FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

DISEÑO DE MODELOS ESTRUCTURALES DE REDES INALÁMBRICAS PARA PYMES

TRABAJO ESPECIAL DE GRADO

Presentado ante la

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

Como parte de los requisitos para optar al título de

INGENIERO DE TELECOMUNICACIONES

REALIZADO POR *Br. Kais Carranza, Johanna Libertad*

Br. Uruburu Márquez, Lisbeth Coromoto

PROFESOR GUÍA *Ing. Pirrone, José*

FECHA *Febrero de 2013*


UCAB
Universidad Católica
ANDRES BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

DISEÑO DE MODELOS ESTRCTURALES DE REDES INALÁMBRICAS PARA PYMES

Este jurado; una vez realizado el examen del presente trabajo ha evaluado su contenido con el resultado: _____.

JURADO EXAMINADOR

Firma:	Firma:	Firma:
Nombre:_____.	Nombre:_____.	Nombre:_____.

REALIZADO POR *Br. Kais Carranza, Johanna Libertad*

Br. Uruburu Márquez, Lisbeth Coromoto

PROFESOR GUÍA *Ing. Pirrone, José*

FECHA *Febrero de 2013*


UCAB
Universidad Católica
ANDRES BELLO

DEDICATORIAS

A Dios, que guía e ilumina cada uno de mis pasos.

A mis padres, Jacinto Kais y Carmen Carranza, por el amor y apoyo inmenso e incondicional que brindan día a día, por impulsarme a ser mejor y llegar cada vez más lejos en la búsqueda de mis sueños. Gracias por dejarme ser YO!

A mis hermanos, Jessica y Rafic Kais, porque han estado ahí para compartir buenos y malos momentos, para crecer, reír y llorar juntos.

A mis abuelos, Ricardo Carranza, Rafic Kais y Milagros Ferrero, esto también es de ustedes, gracias por el amor infinito.

A mis tíos; Roberto Gharibe y Nadia Kais; Alex Yépez y Maritza Bucaran; ustedes son una parte importante de este logro, gracias por la ayuda y los consejos.

A Gladys Yépez y Rafael Kais, a ustedes, que me acompañan siempre desde el cielo.

Johanna Kais

Este trabajo de grado se lo dedico primordialmente a mis padres Hugo Uruburu y Raiza Márquez por hacerme con sus consejos y regaños la persona que soy hoy en día, por su apoyo incondicional en los momentos buenos y en los no tan buenos, por enseñarme que no hay nada imposible y que si se lucha por lo que se quiere los resultados serán los esperados. Se los dedico porque definitivamente sin su apoyo, sin su ayuda y sin su amor este logro no hubiese sido posible.

A mis hermanos Yennifer Uruburu y Nick Uruburu por ser mis cómplices, por ser con quienes comparto mi día a día, por apoyarme en mis decisiones, por siempre estar para oírme, en definitiva por ser esas personitas que pese a la situación siempre podré contar con ellos.

A mis amigos, Nathalia Benavides, Luis Bernal, Pedro Avendaño, Alejandro Loreto, Marlyn Zapata, Guillermo Hernández, Freddy Vásquez por ser esas personas con las que he compartido muchísimas experiencias, por siempre tener una palabra de aliento, por hacerme sonreír, por estar conmigo en las buenas y malas, en fin por ser parte de mi vida.

A mi amiga y compañera de tesis Johanna Kais por estar en todo este proceso, por su ayuda incondicional, por su apoyo, consejos, paciencia y sobre todo por estar cuando más la necesito. Lo logramos.

A todas esas personas que de una u otra manera hicieron que el camino recorrido en estos 5 años y medio fuera simplemente PERFECTO.

Lisbeth Uruburu

AGRADECIMIENTOS

Primeramente a Dios por todos los días vividos, por darnos fuerzas, ánimo, ímpetu y paciencia para lograr una de nuestras metas más anheladas.

A nuestros padres por el infinito esfuerzo realizado para que pudiéramos realizar y culminar nuestros estudios con todas las comodidades y recursos necesarios.

A nuestro tutor Ingeniero José Pirrone, por acceder a ser el responsable del éxito de este Trabajo Especial de Grado y por la ayuda brindada.

Al Ingeniero Luis Molner, por su orientación en la realización del trabajo especial de grado.

A Félix Ziegler, Heumir Ávila y Javier Barrios, por su amistad sincera, comprensión y apoyo a lo largo de toda nuestra carrera.

A Luis Ugas por su colaboración para la culminación del Trabajo Especial de Grado.

A TODOS GRACIAS!

Johanna Kais y Lisbeth Uruburu.

RESUMEN

En el mundo de las telecomunicaciones, los avances tecnológicos, despiertan la meta diaria de ir más lejos y más rápido, sin comprometer la eficiencia, la seguridad ni el costo de manera significativa. Las PYMES, aún con necesidades tecnológicas, no poseen patrones de conexión para el máximo funcionamiento de la empresa. Este Trabajo Especial de Grado plantea una propuesta a los diferentes tipos de PYMES, para implementar una red inalámbrica en su organización y así poder llevar un mejor control de sus recursos y administrar de forma más eficiente sus servicios.

Se diseñaron dos (2) modelos estructurales de redes inalámbricas para una posible implementación en pequeñas y medianas empresas, tomando en cuenta los servicios ofrecidos y los diferentes departamentos de estas organizaciones. Los modelos garantizan segmentación de la red con Redes de áreas locales virtuales (*VLAN's*) y seguridad para un mejor rendimiento de la red, así como proporcionar información de equipos más convenientes en relación precio-calidad.

Definido estos parámetros se llevaron a cabo simulaciones de cobertura de los diferentes modelos establecidos, con el *software* RPS para comprobar que los equipos conectados reciban la intensidad de potencia necesaria para un buen desempeño, lo que conlleva un estudio de la ubicación de los equipos a utilizar para garantizar el mayor provecho de los equipos a instalar.

Se comprobó el rendimiento y correcto funcionamiento de la red bajo los modelos propuestos, haciendo el uso de los paquetes de simulación PACKET TRACER y OPNET, demostrando el buen desempeño de los modelos propuestos.

Palabras claves: PYMES, red inalámbrica, *VLAN's*, seguridad, conectividad.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

Las redes de computadores nos permiten la interconexión entre varios equipos para establecer comunicación, en la actualidad se requiere que esta actividad se realice de forma inalámbrica ya que permite beneficios que un enlace cableado no puede brindar, entre ellos podemos mencionar la movilidad entre los usuarios en un rango determinado y que una red inalámbrica permite economizar recursos tanto materiales como económicos.

La implementación de una red inalámbrica necesita conocimientos básicos con respecto a la tecnología que se desea utilizar, los estándares que maneja, las topologías en las que se puede realizar la conexión, entre otros; además que no se debe dejar de lado los aspectos de seguridad y autentificación.

Hoy en día, el auge de las pequeñas y medianas empresas (PYMES) en Venezuela, genera la interrogante acerca de cómo manejar los aspectos técnicos para el buen funcionamiento de la empresa, aun cuando la mayoría son de carácter familiar y son administrados por sus propios dueños y la heredan de generación en generación, la parte tecnológica es capaz de brindar grandes beneficios y mejorar el nivel de ventas o producción, según sea el caso.

En la actualidad, las empresas administran sus recursos de forma digital, lo que hace necesario que se implementen servicios de seguridad en las redes utilizadas para evitar que terceros sean capaces de acceder a la información que se transmite por medio de la red. La seguridad de redes dependerá del servicio que se esté implementando, de las características de la red y de los deseos de los usuarios.

El diseño de modelos estructurales de redes inalámbricas para PYMES, garantizando conectividad y seguridad a los usuarios surge con la necesidad de atacar las necesidades primordiales de una empresa, que son tener una conectividad estable

y tener resguardo de todos los movimientos que se realicen utilizando la red como medio.

Así mismo, los modelos diseñados, servirán como patrón en la implementación de las funcionalidades tecnológicas de una PYME en nacimiento, ya que se estandarizaran los aspectos departamentales más importantes al igual que sus funciones y necesidades. Estos patrones, permitirán mejorar los niveles de producción o ventas de las empresas al generar esquemas de implementación organizados según las necesidades de cada empresa.

CAPÍTULO I
PLANTEAMIENTO DEL PROYECTO

Buscando justificar el desarrollo del tema de este Trabajo Especial de Grado, se especifica el problema que se busca solucionar, los objetivos que serán llevados a cabo para su cumplimiento, las limitaciones del proyecto y los alcances que tendrá. Así como la contribución que brindará a la Ingeniería de Telecomunicaciones.

1. Planteamiento del problema

Las PYMES como fuentes generadoras de desarrollo económico de la sociedad, pueden ser implementadas en distintas áreas laborales sin importar la actividad desarrollada. En la actualidad el concepto de pequeñas y medianas empresas (PYMES) se encuentra en su mejor auge, debido a sus características ha llegado a convertirse en una de las principales modalidades a la hora de crear o establecer una actividad económica.

Según la ley para PYMES, en Venezuela se clasifican según la cantidad de empleados en las categorías antes mencionadas, como toda empresa (sin importar su dimensión) la comunicación entre los departamentos de la misma, es de suma importancia desde el punto de vista organizativo y para la toma de decisiones a corto, mediano, y largo plazo, sin embargo, no existe un patrón de conexión para este tipo de organizaciones, lo que sin lugar a dudas agilizaría el proceso de iniciar una pequeña o media empresa, tomando en cuenta que este tipo de compañías necesitan una conexión interna segura, rápida y eficaz, además de equipos específicos como servidores, enrutadores y computadoras para la construcción de dicha conexión.

La departamentalización tecnológica de una empresa brinda altos beneficios, ya que, al separar los departamentos como administración, nomina, inventario, producción, etc., le brinda a la empresa la capacidad de trabajar de forma segura y

segmentada, lo que ofrece un mejor desempeño para la empresa y sus trabajadores, evitando rupturas en el tráfico de información general si algún punto de la red fuese a fallar.

Debido al crecimiento significativo de las nuevas tecnologías y de las organizaciones definidas como pequeñas y medianas empresas, haciendo enfoque en la necesidad de estas de generar mayores ingresos y garantizar un mejor desempeño laboral, surge la necesidad de implementar tecnologías de comunicación dentro de las instituciones.

Al momento de diseñar y estructurar una red, la principal característica que se ve comprometida es la movilidad, especialmente ahora que gracias al avance tecnológico, del cual somos testigos día a día, y la aparición de los llamados equipos inteligentes, se ha generado una necesidad de estar conectados en todo momento, lo que, usualmente, se resuelve al conectarse a una red inalámbrica que puede ser pública, o privada, dependiendo si el usuario se encuentra en casa, la oficina, la universidad, centros comerciales, etc.

Otro inconveniente es la falta de seguridad en la conexión, aunque es más común en redes públicas, también puede ocurrir en redes privadas, mostrando vulnerabilidad ante ataques que busquen extraer información personal de los usuarios. Si bien este problema es una molestia para un usuario normal, genera grandes complicaciones en organizaciones donde se desea la máxima seguridad de conexión posible, al intercambiar datos confidenciales.

Con la finalidad de resolver esta situación, se desea diseñar una red inalámbrica que asegure un intercambio de datos de forma confiable para PYMES. Se implementará una red inalámbrica de área local, ya que, brinda ventajas sobre una red cableada, como la poca planificación para la ubicación de equipos, bajo costo de implementación y alta escalabilidad.

Para mantener confidencialidad en la información que se intercambia entre el personal que labora en instituciones privadas, la implementación de la red será orientada al personal de los diferentes departamentos que conformen la organización, para el envío y recepción de los diferentes tipos de datos que maneje la empresa, la conexión a la red podrá ser realizada desde las computadoras empresariales, y dispositivos móviles personales de trabajadores, previamente autorizados, utilizando el método de autentificación más eficiente.

El diseño de la red será aplicada en PYMES y a sus usuarios; para lo cual, basándose en el estudio descrito anteriormente, se establecerán patrones o modelos de estructuras de pequeñas y medianas empresas, para ser el objeto principal de análisis y diseño de las redes, las topologías de redes se modelarán y simularán para verificar su correcto y deseado comportamiento, la red será diseñada con el fin de cumplir los parámetros más significativos del estudio estructural y funcional de las PYMES.

2. Objetivos

2.1. Objetivo general

Diseñar modelos estructurales de redes inalámbricas para PYMES.

2.2. Objetivos específicos

- Estudiar teóricamente las PYMES, para obtener parámetros esenciales de su estructura organizativa y física con el fin de diseñar modelos básicos.
- Especificar las tecnologías aplicables a las redes inalámbricas.
- Estudiar y seleccionar las herramientas de *hardware*, *software* y dispositivos periféricos necesarios que permitan diseñar la red inalámbrica en los modelos de PYMES establecidos.
- Realizar el estudio del espacio físico de los modelos para determinar los lugares más convenientes para colocar los elementos de la red.
- Comprobar la cobertura de los equipos seleccionados, mediante simulaciones.

- Diseñar las topologías de redes inalámbricas para cada modelo y realizar simulaciones de conectividad, transferencia de datos y seguridad sobre la misma

3. Limitaciones y alcances

3.1. Limitaciones

- Se tomarán como máximo tres parámetros relevantes de las PYMES para diseñar los modelos básicos.
- Los modelos a su vez estarán diseñados y divididos según la clasificación más adecuada de las PYMES, luego del estudio teórico.
- Los costos reflejados en esta investigación únicamente servirán de referencia.

3.2. Alcances

- Estudiar estructural y organizativamente las PYMES en Venezuela.
- Diseñar los prototipos para los modelos establecidos y realizar la simulación de los mismos.
- Los modelos establecidos para la implementación de redes inalámbricas para PYMES, servirán de patrón para nuevos empresarios o compañías que deseen interconectar su organización de forma inalámbrica.

