este trabajo se realizó mediante la aplicación Wireshark, es uno de los parámetros analizados por el módulo de llamadas VoIP de este programa. Se tomaron en cuenta los paquetes perdidos medidos en una dirección, desde la laptop HP (extensión 101) con dirección IP 192.168.1.101 hacia la laptop HP con dirección IP 192.168.1.102. En trabajos similares a esta métrica se la denomina *Tasa de Paquetes Perdidos* (*PLR*, del inglés *Packet Loss Rate*), de esta manera denominamos a la métrica.

Errores de secuencia RTP

Los paquetes RTP poseen un número de secuencia, que sirve para el ordenamiento cuando llegan a su destino, la aplicación Wireshark calcula cuantas secuencias de estos paquetes no lograron llegar a su destino, este valor ha sido tomado para todas las mediciones.

Superposición de señales

La distribución de los canales dentro de la banda *ISM* de 2.4GHz ocupa las frecuencias desde 2400 MHz hasta 2495 MHz, en la tabla 11 se muestran los 14 canales establecidos y uso en diferentes regiones.

Tabla 11: Asignación de canales en banda ISM 2400 MHz.

Asignación de Canales en 2400 MHz				
Canal	Frecuencia central (MHz)	EE.UU.	Europa	Japón
1	2412	x	x	x
2	2417	x	x	x
3	2422	x	x	x
4	2427	x	x	x
5	2432	x	x	x
6	2437	x	x	x
7	2442	x	x	x
8	2447	x	x	x
9	2452	x	x	x
10	2457	x	x	x
11	2462	x	x	x
12	2467		x	x
13	2472		x	x
14	2484			x

La densidad espectral de potencia de los canales está distribuida de la siguiente manera, el espectro tiene 0 dBr en un ancho de banda que no exceden los 18 MHz, tomando como referencia central la frecuencia asignada al canal, -20 dBr a 11 MHz de cada lado de la frecuencia central, -40 dBr a 30 MHz de la frecuencia central y -53 dBr en frecuencias posteriores, en la figura 4.7 se muestra una gráfica establecida en el estándar IEEE 802.11 [6], que muestra de manera didáctica lo explicado en las líneas anteriores. La unidad dBr es utilizada para expresar niveles relativos potencia de la misma señal, a lo largo del espectro en este caso, la UIT posee la norma G100.1 [49] donde explica el uso de la unidad dBr.

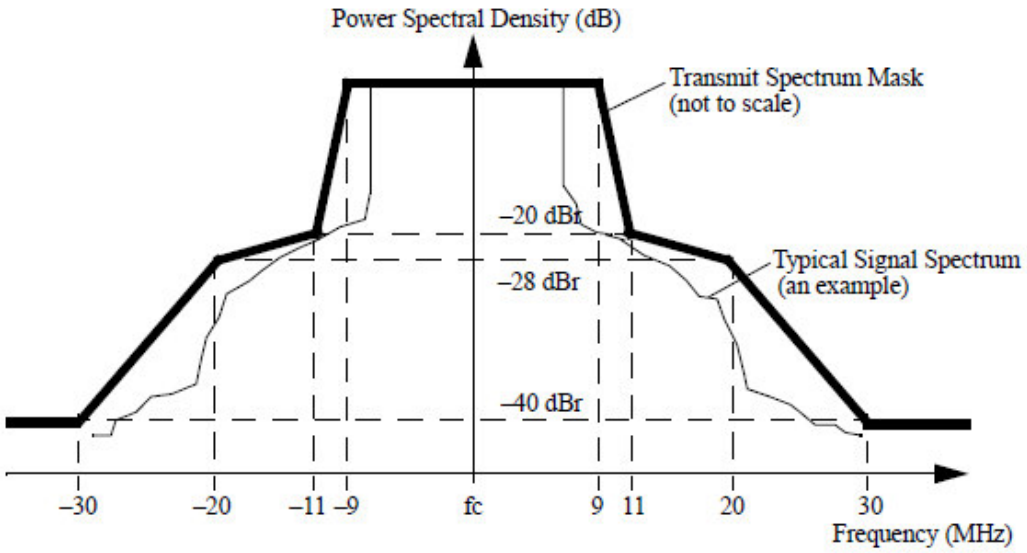


Figura 4.7. Espectro de transmisión de señales 802.11g.

Como se puede apreciar existe superposición de energía entre los canales adyacentes, para lograr transmisiones sin interferencia no es suficiente que no se encuentren señales en el mismo canal, es requerido que los canales en los cuales existan señales no causen superposición.

Para medir este parámetro en nuestro escenario hemos utilizado la aplicación *Acrylic Wi-Fi Professional*, por medio de la captura de los frames beacons, aplicamos un filtro tomando en cuenta la frecuencia de nuestra señal por medio de la herramienta *tshark*, que generó un archivo .csv, tabulando los datos necesarios, el filtro aplicado se muestra a continuación:

```
tshark.exe -r D:pcap\1metro-3.pcap -Y "radiotap.channel.freq == 2462" -T fields -e frame.time_relative -e wlan.sa -e wlan.da -e wlan_mgt.ssid -e wlan_mgt.fixed.capabilities.ibss -e wlan_mgt.ds.current_channel -e radiotap.channel.freq -e radiotap.db_antsignal -e radiotap.antenna -e radiotap.dbm_antnoise -e radiotap.dbm_antsignal -e radiotap.datarate -E header=y -E separator=";" > D:\csvinterferenciaCN\1metro-3-interferencia.csv
```

Originalmente el estándar IEEE 802.11 poseía 3 técnicas de intercambio de datos: infrarrojo, *Espectro Ensanchado por Secuencia Directa*, (*DSSS*, del inglés *Direct Sequence Spread Spectrum*) y *Espectro Ensanchado por salto de frecuencia* (*FHSS*, del inglés *Frequency Hopping Spread Spectrum*). FHSS es más robusto, mientras que DSSS provee mayor tasa de transmisión.

Durante nuestras pruebas la conexión Ad Hoc desde la laptop cliente se detectó por medio del protocolo IEEE 802.11g, este estándar transmite en la banda ISM de 2.4GHz, similar al estándar 802.11b pero con tasas mayores de transmisión, logrando transmitir hasta 54 Mbps, el estándar posee distintas tasas de transferencia dependiendo del tipo de transmisión y del esquema de modulación utilizado, en caso de utilizar OFDM provee tasas máximas de 6 Mbps usando BPSK, 9 Mbps usando BPSK3, 12 Mbps usando QPSK, 18 Mbps usando QPSK1, 24 Mbps y 36 Mbps usando 16QAM, 48Mbps y 54 Mbps usando 64QAM; mientras que con DSSS las tasas son 1 Mbps usando BPSK, 2 Mbps usando QPSK, 5.5 Mbps usando CCK y 11 Mbps por medio de CCK2.

Para nuestro trabajo se realizó la medición de la tasa de transferencia real, no se tomaron en cuenta los valores de tasa de transmisión de datos máximas definidas en el nivel físico, mediante el ejecutable iperf.exe, por medio de comandos en ambos terminales. A cada distancia medida, luego de establecer la comunicación Ad Hoc, se esperó 30 segundos

aproximadamente y posteriormente se procedió a medir la tasa de transmisión, calculada mediante la media aritmética durante un lapso de 60 segundos, antes de realizar la llamada con el objetivo de no interferir en el rendimiento de la llamada al tener el canal saturado por la medición. El valor promedio de transferencia de datos es un valor más sensato que la tasa máxima de transferencia.

La orden aplicada en el servidor fue:

Iperf3.exe – s –i 0 –V –p 5001

Mientras que en el cliente fue:

iperf3.exe -c 192.168.1.101 -u -p 5001 -i 1 -V -b 54M -t 60 -O 1 -R > D:\iperfdemoPL.wordpad

El ancho de banda transmitido durante las pruebas fue de 54 Mbps, fue escogido dado que este valor es la máxima tasa de transferencia para la red Ad Hoc establecida en IEEE 802.11g. La salida del comando ejecutado muestra con detalle la tasa de bits transmitida por cada segundo durante los 60 segundos, además de generar un resumen, que muestran los valores de intervalo, jitter, datagramas perdidos, y cantidad de bytes transferidos, además se omitió que dentro del resumen se tome en cuenta el primer segundo de transferencia con el fin de evitar valores aberrantes en caso de

demorarse la conexión hacia el servidor, se muestra en la figura 4.8 un ejemplo de las salidas obtenidas.

Estas mediciones fueron tabuladas, tomando el valor sumarizado de ancho de banda para cada distancia medida, en cada distancia fueron tomadas tres muestras con el fin de obtener la media aritmética.

```
[  4]  38.00-39.00  sec  1.47 MBytes  12.3 Mbits/sec  1.789 ms  0/188 (0%)
[  4]  39.00-40.00  sec  1.13 MBytes  9.50 Mbits/sec  1.955 ms  0/145 (0%)
[  4]  40.00-41.00  sec  1.24 MBytes  10.4 Mbits/sec  2.564 ms  0/159 (0%)
[  4]  41.00-42.00  sec  1.41 MBytes  11.8 Mbits/sec  1.692 ms  0/180 (0%)
[  4]  42.00-43.00  sec  1.27 MBytes  10.6 Mbits/sec  2.849 ms  0/162 (0%)
[  4]  43.00-44.00  sec  1.34 MBytes  11.3 Mbits/sec  1.992 ms  0/172 (0%)
[  4]  44.00-45.00  sec  1.42 MBytes  11.9 Mbits/sec  1.325 ms  0/182 (0%)
[  4]  45.00-46.00  sec  1.38 MBytes  11.5 Mbits/sec  1.674 ms  0/176 (0%)
[  4]  46.00-47.00  sec  1.41 MBytes  11.8 Mbits/sec  1.833 ms  0/180 (0%)
[  4]  47.00-48.00  sec  1.41 MBytes  11.9 Mbits/sec  2.497 ms  0/181 (0%)
[  4]  48.00-49.00  sec  1.48 MBytes  12.4 Mbits/sec  11.409 ms  0/189 (0%)
[  4]  49.00-50.00  sec  1.48 MBytes  12.5 Mbits/sec  1.809 ms  0/190 (0%)
[  4]  50.00-51.00  sec  1.39 MBytes  11.7 Mbits/sec  2.215 ms  0/178 (0%)
[  4]  51.00-52.00  sec  1.36 MBytes  11.4 Mbits/sec  2.726 ms  0/174 (0%)
[  4]  52.00-53.00  sec  1008 KBytes  8.27 Mbits/sec  2.595 ms  0/126 (0%)
[  4]  53.00-54.00  sec  1.20 MBytes  10.0 Mbits/sec  1.811 ms  0/153 (0%)
[  4]  54.00-55.00  sec  1.09 MBytes  9.17 Mbits/sec  3.804 ms  0/140 (0%)
[  4]  55.00-56.00  sec  1.02 MBytes  8.58 Mbits/sec  2.816 ms  0/131 (0%)
[  4]  56.00-57.00  sec   928 KBytes  7.60 Mbits/sec  15.740 ms  0/116 (0%)
[  4]  57.00-58.00  sec  1.17 MBytes  9.83 Mbits/sec  4.435 ms  0/150 (0%)
[  4]  58.00-59.00  sec   960 KBytes  7.86 Mbits/sec  6.473 ms  0/120 (0%)
[  4]  59.00-60.00  sec  1.05 MBytes  8.78 Mbits/sec  2.614 ms  0/134 (0%)
- - - - - - - - - - - - - - - - - - - - - - - - -
Test Complete. Summary Results:
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.00  sec  84.3 MBytes  11.8 Mbits/sec  2.822 ms  0/10756 (0%)
[  4] Sent 10756 datagrams
CPU Utilization: local/receiver 2.7% (1.1%u/1.6%s), remote/sender 3.4% (0.2%u/3.3%s)
```

Figura 4.8. Resultado orden iperf en cliente.

4.3 ANÁLISIS DE PROBLEMAS EN ESCENARIO

A continuación se exponen los problemas presentados durante la implementación del escenario práctico.

El primer escenario en estudio fue un ambiente en interiores (*indoor*), dentro de una casa, pero esta localidad no fue la idónea debido a que no se poseía

la suficiente longitud como para ejecutar pruebas de hasta 30 metros, además al ser un hogar la distribuciones del volumen del espacio libre son irregulares y la propagación de las ondas sufrían reflexiones y dispersiones que afectan la transmisión, solo se realizaron un par de mediciones, que fueron excluidas en el estudio. Para evitar este efecto, se realizaron pruebas en un lugar a campo abierto, un parque dentro de la ciudadela Ceibos Norte, pero notamos que la presencia de redes del estándar IEEE 802.11 era muy denso, el peor escenario que encontramos fue hasta 31 señales compartiendo el canal. Se realizaron mediciones siguiendo la misma metodología descrita en este capítulo, se tomaron datos hasta 30 metros, con separaciones de un metro.

Con el fin de contrastar la incidencia de la interferencia en el canal fue necesario buscar y localizar un lugar que no posea señales del estándar IEEE 802.11 en cualquiera de sus variantes, con el fin de evitar la incidencia de la interferencia por señales ajenas en las pruebas. Se realizó la búsqueda mediante inspecciones y barridos de los canales de 2.4GHz y 5GHz en parques públicos, estadios, avenidas perimetrales, con ayuda del programa Vistumbler, versión 10.5, además del software Acrylic Wi-Fi Professional pero fue complicado encontrar un lugar que cumpla con esta condición, dentro del perímetro urbano de la ciudad de Guayaquil.

En primera instancia no se logró un completo aislamiento pero el ambiente fue más controlado y sin demasiada aleatoriedad de aparición de nuevas

redes, como se presentó en los ambientes urbanos antes inspeccionados, uno de los lugares que fue considerado luego de un extenso y minucioso recorrido por el campus Gustavo Galindo de la Escuela Superior Politécnica del Litoral (ESPOL), fue en las canchas multifuncionales, cercanas al Club Recreacional ESPOL, frente al área de Tecnologías, es un área extenso sin cobertura externa, pero se localizaron un máximo de 2 señales causando interferencia y 2 señales en el mismo canal, las potencias máximas de estas señales no fueron superiores de -80 dBm. Para evitar estas señales espurias, y con el fin de tener un escenario absoluto sin interferencia, buscamos fuera del perímetro urbano, encontrando el lugar ideal para las pruebas de campo en el Parque Lago, ubicado en el Km. 26 de la vía a la Costa.

Otro de los problemas presentados, fue la selección del sistema operativo que debían ejecutar los agentes de usuario, al inicio de nuestra investigación se probó realizar las pruebas entre un computador y un teléfono móvil en lugar de computadores portátiles, fueron tomados dos teléfonos que corrían el sistema operativo Android, versión 4.3, sin embargo este sistema operativo no detectaba las señales Ad Hoc emitidas desde una laptop con Windows Professional 7, existían mecanismos para lograr establecer la comunicación pero estos métodos no eran reconocidos ni autorizados por el fabricante del sistema operativo, por lo que se decidió efectuar las pruebas entre dos

computadores portátiles que poseían instalados el SO Windows 7 Professional.

CAPÍTULO 5

5. ANÁLISIS DE RESULTADOS EMPÍRICOS

En este capítulo compartimos los resultados obtenidos, se midieron y analizaron las correlaciones lineales entre pares de diferentes parámetros tomados en la etapa de pruebas, una correlación bivariada, es decir entre dos variables.

Hemos procesado las mediciones de los siguientes parámetros de QoS: ruido, jitter, paquetes perdidos, bandwidth (tasa de transferencia media), y RSSI, todas las variables medidas en un solo sentido, para transmisiones desde el computador Samsung, hacia la portátil HP, sentido servidor-cliente, medidas en el cliente.

El coeficiente de correlación de Pearson (R), ofrece una cuantificación de la fuerza de la relación lineal entre las dos variables analizadas, toma valores entre -1 y 1, más cercano a -1 ambas variables se asocian inversamente, 0 indica que no existe relación lineal entre ellas, mientras que un valor cercano

a 1 demuestra una relación positiva. Tomar en cuenta que el coeficiente de Pearson no es un indicador de causalidad. Al elevar al cuadrado el coeficiente de correlación de Pearson obtenemos de coeficiente de determinación (R^2), el cual mide la proporción o porcentaje de variabilidad de la variable en el eje Y, experimentada debido a la variable del eje X. Además se calculó la recta de mínimos cuadrados para aproximar la linealidad de las variables.

Estos cálculos fueron realizados para validar la correlación lineal de las variables medidas en comparación de la variable distancia, también se realizó la comparación de los resultados obtenidos en ambiente con interferencia y sin ella, con el fin de mostrar el impacto de que existen otras señales sobre el mismo canal. Uno de los supuestos para la aplicación del método de regresión lineal es que las variables muestrales se puedan modelar por medio de una variable Normal, se ha comprobado la normalidad de las variables por medio del método de Kolmogorov-Smirnov, se obtuvo que las muestras de las variables siguen una distribución normal a excepción del jitter en ambiente sin interferencia, con intervalo de confianza del 95%.

5.1 ANÁLISIS DE LOS RESULTADOS

En este apartado exponemos con la ayuda de gráficas obtenidas, los resultados después de haber realizado el análisis de las variables medidas.

El análisis fue bivariado, tomando dos de las variables, se analizaron las siguientes variables en relación con la distancia: RSSI, nivel de ruido, jitter y bandwidth.

Distancia vs RSSI

En la figura 5.1 mostramos el gráfico de las variables distancia y RSSI, realizando una comparación de sus resultados en los ambientes de con interferencia y sin interferencia.

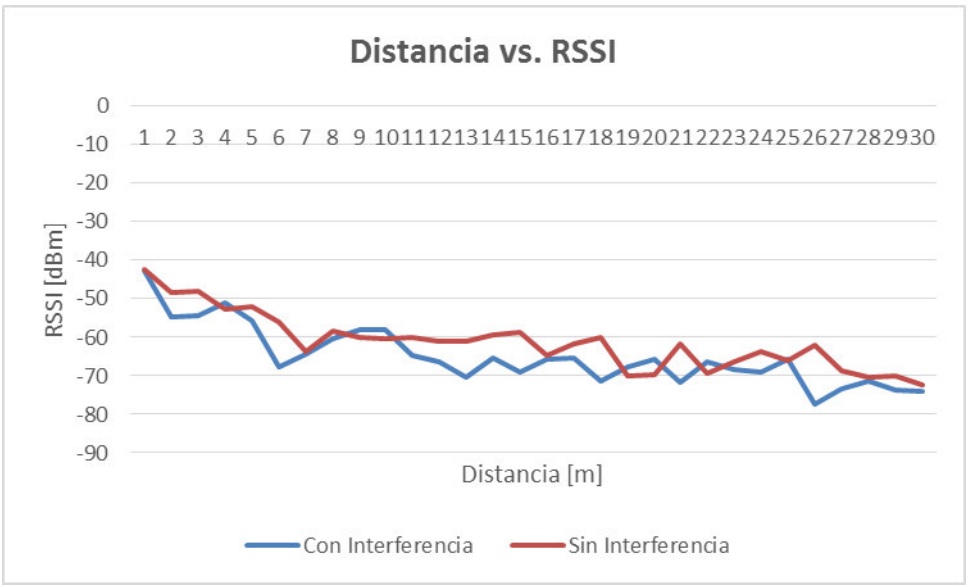


Figura 5.1. Gráfico Distancia vs RSSI.

A continuación en la figura 5.2 se muestra el cálculo del coeficiente de determinación de linealidad entre estas dos variables, en un ambiente con interferencia.

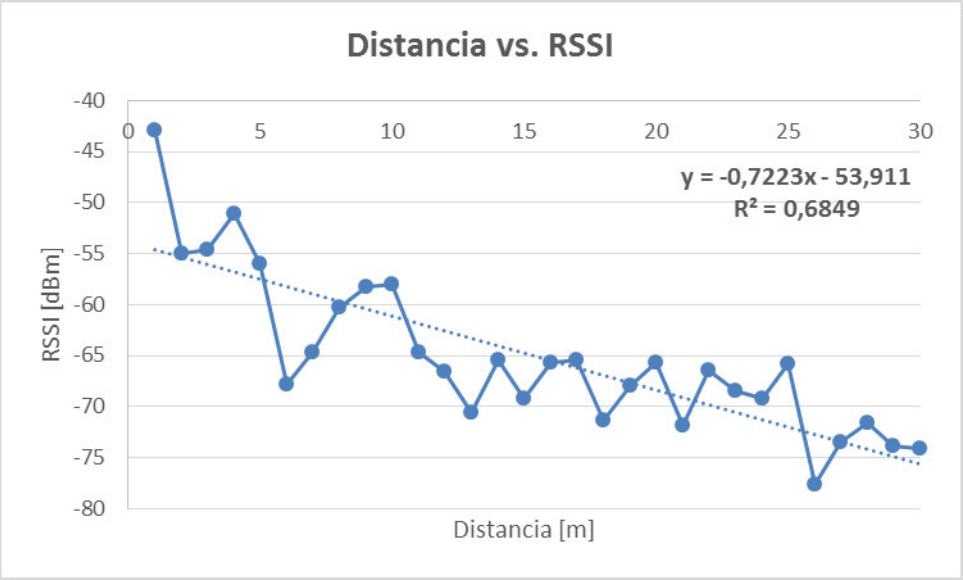


Figura 5.2. Distancia vs RSSI con interferencia.

Mientras que en un ambiente sin interferencia la dispersión entre estas dos variables se comporta según se muestra en la figura 5.3.

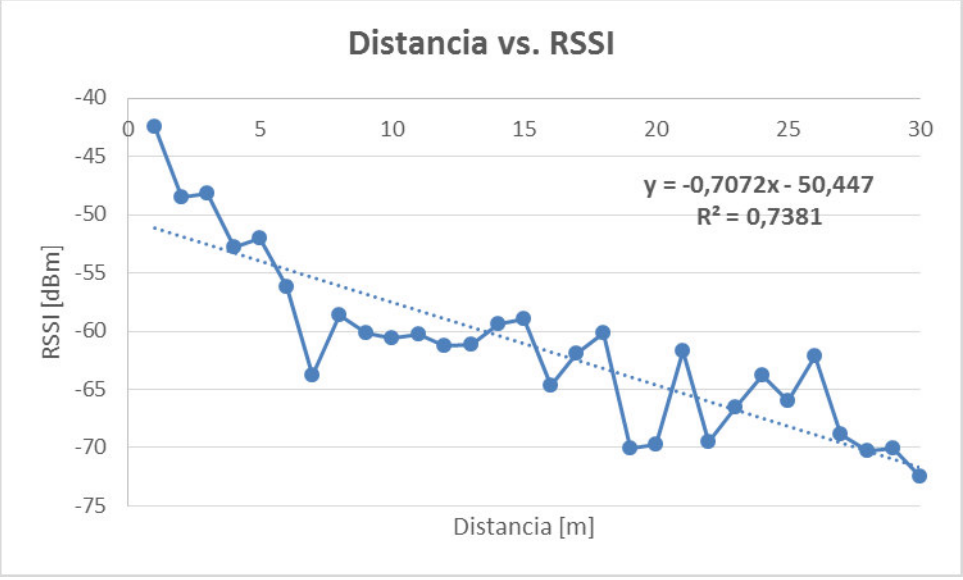


Figura 5.3. Distancia vs RSSI sin interferencia.

Distancia vs Nivel de ruido

Se muestra en la figura 5.4 el gráfico de las variables distancia y nivel de ruido, hemos realizado una comparación de sus resultados en los ambientes de con interferencia y sin interferencia.

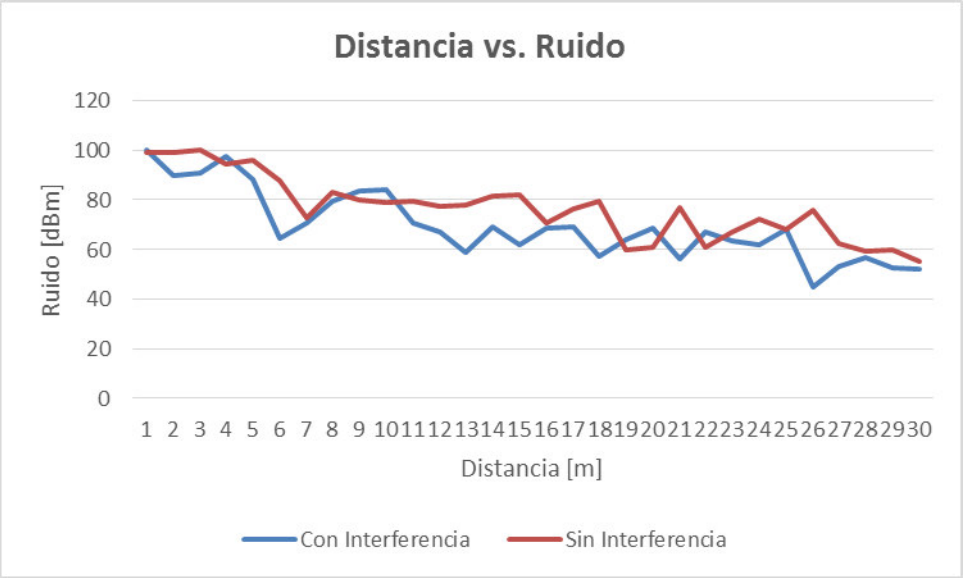


Figura 5.4. Gráfico Distancia vs Nivel de ruido.

En la figura 5.5 se muestra el cálculo del coeficiente de determinación de linealidad entre la variable distancia vs. Nivel de ruido, en un ambiente con interferencia.

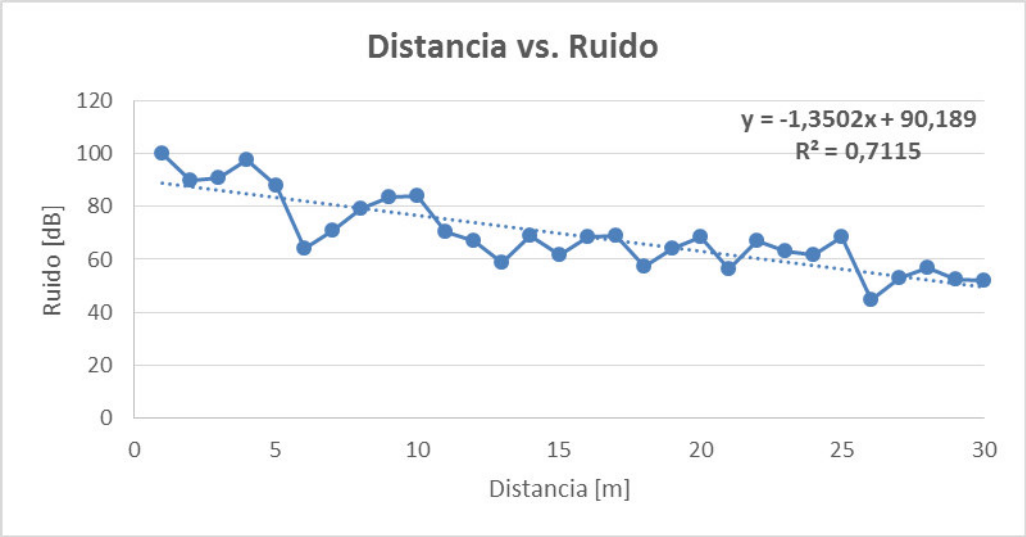


Figura 5.5. Distancia vs ruido con interferencia.

Sin embargo en un ambiente sin presencia de señales en el mismo canal la dispersión entre estas dos variables se comporta según se muestra en la figura 5.6.

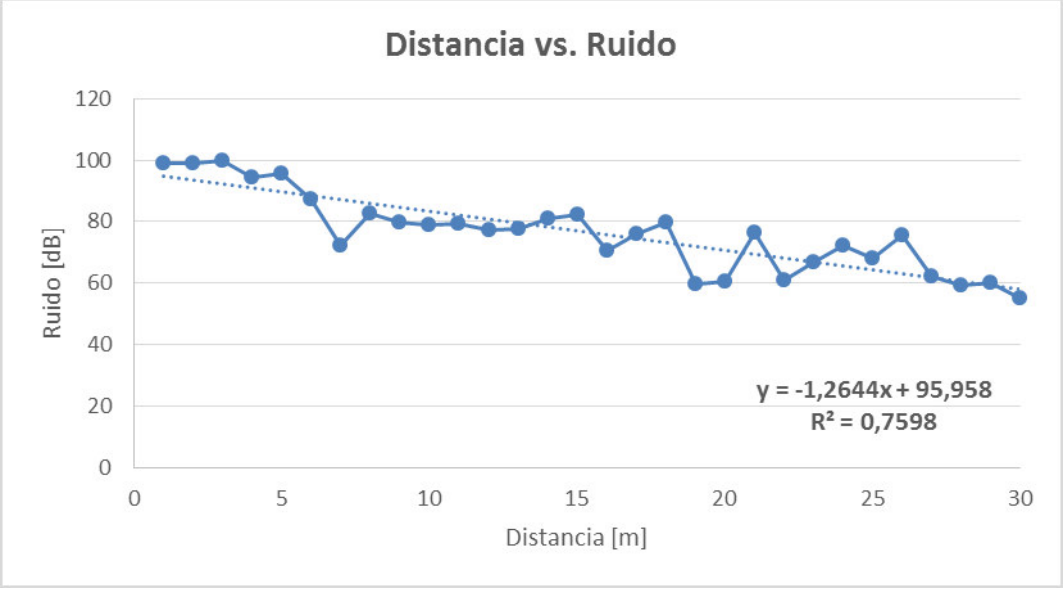


Figura 5.6. Distancia vs ruido sin interferencia.

Distancia vs jitter

Se muestra en la figura 5.7 el gráfico comparativo de las variables distancia y jitter, tomando en cuenta los ambientes con interferencia y sin interferencia.

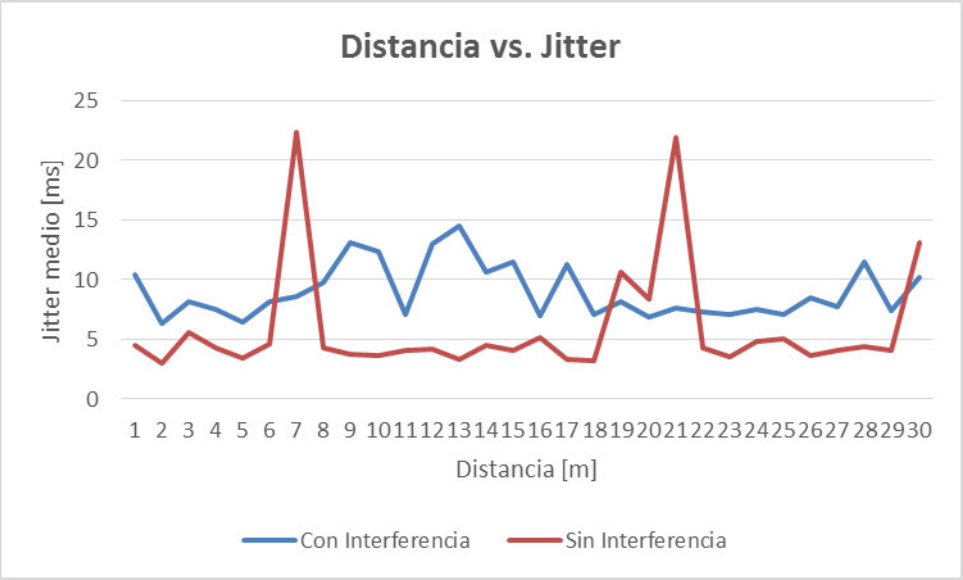


Figura 5.7. Gráfico Distancia vs jitter.

En la figura 5.8 se muestra el cálculo del coeficiente de determinación de linealidad entre las variables distancia y jitter, en un ambiente con interferencia.

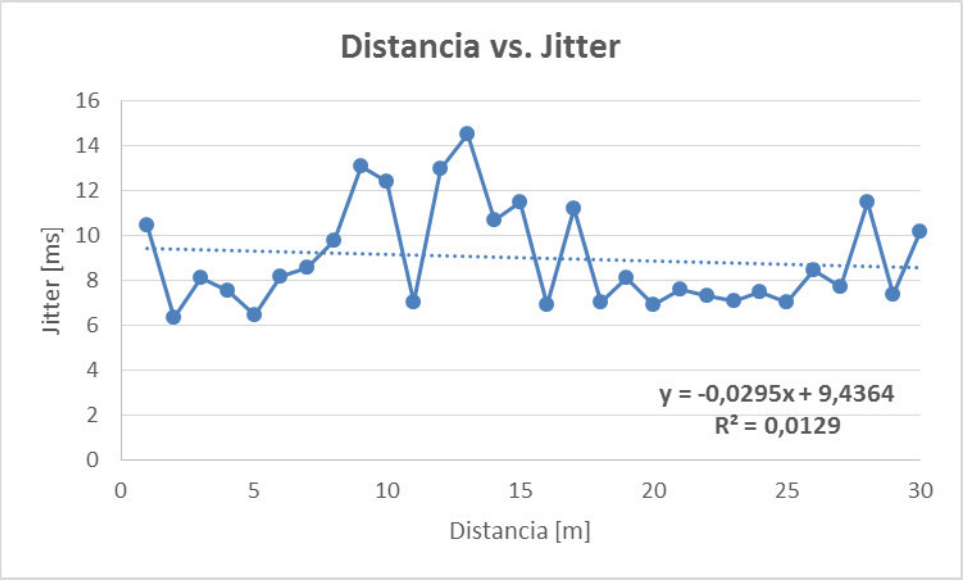


Figura 5.8. Distancia vs jitter con interferencia.

En la figura 5.9 se muestra el gráfico de dispersión en un ambiente sin interferencia entre las variables distancia y jitter.

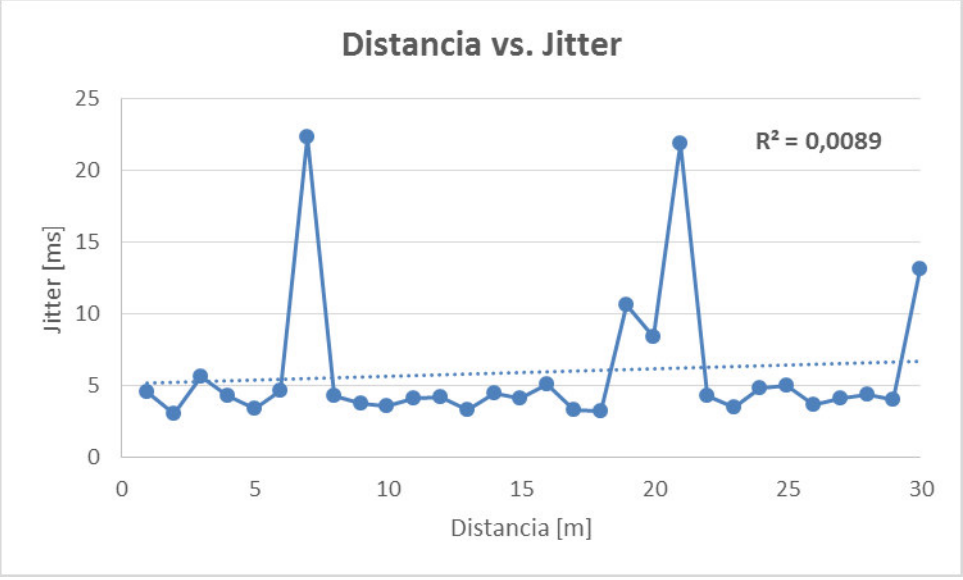


Figura 5.9. Distancia vs jitter sin interferencia.

No es estadísticamente correcto aplicar el método de regresión lineal en este caso, dado que según la prueba de Kolmogorov-Smirnov aplicada a los datos de jitter medio en un ambiente sin interferencia no se pueden modelar como una población normal, el cual es una condición supuesta para la aplicación del método de regresión lineal. Si se realizó el cálculo del coeficiente de determinación.

Distancia vs Bandwidth

Se muestra en la figura 5.10 el gráfico que relaciona las variables distancia y bandwidth, se realizó una comparación de sus resultados en los ambientes con interferencia y sin interferencia.

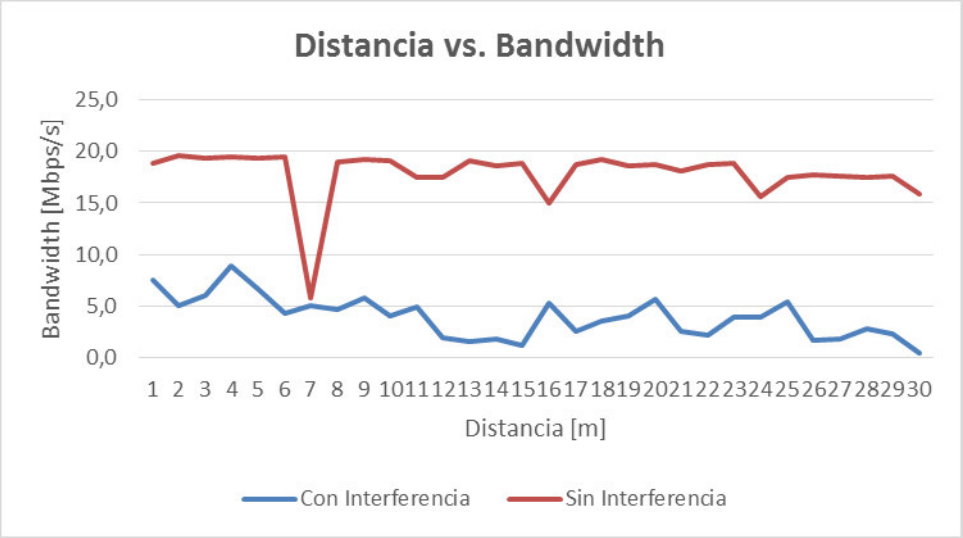


Figura 5.10. Distancia vs bandwidth.