4. Justificación del proyecto

Diariamente, pequeñas y medianas empresas tienen constante transferencia de información entre las oficinas y/o departamentos que las integran, sin embargo, al usar computadoras de escritorio, la movilidad de dichos archivos se vuelve un poco limitada. Al desear mantener el tráfico de datos y la movilidad de los usuarios con dispositivos portátiles, se origina el proyecto "Diseño de modelos estructurales de redes inalámbricas para PYMES".

De esta manera, se le brinda a las empresas el servicio continuo de conexión entre los usuarios y el internet, garantizando a su vez, la integridad de los datos que circulan a través de la red, ya que muchos pueden ser datos confidenciales y pueden estar expuestos a ataques ajenos, más si se trata de agrupaciones laborales.

Este proyecto, realiza un aporte al mundo de las telecomunicaciones. En el ámbito individual, rompe las barreras que encierran a los usuarios, permitiendo libertad de movimiento dentro del rango de cobertura y asegurando que la información que es intercambiada entre usuarios o con la nube viaja de forma segura. Empresarialmente, permite la inclusión de nuevas tecnologías para mejor desempeño de las actividades cotidianas en búsqueda de mayor productividad.

Capítulo II

Marco Teórico

El desarrollo de un Trabajo Especial de Grado implica una investigación profunda acerca de los conocimientos teóricos que servirán como apoyo al desarrollo del diseño de modelos estructurales de redes inalámbricas para PYMES; entendiéndose como modelo al patrón de diseño que se plantea establecer. En este capítulo se desarrollan todos estos conceptos, con un énfasis especial en PYMES y sus clasificaciones, redes inalámbricas locales (*WLAN*) y sus características más importantes, tecnologías para estas redes y por último, seguridad de datos y tipos de autenticación.

La distribución de los conceptos antes mencionados, se muestra en el siguiente mapa mental:

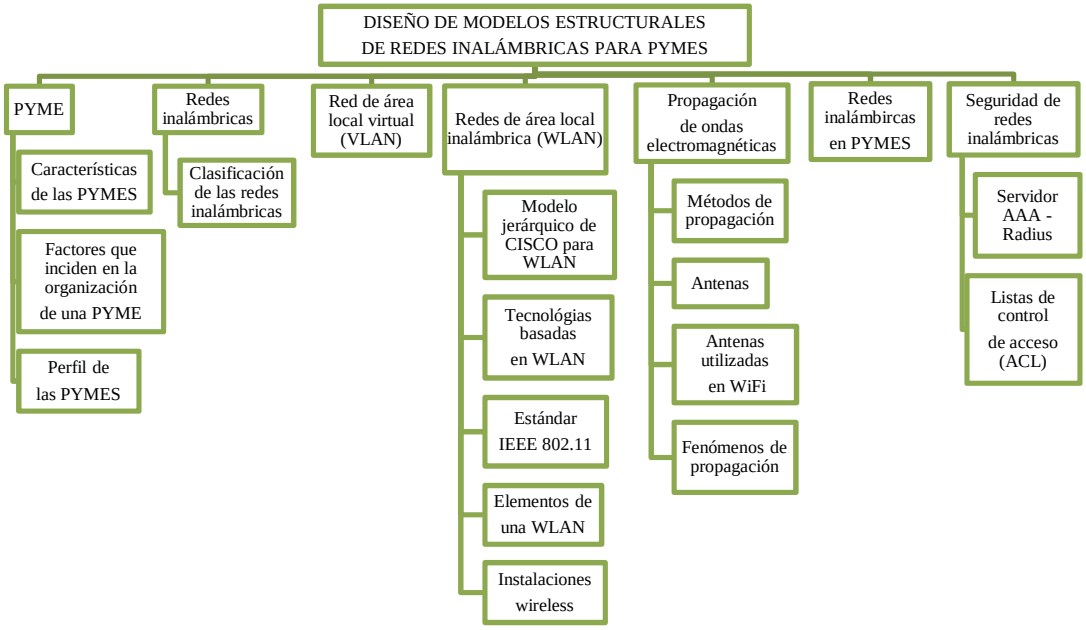

Figura 1 - Diagrama de contenido del Marco Teórico

Fuente: (Propia)

1. PYME (Pequeña y Mediana Empresa)

Toda unidad organizada jurídicamente con la finalidad de desarrollar un modelo económico productivo mediante actividades de transformación de materias prima en insumos, en bienes industriales elaborados o semi-elaborados, dirigidas a satisfacer las necesidades de la comunidad es una PYME.

Se considerará pequeña industria a aquéllas que tengan una nómina promedio anual de hasta cincuenta (50) trabajadores y con una facturación anual de hasta cien mil Unidades Tributarias (100.000 UT). Se considerará mediana industria a aquéllas que tengan una nómina promedio anual de hasta cien (100) trabajadores y con una facturación anual de hasta doscientas cincuenta mil Unidades Tributarias (250.000 UT). (Decreto N° 6.215, 2008)

La pequeña y mediana industria, y unidades de propiedad social, son inexorablemente, fuentes de desarrollo autosustentable, que redundan en la ocupación laboral de las distintas organizaciones socio comunales de la Nación, ya que generan constantemente nuevas inversiones, instituyéndose así en un mecanismo de energía activa y propulsora de la economía, que respalda el progreso nacional equitativo.

En términos generales, la PYME es aquella que, sin importar las actividades que realiza y el sector al que pertenece, no ocupa una opción dominante en su ramo, no dispone de elevados recursos económicos, posee una plantilla reducida de su personal, es dirigida personalmente por sus propietarios, no está vinculada directa o indirectamente a grupos financieros, y su cifra de facturación anual y su capital es reducido. (Sánchez, 2010)

Un aspecto técnico, vinculado directamente con el tamaño, que responde a la estructura industrial alcanzada por cada país, y que se obliga a definir políticas diferenciadas de fomento para este estrato.

1.1. Características de las PYMES

- Se encuentra establecida en todos los países del mundo ya que otorga elasticidad para amoldarse al actual ambiente incierto y cambiante.
- Es un motor en el proceso de desarrollo económico y, por ende, del bienestar social, ha sido generadora y distribuidor de ingresos para el desarrollo económico en todos los países del mundo, en donde logran mayor eficiencia a través de la delegación de aspectos sensibles, o no manejables, de sus procesos productivos. (Sánchez, 2010)
- Son fáciles de establecer, generan empleo y pueden constituir el inicio de grandes empresas.
- Responden con mayor facilidad a los cambios del entorno, lo que justifica cualquier inversión que realicen los gobiernos en proyectos de apoyo dirigidos a estas, tiene la mayor justificación económica social.
- Tienen alta posibilidad de fracaso.
- Operan con volúmenes limitados, lejos de la economía de escala, ergo, de la mayor productividad. No pueden competir en negocios donde manda la magnitud. (Sánchez, 2010)
- La debilidad financiera es incierta, pero no necesariamente grave.
- La localización inadecuada, muchas veces nacen en localizaciones que no son las más apropiadas. Esto limita su acceso a mercados importantes, sus relaciones con grandes empresas y con los grandes centros tecnológicos, académicos y de decisión política y económica.
- Se considera pequeña empresa aquellas que tengan en nómina un promedio anual de 50 trabajadores y mediana empresa tiene una nómica anual de 100 trabajadores.

1.2. Factores que inciden en la organización de una PYME

Factores internos son los elementos que buscan medir la eficiencia interna de la organización, entre los cuales encontramos:

- Físicos: son las variables de las que depende el sustento, o permanencia, de la empresa, guarda relación con la satisfacción de los clientes y la rentabilidad del negocio.
- Estructura organizativa: define la organización, jerarquías y funciones de cada área o departamento, lo cual dependerá del tipo y del tamaño de cada negocio. De acuerdo con las necesidades de la empresa, se crean áreas de ventas, servicio, recursos humanos, atención a clientes, contabilidad, entre otros, al definir las áreas y las jerarquías se permite generar un organigrama para obtener una herramienta de organización de la empresa.
- Recurso humano: permite mantener un orden de las actividades para implementar el sistema de gestión de la empresa y para realizar las mejoras de la organización
- Financieros: el empresario debe tener conocimiento de las finanzas de los negocios para así generar un verdadero compromiso con su empresa.
- Legal: asume los asuntos legales y jurídicos de los documentos y asuntos de la organización. (Viloria, 2007)

Factores externos: se refiere a los aspectos a los cuales las acciones de la empresa no tienen efecto alguno.

- Socioeconómicos: indica que, en la nación hay cambios políticos, económicos y sociales y, ya que, el gobierno está tratando de instaurar un nuevo modelo económico del país, este desarrollo plantea generar efectos como participación de la comunidad, la protección del medio ambiente, entre otros. También se plantea el fomento de políticas estratégicas que eleven la productividad de las pequeñas y medianas empresas, enmarcado en el principio de igualdad, cero discriminación y mínimo gasto.
- Tecnológicos: se deben considerar las nuevas tecnologías, su ritmo de evolución y las posibles aplicaciones, por ejemplo el avance de la electrónica, de la informática, entre otros.

- Gubernamentales: el gobierno siempre afecta de forma directa, y creciente, las condiciones en que funciona la empresa, el análisis de los factores socioeconómicos tanto en el ámbito nacional como internacional pueden generar cambios relevantes. (Viloria, 2007)

1.2. Perfil de las PYMES

- Datos estructurales: los criterios para establecer dimensiones, tamaño y estructura física de las PYMES son específicos para cada empresa, ya que esta depende de la rama de trabajo, por lo general, la estructura orgánica de estas empresas es familiar.
- Tecnología: sistema de producción tradicional.
- Medio ambiente: es complejo, sostiene relaciones con proveedores, asociaciones, gobierno, etc.
- Valores y objetivos: la toma de decisiones es centralizada, por lo general, la realizan los jefes o en su defecto, los jefes de cada área. (Peinado & Prado, 2008)

2. Red Inalámbrica

Inicialmente se define una red de computadoras como, la interconexión de equipos con el fin de lograr un intercambio de datos, recursos o servicios. Por su parte, "inalámbrico" es un sistema de comunicación eléctrica que no utiliza alambres conductores, esto quiere decir que la comunicación se establece sin enlaces físicos entre los equipos (Tanenbaum, 2003).

Por lo tanto, una red inalámbrica permite conectar varios nodos sin el uso de conexiones físicas sino estableciendo una vía de comunicación a través de ondas electromagnéticas. Esta modalidad de conexión supone una mayor comodidad y un ahorro de dinero en infraestructura, aunque suele tener un bajo nivel de seguridad.

2.1. Clasificación de las redes inalámbricas

Las redes inalámbricas se clasifican bajo varios parámetros, el más significativo es según la extensión, o cobertura, que abarcara la red, cuyas categorías son:

- *WPAN* (Red inalámbrica de área personal): está conformada por redes de corto alcance abarcando aéreas de algunas decenas de metros, es usada generalmente para conectar dispositivos periféricos a una computadora o para conectar dos computadoras cercanas, las velocidades de transmisión se encuentran entre los 250Kbps hasta 10Mbps. Las tecnologías usadas son Infrarrojos, *BLUETOOTH*, *HOMERF* (*Home Radio Frecuency*) y ZIGBEE.
- *WLAN* (Red inalámbrica de área local): cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros y una velocidad máxima de transmisión de 450Mbps, las tecnologías más importantes utilizadas en estas redes son *WiFi* e *HiperLAN2*.
- *WMAN* (Red inalámbrica de área metropolitana): son también conocidas como *WLL* (*Wireless Local Loop*), o bucle local inalámbrico, se basan en el estándar IEEE 802.16, ofreciendo una velocidad de 1 a 10Mbps y un alcance hasta diez kilómetros. La tecnología más conocida es *WiMax* alcanzando hasta 70Mbps a varios kilómetros de cobertura.
- *WWAN* (Red inalámbrica de área amplia): tienen el alcance más amplio de todas las redes inalámbricas, es utilizada para dar servicio a la telefonía móvil, las tecnologías más utilizadas son: *GSM* (*Global System for Mobile Communication*), *GPRS* (*General Packet Radio Service*) y *UMTS* (*Universal Mobile Telecommunication System*). (Andreu, Pellejero, & Lesta, 2006)

3. Red de Área Local Virtual (VLAN)

Una *VLAN* es una agrupación lógica de dispositivos, o servicios de red, en base a funciones o departamentos, equipos de trabajo o aplicaciones, sin considerar la localización física o conexiones de red. Su función principal es la segmentación lógica de la red en diferentes dominios de *broadcast*, es decir, que los paquetes son

solamente conmutados entre puertos que han sido asignados a la misma *VLAN*. Los *router* que operan bajo este concepto proveen filtrado, escalabilidad, seguridad y administración del flujo de tráfico y mejor desempeño de la red. (Molina, 2012)

Entre las ventajas que ofrece el uso de VLAN, encontramos:

- Incrementan el desempeño de la red, agrupando estaciones de trabajo, recursos y servidores según su función.
- Facilidad en la administración, ya que permite el fácil movimiento y cambio de estaciones de trabajo en la red.
- Mejoran la seguridad de la red porque solo se podrán comunicar las estaciones de servicio pertenecientes a la misma *VLAN* (Sin enrutamiento).
- Facilitan el control de flujo de tráfico porque permiten controlar la cantidad y tamaño de los dominios de broadcast.
- La configuración de *VLAN's* no requieren movimientos o conexiones físicas de los equipos de red (Molina, 2012)

4. Red de Área Local Inalámbrica (*WLAN*)

Describe un sistema de comunicación de datos que transmite y recibe utilizando ondas electromagnéticas, en lugar del par trenzado, coaxial o fibra óptica utilizados en *LAN* convencionales. (Andreu, Pellejero, & Lesta, 2006). Proporcionan conectividad inalámbrica dentro de un edificio, una pequeña área residencial/urbana o de un campus universitario.