En la figura 5.11 se muestra el cálculo del coeficiente de determinación de linealidad entre la variable distancia y bandwidth, en un ambiente con interferencia.

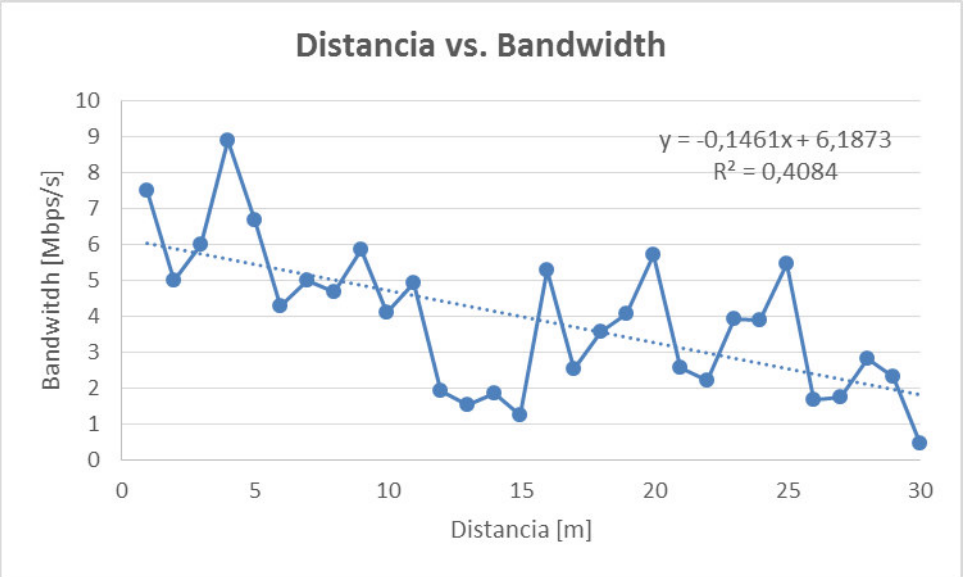


Figura 5.11. Distancia vs bandwidth con interferencia.

Mientras que en la figura 5.12 mostramos los resultados en la dispersión de estas dos variables en un ambiente sin interferencia.

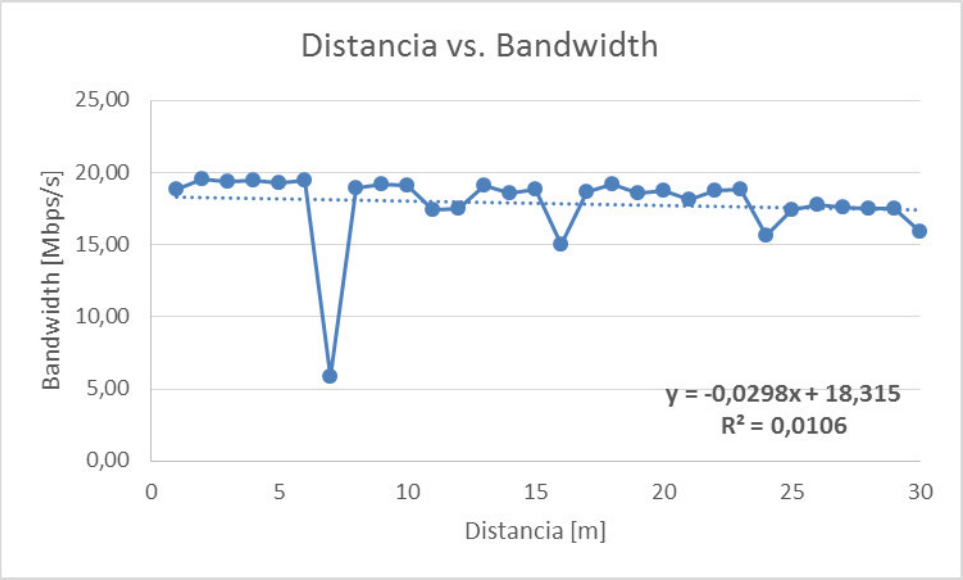


Figura 5.12. Distancia vs bandwidth sin interferencia.

Los resultados de las mediciones de errores de secuencia de paquetes RTP y paquetes perdidos en ambos ambientes, se presentan a continuación en las figuras 5.13 y 5.14 respectivamente.

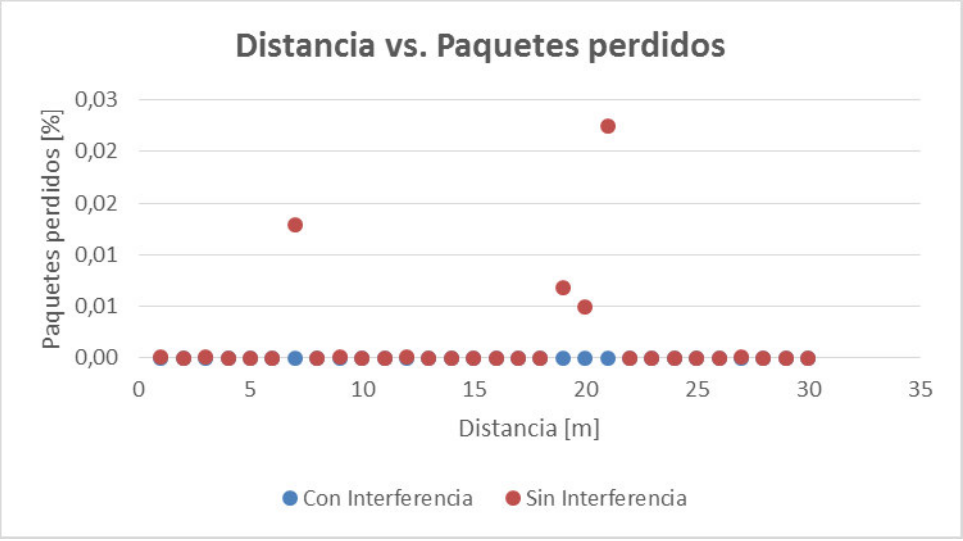


Figura 5.13. Distancia vs paquetes perdidos.

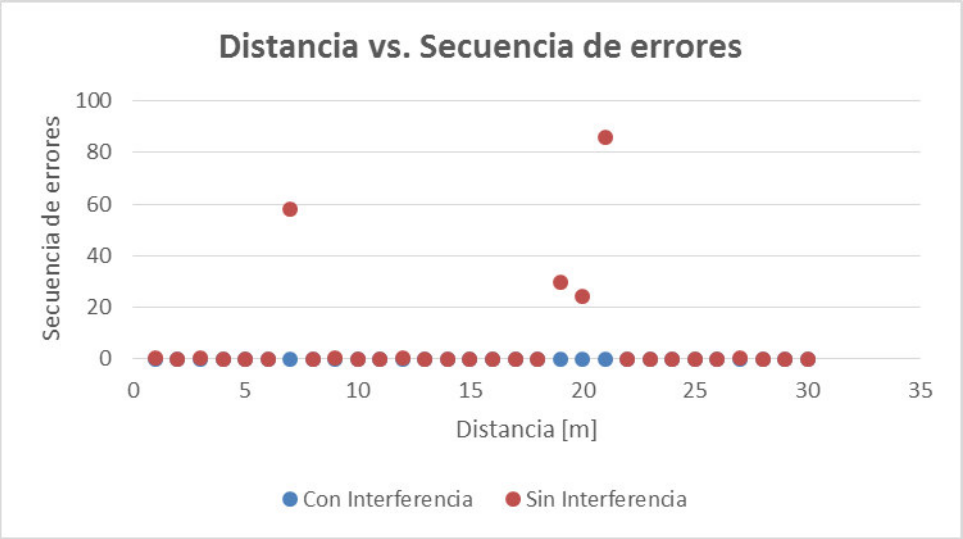


Figura 5.14. Distancia vs errores de secuencia RTP.

Con estos resultados hemos cumplido con los objetivos del trabajo de investigación, de relacionar la distancia en función de los distintos parámetros de QoS, a continuación se mostrarán resultados producto de la prueba de relación lineal entre algunos de los parámetros de QoS.

En la figura 5.15 se muestra el gráfico de dispersión entre dos variables, RSSI y bandwidth en ambos ambientes.

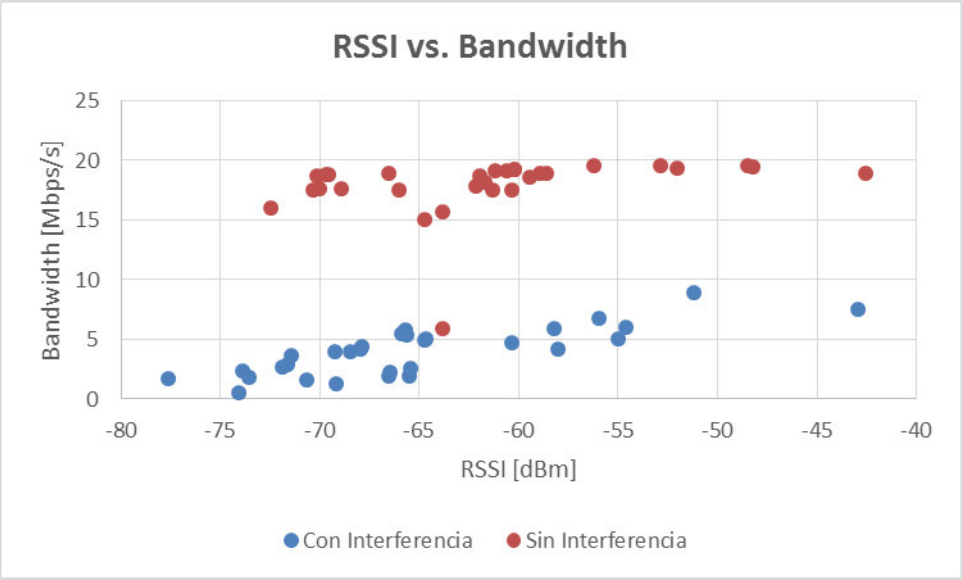


Figura 5.15. Gráfico de dispersión RSSI y bandwidth.

En base a la figura 5.15 se visualiza claramente que los valores de ancho de banda son mayores en escenarios sin interferencia manteniendo una estabilidad de 15 a 20Mbps. En ambientes con interferencia, el ancho de banda se reduce considerablemente, llegando hasta valores cercanos a cero y además se visualiza una mayor dispersión.

En la figura 5.16 se muestra el gráfico de dispersión entre dos variables, ruido y bandwidth en ambos ambientes. Se registra que la relación entra las variables es similar al mostrado en la figura 5.15 dado que entre RSSI y ruido existe una estrecha relación.

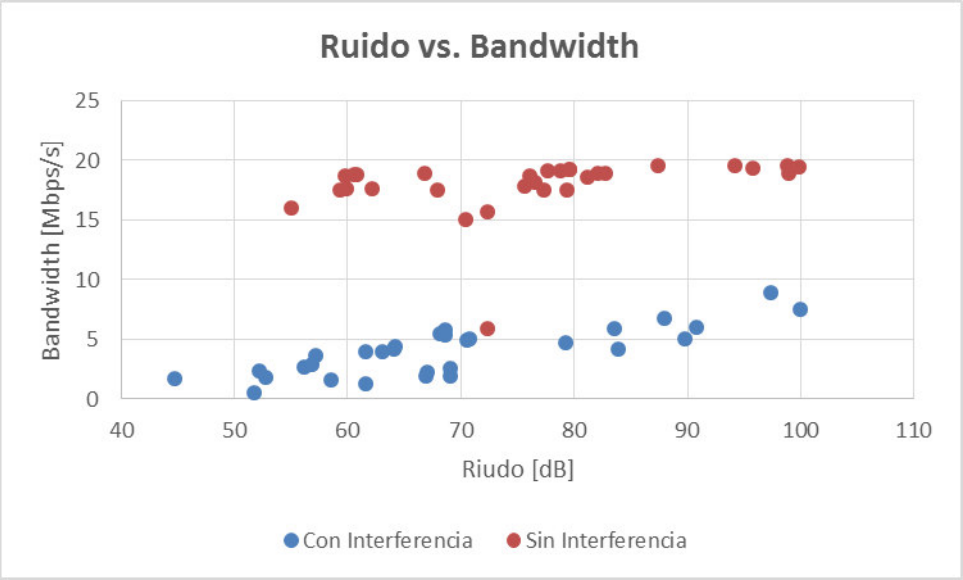


Figura 5.16. Gráfico de dispersión ruido y bandwidth.

En la figura 5.17 se muestra el gráfico de dispersión entre dos variables, ruido y jitter en ambientes con interferencia y sin interferencia. Se registra un jitter más estable en ambientes sin interferencia y se obtuvo una media de 5,96ms, mientras que en ambientes con interferencia se obtuvo una media de 8,98ms lo cual indica que para aplicaciones que requieran un jitter moderado no es recomendable este tipo de ambientes.

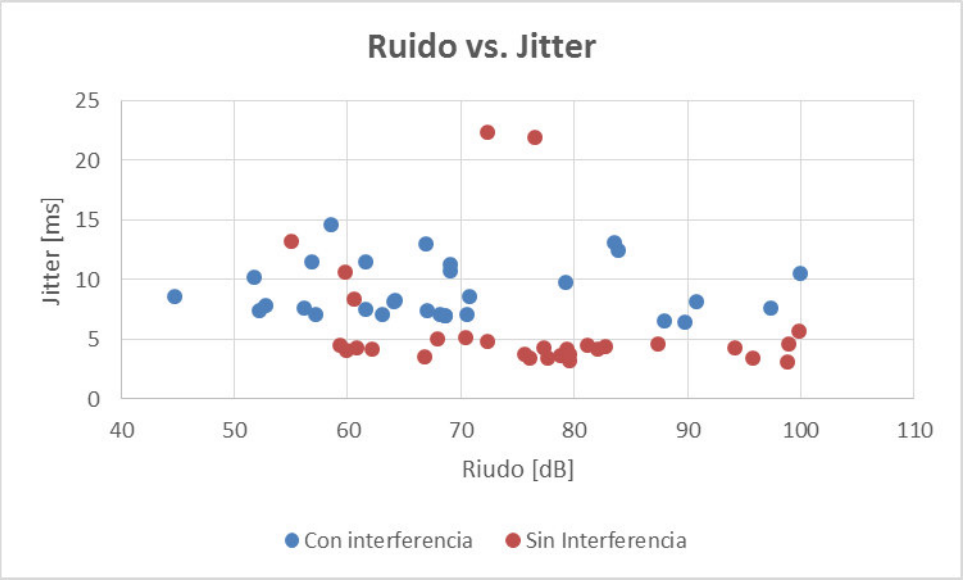


Figura 5.17. Gráfico de dispersión ruido y jitter.

5.2 INTERPRETACIÓN DE RESULTADOS

En este apartado se interpretan los resultados y las gráficas obtenidas. A continuación, en la Tabla 12, se expone un resumen y comparación de los coeficientes de determinación obtenidos al analizar estadísticamente las variables medidas, la comparación fue realizada tomando en cuenta ambos escenarios propuestos, con y sin interferencia en los canales.

Tabla 12: Coeficientes de determinación de las variables.

Parámetro	Con interferencia	Sin interferencia
Distancia vs Jitter	0,0129	0,0089
Distancia vs Bandwidth	0,4084	0,0106
Distancia vs RSSI	0,6849	0,7381
Distancia vs Ruido	0,7115	0,7598

Calculando el coeficiente de determinación el cual nos indica el porcentaje de ajuste que se ha conseguido con el modelo lineal presentado, es decir, el porcentaje de variación de la variable en el eje Y que se explica a través del comportamiento de la variable del eje X [50].Tomando los valores presentados en la Tabla 12 se obtuvo un coeficiente de correlación entre la distancia y el jitter en ambiente con interferencia de 0,0129, mientras que sin interferencia se obtuvo un valor de 0,0089; esto nos muestra que bajo las condiciones que se ejecutaron las pruebas de campo, el 1.29% de la variabilidad del Jitter es explicada por la distancia, según la recta de regresión, mientras que en ambiente sin interferencia este porcentaje disminuyó a 0.8%.

Tendencia similar a la anterior se presentó en el análisis de las variables distancia y bandwidth, en ambiente con interferencia se mostró un 40,84% de influencia de la distancia, mientras que sin interferencia disminuyó a 1,06%.

En el caso del análisis de las variables distancia y RSSI se obtuvo un porcentaje de 68,49% de influencia por parte de la distancia, mientras que en un ambiente libre de interferencia registró un aumento a 73,81%, es decir en ambientes sin interferencia se aprecia un valor alto de correlación lineal entre estas dos variables.

Con respecto a las variables distancia y ruido, obtenemos 71,15% y 75,98% de influencias en ambientes con interferencia y sin interferencia respectivamente.

Finalmente, de acuerdo a la recomendación realizada por el Sector de Normalización de las Telecomunicaciones de la UIT, G.1010, denominada Categoría de calidad de servicio para los usuarios de extremo de servicios multimedios, se nota que bajo este tipo de comunicación en los escenarios expuestos en la figura 5.7 no cumplen con la política exigida que, para aplicaciones en tiempo real de gran calidad como lo ofrece el códec G.711 tipo u-law, la variación de retrasos debería ser menor a 1 ms. Es posible que en el futuro replicando este escenario de comunicación Ad Hoc mediante nuevos estándares que se desarrollen en el campo se logre cumplir con esta normativa.

5.3 DISCUSIÓN

El SNR se lo puede considerar como un parámetro idóneo para estimar las atenuaciones por distancia en comunicaciones Ad Hoc, mientras que el RSSI es un parámetro no muy relacionado con las distancias entre 2 puntos de transmisión Ad Hoc mediante el estándar 802.11 g, existen estudios similares que tampoco recomiendan el RSSI como parámetro de medición debido a su poca precisión [51].

Tomar en cuenta que estos resultados se obtuvieron usando el códec G.711 tipo u-law, el cual es uno de los codecs que proporciona mayor calidad en la transmisión de voz, que soporta Asterisk, ocupa una tasa de 80 Kbps en promedio por paquete RTP enviado; bajo estas condiciones se demostró que el jitter no lleva una correlación lineal en comparación con el nivel de ruido, en el estudio realizado por Edzerieq *et al* [52] se muestra una mediana relación lineal usando otros codecs de voz.

Los valores registrados en las gráficas 5.13 y 5.14 corroboran que el campo de número de secuencia del paquete RTP está directamente relacionado con los valores de paquetes perdidos, según muestra la literatura del RFC 3550. En nuestro estudio los paquetes perdidos han sido medidos tomando en cuenta solo los paquetes RTP.

La cantidad de llamadas que puedan ejecutarse en la comunicación Ad Hoc bajo CODEC G.711 aumenta considerablemente en ambientes sin interferencia dado que se tiene una media de 17,9 Mbps de ancho de banda brindando una capacidad de realizar más de 200 llamadas simultáneas, a diferencia de ambientes con interferencia se pueden realizar aproximadamente 49 llamadas dado que se obtuvo un ancho de banda promedio de 3,92 Mbps.

Este trabajo de investigación deja establecidas características del comportamiento de varios parámetros de QoS para el establecimiento de

llamadas VoIP usando el estándar IEEE 802.11g en modo Ad Hoc. Además cabe indicar que el método utilizado es un modelamiento de correlación lineal, dejando de lado otras correlaciones válidas estadísticamente como lo son las relaciones logarítmicas, exponenciales que en futuros trabajos podrían ser abordados con el fin de compararlos en base a los resultados obtenidos.

CONCLUSIONES

En el presente trabajo se realizó un estudio descriptivo y bibliográfico de la comunicación VoIP sobre redes Ad Hoc utilizando el estándar IEEE 802.11g, coloquialmente conocido como WiFi, y se elaboró un escenario de pruebas donde se establecieron llamadas VoIP con el fin de estudiar algunas propuestas para mejorar el rendimiento de distintas aplicaciones que usen el escenario estudiado. Las conclusiones obtenidas se sintetizan en los siguientes puntos:

- Se comprobó que las variables sobre las cuales la distancia influye con un gran porcentaje de relación sobre sus resultados, son ruido y RSSI.
- Se analizó la dispersión de los valores obtenidos de ancho de banda en ambos ambientes y se comprobó una gran diferencia de resultados, obteniendo que mientras se realice la transferencia de datos por medio de una llamada VoIP en ambientes sin interferencia la capacidad de llamadas aumenta en un 400% en referencia al ambiente con

interferencia, capacidad de 49 a 200 llamadas VoIP de acuerdo al escenario propuesto.

- Los resultados obtenidos del análisis de la variables ruido y jitter, muestran que el jitter se comporta de una manera estable y muestra un valor menor en ambientes sin interferencia, mientras que sobre ambientes con interferencia se torna inestable y el jitter aumenta a valores cercanos a los 8.98 ms en promedio.
- Los tiempos de variación de retrasos obtenidos en las pruebas realizadas no cumplen con las normas establecidas en la Norma G.1010 de la UIT, cabe notar que en esta recomendación se indica que estos valores fueron establecidos a largo plazo y que es posible que los estándares actuales no la cumplan.
- De acuerdo al RFC 3550, que indica que el campo de número de secuencia puede ser usado por el receptor para estimar la cantidad de paquetes perdidos en la transmisión en un solo sentido, se demostró que es verdadera esta afirmación y que están fuertemente relacionados linealmente la cantidad de paquetes perdidos RTP y los errores de secuencia de los paquetes RTP.
- Se observó que la conexión Ad Hoc se estableció en el canal 11, en todos los casos.

RECOMENDACIONES

Para el presente trabajo, se enuncian las siguientes recomendaciones para futuros trabajos de investigación:

- Realizar estudios similares midiendo las mismas variables y escenarios propuestos en la presente tesis pero utilizando un estándar diferente como 802.11n y/o 802.11ac, en medida de que sea posible.
- Medir en un ambiente controlado a nivel de potencia de transmisión la señal de recepción para determinar el grado de influencia en el deterioro de la voz de extremo a extremo.
- Agregar al presente estudio una evaluación subjetiva como el MOS para determinar la percepción del usuario final a diferentes metros del origen pero disminuyendo la cantidad de muestras dado que la recomendación P.800 indica que las sesiones máximo deben durar 20 minutos.
- Modelar diferentes parámetros a los mencionados en la presente tesis como el consumo de energía o comparaciones contra el modo infraestructura.

ANEXO A

INSTALACIÓN DE LOS PROGRAMAS

A.1 Instalación Wireshark

Ingresar a https://www.wireshark.org/download/win64/all-versions/ y seleccionar el archivo Wireshark-win64-1.12.8.exe. Una vez guardado en el disco local, se debe ejecutar.

Se iniciará un Wizard que ayudará con la configuración de la aplicación. Presionamos el botón Next de acuerdo a lo mostrado en la figura A.1.

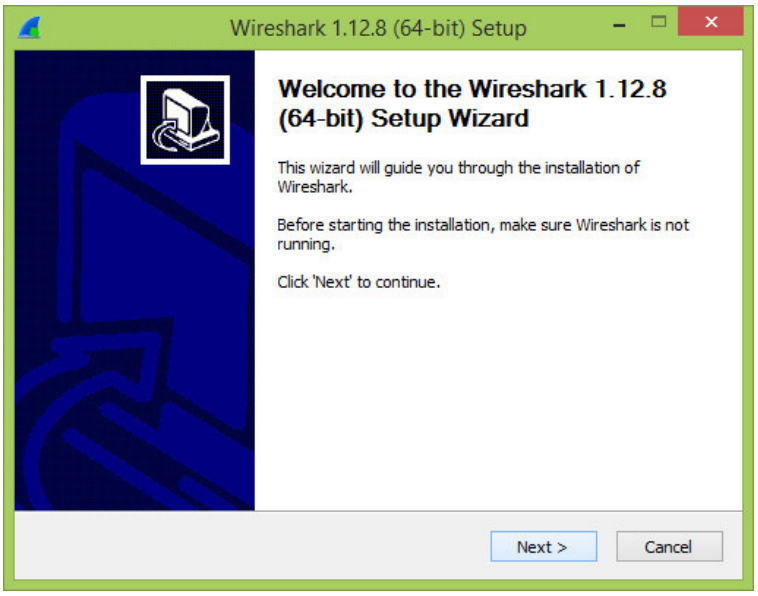


Figura A.1. Inicio de wizard de instalación

Damos click en I agree, aceptando el Acuerdo de Licencia como se muestra en la figura A.2.

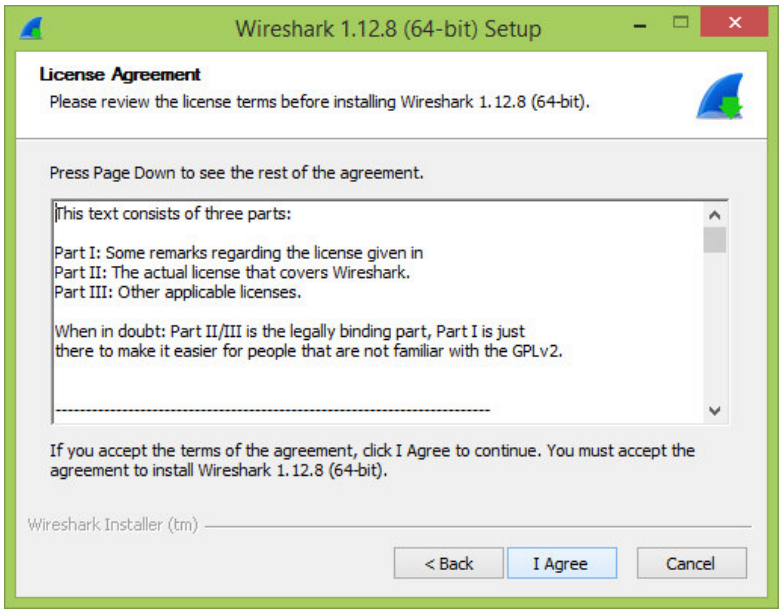


Figura A.2. Aceptación del acuerdo de licencia de Wireshark.

Posteriormente seleccionamos los componentes requeridos para la instalación, dejar los puntos seleccionados y damos Next tal como se muestra en la figura A.3.

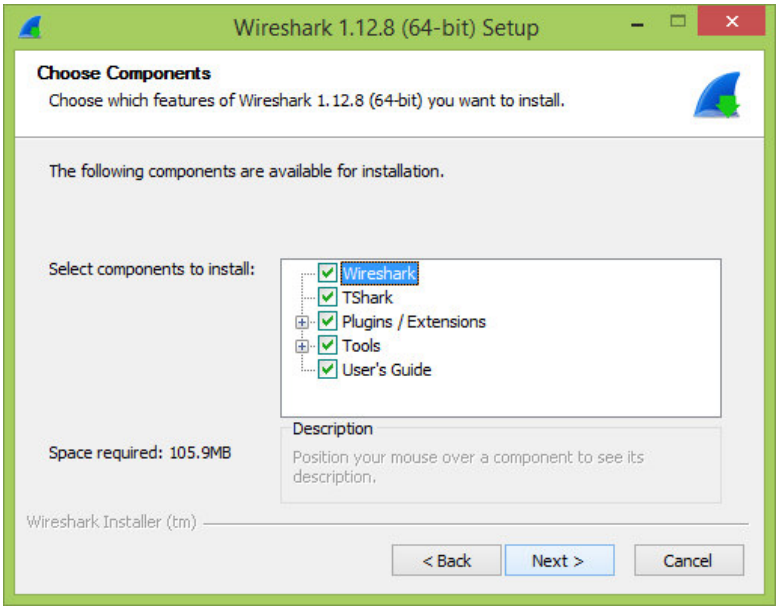


Figura A.3. Elección de componentes a instalar de Wireshark.

Luego seleccionamos las opciones de Iconos deseados y presionamos el botón Next (figura A.4).

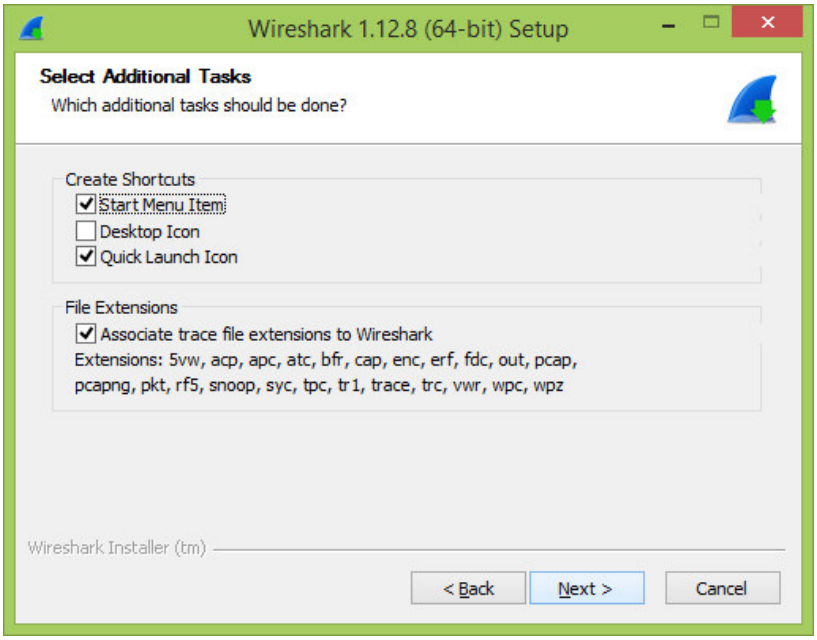


Figura A.4. Elección de extensiones e iconos de Wireshark.

En la figura A.5 escogemos el directorio de instalación y damos clic al botón Next.

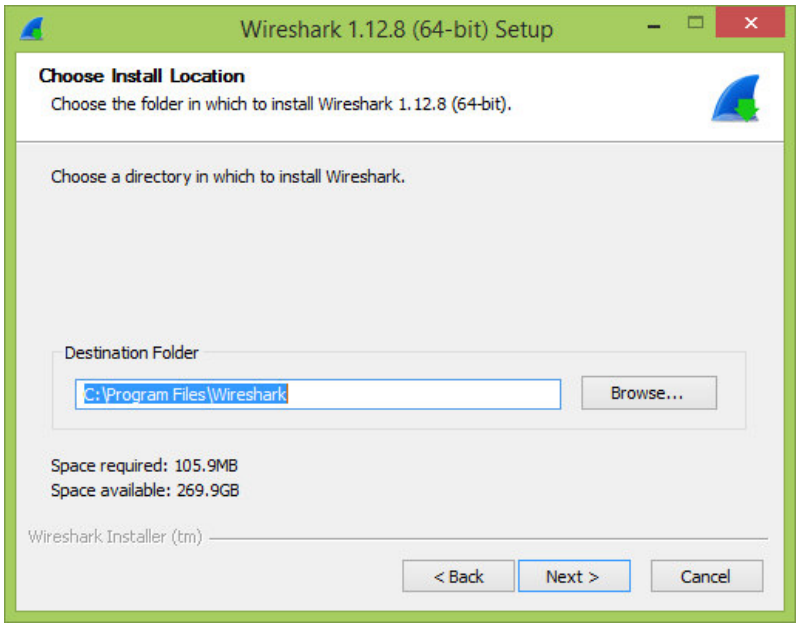


Figura A.5. Elección de directorio de instalación de Wireshark.

Posteriormente permitimos la instalación de Wincap. Damos clic en Install y se desplegará el listado de los archivos en descarga según lo visualización en las figuras A.6 y A.7.

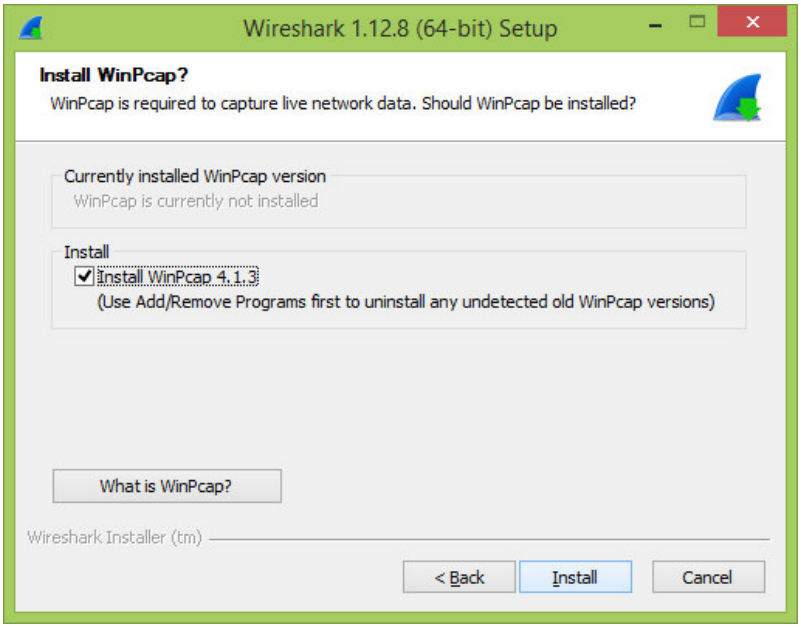


Figura A.6. Elección de instalación de Winpcap.

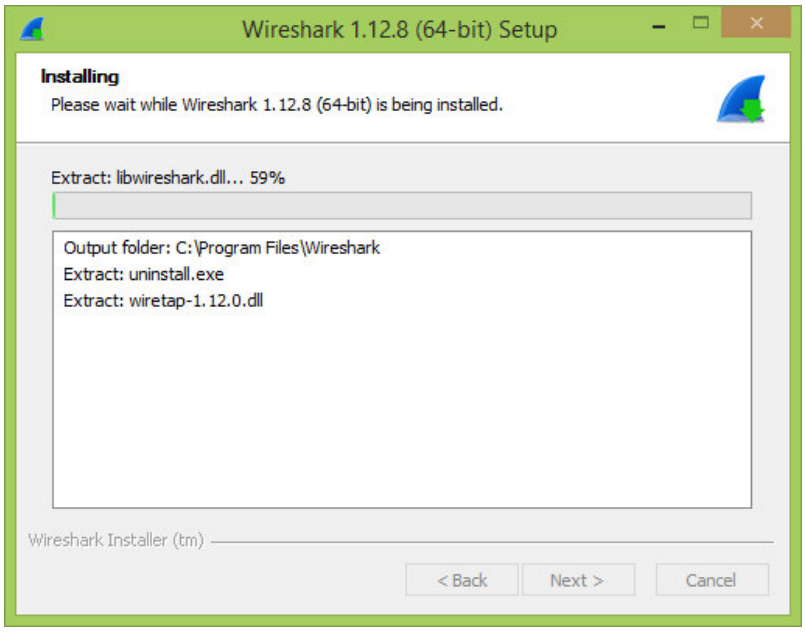


Figura A.7. Proceso de instalación de Winpcap.

Una vez descargado todos los archivos necesarios para su instalación, nos muestra la pantalla de Bienvenida de Winpcap, presionamos el botón Next como se visualiza en la figura A.8.

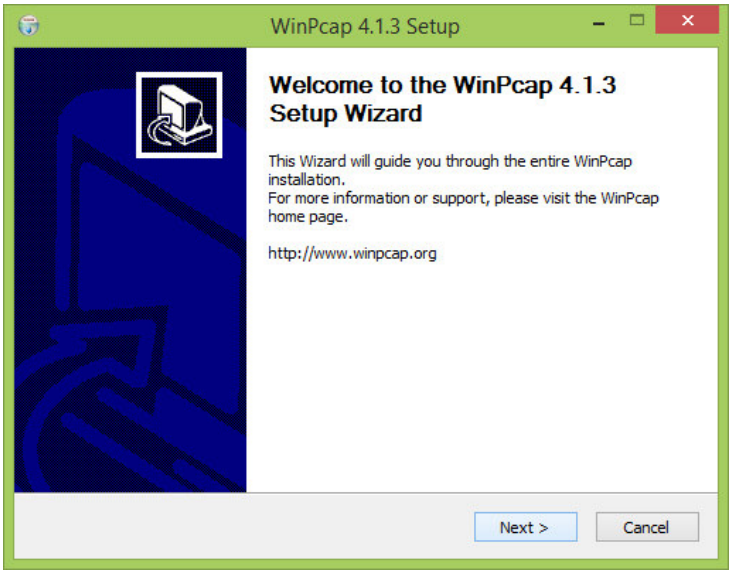


Figura A.8. Bienvenida de instalación de Winpcap.

Seguidamente Aceptamos el Acuerdo de Licencia de Winpcap dando clic en el botón I Agree. Finalmente nos aparece informa la culminación de instalación de Wincap. Ver figura A.9 y A.10.