Este tipo de redes se componen fundamentalmente de puntos de acceso y los dispositivos de cliente, donde el punto de acceso actúa como un concentrador, o *hub* que recibe y envía información, vía radio, a los dispositivos de cliente, habitualmente una computadora o un dispositivo personal que incluya una tarjeta de red inalámbrica con o sin antena. (Monachesi, Frenzel, Chaile, Carrasco, & Gómez, 2011)

Una de las ventajas de este tipo de redes es que además de permitir la libertad de movimiento a los usuarios que requieren tener información disponible en cualquier lugar, también se caracteriza por ser mucho más sencilla de instalar que las redes de cable y permiten una reubicación más rápida de los terminales.

La desventaja principal de esta red es la seguridad, ya que son propensas a sufrir ataques (más que todo pasivos) si los parámetros de seguridad no fueron configurados de forma correcta. Otro punto débil son las interferencias que puede sufrir la comunicación, debido a rango de frecuencia (2,4 o 5GHz) puede sufrir obstrucciones por objetos de uso común como teléfonos inalámbricos, controles remotos y otros. (Andreu, Pellejero, & Lesta, 2006)

4.1. Modelo Jerárquico de CISCO para redes *WLAN*

4.1.1. Capa Núcleo (Backbone)

Está diseñado para hacer que los paquetes conmuten lo más rápido posible, es el responsable del transporte de grandes cantidades de tráfico en forma rápida y confiable. En esta capa no se debe realizar ninguna manipulación de paquetes porque estas acciones reducen el tráfico. (Ariganello, 2006)

4.1.2. Capa de Distribución (Routing)

Las principales funciones son proveer enrutamiento, filtros, acceso *WAN* y determinar como pueden acceder los paquetes. La capa de distribución es donde se implementan las políticas para la red, las acciones más comunes que deben hacerse en esta capa son:

- Enrutamiento
- Implementación de listas de control de acceso.
- Implementación de seguridad y políticas de red, incluyendo traslado de direcciones y *firewalls*.
- Calidad de servicio.
- Enrutamiento entre *VLAN's* y otras funciones.

- Posible punto para acceso remoto.
- Traslado de medios de comunicación.

4.1.3. Capa de Acceso (Switching)

Es el punto en el cual los usuarios finales son conectados a la red. Esta capa puede usar listas de acceso o filtros para optimizar las necesidades de los usuarios. Entre sus funciones se encuentran:

- Continúa el control de acceso y políticas.
- Creación de dominios de colisión separados.
- Conectividad de los grupos de trabajo dentro de la capa de distribución.
- Habilitar filtros de direcciones *MAC*.
- También es posible tener acceso a grupos de trabajo remotos. (Ariganello, 2006)

4.2. Tecnologías basadas en WLAN

El uso de redes inalámbricas locales puede ser manejado de diversas maneras, las tecnologías más utilizadas para este tipo de red, se definen a continuación:

- *HiperLAN/2*: es una solución estándar para un rango de comunicación corto que permite una alta transferencia de datos y *QoS* del tráfico entre estaciones base *WLAN* y terminales de usuarios. La seguridad está provista por lo último en técnicas de cifrado y protocolos de autenticación. Usa la banda de 5GHz y una velocidad de transmisión de hasta 54Mbps. Los servicios básicos son transmisión de datos, sonido, y vídeo. (Pahlavan & Krishnamurthy, 2002)
- *WiMax*: es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2.3 a 3.5GHz. También conocidas como bucle local que permite la recepción de datos por microondas y retransmisión por ondas de radio. Una de sus ventajas es dar servicios de banda ancha en zonas donde el despliegue de cable o fibra por la baja densidad de población presenta unos costos por usuario muy elevados (zonas rurales). (WiMax, 2012)

- *WiFi*: se refiere a una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día, también llamada estándar IEEE 802.11. Los más conocidos en la actualidad son:
    a. 802.11b, emite a velocidades de hasta 11Mbps
    b. 802.11g, con una velocidad máxima de 54Mbps
    c. 802.11n, la más rápida en la actualidad, a 450Mbps

  Su alcance es de hasta 150 metros en hardware asequible. El funcionamiento de la red es bastante sencillo. Al tratarse de conexiones inalámbricas, no es difícil que se intercepte la comunicación y se tenga acceso al flujo de información, por lo que los *routers* incluyen herramientas de configuración para controlar el acceso a la red. Por esto, es recomendable la encriptación de la transmisión para emitir en un entorno seguro. (WiFi Alliance, 2012)

	WiFi (802.11g)	***WiFi (802.11n)***	***WiMax***
Protocolo	Media Access Control (CSMA/CA)	Media Access Control (CSMA/CA)	Conexión orientada a MAC
QoS	Afirmación de acceso	Afirmación de acceso	Basado en conexiones base-usuario
Tipo de red	Punto a punto y *Ad Hoc*	Punto a punto y *Ad Hoc*	Punto a punto y *Ad Hoc*
Distancia	100 metros	70 metros	30-60 kilómetros
Tasa de Tx	15-54 Mbps	450 Mbps	124 Mbps
Costo	Bajo	Bajo	Alto

Tabla 1 - Diferencias entre WiFi y WiMax

Fuente: (Propia)

4.3. Estándar IEEE 802.11

La norma IEEE 802.11 define el uso de los niveles más bajos de la arquitectura *OSI (Open System Interconnection)*: capa física y de enlace. Los protocolos de la rama 802.x definen la tecnología de aérea local. La familia IEEE 802.11 incluye varias técnicas de transmisión usando los mismos protocolos (Andreu, Pellejero, & Lesta, 2006). Los estándares más utilizados en la actualidad son:

Estándar	Frecuencia	Velocidad	Rango	Tecnología
802.11 a	5 GHz	54 Mbps	10 mts	OFDM
802.11b	2,4 GHz	11 Mbps	100 mts	OFDM
802.11g	2,4 GHz	54 Mbps	100 mts	OFDM
802.11n	2,4 - 5 GHz	> 100 Mbps	70 mts	OFDM

Tabla 2 - Características de los estándares 802.11

Fuente: (Propia)

Es importante mencionar que los dispositivos 802.11a y 802.11b son incompatibles, sin embargo existen equipos que incorporan ambos chips, por lo que se llaman dispositivos de "banda dual". (Alliance, 2012)

4.4. Elementos de una WLAN

- *Router o* enrutador: son dispositivos de red suficientemente inteligente para enviar tráfico desde una red a otra, dependiendo del origen y del destino. Un enrutador examina cada paquete que le llega y, dependiendo de la dirección del nodo origen y del nodo destino, el enrutador decide si el paquete debe permanecer en la red o debe enviarlo a otra red. (Seoane, 2005)

  Un *router* inalámbrico comparte el mismo principio que el tradicional. La diferencia es que este permite la conexión de dispositivos inalámbricos (como estaciones *WiFi*) a las redes a las que el *router* está conectado mediante conexiones por cable, generalmente ETHERNET. Otra característica de los routers inalámbricos es que incluyen un switch y un punto de acceso.
- Puntos de acceso: también llamados *AP's* o *wireless access point*, son equipos *hardware* configurados en redes *WiFi* y que hacen de intermediario entre el computador y la red externa (local o Internet). El access point, hace de transmisor central y receptor de las señales de radio en una red *wireless*, normalmente van conectados físicamente, por medio de un cable de pares a otro elemento de red en caso de una oficina, o directamente a la línea

telefónica si es una conexión doméstica. Son los llamados *Wireless Routers* y soportan los estándar 802.11a, 802.11b, 802.11g y 802.11n.

- *Firewall*: funciona como barrera entre redes, permitiendo o negando las transmisiones de una red a otra. Un uso típico es situarlo entre una red local y la red internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial. El *firewall* es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o no el paso, para esto, se examina el servicio al cual corresponde, y si la comunicación entra o sale. (Seoane, 2005)
- Servidor: puede ser *software* o *hardware*, su función principal es proveer diferentes servicios a los usuarios de la red en la que se encuentra. El uso de los servidores es generalmente para satisfacer las peticiones de los usuarios de una red, administrando los recursos según convenga. Los servidores existen en una amplia variedad, proporcionando servicios de impresión, seguridad, correo, telefonía, configuración proxy, base de datos, *WEB*, etc.
- Conmutador: también llamado *switch,* es un dispositivo digital lógico de interconexión. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección *MAC* de destino de las tramas en la red. Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

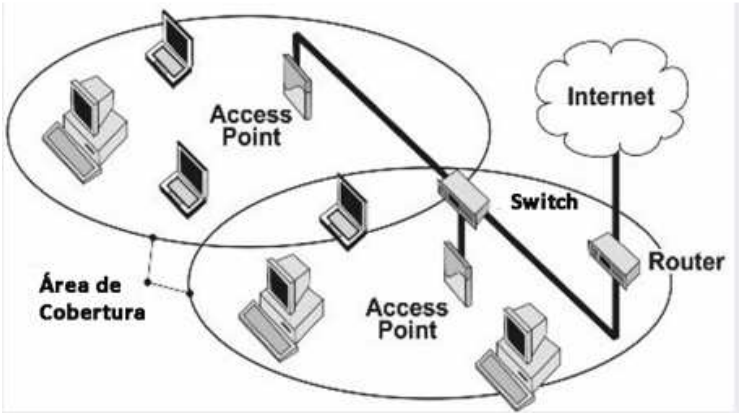

Figura 2 - Red inalámbrica básica

Fuente: (Andreu, Pellejero, & Lesta, 2006)

4.4. Tipos de instalaciones Wireless

Básicamente existen dos tipos de instalaciones, las internas que pueden realizarse punto a punto, o multipunto (utilizando puntos de acceso) y las de exteriores (usando el modo "*Bridge*" o "*Mesh*"), las cuales son un poco más complicadas, ya que sus condiciones son más propensas a cambios y sufren inconvenientes por distancia u obstáculos:

- Punto a punto: es la conexión entre dos puntos distantes, lo que permite mantener un canal de comunicación por donde se pueden transferir servicios multimedia (voz, datos, video), utilizando frecuencias licenciadas, y no licenciadas, entre 900MHz y 5GHz. Con este tipo de comunicación se pueden cubrir hasta 30 Km de distancia, dependiendo de la potencia de los equipos y el diseño utilizado. (Técnicas Profesionales, 2012)
- Basadas en puntos de acceso: su principal función es conectar dispositivos inalámbricos con dispositivos basados en cableado físico. Esta es la instalación típica utilizada en empresas, ya que desean conectar máquinas de forma inalámbrica sin que pierdan las funcionalidades de una red cableada.
- Instalación tipo *Bridge*: es una de las funciones más solicitadas, su función es conectar dos redes situadas en edificios distintos ahorrando el cableado. En este caso, los puntos de acceso no hacen el papel de concentrador inalámbrico,

sino se conectan entre ellos para formar un *bridge* o puente entre los edificios y brindan la conexión. (Técnicas Profesionales, 2012)

- Instalación tipo *Mesh*: se trata de redes malladas, sin estructura concreta, pero con máxima cobertura, las redes inalámbricas de este tipo mejoran la confiabilidad al establecer caminos de redundancia. Son redes que permiten extender la cobertura *WiFi* a zonas a las cuales no se puede cablear, o que las instalaciones de cableado son inviables a nivel económico. Los *access point*, además de dar señal a los clientes locales, hacen de repetidores de la señal.

5. Propagación de Ondas Electromagnéticas

El estudio de la propagación de ondas electromagnéticas en el espacio libre es llamada "Propagación de radiofrecuencia" (RF) o radio propagación. Según la frecuencia y la distancia, los circuitos radioeléctricos pueden establecerse en la parte interior, media o superior de la atmosfera, donde cada una posee características distintas.

5.1. Métodos de propagación.

- Onda de tierra: es la forma predominante de propagación a frecuencias de hasta 3MHz, la polarización de onda y las características del terreno juegan un papel importante. (Pérez, Zamanillo, & Casanueva, 2007)
- Onda ionosférica: transmite señales a frecuencias entre 3 y 30 MHz, esta propagación aprovecha las características de la ionósfera que actúa como reflector permitiendo alcanzar distancias de miles de kilómetros.
- Onda espacial: también llamada onda directa, predomina en la transmisión de frecuencias mayores a 30MHz e intervienen varios fenómenos como la absorción, reflexión, difracción y refracción. (Pérez, Zamanillo, & Casanueva, 2007)

5.2. Antenas

Una antena es un dispositivo metálico encargado de convertir ondas electromagnéticas "conducidas" por una línea de transmisión o guía de ondas, en ondas que pueden propagarse libremente en el espacio. Una antena es entonces una interfaz entre el espacio libre y la línea de transmisión. (Monachesi, Frenzel, Chaile, Carrasco, & Gómez, 2011).

Las antenas poseen parámetros que pueden ser medidos para definir las características y funcionalidades de las antenas, entre estos parámetros, tenemos:

- Directividad: es la propiedad que tiene la antena de transmitir o recibir energía irradiada en una dirección particular.
- Ganancia: se define como la relación entre dos magnitudes físicas iguales (energía, potencia, tensión, etc.), es decir, un numero adimensional expresado en función de la energía radiada de otra antena, generalmente isotrópica o dipolo.
- Patrón de radiación: es la representación gráfica de la forma en que la energía electromagnética de una antena se distribuye en el espacio. Puede ser representado de forma cartesiana o polar.
- Ancho del haz: es la distancia angular entre los puntos potencia mitad de la antena, se estudia vertical y horizontalmente. Es inversamente proporcional a la ganancia. (Monachesi, Frenzel, Chaile, Carrasco, & Gómez, 2011)
- Eficiencia de la antena: está definida por la relación entre la potencia radiada por la antena y la potencia total que se le entrega en determinada frecuencia.
- Polarización: se refiere a la orientación de la transmisión del campo electromagnético. Puede ser lineal o elíptica.
- Ancho de banda: es el intervalo de frecuencia en el cual debe funcionar satisfactoriamente la antena. Las limitaciones del ancho de banda, varían según el tipo de antena. (Monachesi, Frenzel, Chaile, Carrasco, & Gómez, 2011)

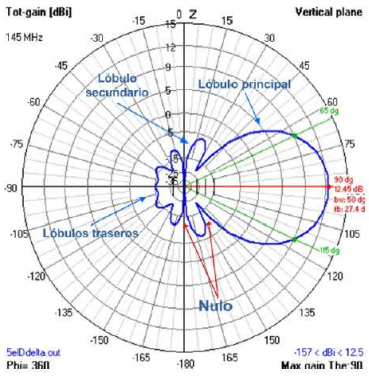

Figura 3 - Ejemplo de patrón de radiación

Fuente: (Monachesi, Frenzel, Chaile, Carrasco, & Gómez, 2011)

5.3. Antenas utilizadas en Wifi

- Antena dipolo: es la más simple de las antenas y consta de dos elementos metálicos rectilíneos que se colocan en el terminal de una línea que transporta la energía electromagnética de una fuente.
- Antena cúbica: se construye mediante espiras de alambre formando anillos de forma cuadrada.
- Antena de apertura: está formada por chapas de metal de forma cónica para lograr diferentes ángulos de apertura respecto al vértice y a los ejes vertical y horizontal.
- Arreglo de antenas: agrupa varias antenas formando una matriz para lograr una determinada direccionalidad y efectividad controlando las fases de las ondas.
- Antenas con reflectores: se colocan elementos adicionales a la antena para modificar su direccionalidad. (Monachesi, Frenzel, Chaile, Carrasco, & Gómez, 2011)

5.4. Fenómenos de propagación

Son los procesos físicos que intervienen en la propagación de las ondas electromagnéticas en el espacio, las más importantes son:

- Propagación y pérdidas por espacio libre: son aquellos cambios de dirección y potencia que sufre la onda en su trayecto debido a las diferentes características del medio en que se propaga.
- Atenuación: describe la perdida de intensidad de la onda a medida que se aleja de la fuente, se debe a la dispersión esférica de la onda.
- Refracción: es el cambio de dirección que sufre una onda al pasar de un medio a otro que tiene una velocidad de propagación diferente.
- Reflexión: se presenta cuando la onda incidente choca con una frontera entre dos medios y parte de la potencia no entra al segundo material. Puede ser difusa si la superficie del segundo medio es irregular, lo que genera varios haces en distintas direcciones o especular cuando la superficie es lisa y el haz de divide en una única dirección. (Peredo, 2004)
- Difracción: se define como la redistribución de energía de la onda, cuando esta pasa por un objeto opaco.
- Interferencia: se produce cuando se combinan dos o más ondas en un mismo espacio simultáneamente, está ligado al principio de superposición lineal.

6. Redes inalámbricas en PYMES

La época de enredarse entre cables a la hora de interconectar las computadoras está quedando atrás, las opciones inalámbricas ganan terreno, sus precios bajan y comienzan a derribarse mitos históricos. Hoy se presentan como una alternativa con dos ventajas clave: resultan fáciles de instalar y promueven la movilidad de los usuarios de la empresa.

Las redes inalámbricas, o *wireless* proponen alternativa “fácil” ya que su propuesta es eliminar los cables de la infraestructura y hacer que los equipos se interconecten gracias a la existencia de un *access point*, un *hardware* que se encarga de la conexión y la transmisión de información entre los dispositivos integrantes de la

red, y los equipos del usuario, que deben tener una placa específica que soporte este tipo de conexión.

Hoy por hoy, en líneas generales, casi todos los dispositivos móviles (*notebooks, handhelds* y cada vez más teléfonos inteligentes) disponen de conectividad a redes inalámbricas, lo cual hará más rentable la instalación de este tipo de soluciones en el corto y mediano plazo.

El uso eficiente de la tecnología se convierte en una estrategia competitiva de las empresa, siempre y cuando el talento humano la sepa asimilar y utilizar. Las PYMES en Venezuela deben ampliar su visión de cara al futuro para anticipar, planificar, actuar con constancia y disciplina, de la mano de la tecnología, para asegurar la competitividad.

Las PYMES necesitan incorporar tecnología a sus estrategias de negocio para poder ser más productivas ya que requieren del desarrollo e implementación de proyectos que involucran a las tecnologías de información y así, lograr mejorar la producción, la administración, la integración funcional y la relación con clientes. Con el manejo de la tecnología se automatizan de manera eficiente los procesos, tanto internos como externos.

Algunas de las ventajas que proporcionan las redes inalámbricas a las empresas, son las siguientes:

- Accesibilidad: todos los equipos portátiles y la mayoría de los teléfonos móviles de hoy día vienen equipados con la tecnología *WiFi*, necesaria para conectarse directamente a una *LAN* inalámbrica. Los empleados pueden acceder de forma segura a sus recursos de red desde cualquier ubicación dentro de su área de cobertura. Generalmente, el área de cobertura es su instalación, aunque se puede ampliar para incluir más de un edificio. (Cisco)

- Movilidad: los empleados pueden permanecer conectados a la red incluso cuando no se encuentren en sus mesas. Los asistentes de una reunión pueden acceder a documentos y aplicaciones. Los vendedores pueden consultar la red para obtener información importante desde cualquier ubicación.
- Productividad: el acceso a la información y a las aplicaciones clave de su empresa ayudan a su personal a realizar su trabajo y fomentar la colaboración. Los visitantes (como clientes, contratistas o proveedores) pueden tener acceso, de invitado seguro, a Internet y a sus datos de empresa.
- Fácil configuración: al no tener que colocar cables físicos en una ubicación, la instalación puede ser más rápida y rentable. Las redes LAN inalámbricas también facilitan la conectividad de red en ubicaciones de difícil acceso, como en un almacén o en una fábrica. (Cisco)
- Escalabilidad: conforme crecen sus operaciones comerciales, puede que necesite ampliar su red rápidamente. Generalmente, las redes inalámbricas se pueden ampliar con el equipo existente, mientras que una red cableada puede necesitar cableado adicional.
- Seguridad: controlar y gestionar el acceso a su red inalámbrica es importante para su éxito. Los avances en tecnología *WiFi* proporcionan protecciones de seguridad sólidas para que sus datos sólo estén disponibles para las personas a las que le permita el acceso. (Cisco)
- Costes: con una red inalámbrica puede reducir los costes, ya que se eliminan, o se reducen, los costes de cableado durante los traslados de oficina, nuevas configuraciones o expansiones.

7. Seguridad de redes inalámbricas

El protocolo 802.11 implementa encriptación *WEP*, pero no se puede mantener como única estrategia de seguridad ya que no es del todo seguro. Más que hablar de la gran regla de la seguridad puede hablar de una serie de estrategias que,

aunque no definitivas de forma individual, en su conjunto, pueden mantener la red oculta o protegida de ojos ajenos:

- Cambiar la contraseña por defecto: todos los fabricantes establecen un *password* por defecto de acceso a la administración del punto de acceso. Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible que el intruso la conozca. (Ruíz, 2004)
- Usar encriptación *WEP/WPA*: activa en el *AP* la encriptación *WEP*. Mejor de 128bits que de 64bits, ya que en cuanto mayor sea el número de bits mejor es la seguridad. Los puntos de acceso más recientes permiten escribir una frase a partir de la cual se generan automáticamente las claves. Si se activa *WPA* en el punto de acceso, tanto los accesorios y dispositivos *WLAN* de la red como el sistema operativo deben soportarlo.
- Cambiar el SSID por defecto: suele ser algo del estilo a "*default*", "*wireless*", "101", "linksys" o "SSID". En vez de "MiAP", "APManolo" o el nombre de la empresa es preferible escoger algo menos atractivo para el intruso, como puede ser "Conectividad Limitada" o "Desconectado". (Ruíz, 2004)
- Desactivar el *broadcasting* SSID: el *broadcasting* SSID permite que los nuevos equipos que quieran conectarse a la red *WiFi* identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual. Al desactivarlo se tiene que introducir manualmente el SSID en la configuración de cada nuevo equipo que se quiera conectar.
- Activar el filtrado de direcciones *MAC*: al activar el filtrado *MAC* dejará que sólo los dispositivos con las direcciones *MAC* especificadas se conecten a la red *WiFi*.
- Establecer el número máximo de dispositivos que pueden conectarse: si el *AP* lo permite, es recomendable establecer el número máximo de dispositivos que pueden conectarse al mismo tiempo al punto de acceso.
- Desactivar *DHCP*: de esta manera se deberá configurar de forma manual los dispositivos *WiFi*, colocando datos como: la dirección IP, la puerta de enlace, la máscara de subred y el *DNS* primario y secundario. (Ruíz, 2004)

Además de estas configuraciones y recomendaciones para la seguridad de la red también se contara con medios de gestión de usuarios, será un Servidor AAA (Autentificación, Autorización y Gestión de cuentas, o *Authentication, Authorization and Accounting management*).

7.1. Servidor AAA- Radius

Es un protocolo de autorización, autenticación y gestión de usuarios para aplicaciones de acceso a la red, además facilita la administración de usuarios y su acceso a los diferentes dispositivos de la red. El servidor AAA tiene funciones como autenticación y encriptación a un cliente, maneja usuarios y contraseñas por cada cliente, define los servicios que maneja y contabiliza el uso de recursos de la red. Por ejemplo: tiempo de conexión, bytes enviados/recibidos, etc. (Molina, 2012)

7.2. Listas de Control de Acceso - ACL (*Access Control List*)

Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido. Los ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores, su objetivo fundamental es filtrar el tráfico, permitiéndolo o denegándolo de acuerdo a alguna condición. (Molina, 2012)

7.3. Filtrado por Direcciones MAC

Antes de explicar esta configuración de seguridad, es importante, definir la definición de una *MAC Address* o dirección *MAC*, la cual está compuesta de 12 dígitos hexadecimales, esta dirección está físicamente en cada tarjeta y no se puede cambiar. Es decir, esta dirección es única en cada tarjeta de cada computadora.

Filtrado de *MAC*: Método de configuración de seguridad en puntos de acceso que restringe a determinadas direcciones *MAC* la posibilidad de unirse a la red y autenticarse, este filtro debe estar configurado en tu *router* o *AP*, consiste en dejar

entrar a la red solo a los *PC's* con las direcciones *MAC* que uno diga, y como ya dijimos antes, cada tarjeta de red tiene su dirección MAC, y además no pueden haber direcciones *MAC* duplicadas en una red, por lo que es bastante útil, pero si cambias de tarjeta de red, debes también cambiar el filtro o si no, no podrás entrar a la red. (Roman, 2005)

Filtro IP: es simplemente un mecanismo que decide qué tipos de datagramas de IP serán procesados normalmente y cuáles serán descartados. Por *descartados* se entiende que el datagrama se elimina y se ignora completamente, como si nunca se hubiera recibido. Se puede aplicar muchos criterios, y en diferentes ordenamientos, para determinar qué datagramas desea filtrar, funciona básicamente igual al filtro anterior, pero con la dirección IP, pero cualquier computadora con la dirección *IP* que esté habilitada podrá entrar, teniendo en cuenta que no pueden existir dos direcciones *IP's* iguales en una red.

El filtrado MAC, es el método de autentificación más conveniente para aplicar en la implementación de este tipo de topología, ya que ofrece ventajas a la hora de relacionar le dirección física del equipo con su ubicación dentro de la empresa, lo permite tener una mejor administración de los recursos de la red. (Roman, 2005)

Es necesario que cada *router* inalámbrico cuente con filtrado *MAC* y así solo los equipos autorizados podrán tener acceso al mismo, para lograrlo se administra por medio del *router*, conociendo previamente la dirección IP que le pertenece, el nombre de usuario y la clave de acceso para ingresar a las configuraciones.

Capítulo III

Marco Metodológico

La investigación se enmarca dentro del tipo denominado Proyecto Factible, ya que consiste en el desarrollo de un modelo óptimo para la solución de problemas o necesidades de la organización. Este proyecto de investigación permite realizar un análisis del modelo a desarrollar para lograr proponer un plan factible con la finalidad de resolver un problema, como lo es el diseño de modelos estructurales de redes inalámbricas para PYMES.

El desarrollo del proyecto está constituido por varias fases cuya base es la descripción del contexto, en el cual, se plantea la problemática del proyecto y se realiza la investigación de todos los aspectos y equipos tecnológicos necesarios para la implementación del mismo, para luego, explicar el desarrollo del proyecto y así culminar el trabajo especial de grado.

El esquema que describe las fases asociadas a la realización del proyecto, se muestra en la Figura 4:

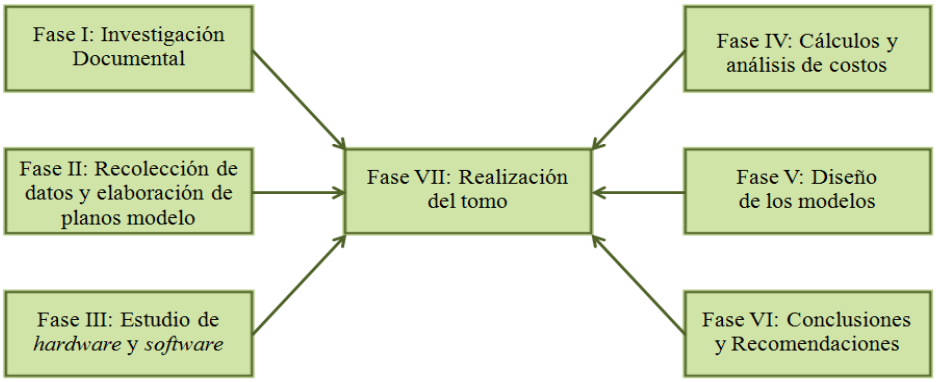

Figura 4 - Fases metodológicas del proyecto

Fuente: (Propia)

1. Fase I: Investigación Documental

Es la recopilación de la información teórica necesaria para la elaboración del trabajo especial de grado, esta búsqueda fue a través de libros, información electrónica y tesis antiguas y relacionadas con este tema. Los principales temas en los cuales se basó la investigación se derivaron, en su mayor parte, del propio título del proyecto, de donde se extrajo como objeto de búsqueda las diferentes tecnologías que permiten la identificación y seguridad inalámbrica.