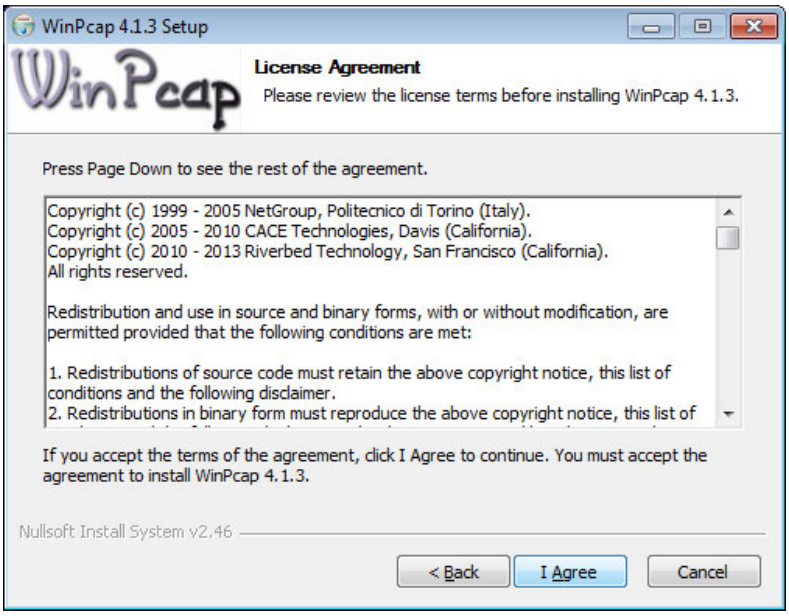


Figura A.9. Aceptación de acuerdo de licencia de Winpcap.

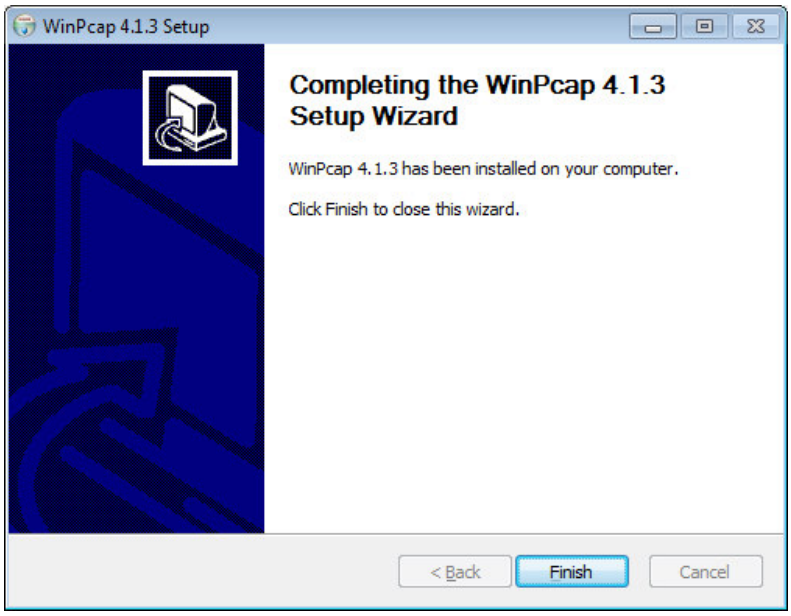


Figura A.10. Finalización de instalación de Winpcap.

Una vez culminado el proceso de instalación de Wincap, nuevamente nos redirecciona a la instalación de Wireshark, damos clic en Next y finaliza exitosamente la instalación. Presionamos el botón Finish.

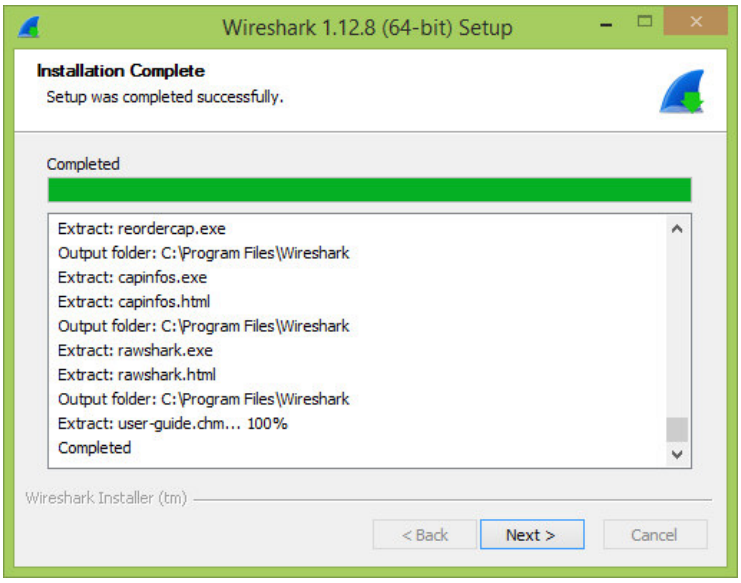


Figura A.11. Finalización de instalación de Wireshark.

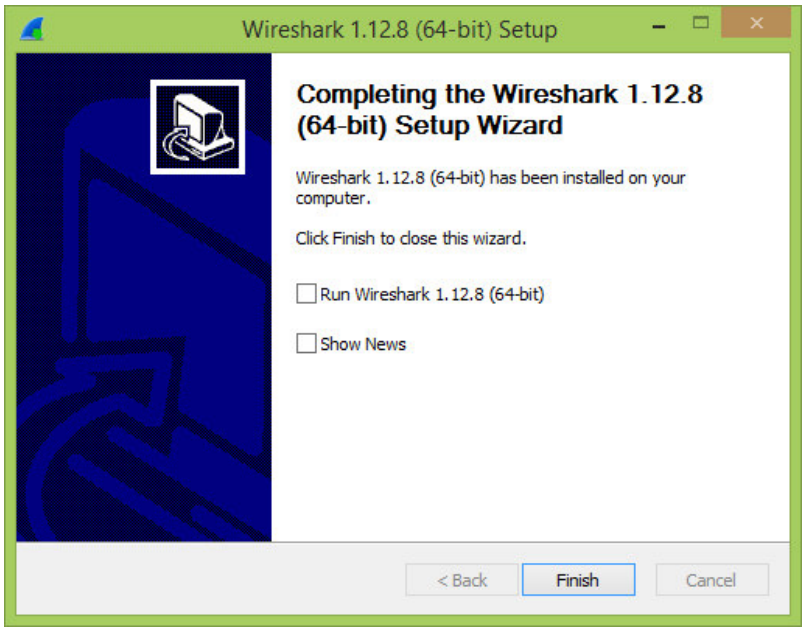


Figura A.12. Wireshark instalado.

A.2 Instalación Iperf

Se ingresa a https://iperf.fr/ y en la sección Download Iperf pre-compiled binaries damos click en la última versión disponible del programa; para la presente tesis usamos el iperf3.exe, el archivo descargado es el llamado: iperf-3.0.11-win64.zip. Una vez guardado el archivo en el disco local, lo descomprimimos en una ruta de fácil acceso, para nuestro caso lo descomprimimos en D:\iperf-3.0.11-win64.

Abrimos una consola de comandos de Windows y nos posicionamos en la ruta donde colocamos la carpeta iperf-3.0.11-win64 mediante comandos de consola Windows, tal como se muestra en la figura A.12.

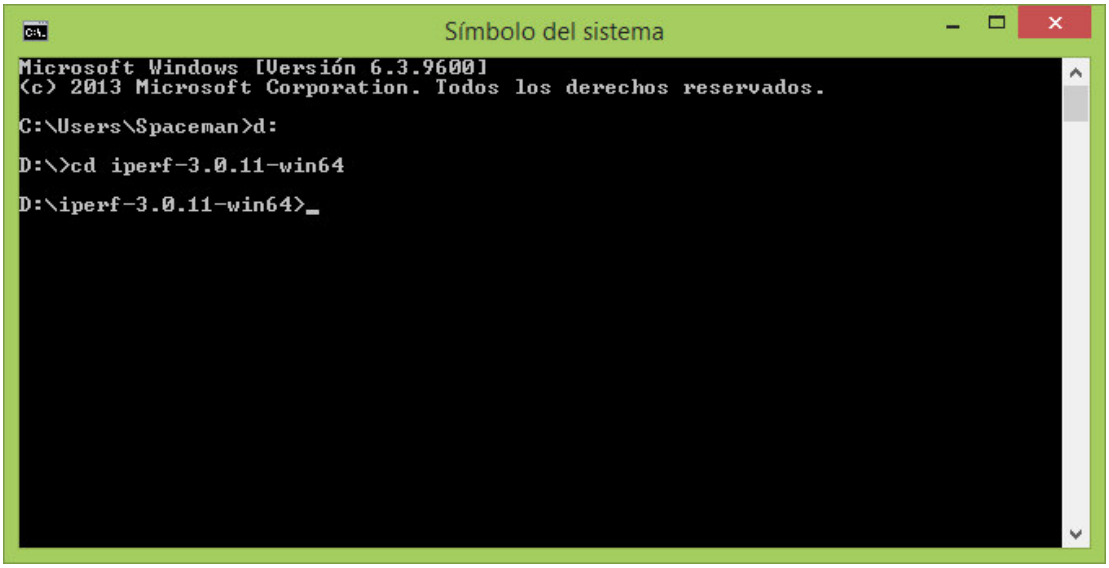


Figura A.12. Directorio de la carpeta iperf.

Dado que es una aplicación cliente-servidor, realizamos los mismos pasos en los dos equipos donde se realizaran las pruebas.

Tal como se muestra en la figura A.13, el equipo destinado a ser servidor ejecutamos el comando iperf3.exe -s, donde el equipo empezara a escuchar las peticiones en el puerto 5201.

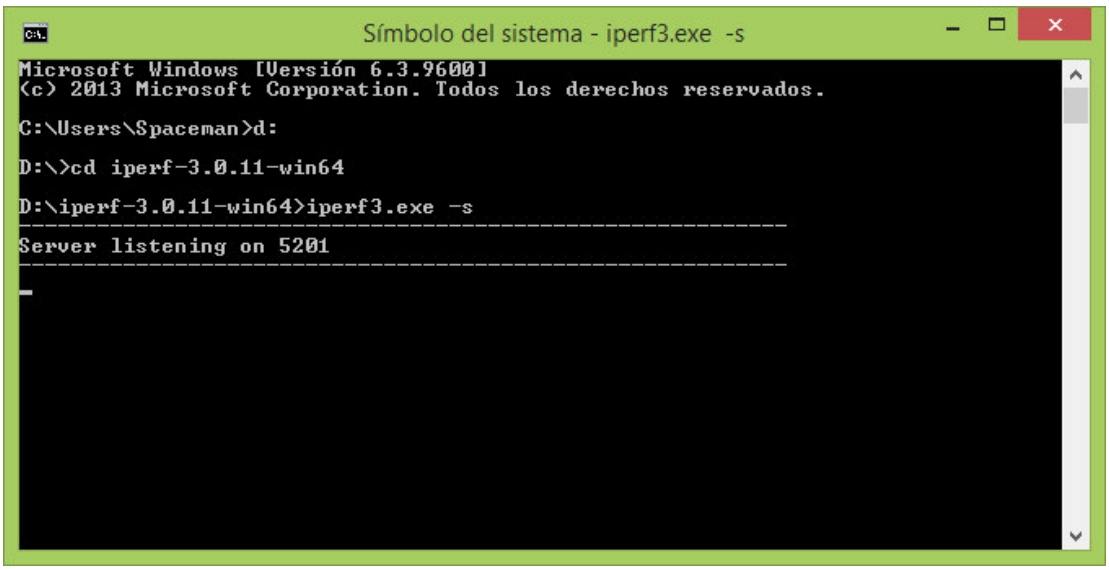


Figura A.13. Ejecución de comando para equipo tipo servidor iperf.

Para el equipo cliente, ejecutamos el comando iperf -c (ip_servidor), por default el comando evaluara el throughput del enlace por 10 segundos de la dirección IP señalada como servidor, además es posible customizar las propiedades del flujo que se espera enviar o recibir desde el servidor.

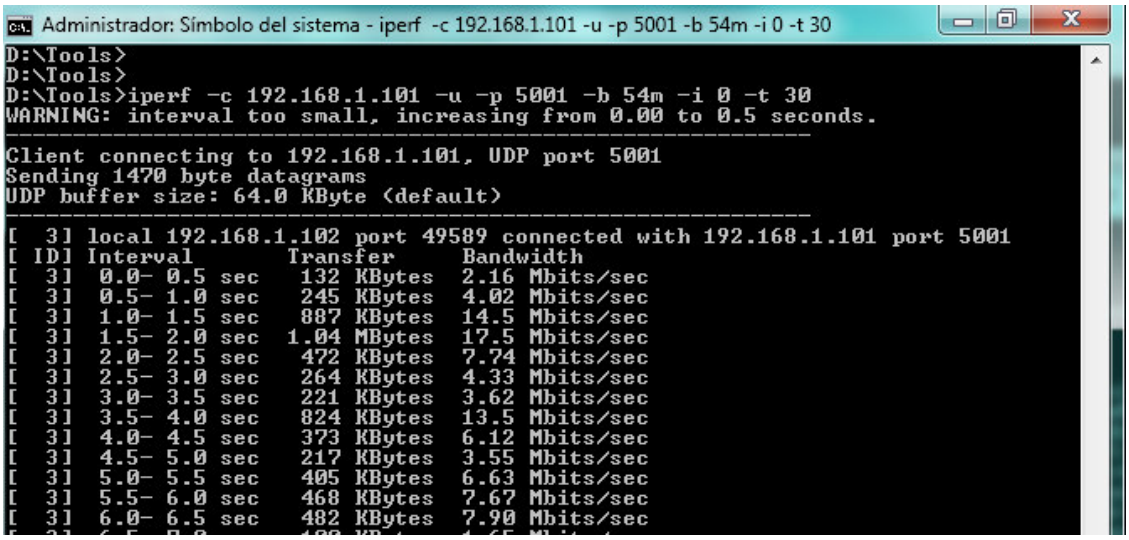


Figura A.14. Ejemplo de comando para equipo tipo cliente en iperf.

Con el comando iperf3.exe -help podemos visualizar todas las opciones disponibles para un análisis más personalizado, podemos configurar el puerto de conexión, el intervalo de tiempo de cada paquete enviado, formato, dirección, envío en modo reverso, entre otros. En la siguiente tabla se especifican las opciones disponibles en cada extremo del análisis.

Tabla 13: Comandos iperf.

ORIGEN	OPCIÓN	DESCRIPCIÓN	DETALLE
Cliente/Servidor	-f	--format	Formato del reporte: Kbits, Mbits, KBytes, MBytes
Cliente/Servidor	-i	--interval	segundos entre reportes de ancho de banda periódicos
Cliente/Servidor	-l	--len	longitud del buffer para leer o escribir (8 KB por default)
Cliente/Servidor	-m	--print_mss	imprimir el máximo tamaño de segmento en TCP (MTU - TCP/IP header)
Cliente/Servidor	-p	--port	puerto para conectarse/escuchar
Cliente/Servidor	-u	--udp	usar UDP en vez de TCP
Cliente/Servidor	-w	--window	Tamaño de la ventana de TCP (tamaño de buffer del socket)
Cliente/Servidor	-B	--bind	amarrar a cliente, interfaz o dirección de multicast
Cliente/Servidor	-C	--compatibility	para usarse con versiones anteriores, no envía mensajes extras
Cliente/Servidor	-M	--mss	fija el máximo tamaño de segmento de TCP (MTU - 40 bytes)

ORIGEN	OPCIÓN	DESCRIPCIÓN	DETALLE
Cliente/Servidor	-N	--nodelay	fija TCP sin retraso, deshabilitando el algoritmo de Nagle
Cliente/Servidor	-V	--IPv6Version	fija el dominio a IPv6
Servidor	-s	--server	Ejecutar en modo servidor
Servidor	-U	--single_udp	Ejecutar en modo de un solo hilo en UDP
Servidor	-D	--daemon	ejecutar el servidor como demonio
Cliente	-b	--bandwidth	Para UDP, ancho de banda a utilizar en bits/sec (por default 1 Mbit/sec, implica -u)
Cliente	-c	--client	ejecutar en modo de cliente, conectándose a "host"
Cliente	-d	--dualtest	Realizar una prueba bidireccional simultáneamente
Cliente	-n	--num	numero de bytes a transmitir (en vez de -t)
Cliente	-r	--tradeoff	Realizar una prueba bidireccional individualmente
Cliente	-t	--time	tiempo en segundos para transmitir (10 segundos por default)
Cliente	-F	--fileinput	introducir los datos a transmitir desde un archivo
Cliente	-I	--stdin	introducir los datos a ser transmitidos desde stdin
Cliente	-L	--listenport	puerto en que se recibirán pruebas bidireccionales de vuelta
Cliente	-P	--parallel	numero de de hilos paralelos a ejecutar
Cliente	-T	--ttl	time-to-live, paramulticast (por default 1)

A.3 Instalación Acrylic Wifi Professional

Se ingresa a la dirección web https://www.acrylicwifi.com/en/wlan-software/wifi-analyzer-acrylic-professional/, damos clic en Free Download y guardamos el archivo en el directorio local para su posterior instalación.

Ejecutamos el instalador y visualizamos la pantalla de la figura A.15.

Figura A.15. Pantalla inicial al ejecutar Acrylic Wi-Fi Professional.

Seguidamente visualizaremos una pantalla solicitando la Aceptación del acuerdo de licencia, seleccionamos la casilla y damos clic en Acepto.

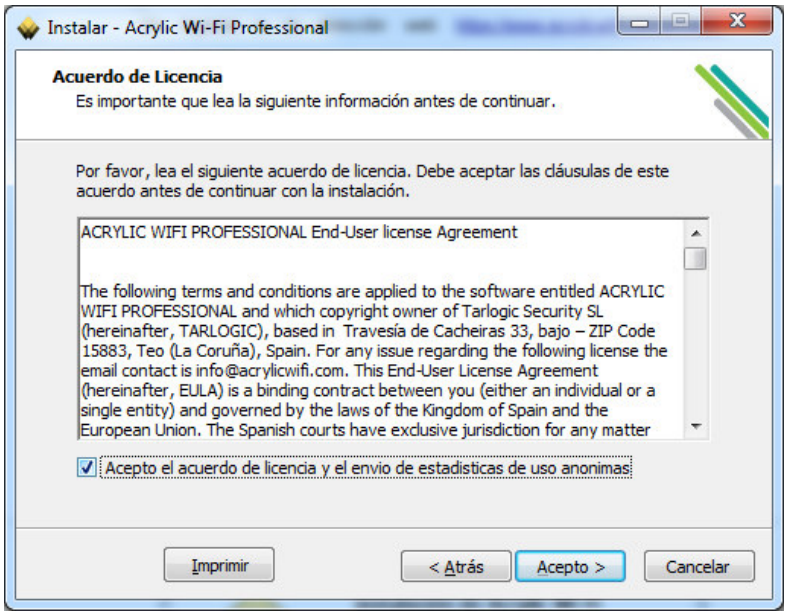


Figura A.16. Aceptación de los Acuerdos de Licencia.

Posteriormente nos solicita el directorio donde deseamos guardar nuestro programa. Por default viene la ruta donde alojamos nuestros Archivos de Programas en el disco principal o C:\. Si deseamos cambiar dicha ruta damos clic en el botón Examinar, caso contrario seleccionamos el botón Siguiente.