La parte teórica también se basó en la búsqueda de patrones comunes que sean característicos de las pequeñas y medianas empresas con el fin de establecer los diferentes modelos para los cuales se diseñaran las redes inalámbricas. Para ello hay que tener claro los conceptos de PYME, su clasificación y sus principales funciones y necesidades, las cuales, estarán ligadas a los requerimientos de cada empresa.

Esta es una etapa necesaria en el desarrollo del trabajo de grado, ya que, permite adquirir los conocimientos básicos para lograr el diseño de la red inalámbrica, saber cuáles son los posibles estándares que rigen el funcionamiento de la misma, cuales son los protocolos utilizados y cuáles son los fenómenos que pueden afectar la propagación, control de acceso a la red, entre otros, son conocimientos primordiales que hay que garantizar para poder lograr con éxito el desarrollo del trabajo.

2. Fase II: Recolección de datos y elaboración de planos modelo

Una vez recolectados los conceptos básicos se procederá a implementar los datos de pequeñas y medianas empresas, para establecer planos físicos que permitan establecer con base la estructura y topología de la red inalámbrica a diseñar.

Para la recolección de datos significativos se recurrirá a organizaciones venezolanas dedicadas al área en que se trabajará durante la elaboración de este

proyecto, INAPYMI (Instituto nacional de pequeñas y medianas industrias), INE (Instituto Nacional de Estadísticas) y por último se realizaran visitas a distintas empresas consideradas PYMES para conocer y poder establecer modelos genéricos con respecto a sus estructuras tanto físicas como organizativas.

Luego de recolectar la información necesaria de los requerimientos de las PYMES, se elaboraron dos planos genéricos, uno para cada tipo de empresa, tomando en cuenta las diferentes características de cada una y como éstas inciden en las estructuras físicas y organizativas de las empresas. En la elaboración de los planos se considerarán elementos como material de paredes, puertas y alturas de las edificaciones.

3. Fase III: Estudio de *hardware* y *software* a utilizar

En esta fase del proyecto se basa en la investigación de todos los elementos de *hardware, software* y periféricos necesarios para la elaboración del Trabajo Especial de Grado. Esta investigación se realizó por medios electrónicos, ya que se necesitan manuales teóricos para conocer el funcionamiento de los dispositivos y programas necesarios.

Se escogieron los equipos y *softwares* más apropiados, haciendo comparaciones entre sus características y propiedades para seleccionarlos, basándose en las necesidades que se desean cubrir en la investigación. La cantidad de equipos dependerá del modelo establecido de PYME, ya que las empresas, dependiendo de sus requerimientos, pueden necesitar un mayor o menor número de equipos para la instalación de la red inalámbrica.

4. Fase IV: Cálculos y análisis de costos

Se recopilaron datos de la infraestructura de los edificios o estructuras donde se implementará la red inalámbrica, en este caso, serán los principales modelos

estructurales seleccionados, según la clasificación y requerimientos de las empresas, los planos de la estructura serán planos genéricos, basados en los requerimientos básicos de cualquier empresa, en cada uno de ellos se especificaran sus medidas y dimensiones.

Además se acopiaron datos con respecto a los parámetros de propagación de ondas necesarios para establecer el enlace que a su vez también dependerán de los equipos seleccionados para el diseño e implementación de la red y de la cantidad de usuarios para la cual este diseñada la misma. El análisis de costo será realizado en base a precios referenciales para la fecha actual y también dependerán del servicio que preste cada compañía y de su división estructural y organizacional, se trató de que los equipos a utilizar fueran equipos de marcas reconocidas.

5. Fase V: Diseño de los modelos

Es la fase más importante del proyecto, ya que, es la etapa donde se realiza el diseño de la red a implementar, basándose en los parámetros previamente establecidos por los equipos y *software* a utilizar y en el estudio de los lugares más apropiados para la conexión de los equipos dentro de la estructura de los modelos seleccionados.

Los modelos seleccionados serán basados en la clasificación de pequeñas y medianas empresa, según la ley de promoción y desarrollo de pequeñas y medianas industrias en Venezuela, se aplicaran distintos modelos de redes, dependiendo de los servicios que se quiera implementar, considerando la forma de conexión o de posible acceso a la información de la empresa. Tomando siempre en cuenta las condiciones de seguridad más apropiados para el respaldo del tráfico de datos y que, el servicio a implementar, se guiará de acuerdo a los servicios por tipo de industria a la cual pertenezca.

Luego de seleccionar el tipo de tecnología, y de haber seleccionado los servicios que generará cada modelo, se procede a desarrollar el diseño de la red, en cuanto a topología, equipos y técnicas de ingeniería necesarias para la instalación y conexión de los equipos y enlaces dentro de cada modelo.

Se realizarán simulaciones de propagación de ondas utilizando el simulador de propagación de ondas RPS (*Radiowave Propagation Simulator*) para hacer análisis de cobertura de cada modelo y se modelará la red a implementar, verificando su funcionamiento en el *software* OPNET el cual, permite verificar aspectos como ancho de banda, rendimiento y tráfico, bajo la respectiva configuración de cada uno de los equipos a utilizar. Ambos simuladores permitirán visualizar el boceto de la red a implementar, así como verificar el correcto tráfico de datos y la confiabilidad de la misma.

Por otra parte se simularán las redes utilizando el *software* CISCO PACKET TRACER, para comprobar la interconectividad entre cada uno de los dispositivos conectados a la red y se verificarán las posibles aplicaciones de seguridad más convenientes para las empresas. En esta fase hay que considerar la ubicación exacta de los equipos ya que tienen que estar colocados en sitios donde se puedan prevenir peligros relacionados a posibles hechos violentos o vandálicos.

6. Fase VI: Conclusiones y recomendaciones

Al finalizar la fase de pruebas y simulaciones se procede a la realización de las conclusiones y recomendaciones, donde se registrarán los aportes más significativos del trabajo especial de grado y se especificarán posibles mejoras al proyecto realizado para posibles trabajos futuros a desarrollar.

7. Fase VII: Realización del tomo

Es la última fase en elaborarse, ya que en dicha fase es donde se agrupa toda la información obtenida y analizada a lo largo del proyecto, realizando el tomo del Trabajo Especial de Grado.

Capítulo IV
Desarrollo y Resultados

El capítulo de desarrollo explica la forma en que fue desarrolla cada una de las fases planteadas para la implementación de la red inalámbrica para distintos modelos estructurales y organizativos de PYME, garantizando una conexión fiable y segura. Siguiendo los parámetros previamente establecidos en el capítulo anterior se obtienen como resultados siguientes fundamentos necesarios y relacionados a cada una de las fases a desarrollar.

1. Fase I: Investigación documental

La investigación documental se basó en el estudio de las bases teóricas necesarias para el desarrollo y la implementación de una red inalámbrica, como los estándares que rigen las redes inalámbricas, tipos de conexión inalámbricas, y equipos necesarios para la simulación, diseño e implementación de la misma, así como los métodos más confiables para garantizar la seguridad requerida por la empresa.

A su vez fue necesaria la documentación relacionada a las PYMES, ya que dependiendo de los parámetros fundamentales de la organización de las pequeñas y medianas empresas, es que se pueden establecer las condiciones, equipos y servicios que se pueden implementar para el desarrollo de la red inalámbrica dentro de la misma y así poder establecer futuros patrones a la hora de implementar redes inalámbricas en pequeñas y medianas empresas.

Para la elaboración de esta fase se utilizaron diversas fuentes de investigación, como fueron: tesis de grado, libros de redes inalámbricas y páginas electrónicas. Los Trabajos de Grado más relevantes con respecto a este trabajo fueron:

- Trabajo Especial de Grado, realizado por los ingenieros Mario Daniel Di Paolo y Gabriela Zarinha Giménez cuyo título es "Diseño y estudio de una red *WIFI* y su cobertura en la maternidad Concepción Palacios" la cual consiste en el diseño detallado de una red inalámbrica para la Maternidad Concepción Palacios , llevando a cabo simulaciones de cobertura de los diferentes pisos de la Maternidad, realizando estudios de propagación de ondas electromagnéticas basados en los estándares 802.11n para determinar la ubicación óptima de los puntos de acceso inalámbricos a instalar, y así poder brindar la solución más idónea a los requerimientos del cliente. Se estudió el comportamiento de los fenómenos de propagación para comprobar el buen funcionamiento y rendimiento de la red. Se realizó un levantamiento planimétrico de cada piso, se comprobó interconectividad entre equipos y se diseñó una evaluación de costos para su posible implementación. Este trabajo proporcionó información de redes inalámbricas, patrones de radiación, de equipos necesarios para el mejor aprovechamiento de la red y de posibles *softwares* de simulación para comprobar el correcto funcionamiento del diseño de la red.
- Trabajo Especial de Grado realizado por el Ing. Julio Edgar Molina Ruiz cuyo título es " Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red *LAN* en la empresa Editora El Comercio planta Norte" la cual consiste en una propuesta de segmentación con Redes de Áreas Locales Virtuales *VLAN´s* para la mejora y rendimiento y seguridad de la red de área local en la empresa Editora El Comercio, en donde se plantean un rediseño de la red para el soporte de las redes *LAN* virtuales y así poder segmentar las áreas en subredes para lograr un mayor nivel de protección a través de Listas de control de acceso, tecnologías emergentes de seguridad *Windows Server* 2008, Nivel de autentificación – Radius, mejorar el consumo de ancho de banda, implementar nuevos protocolos en tecnología CISCO, e instalar redes inalámbricas y nuevos servicios de transferencia de archivos (Protocolo de transferencia de Archivos FTP). Es un trabajo de grado que brindó

información acerca de conceptos básicos, así como información de equipos necesarios para implementar redes inalámbricas y redes virtuales, proporciona características de los protocolos a utilizar y sistemas de seguridad que se pueden utilizar en las empresas, para así garantizar un buen aprovechamiento de la red con respecto a su ancho de banda y tráfico de datos.

- Trabajo Especial de Grado, realizado por Lic. Peinado Virginia y Lic. Prado Rossana cuyo título es "Propuesta de una guía general de acción para la aplicación del marketing digital en las pequeñas y medianas empresas (PYMES), en la ciudad de Cumaná- Estado Sucre" trabajo que consiste en el estudio y la importancia de que las PYMES introduzcan nuevas tecnologías para poder ser productivos y así aumentar su competitividad. Haciendo enfoque en los diferentes beneficios de diferentes estrategias y herramientas para impulsar la imagen, razón de ser de la empresa, sus productos y cada uno de sus servicios que pudiese prestar. Este trabajo facilitó información acerca de definiciones, características, clasificación e importancia de las PYMES, así como la influencia que pudiesen tener las diferentes tecnologías dentro de la conformación, estabilidad y buen desempeño de las empresas.

Otra parte importante fue la información recolectada en libros de redes inalámbricas, de los cuales, se extrajo información relacionada con los tipos de topologías, implementación, estándares y equipos necesarios para la implementación de redes en distintos ambientes, el más significativo fue "*Estrategias para la implementación de nuevas tecnologías en PYMES*" por Eloy Seoane. También se utilizaron diferentes manuales, o tutoriales, relacionados a los diferentes *softwares* de simulación para la comprobación de los diferentes aspectos de la red, como interoperabilidad, conectividad, cobertura, entre otros.

La referencia de documentación más importante fue internet, debido a la amplia gama de información que ahí se encuentra, de esta súper herramienta fue de

donde se extrajo la mayor cantidad de información posible para la realización de este proyecto, garantizando fuentes certificadas.

2. Fase II: Recolección de datos y elaboración de planos modelo

Las PYMES no tienen características estructurales definidas, debido a que la misma va a depender de la clase de servicio que brinde, además, de la cantidad de trabajadores y la distribución departamental de los mismos, es importante tomar en cuenta que las estructuras no se adecuan a las necesidades de la empresa, por el contrario, las empresas (dependiendo de sus necesidades y servicios a ofrecer) son las que se adecuan a las edificaciones y la distribución ya establecida, por lo tanto, el componente tecnológico va a depender de las condiciones de dicha estructura.

Para el diseño de los planos de los modelos a trabajar hay que tener presente ciertas características a nivel organizacional de la empresa entre ellas podemos mencionar:

- Misión de la empresa.
- Servicios necesarios para su buen funcionamiento.
- Cantidad de personas que integraran la organización.

Estas características son de vital importancia para el tipo de trabajo que está en desarrollo porque no todas las empresas requieren los mismos servicios, a pesar de que en un futuro lo ideal sería que todas las empresas cuenten con un servicio de red estandarizado, en la actualidad existen muchas instituciones que no consideran este tipo de servicio como fundamental, ya sea por falta de recursos o por considerar que es un servicio innecesario para su tipo de empresa.

Generalmente, la mayoría de las pequeñas empresas son administradas por sus propios dueños y el conjunto familiar, ya que son empresas las cuales, desarrollan alguna actividad comercial (compra-venta), por otra parte las medianas empresas son

administradas por un conjunto de personas seleccionadas, y sus dueños ocupan funciones específicas de gerencia o presidencia, estas empresas por lo general son manufactureras (servicios-producción).

Considerando que: las PYMES tienen una gran cantidad de características que las describen, para la realización de los modelos de redes inalámbricas fueron seleccionados tres parámetros que son:

- La cantidad de usuarios de la misma,
- El tipo de información de maneja la red y
- Los servicios que se ofrecen.

Los planos seleccionados como patrones para el diseño de los modelos estructurales de redes inalámbricas, fueron seleccionados basándose en patrones de empresas consideradas como PYMES, el estudio fue realizado considerando siempre la clasificación entre pequeña y mediana empresa, es decir, para pequeñas se seleccionó un sitio cuya capacidad máxima es de 49 personas y para medianas una capacidad máxima de 100 personas. Las condiciones estructurales son similares con respecto a materiales de paredes, altura de los pisos, entre otros.

Tomando en cuenta las diferencias antes mencionadas, las estructuras físicas de ambas son muy distintas, sin embargo, ambos tipos en la mayoría de los casos requieren de los mismos servicios a implementar. Los planos fueron diseñados para PYMES que cuenten con los servicios básicos de:

- Impresión
- Administración y contaduría.
- Inventario.
- Recursos Humanos.
- Facturación.
- Correo.

- *WEB.*

Esto servicios fueron seleccionados, ya que aportan los mayores beneficios y departamentalización a las empresas, ya que siendo pequeñas o medianas, se desea que el avance tecnológico de las mismas escale, hasta un punto donde se automaticen al máximo los servicios, optimizando la administración de los diversos recursos de las empresas y por lo tanto, la producción de las mismas.

Según la clasificación básica de PYMES, se establecieron dos planos modelo, uno para pequeñas y otro para medianas empresas. La digitalización de los planos fue realizada en el *software* SKETCHUP PRO de GOOGLE, el cual muestra vistas en 2D (Figuras 5 y 6) y 3D de los planos realizados (Figuras 6 y 8), como se muestra:

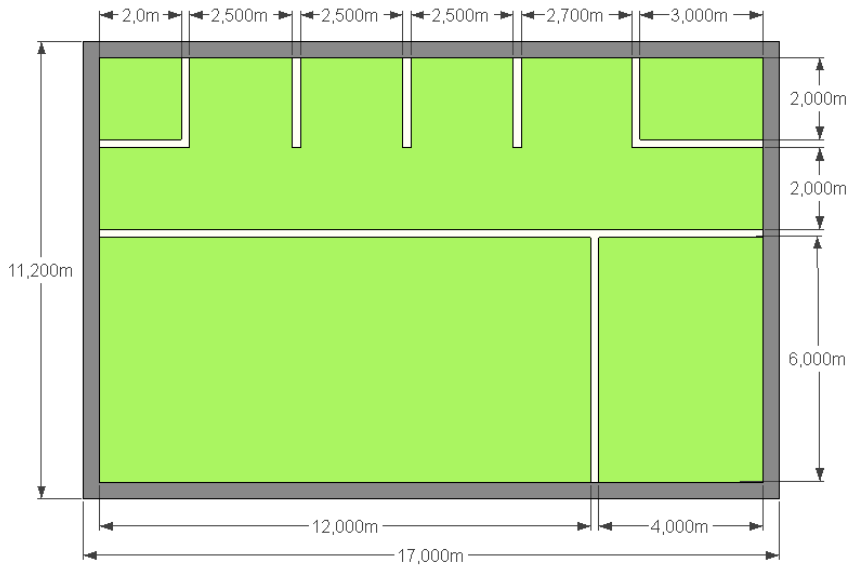

Figura 5 - Plano 2D de pequeña empresa. *Software* SKETCHUP PRO

Fuente: (Propia)

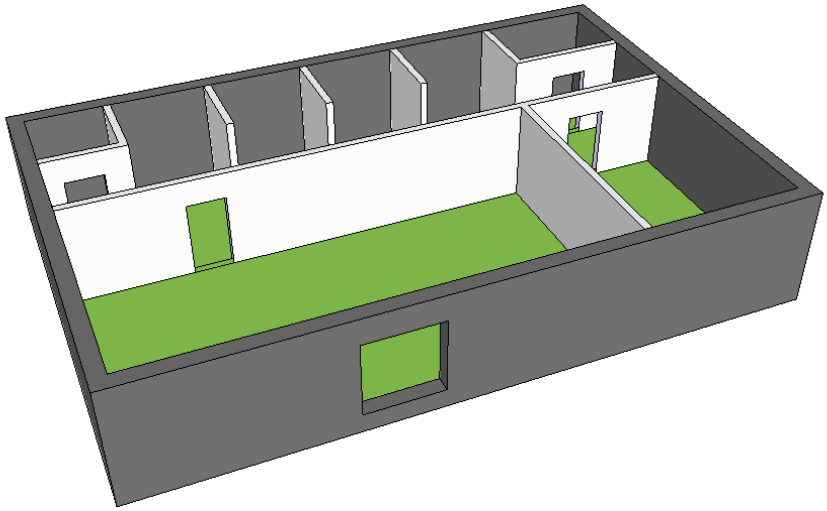

Figura 6 - Plano 3D de pequeña empresa. *Software* SKETCHUP PRO

Fuente: (Propia)

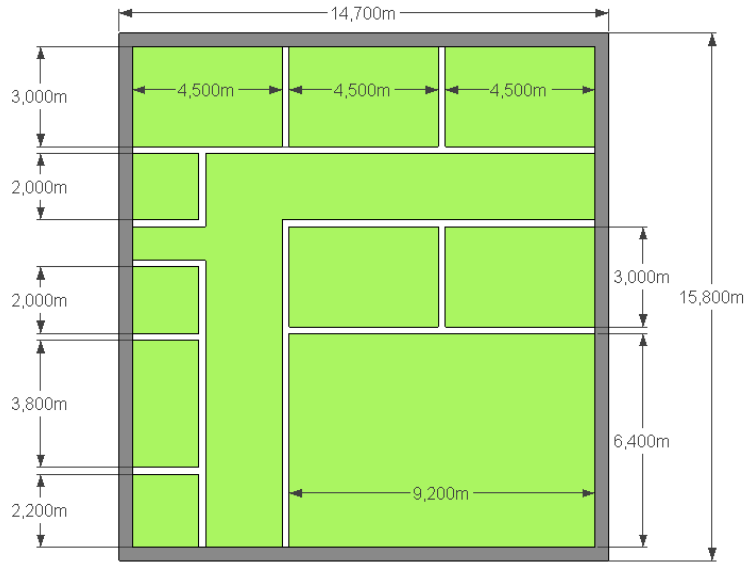

Figura 7 - Plano 2D empresa mediana. *Software* SKETCHUP PRO

Fuente: (Propia)

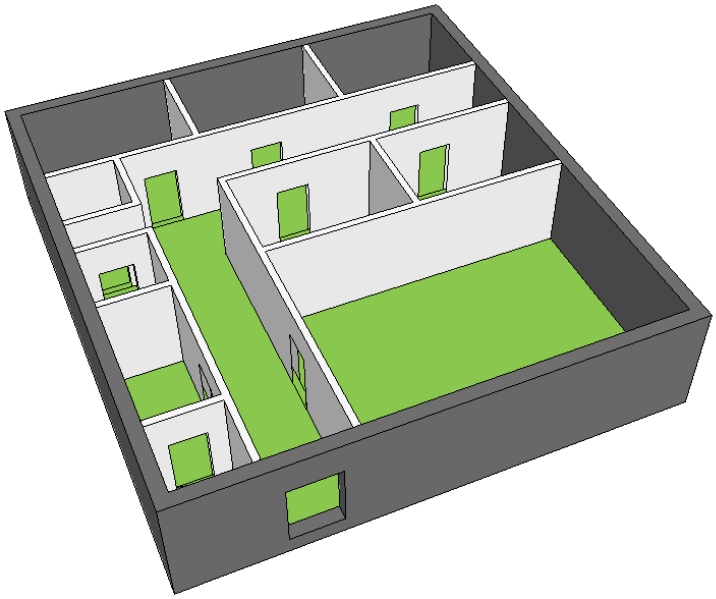

Figura 8 - Plano 3D empresa mediana. *Software* SKETCHUP PRO

Fuente: (Propia)

3. Fase III: Estudio de *hardware* y *software*

En esta fase se realizó un estudio de los diferentes equipos de *software* y *hardware* que se podrían utilizar en la implementación. El estudio se basó en equipos que cumplieran con características más eficientes que nos permitan alcanzar los objetivos planteados.

3.1. Software

Para la verificación del funcionamiento y rendimiento de la red se utilizó el *software* de simulación OPNET, PACKET TRACER de CISCO para realizar pruebas de interconectividad de equipos y para la simulación de cobertura de red se utilizó el *software* de simulación RPS (*Radiowave Propagation Simulator*).

- RPS: es un sistema que facilita el planeamiento de cobertura y desempeño de sistemas de radioenlaces, el cual, permite considerar el entorno y predecir la cobertura y capacidad de la implantación de cualquier dispositivo *hardware*. Para realizar una simulación en RPS se necesita recrear el entorno físico del

lugar, lo que permite la investigación de los efectos de la penetración, reflexión, difracción y otros. RPS se puede utilizar para generar simulaciones de entornos internos y externos, utilizando redes: WLAN, WiMAX, Mesh, UMTS, CMDA2000 y LTE (ArticlesBase, 2012). Este *software* permite importar archivos que contengan especificaciones de escalas como DXF/DWG (principalmente AutoCAD).

- PACKET TRACER: desarrollado por CISCO, permite crear topologías de red mediante la selección de los dispositivos y su respectiva ubicación en un área de trabajo, utilizando una interfaz gráfica (Cisco). Además soporta la detección y corrección de errores en sistemas de comunicaciones, ofreciendo como ventaja adicional el análisis de cada proceso ejecutado según la capa de modelo OSI (*Open System Interconnection* ó Interconexión de sistemas abiertos) que pertenezca, por lo tanto, es de gran ayuda en el estudio y aprendizaje del funcionamiento, configuración de redes y sus aplicaciones. Adicionalmente, se puede ingresar a sus consolas de configuración, donde están soportados todos los comandos de operación. Una vez completada la configuración física y lógica de la red también se pueden hacer simulaciones de conectividad desde las consolas incluidas (Cisco).
- OPNET IT GURU ACADEMIC: es un *software* libre para ser utilizado con fines académicos. Permite la creación, simulación y análisis de redes, soportando todas las redes móviles (*GSM, CDMA, UMTS, WiFi, WiMax, LTE*), logrando el estudio de redes inalámbricas en toda su extensión. Posee un entorno gráfico de fácil comprensión y una gran variedad de equipos para recrear la topología de la red, una vez realizada la simulación se configuran las consolas de los equipos para indicar los datos relevantes que se desean analizar, entre los cuales se encuentran: retraso de la información en función de la cantidad de paquetes y megabits por segundo, utilización de interfaces entre equipos, *throughput* (volumen de tráfico), retransmisión y perdida de la información, entre otros. (OPNET, 2012)

3.2. Hardware

Los equipos utilizados para la implementación física de la red inalámbrica fueron seleccionados en base a los posibles servicios que se requieren en las empresas, como conectividad efectiva, administración de recursos y servicios, seguridad en la implementación y velocidades accesibles para control del flujo de la información.

Los equipos de referencia seleccionados son de una marca reconocida para garantizar la certificación y buen desempeño de los mismos, igualmente se seleccionaron los equipos de la misma marca para evitar problemas de interconectividad entre los mismos, además de cumplir con los estándares seleccionados para el diseño de la red inalámbrica, para pequeñas y medianas empresas.

Es importante tomar en cuenta que para cada diseño, el número de equipos que interconectan las redes internas de la empresa (servidores internos y usuarios) será fijo, los equipos que varían son los personales, ya que para cada modelo hay una capacidad máxima limitada (50 para pequeñas y 100 para medianas empresas). Esta variable modifica el área de cobertura de los equipos inalámbricos, ya que la potencia transmitida debe redistribuirse entre un mayor o menor cantidad de usuarios, por lo tanto, modificará (en caso de necesitarlo) la cantidad de *AP's* utilizados para el diseño de las redes.

Los equipos necesarios para realizar los enlaces internos fueron los siguientes:

- *Router*: debe soportar la configuración de listas de acceso y tráfico SMTP y POP3. Debe utilizar el estándar IEEE 802.3u o *Fast Ethernet*, además del 802.1Q (*VLAN's*). Este equipo también debe soportar la creación de sub interfaces mediante ingreso de comandos. El *router* CISCO modelo 2801, cumple estas características.

- *Router* inalámbrico: es necesario que el enrutador posee cifrado WPA2-PSK y filtrado por dirección *MAC*, de igual forma el tipo de cifrado debe ser AES. Este modelo coincide con el modelo de CISCO Linksys N Lvbp1.
- *Switch* (utilizado en modo *CORE* y cliente): debe soportar los estándares IEEE 802.1Q (*VLAN's*) y el 802.3u (*Fast Ethernet*). Si es posible obtener los modelos con el número máximo de puertos RJ-45, en caso de ser necesario la expansión de la red. Un ejemplo, sería el *switch* Catalyst 2960 de CISCO.

4. Fase IV: Cálculos y análisis de costos

Previo a la realización de los modelos estructurales de redes inalámbricas para PYMES, se llevó a cabo una serie de cálculos, los cuales, permitieron elaborar las simulaciones necesarias para seleccionar los diseños más aptos para cubrir los parámetros seleccionados. Estas simulaciones, como se ha comentado con anterioridad, abarcan tres aspectos principales:

- La cobertura de los transmisores configurando parámetros fundamentales, como: tipo de antena, ubicación de receptores, potencia de transmisión, etc.; por medio del *software* RPS
- La interconectividad de los equipos de las redes internas y externas, conjuntamente configurando las interfaces de conexión y realizando la departamentalización de equipos clientes, usando PACKET TRACER.
- Analizar el tráfico de la red en sus diversas interfaces, evaluando retardos, información recibida y enviado, volumen de información (*throughput*) y otros, mediante el *software* OPNET.

En este apartado, solo se tomará en cuenta el análisis en RPS, ya que es el primer paso para el diseño de la red, debido a que este estudio arroja como resultado la cantidad de transmisores necesarios para cada modelo y la cobertura de cada equipo transmisor. Para el uso de este *software*, luego de obtener la digitalización de los planos en SKETCH UP PRO, se exporta a un formato .DWG (del inglés

DraWinG, es un tipo de archivo capaz de guardar datos vectoriales en dos y tres dimensiones).