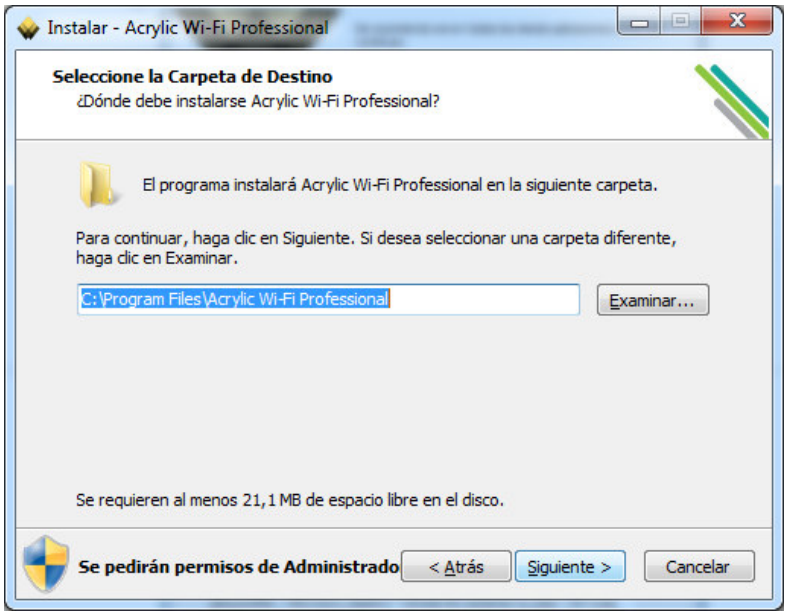


Figura A.17. Selección de directorio para guardar programa.

Luego nos aparecerá una ventana donde nos permite seleccionar los componentes a instalar, para el desarrollo de la presente tesis únicamente dejamos seleccionado el componente por default. Damos clic en el botón Instalar.

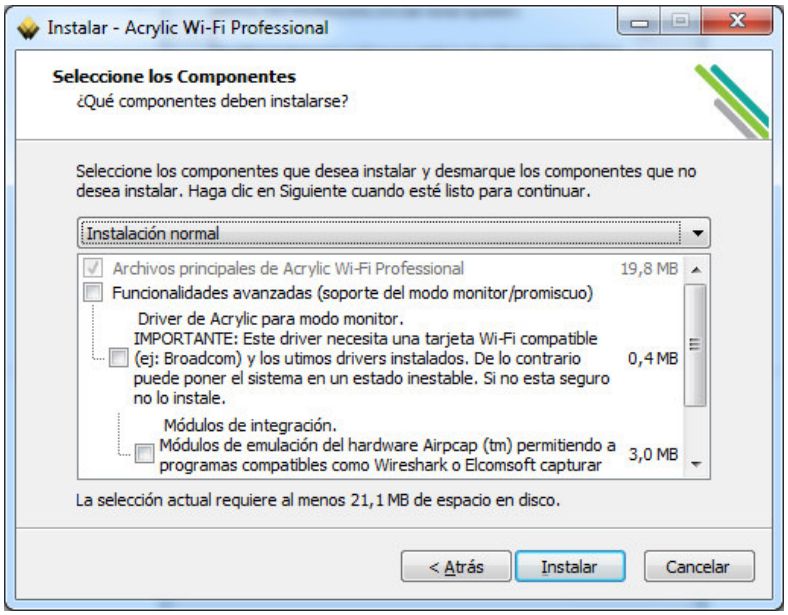


Figura A.18. Selección de componentes a instalarse.

Una vez elegido los componentes, nos aparecer la barra de progreso de instalación para luego iniciar a usar el aplicativo.

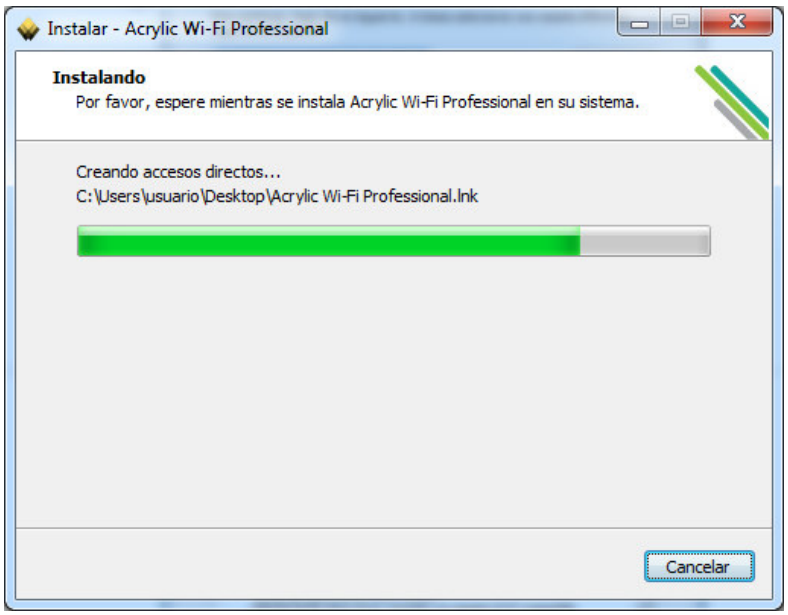


Figura A.19. Progreso de instalación del Software.

A.4 Instalación Virtualbox

Se ingresa a https://www.virtualbox.org/wiki/Downloads y seleccionamos la opción que se ajuste a nuestro equipo y sistema operativo. Para el desarrollo de la presente tesis se utilizar VirtualBox-4.2.12-84980-Win. Una vez guardado el archivo en el disco local, se ejecuta el archivo.

Una vez ejecutado el programa, nos aparece la figura A.20, el cual es un asistente que nos permite realizar el proceso de instalación de forma guiada. Damos clic en Next para iniciar.

Figura A.20. Inicio de wizard para instalación de VirtualBox.

Luego nos pregunta sobre los componentes que deseamos instalar para la aplicación, por default se encuentran seleccionados todos los ítems, estos es puerto USB, tarjetas de red y soporte para Python. Adicionalmente, se puede

seleccionar la ruta de instalación del programa, en caso de cambiar presionamos el botón Browse y seleccionamos la nueva ubicación; por default la ruta es C:\Program Files (x86)\Oracle tal como nos muestra en la figura A.21. Damos clic en Next para continuar.

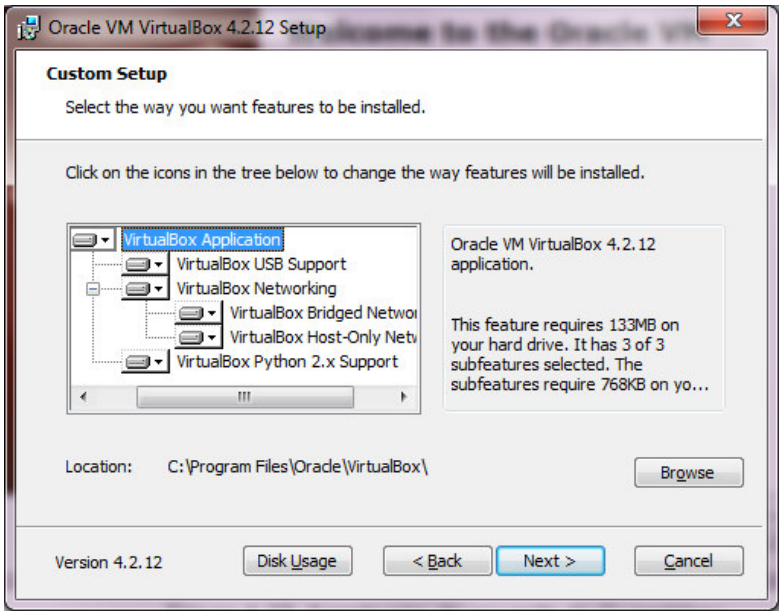


Figura A.21. Componentes y ruta de instalación de VirtualBox.

Seguidamente tenemos la opción de escoger los accesos directos necesarios para la aplicación tal como se visualizar en la figura A.22. Damos clic en Next para continuar.

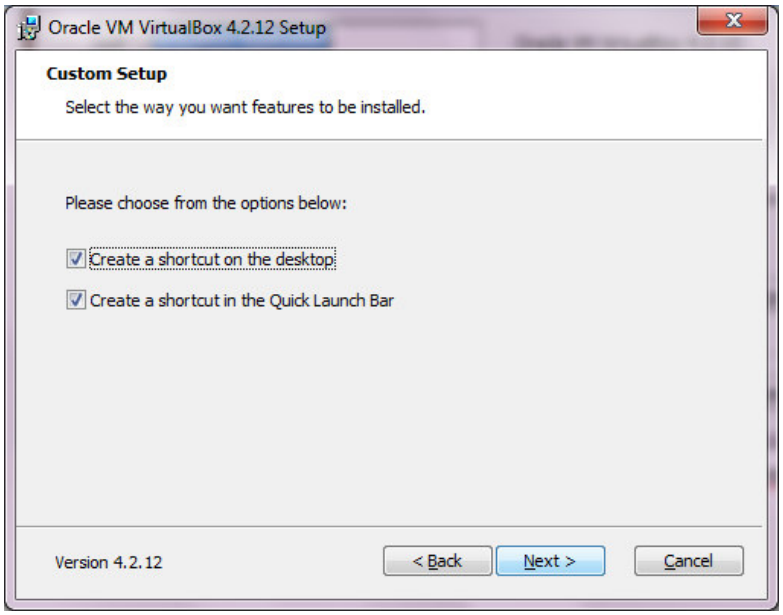


Figura A.22. Accesos directos para VirtualBox.

A continuación visualizamos un mensaje de alerta indicando que el acceso a la red será interrumpido por la instalación de los componentes de red de VirtualBox, tema que aceptamos mediante el botón Yes para continuar con el proceso tal como lo muestra la figura A.23.

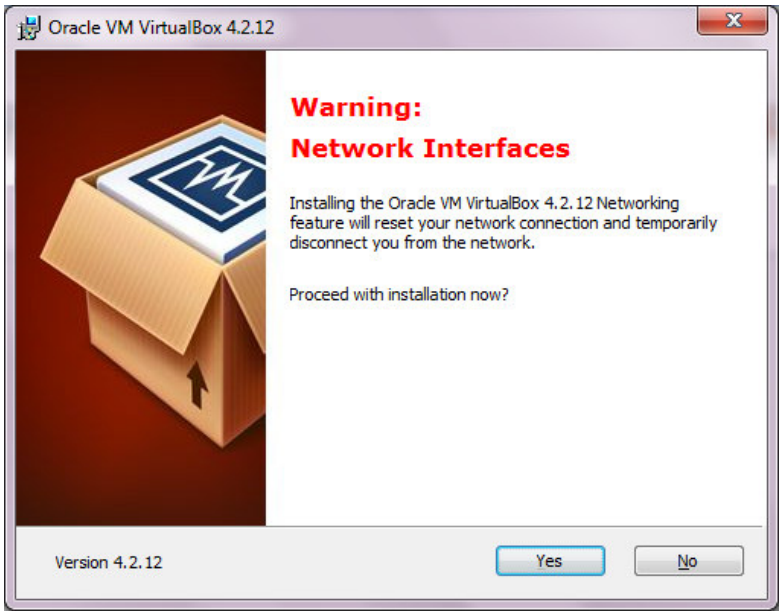


Figura A.23. Mensaje de inicio de instalación de VirtualBox.

Inicia el proceso de instalación, presionamos el botón Install.

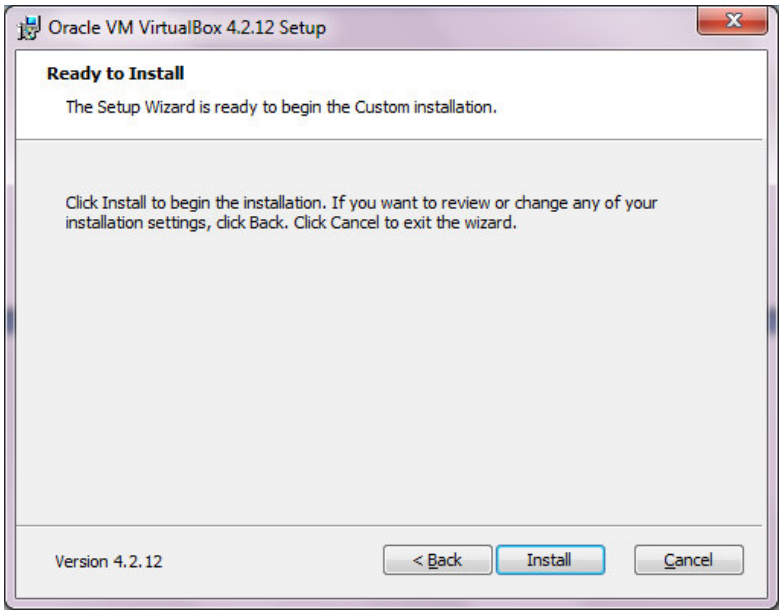


Figura A.24. Confirmación de instalación del Programa.

El proceso de instalación puede tardar varios minutos. Oracle Corporation solicita la autorización para la instalación de Controladora de Bus, servicio de red y adaptadores de red como se visualiza en las figuras A.25, A.26 y A.27, solicitudes que debemos aceptar para que la máquina virtual a instalar tenga contacto con el mundo exterior a través de interfaces de red virtuales.

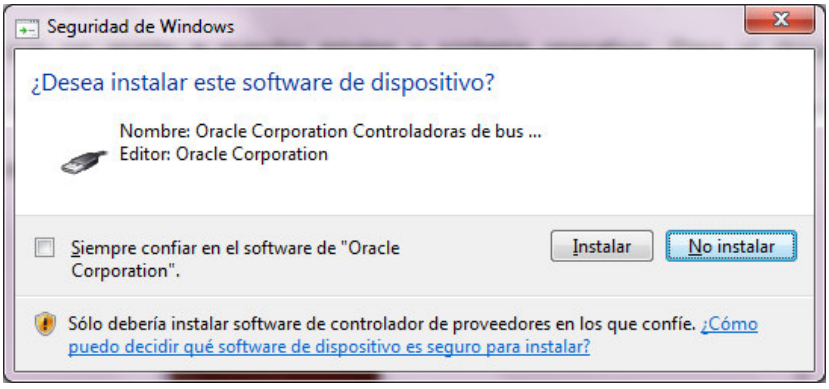


Figura A.25. Creación de interfaz virtual

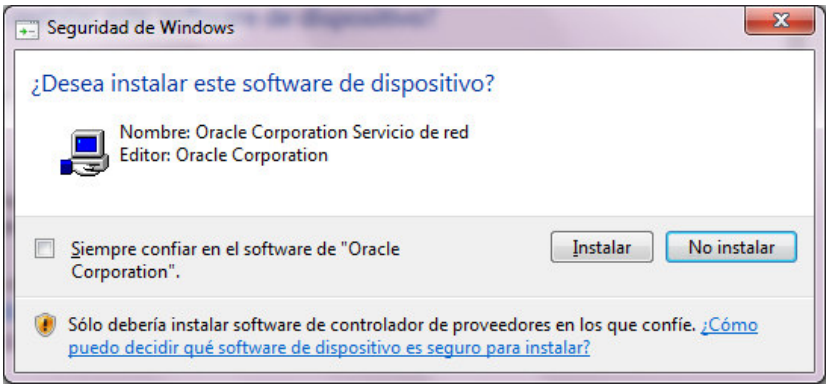


Figura A.26. Confirmación de instalación de servicios de red.

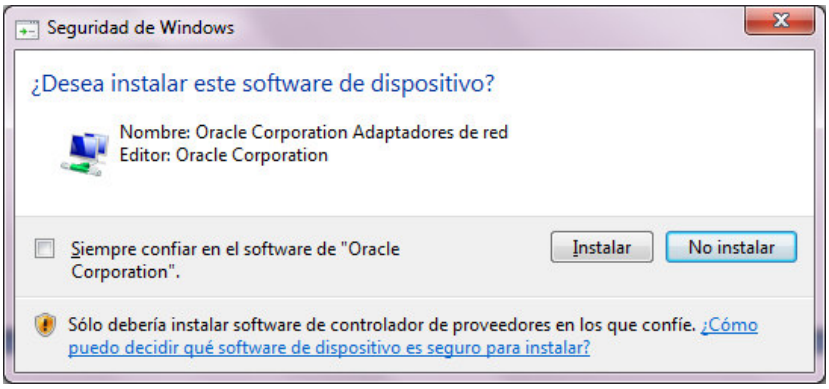


Figura A.27. Confirmación de instalación de adaptadores de red.

Finalmente nos aparece la venta de instalación completada presionamos el botón Finish.

Figura A.28. Mensaje de finalización de instalación.

Ejecutamos VirtualBox y nos vamos al icono Nueva a fin de crear una nueva máquina virtual tal como se visualizar en la figura A.29.

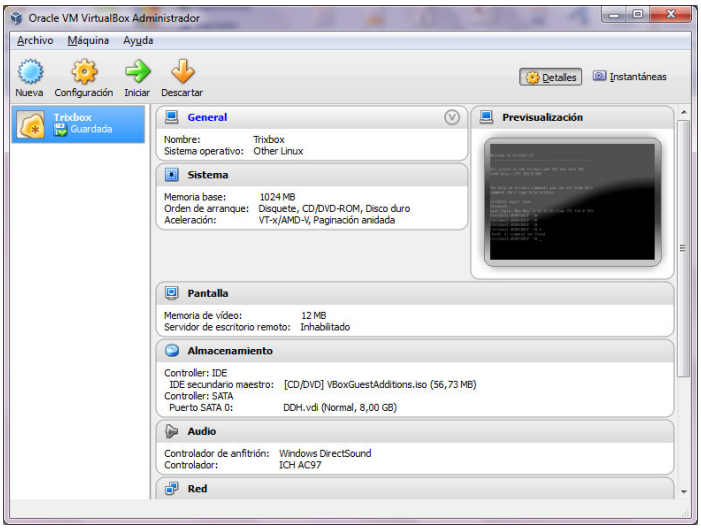


Figura A.29. Ejecución de maquina virtual.

Posteriormente seleccionaremos de entre un listado, el sistema operativo que más se asemeje a la instalación a realizar. Para nuestro caso es Linux, versión Other Linux debido a que no se encuentra disponible Trixbox como visualizamos en la figura A.30. Damos clic en Next.

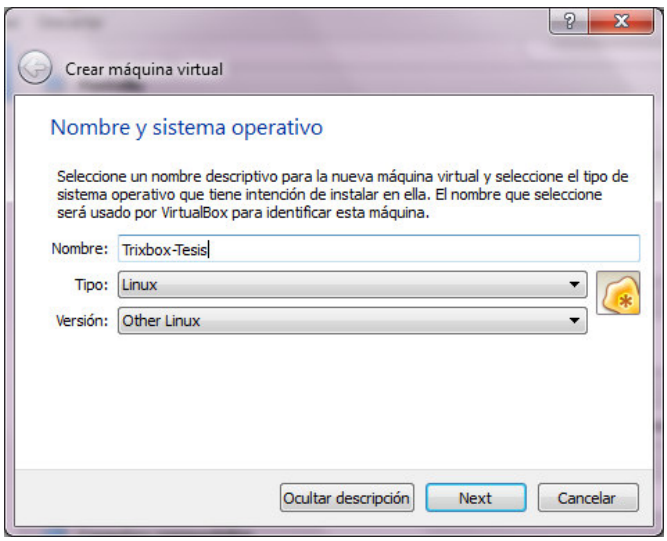


Figura A.30. Creación de máquina virtual y SO.