Posteriormente, el plano digitalizado, y en el nuevo formato, se importa al programa RPS, en el cual, se trabaja en *layers*, o capas de vectores, a cada *layer* se le asigna un material en que se configura el tipo de material (acero, concreto, ladrillo, madera, vidrio, etc.), color y otros parámetros de manera que el *software* puede analizar los fenómenos de propagación de forma correcta.

Para realizar la configuración de los planos, se colocó el tipo de material (desde la base de datos de RPS), el grosor de esta capa, un nombre de identificación y se seleccionan los fenómenos de propagación que soporta (difracción, penetración, reflexión), además de "activar" la capa para que sea visible y "bloquear" los elementos para que no puedan ser modificados. Cabe resaltar, que las constantes de propagación son auto configurables una vez se selecciona la descripción del material.

La definición de las capas puede ser realizada directamente en RPS, o puede predefinirse en el *software* SKETCH UP PRO, y dicha información se importa desde el archivo .DWG. En este caso, se crearon dos *layers*, las paredes internas y las externas de ambos planos. La clasificación de los materiales de cada capa (comunes para ambos planos) se llevó a cabo a través de las configuraciones mostradas en las Figuras 9 y 10:

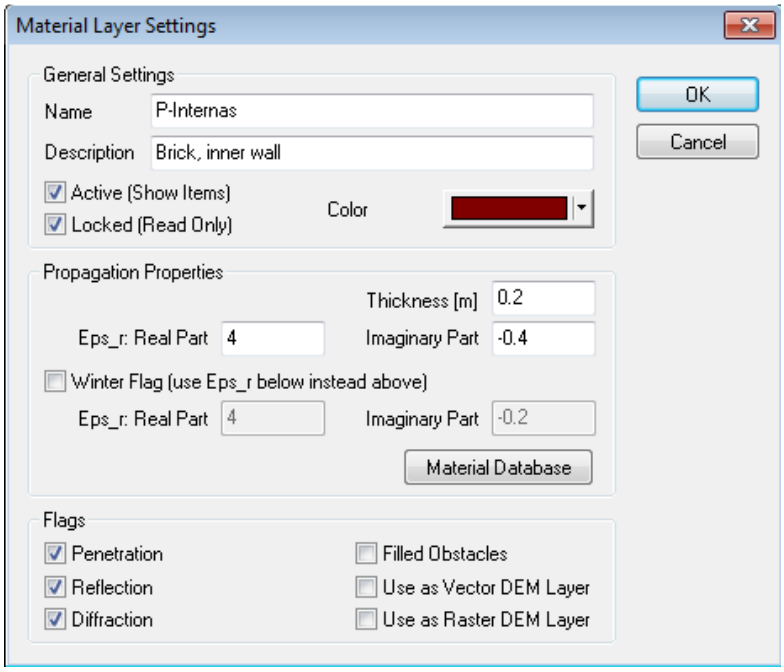

Figura 9 - Configuración paredes internas. *Software* RPS

Fuente: (Propia)

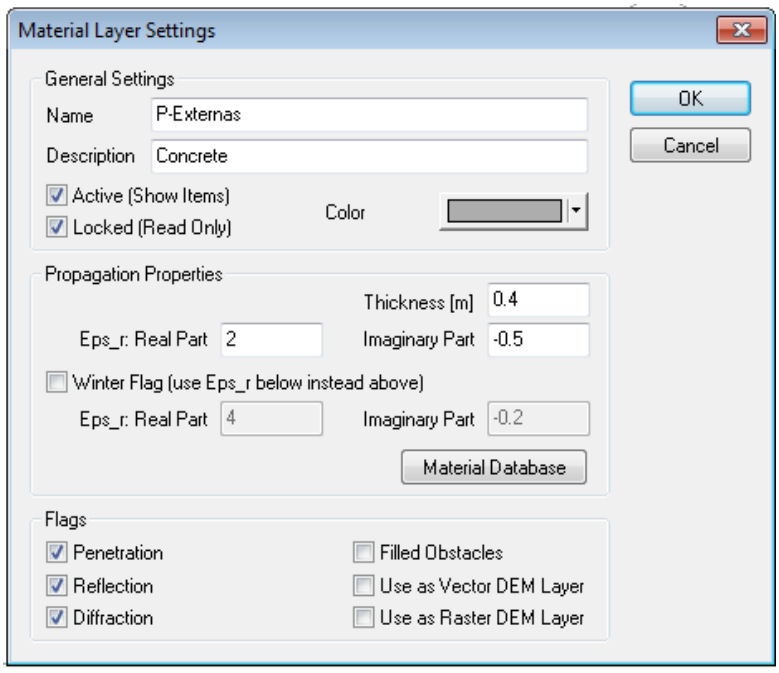

Figura 10 - Configuración paredes externas. *Software* RPS

Fuente: (Propia)

Luego de realizar las clasificaciones para cada capa, se añaden los equipos transmisores (Figura 11) y receptores (Figura12), donde se configuran los parámetros de cada uno (con las mismas características por tipo de equipo), como la ubicación y las antenas que utiliza, como se muestra en las Figuras 11 y 12 respectivamente:

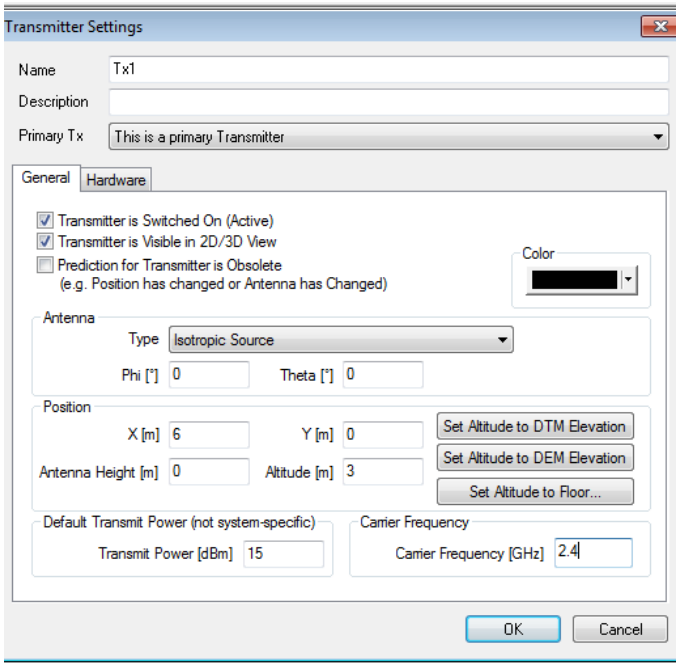

Figura 11 - Configuración de transmisores. *Software* RPS

Fuente: (Propia)

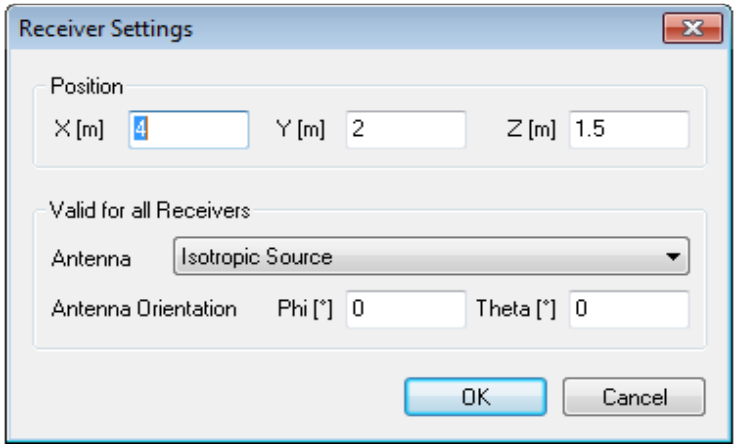

Figura 12 - Configuración de receptores. *Software* RPS

Fuente: (Propia)

Seguidamente, se realiza la simulación, la cual, muestra los patrones de radiación de cada transmisor ubicado en el plano, mostrando la potencia recibida por cada receptor y la escala correspondiente, los resultados de los planos, son mostrados en las Figuras 13 y 14:

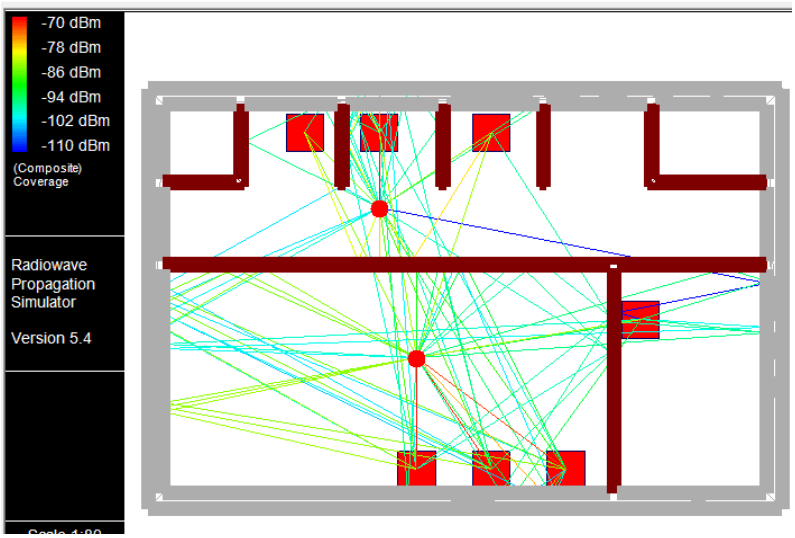

Figura 13 - Análisis de cobertura, empresa pequeña. *Software* RPS

Fuente: (Propia)

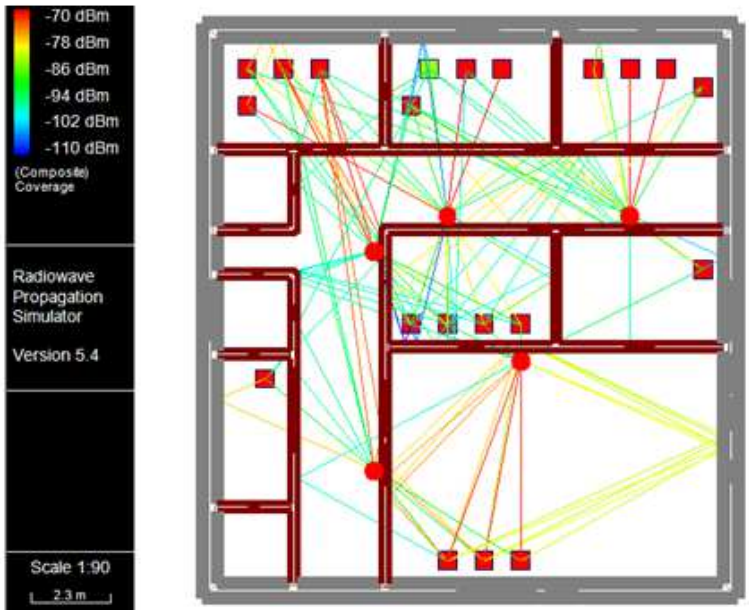

Figura 14 - Análisis de cobertura, empresa mediana. *Software* RPS

Fuente: (Propia)

Aun cuando la ubicación de los transmisores busca maximizar el área de cobertura de la señal, se puede observar que, en el plano de la mediana empresa, uno de los receptores no recibe una potencia tan alta como los demás, esto se debe a que a mayor cantidad de equipos de recepción, la potencia recibida disminuye proporcionalmente, se intentó maximizar la potencia en todos los receptores, pero esta ubicación de transmisores generó el mejor patrón de cobertura.

El análisis de costo depende de la cantidad de equipos de conexión utilizados para la implementación de la red, estos equipos dependerán de si es una pequeña o mediana empresa, pero solo en las cantidades, debido a que los servicios serán los mismos para ambos casos. Hay que considerar que el costo de los equipos son precios referenciales debido a las constantes modificaciones en el control de cambio, la mayoría los equipos son conseguidos en precios de moneda extranjera y, por tanto, pueden existir diferencias de precios según la fecha consultada. Los equipos seleccionados serán de marcas reconocidas para garantizar su existencia y buen desempeño (Calidad).

Según la cantidad de equipos para utilizarse en cada diseño, se elaboró una tabla de costos (Tabla 3), que indica de forma referencial, la inversión que debería realizar una empresa si tuviese la intención de implementar alguno de los diseños definidos en este Trabajo Especial de Grado.

	EMPRESA				
EQUIPO	**PEQ**	**MED**	**COSTO UNITARIO**	**COSTO TOTAL (PEQ)**	**COSTO TOTAL (MED)**
Router Inalámbrico	2	5	950 BsF	1.900 BsF	4.750 BsF
Router	2	2	4.500 BsF	9.000 BsF	9.000 BsF
Switch	3	3	29.000 BsF	87.000 BsF	87.000 BsF
Cables UTP Cat. 6	40 mts	70 mts	8 BsF/metro	320 BsF	560 BsF
Ups	1	2	1.000 BsF	1.000 BsF	2.000 BsF
TOTAL				**99.220 BsF**	**103.310 BsF**

Tabla 3 - Cantidad de equipos necesarios y precios por empresa

Fuente: (Propia)

5. Fase V: Diseño de los modelos

Luego del diseño de los planos y el estudio de cobertura, obtenida por los transmisores utilizando el *software* RPS y haber establecido los servicios requeridos para implementar la red inalámbrica en las PYMES, se procede al análisis de los parámetros necesarios para desarrollar los modelos para cada tipo de organización. El diseño será basado en los criterios fundamentales que son requeridos para el buen funcionamiento de una red dentro de una empresa. Las condiciones necesarias son implementación de seguridad, su correcto funcionamiento, escalabilidad y adaptación de la red.