Para crear una máquina virtual necesitamos definir el tamaño de la memoria, la unidad de disco duro, el tipo de archivo de la unidad de disco duro, la forma de almacenamiento de la unidad de disco duro, nombre y ubicación de la unidad de disco duro y su tamaño, tal como visualizamos en la figuras A.31, A32, A.33, A.34 y A.35.

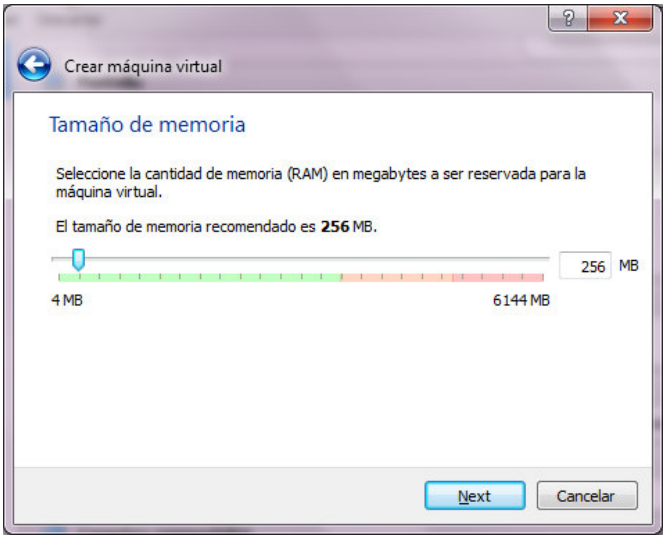


Figura A.31. Tamaño de memoria a usar en la máquina virtual.

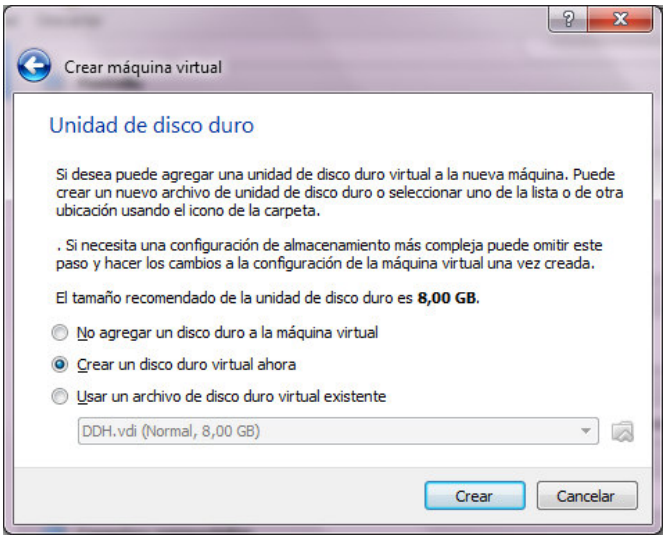


Figura A.32. Unidad de disco duro en la máquina virtual.

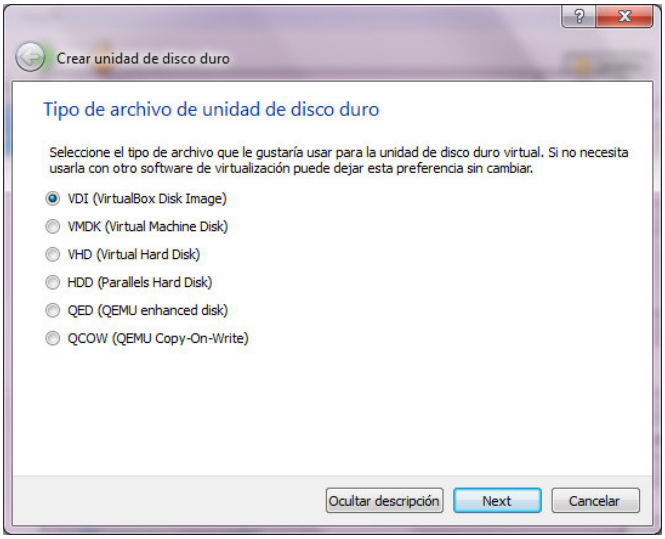


Figura A.33. Tipo de archivo del disco dura en la máquina virtual.

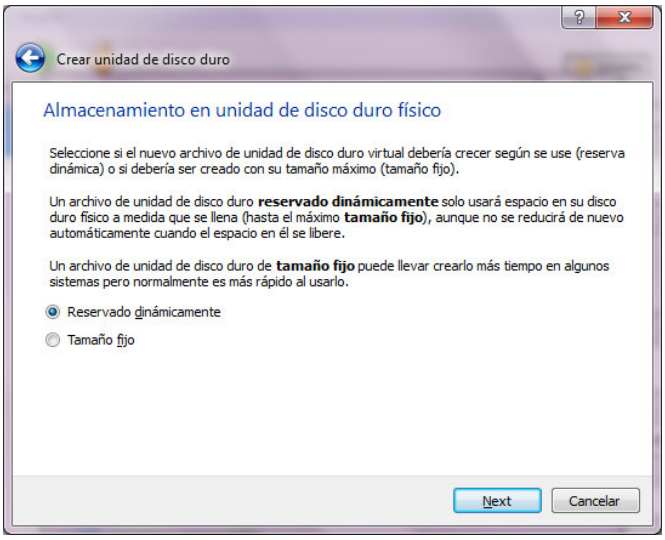


Figura A.34. Almacenamiento en el disco dura de la máquina virtual.

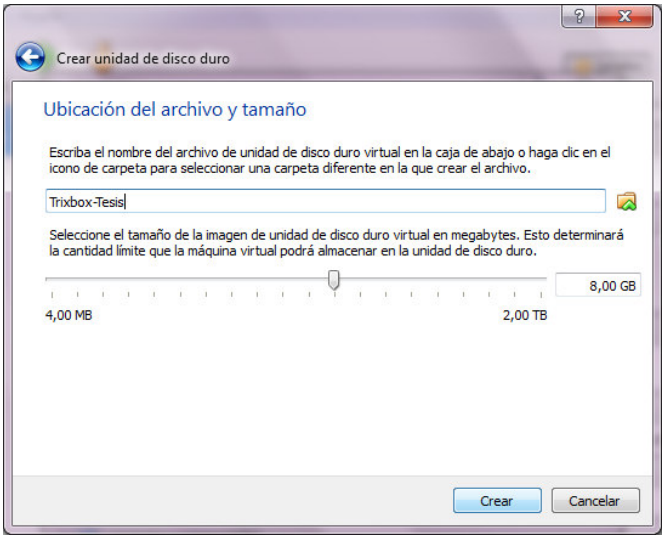


Figura A.35. Nombre y tamaño del disco duro en la máquina virtual.

Estamos listos para cargar el sistema operativo deseado en la máquina virtual creada.

A.5 Instalación Trixbox

Posterior a la instalación de VirtualBox, procedemos a instalar Trixbox como un sistema operativo dentro de la máquina virtual creada en la sección A.4.

Damos clic en el botón Iniciar para arrancar la máquina virtual tal como mostramos en la figura A.36.

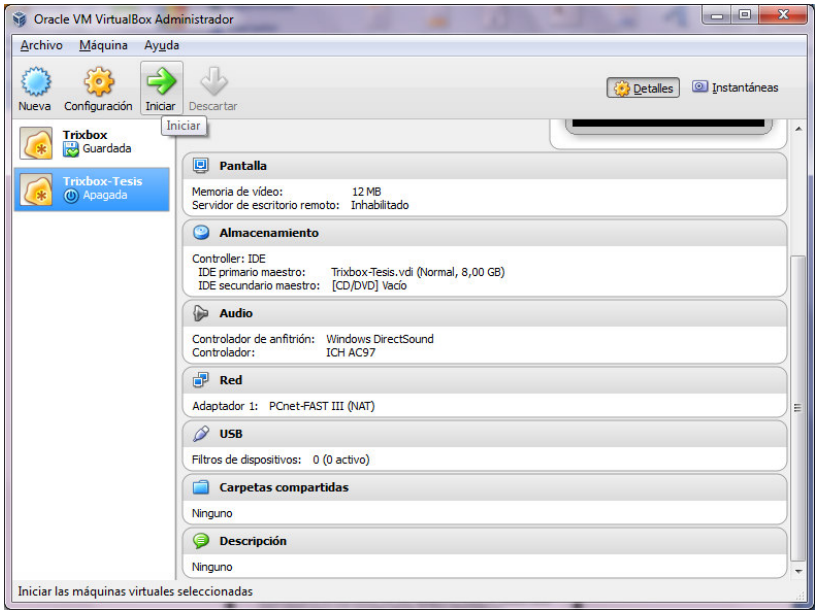


Figura A.36. Mensaje de inicio de instalación de VirtualBox.

Una vez iniciada la máquina virtual, nos aparece una pantalla en la cual debemos escoger el disco de inicio, en este momento escogemos la imagen ISO de Trixbox para comenzar la instalación del sistema operativo. La imagen de Trixbox la podemos descargar de la web, está disponible en el link

http://sourceforge.net/projects/asteriskathome/files/trixbox%20CE/trixbox%202.8/.

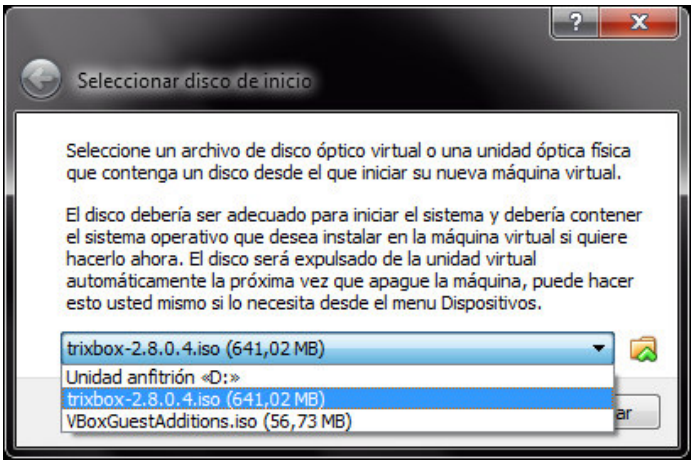


Figura A.37. Booteo desde la unidad virtual para instalar Trixbox.

Una vez arrancada la imagen .iso en la unidad virtual, presionamos Enter para poder iniciar la instalación según lo visualizado en A.38.

Figura A.38. Inicio de la instalación de Trixbox.

A continuación seleccionaremos el idioma del teclado y la zona horario donde nos encontramos y presionamos el OK. Cabe indicar que en estas pantallas el dispositivo de mouse no se encuentra activado, por tal motivo el desplazamiento entre las opciones debe ser realizado mediante la tecla Tab y la tecla Enter para aceptar.

Figura A.39. Idioma del teclado en la instalación de Trixbox.

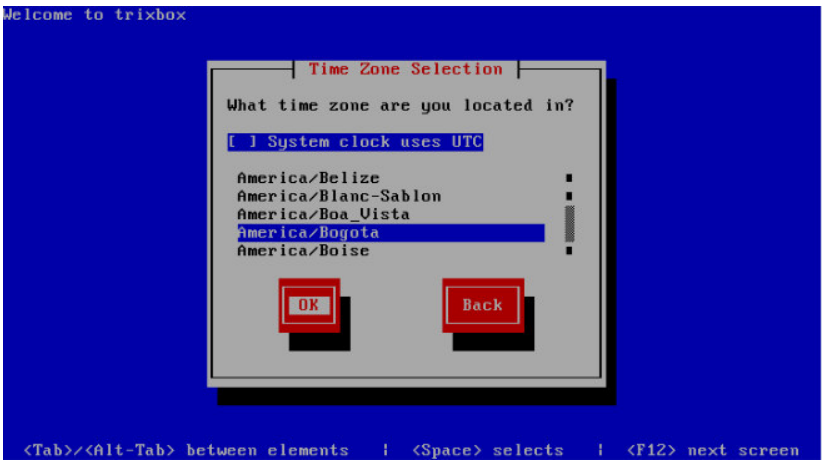


Figura A.40. Zona horaria de la localidad.

Luego, nos solicita la configuración de una contraseña para el usuario root, usuario administrador de la máquina virtual y sistema operativo instalado como se visualiza en la figura A.41.

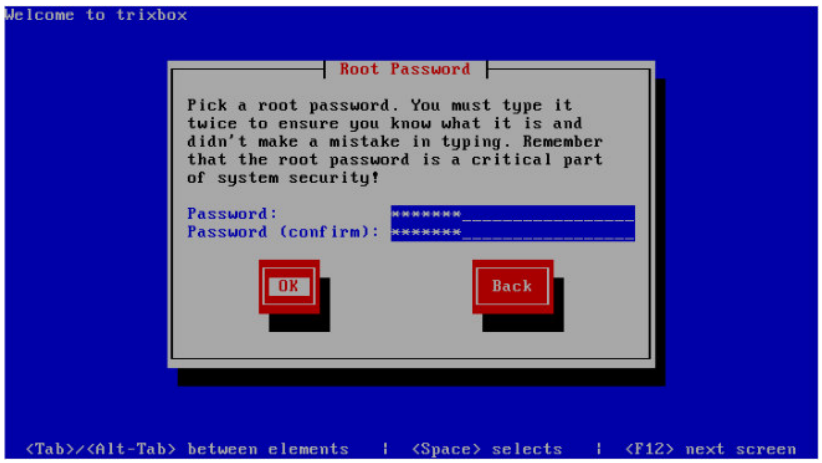


Figura A.41. Seteo de contraseña para el usuario root.

Finalmente iniciara el proceso de instalación e inicialización del sistema operativo tal como visualizamos en la figura A.42 y A43.

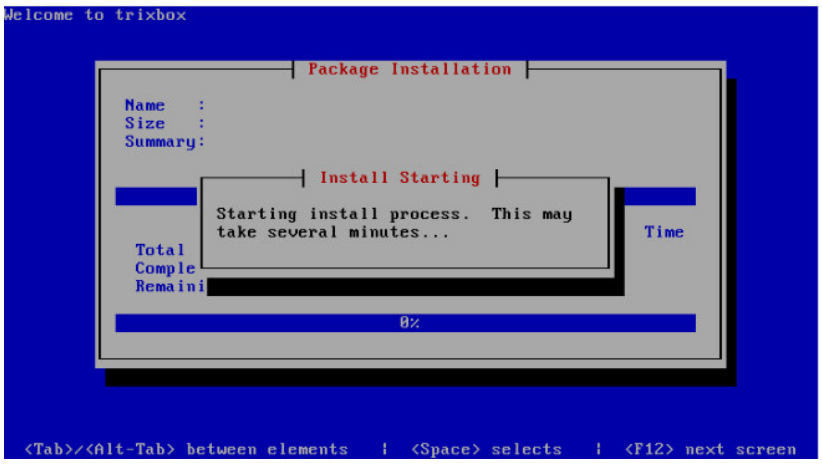


Figura A.42. Progreso de la instalación de Trixbox.

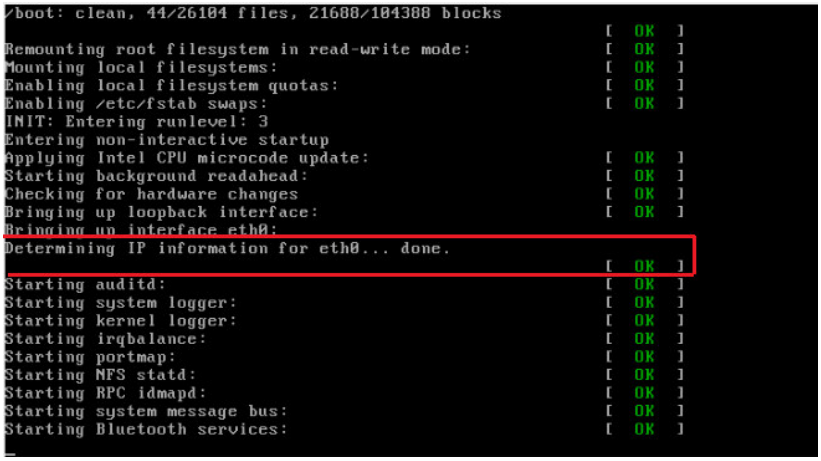


Figura A.43. Inicialización de Trixbox.

Una vez finalizada la instalación, nos aparece una pantalla solicitando autenticación, es decir usuario y contraseña de acceso. Se coloca la contraseña configurada en el paso descrito por la figura A.44.

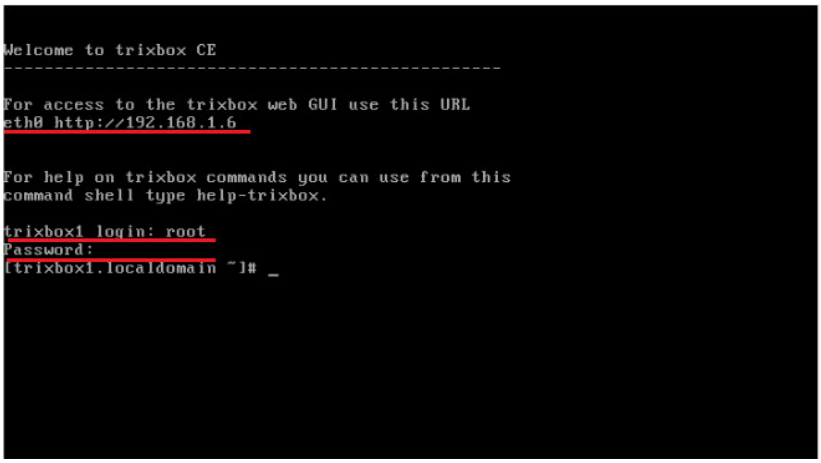


Figura A.44. Ventana de autenticación de Trixbox.

Para poder inicializar la máquina virtual debemos desactivar el booteo desde la imagen iso de Trixbox. Vamos al menú Dispositivos - Dispositivos CD/DVD y damos click en la opción seleccionado, tal como se presenta en la figura A.45. Con este cambio cada vez que se reinicie la máquina virtual arranca desde el disco duro virtual donde está instalado el sistema operativo.

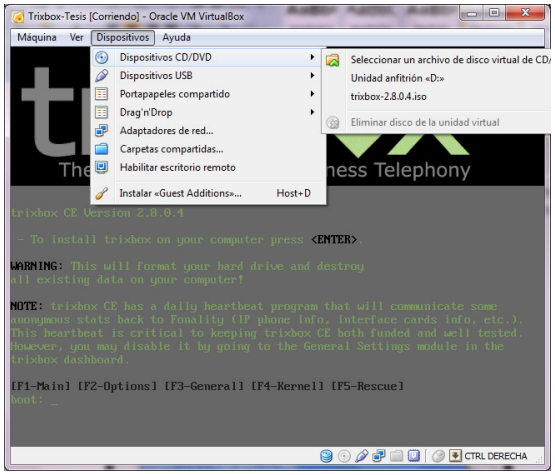


Figura A.45 Desactivar booteo desde imagen iso.

A.6 Instalación Zoiper

Se ingresa a http: //www.zoiper.com/en/voip-softphone/download/zoiper3, escogemos la plataforma del equipo a instalar, para nuestro caso Windows, y presionamos el botón Next, posteriormente elegimos la opción Free e inicia la descarga de la última versión disponible de la aplicación. Para la presente tesis se utilizó la versión 3.9. Una vez guardado en el disco local, se debe ejecutar.

Automáticamente inicia un Wizard que ayuda con la configuración de la aplicación. Se debe presionar el botón Next de acuerdo a lo mostrado en la figura A.46 para continuar con la instalación.

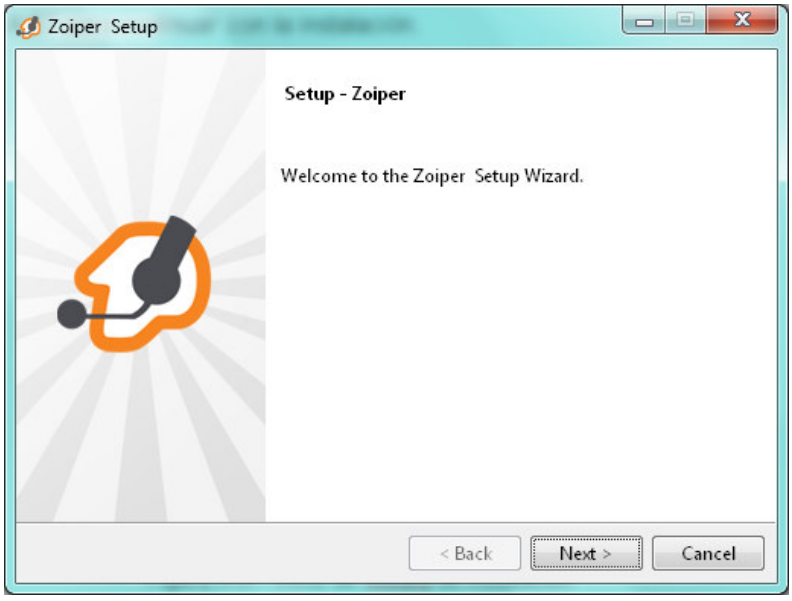


Figura A.46. Inicio de wizard de instalación

Posteriormente, nos solicita la aceptación del acuerdo de licencia para el uso de la aplicación, se debe presionar el botón I Agree según lo mostrado en la figura A.47.

Figura A.47. Aceptación del acuerdo de licencia de Zoiper.

Luego, nos aparece una ventana donde solicita la selección de la ruta donde será instalada la aplicación, por defecto la ruta es C:\Program Files (x86)\Attractel\Zoiper para nuestro caso, si se desea cambiar dicha ruta se debe presionar el botón Browse y elegir el nuevo directorio tal como se visualiza en la figura A.48 y luego presionar el botón Next.

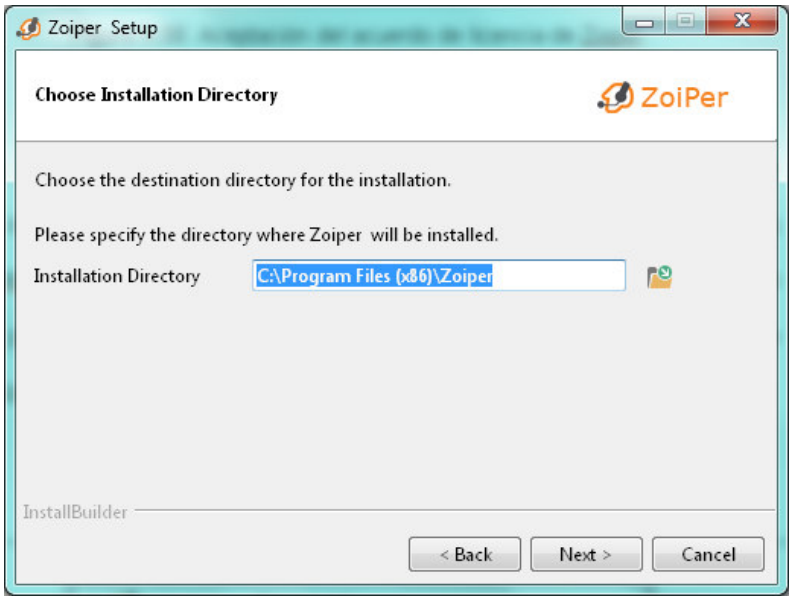


Figura A.48. Directorio de instalación de Zoiper.

Posteriormente como se visualiza en la figura A.49 se debe seleccionar la ubicación del acceso directo a Zoiper dentro del menú de Inicio de Windows, una vez seleccionado se presiona el botón Next.

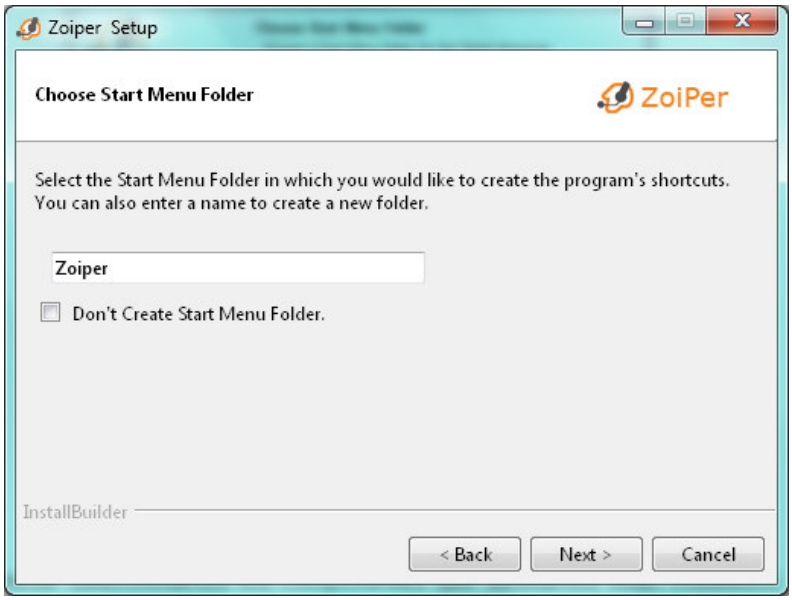


Figura A.49. Creación de acceso directo en el menú de inicio.

Finalmente seleccionamos los componentes que deseamos sean instalados en nuestro equipo, por defecto se encuentran seleccionados los accesos directos del menú inicio, escritorio y la aplicación en sí tal como lo muestra la figura A.50. Damos clic en Next y luego de unos minutos la instalación finaliza con la última ventana, presionamos el botón Finish como se visualiza en la figura A.51.

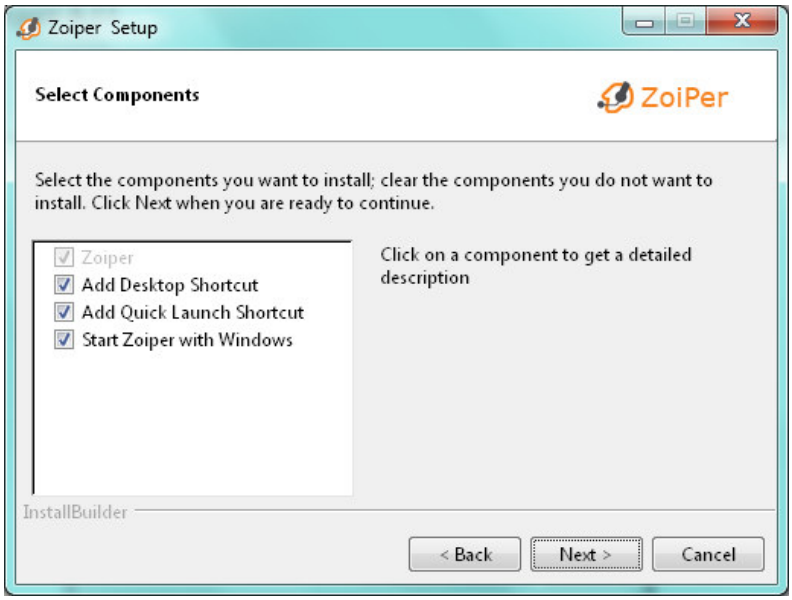


Figura A.50. Selección de componentes de instalación de Zoiper.

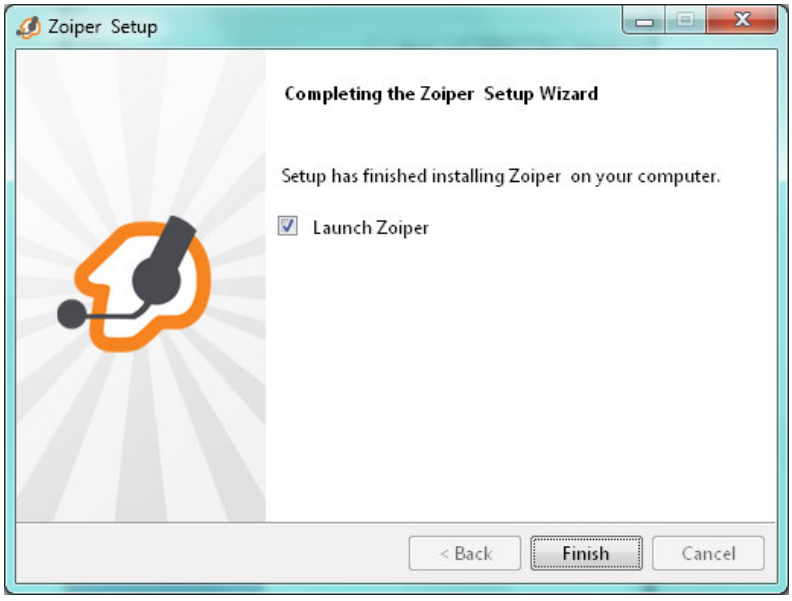


Figura A.51. Finalización de la instalación de Zoiper.

2 Bibliografía

[1] Cisco. [En línea]. Available: http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html.

[2] S. Basagni, C. Marco, S. Giordano y I. Stojmenovic, Mobile Ad Hoc Networking, John Wiley & Sons, 2004.

[3] Wi-Fi Alliance, [En línea]. Available: http://www.wi-fi.org/who-we-are/member-companies.

[4] Wi-Fi Alliance, «Wi-Fi Alliance,» [En línea]. Available: http://www.wi-fi.org.

[5] IEEE. [En línea]. Available: http://standards.ieee.org/news/2014/ieee_802_11ac_ballot.html.

[6] IEEE, [En línea]. Available: http://standards.ieee.org/getieee802/download/802.11-2012.pdf.

[7] [7struments, «High-Performance Wireless Ethernet,» *IEEE Communications Magazine,* 2001.

[8] S. C. Y. P. K. L. J. M. Haitao Wu, «Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN: Analysis and Enhancement,» *IEEE,* 2002.

[9] B. Y. W. K. H. H. Dubois Daniel, «shair.media.mit.edu,» [En línea]. Available: http://shair.media.mit.edu/publications/saso13/ShAir_SASO13.pdf. [Último acceso: 25 Diciembre 2015].

[10] R. K. L. B. M. P. L. Boroumand, «A Review of Techniques toResolve the Hidden NodeProblem in WirelessNetworks,» *Smart Computing Review,* vol. 2, nº 2, pp. 95-110, 2002.

[11] I. Biju, «Performance Evaluation of 802.11 Mobility and Interference Issues,» de *International Conference on* , Singapur, 2011.

[12] X. J. H. N. a. N. K. Jiajia Liu, «Exact Throughput Capacity under Power Control in Mobile Ad Hoc Networks,» de *IEEE INFOCOM 2011*, Shangai, 2011.

[13] A. Rahmati, «www.ruf.rice.edu,» [En línea]. Available: http://www.ruf.rice.edu/~mobile/publications/rahmati07mobisys.pdf. [Último acceso: 25 Diciembre 2015].

[14] K.-H. Jung, «academic.csuohio.edu,» [En línea]. Available: http://academic.csuohio.edu/yuc/papers/1569807749.pdf. [Último acceso: 25 Diciembre 2015].

[15] UIT-T, «Plan internacional de numeración de telecomunicaciones públicas,» UIT, Ginebra, 2011.

[16] UIT-T, «Visión general de las redes de próxima generación,» UIT, Ginebra, 2005.

[17] K.-H. Lee y K.-O. Lee, «Architecture To be Deployed on Strategies of Next-Generation Networks,» *IEEE,* 2003.

[18] R. M. Gray, «The 1974 Origins of VoIP,» *IEEE Signal Processing Magazine ,* vol. 22, nº 4, pp. 87-90, 2005.

[19] J. Hallock, «A brief history of VoIP,» Washington, 2004.

[20] H. D. Lüke, «www.hit.bme.hu,» *IEEE Communications Magazine,* vol. 37, nº 4, pp. 106-108, 1999.

[21] M. &. E. Y. C. Mishali, «Sub-nyquist sampling,» *Signal Processing Magazine,* vol. 28, nº 6, pp. 98-124, 2011.

[22] J. S. M. M. &. H. Y. (. Benesty, «book_sc_bas,» de *Springer handbook of speech processing*, Berlin, Springer Science & Business Media, 2008, p. 284.

[23] L. M. I. H. J. E. &. I. E. Sun, «Compresión de voz,» de *Guide to Voice and Video over IP*, Londres, Springer, 2013, pp. 17-51.

[24] N. N. S. &. A. S. Saleem, «Comparative Analysis of Speech Compression

Algorithms with Perceptual and LP based Quality Evaluations,» *International Journal of Computer Applications,* vol. 51, nº 15, pp. 37-41, 2012.

[25] W. Kleijn, «maxwell.ict.griffith.edu.au,» 1995. [En línea]. Available: https://maxwell.ict.griffith.edu.au/spl/publications/papers/book_sc_bas.pdf. [Último acceso: 25 Diciembre 2015].

[26] J. Davidson, «Voice coding stardards,» de *Voice over IP fundamentals*, Indianapolis, Cisco Press, 2006, p. 152.

[27] UIT-T, «Evaluación de la calidad vocal por percepción: Un método objetivo para la evaluación de la calidad vocal de extremo a extremo de redes telefónicas de banda estrecha y códecs vocales,» UIT, Ginebra, 2001.

[28] UIT-T, «Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs,» UIT-T, Ginebra, 2001.

[29] J.-H. Chen, «The BroadVoice Speech Coding Algoritm,» de *Codec WG meeting, IETF77*, Anaheim, 2010.

[30] J. A. C. Falcón, «La Arquitectura SIP,» de *VoIP: la telefonía de Internet*, Madrid, Editorial Paraninfo, 2007, p. 133.

[31] IETF, «SIP: Session Initiation Protocol,» IETF, 2002.

[32] IETF, «RFC 3261 - SIP: Session Initiation Protocol,» 2002.

[33] UIT-T, «H.323 : Sistemas de comunicación multimedia basados en paquetes,» UIT-T, Génova, 2009.

[34] M. Spencer, B. Capouch, E. Guy, F. Miller y F. Shumard, «IAX: Inter-Asterisk eXchange Version 2,» IETF, 2010.

[35] O. Salcedo, N. Diaz y G. López, «Session initiation protocol improvement using inter-asterisk exchange,» ACM, New York, 2011.

[36] C. Perkins, RTP Audio and Video for the Internet, Boston: Pearson Education, Inc., 2003.

[37] H. Schulzrinne, S. Casner, R. Frederick y V. Jacobson, «RTP: A Transport Protocol for Real-Time Applications,» The Internet Society, 2003.

[38] M. Baugher, D. McGrew, M. Naslund, E. Carrara y K. Norrman, «The Secure Real-time Transport Protocol (SRTP),» The Internet Society, 2004.

[39] L. J. A. K. Michal Halas, «IMPACT OF SRTP PROTOCOL ON VOIP CALL,» Slovak University of Technology, 2012.

[40] P. Gupta, «GSM and PSTN gateway for asterisk EPBX,» Tenth International Conference on, Aligarh, 2013.

[41] F. Iseki, Y. Sato y M. Wan Kim, «VoIP System based on Asterisk for Enterprise Network,» Tokyo University of Information Sciences, Tokyo , 2011.

[42] S. El brak, M. Bouhorma y A. A.Boudhir, «VoIP over MANET (VoMAN): QoS & Performance Analysis of Routing Protocols for Different Audio Codecs,» International Journal of Computer Applications, Tangier, 2011.

[43] P. Sing-Borrajo, «Evaluación de desempeño de VoIP en redes,» Universidad Central Marta Abreu de Las Villas., La Habana, 2013.

[44] P. Uchenna, M. Murtala y A. Nneka, «Optimising VoIP Traffic over MANET: Leveraging the Power of TORA On-Demand Routing Protocol,» International Journal of Computer Applications, Nigeria, 2013.

[45] University of Illinois, «iperf.fr,» [En línea]. Available: https://iperf.fr/. [Último acceso: 30 Abril 2015].

[46] Tarlogic Security, «www.acrylicwifi.com,» [En línea]. Available: https://www.acrylicwifi.com/software/analizador-wifi-acrylic-wifi-profesional/. [Último acceso: 25 Diciembre 2015].

[47] The Wireshark Team, «www.wireshark.org,» [En línea]. Available: https://www.wireshark.org/download.html. [Último acceso: 25 Diciembre 2015].

[48] Kwak y J. A., «Received signal to noise indicator». Estados Unidos Patente

9,014,650, 21 Abril 2015.

[49] UIT-T, «The use of the decibel and of relative levels in speechband telecommunications,» UIT, Génova, 2002.

[50] M. S. A. L. A. A. Alicia Vila, «www.uoc.edu,» [En línea]. Available: http://www.uoc.edu/in3/emath/docs/RegresionLineal.pdf. [Último acceso: 25 Diciembre 2015].

[51] A. L. L. K. B. I. K. S. V. &. F. M. Vlavianos, «Assessing link quality in IEEE 802.11 wireless networks: which is the right metric?,» de *PIMRC 2008, IEEE 19th International Symposium on IEEE*, Cannes, 2008.

[52] I. E. S. S. A. M. &. H. T. Kamarudin, «Performance Analysis on the Effect of G. 729, Speex and GSM Speech Codec on 802.11 g Wireless Local Area Network over VoIP using Packet Jitter,» *International Journal of Control and Automation,* vol. 6, nº 4, pp. 387-395, 2013.