Primeramente, se seleccionan los fundamentos básicos de topología a implementar, direccionamiento y protocolos de enrutamiento. Para que los ordenadores y otros dispositivos digitales puedan comunicarse por internet, necesitan una dirección *IP*, la cual, es una dirección que permite diferenciar todos los ordenadores del mundo. En esencia, una dirección *IP* es la identidad del equipo. Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz de un dispositivo dentro de una red que utilice el protocolo IP, que corresponde al nivel de red del Modelo OSI.

El direccionamiento utilizado en el diseño será el IPv4. Las direcciones IPv4 se expresan por un número binario de treinta y dos (32) bits y se pueden expresar como números en notación decimal: se dividen los bits totales de la dirección en cuatro octetos, cada uno de estos octetos están comprendidos entre 0 y 255, salvo algunas excepciones. La clasificación corresponde a varias clases la utilizada para este diseño será una clase C, en ella se asignan los primeros tres (3) octetos para identificar la red, y se reserva el octeto final para que sea asignado a los hosts, de modo que la cantidad máxima de host es de 254 host, lo cual, es un número considerable, ya que en el caso donde se requiere mayor personal en los modelos a

implementar es de hasta cien (100) usuarios, por ende esta clasificación es la más conveniente.

Los sitios de internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija, que no cambia con el tiempo. Los servidores de correo DNS, FTP públicos y servidores de páginas WEB necesariamente deben contar con una dirección IP fijo o estático, ya que de esta forma se permite su localización en la red.

El enrutamiento es fundamental para cualquier red de datos, ya que se transfiere información a través de una red de origen a destino. Los router aprenden sobre redes remotas ya sea de manera dinámica, utilizando protocolos de enrutamiento adaptivo, o de manera manual, utilizando rutas estáticas. Las rutas estáticas son muy comunes y no requieren la misma cantidad de procesamiento y sobrecarga que requieren los protocolos de enrutamiento dinámico. La principal decisión de envío de los routers se basa en la información de capa 3, la dirección *IP* de destino.

La tabla de enrutamiento del router se utiliza para encontrar la mejor coincidencia entre la dirección *IP* del destino de un paquete y una dirección de red en la tabla de enrutamiento. Dicha tabla determinará finalmente, la interfaz de salida para enviar el paquete, y el router lo encapsulará en la trama de enlace de datos apropiada para dicha interfaz de salida.

El conocimiento de las rutas estáticas es gestionado manualmente por el administrador de red, que lo introduce en la configuración de un router. El administrador debe actualizar manualmente cada entrada de ruta estática siempre que un cambio en la topología de la red requiera una actualización.

Las principales características de la red de una PYME son:

- La red es pequeña.
- Solo hay un punto de unión hacia el resto de la red.
- No hay rutas redundantes.

Por otra parte el protocolo dinámico se utiliza cuando alguna de las condiciones estáticas falla, es un protocolo que está construido por información intercambiada a través de los diferentes protocolos de enrutamiento, manejan complejas situaciones de enrutamiento más rápido de lo que un administrador del sistema podría hacerlo. Es ideal para redes con múltiples caminos a un mismo destino.

	Enrutamiento Dinámico	**Enrutamiento Estático**
Complejidad en la configuración.	Es independiente del tamaño de la red.	Se incrementa con el tamaño de la red.
Conocimientos requeridos del administrador.	Se requiere un conocimiento avanzado.	No se requieren conocimientos adicionales.
Cambios de topologías.	Se adapta automáticamente a cambios.	Se requiere la intervención del administrador.
Seguridad.	Es menos segura.	Es más segura.
Uso de recursos.	Utiliza CPU, memoria y ancho de banda de enlace.	No requiere recursos adicionales.
Escalamiento.	Adecuado para topologías simples y complejas.	Adecuada para topologías simples.
Capacidad de predicción.	La ruta depende de la topología actual.	La ruta hacia el destino es siempre la misma.

Tabla 4 - Comparación entre tipos de enrutamiento

Fuente: (Propia)

Dadas estas características y a la topología diseñada para las pequeñas y medianas empresas es recomendable aplicar un protocolo de enrutamiento de forma Estática ya que para los requerimientos necesarios es el protocolo más apropiado.

Además, se trabajará con una topología jerárquica La topología jerárquica se desarrolla de forma similar a la topología en estrella extendida pero, en lugar de enlazar los hubs/switches, el sistema se enlaza con un computador que controla el tráfico de la topología, es decir, la administración de las funciones de la red va a depender solo de la configuración de algún computador en específico.

Esta estructura se utiliza en la mayor parte de las redes locales actuales, es decir, un sistema jerárquico no es más que una red cuya configuración obedece un conjunto de reglas específicas

Recordando que el objetivo principal es el diseño de modelos de redes inalámbricas para PYMES, se utilizarán aplicaciones de redes y tecnologías. La red contará con una distribución básica de seis (6) servidores, cuatro (4) de ellos orientados a satisfacer las necesidades departamentales de la empresa, conformando la red interna de la misma, y los dos (2) restantes serán para el manejo y control del acceso a servicios que requieran de internet y correo electrónico, en este caso la denominamos red externa de la empresa. (Figura 15)

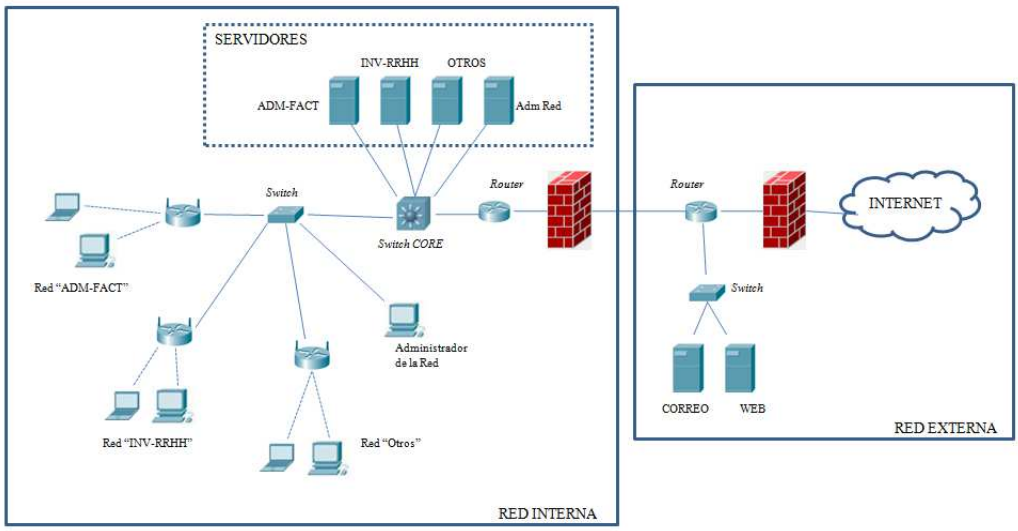

Figura 15 - Modelo de topología de la red

Fuente: (Propia)

El diseño también cuenta con tres (3) *switchs*, y dos (2) *routers* con *software* de *firewall* implementados previamente, su distribución corresponde a: un *switch* y un *router* implementados en la red interna, un *switch* y un *router* manejaran la red externa y el *switch* restante es para controlar los diferentes tipos de servidores existentes, según las necesidades de la empresa, el cual está ubicado en la red interna. El uso de protección de *firewall* en ambos enrutadores, se debe únicamente a razones de seguridad, ya que su función es permitir acceso a la red únicamente de la información que ha sido autenticada, por lo tanto, si la red estuviese bajo algún ataque, el intruso deberá superar ambos bloques de seguridad, lo que dificulta el acceso a la red privada de la empresa (Figura 16).

Figura 16 - Funcionamiento de *Firewall*
Fuente: (Cooper, 2011)

Para el correcto funcionamiento de la red se realizó una segmentación de servicios usando *VLAN's*, para tener un mejor manejo de la información y de los recursos de la red, ya que ellas permiten un uso más eficiente y más seguro de la misma y es manejable a niveles de capa 2 y 3. Por otra parte, la conexión entre equipos manejados por los empleados de la empresa (computadoras, laptops), será realizada de forma inalámbrica y, por ende, es necesario el uso de puntos de acceso. La cantidad de estos equipos dependerá de la cantidad de equipos a las cuales haya que brindarle conexión inalámbrica y de la calidad de servicio que se quiera ofrecer.

De esta manera se definen la red troncal y la red de acceso, entendiendo por red troncal la red que permite interconectar los diferentes emplazamientos que se utilizaran en la red, como el nexo de unión entre la red de acceso y el centro de datos (acceso a internet y servidores necesarios para gestionar la red), por su parte la red de acceso es la red que despliega cobertura inalámbrica para el acceso de los usuarios finales, suele tener menos requerimientos en cuanto a disponibilidad y ancho de banda soportado.

Una vez realizado el diseño modelo de la arquitectura de red, se procederá a simular los servicios implementados. Estos servicios son destinados a la seguridad, medidas referidas a la configuración de *firewalls* para que tengan las respectivas listas de control de acceso, el servidor *AAA* que garantiza la autentificación, autorización y control de acceso de los usuarios y por supuesto las respectivas *VLAN's* para el control de acceso a los diferentes servidores existentes en la red.

Para el análisis del rendimiento de la red, se utilizó el *software* OPNET, esta herramienta permite diseñar la topología de la red (Figura 17), a partir de la cual se configuran los equipos a utilizar y los servicios ofrecidos por la red, para simular los flujos de información en un intervalo de tiempo determinado y obtener los indicadores estadísticos seleccionados previamente.

Para realizar la simulación se dividió la estructura organizativa de la empresa en departamentos conjuntos de administración y facturación (ADM-FACT), inventario y recursos humanos (INV-RRHH), otros usuarios (OTROS) y el administrador de la red (ADM-RED), cada sección con un servidor específico en la red interna más los servidores de correo y *WEB* en la red externa, para un total de seis servidores.

En la interfaz principal del *software*, se puede observar la topología seleccionada (mencionada con anterioridad), sin embargo, para el funcionamiento del software, se incluyeron las configuraciones de aplicaciones y perfiles. Con el fin de facilitar la visibilidad de las subredes y de la red interna en general; se agruparon los departamentos en subredes, las cuales contienen cada una el router indicado, además de las estaciones de trabajo personales, la configuración de subredes (en diferentes departamentos) para pequeñas (Figura 18) y medianas empresas (Figura 19).

Los escenarios de las empresas, están básicamente configurados de la misma manera, la diferencia, como ya se ha comentado reside en la cantidad de usuarios que conforman cada organización, tomando en cuenta que las pequeñas y medianas empresas generalmente son del tipo comercial y productor respectivamente, se configuró bajo un concepto de trabajos a doble turno, donde cada turno y por empresa, los departamentos tienen una distribución como se muestra en la Tabla 5:

	EMPRESA	
DEPARTAMENTO	**PEQUEÑA**	**MEDIANA**
Administración y Facturación	3	10
Inventario y Recursos Humanos	3	10
Otros Usuarios	10	20
Administrador de la Red	1	1
TOTAL (POR TURNO)	**17**	**41**

Tabla 5 - Distribución de trabajadores por empresa y departamento

Fuente: (Propia)

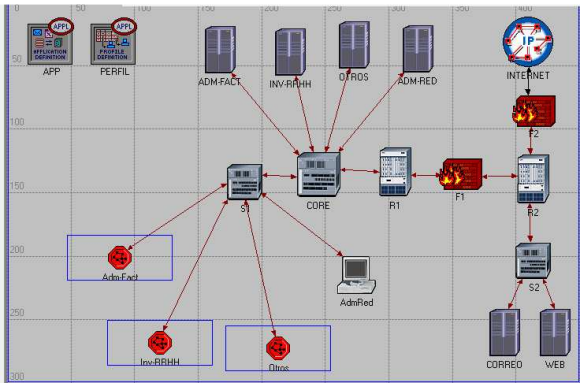

Figura 17 - Topología en *Software* OPNET

Fuente: (Propia)

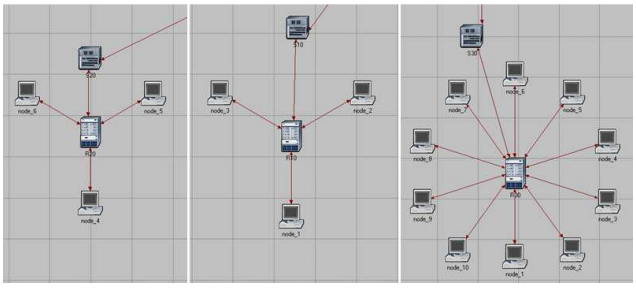

Figura 18 - Distribución departamental en empresa pequeña. *Software* OPNET

Fuente: (Propia)

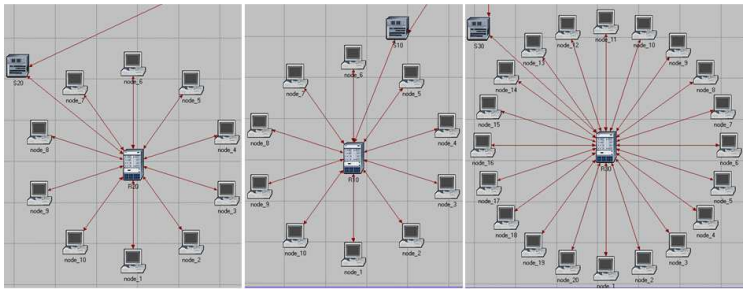

Figura 19 - Distribución departamental en empresa mediana. *Software* OPNET

Fuente: (Propia)

Seguidamente, se crearon las aplicaciones que serían utilizadas por los usuarios de la red (Figura 20), a esta configuración se le asigna el tipo de tráfico (Tabla 6) para cada servicio que será simulado por el *software* OPNET, los cuales incluye:

APLICACIÓN	TIPO DE TRÁFICO
Impresión	Archivos de texto
Correo	Alta carga
Datos	Alta carga
WEB	Navegación pesada
Acceso Remoto	Media carga

Tabla 6 - Tipo de tráfico por aplicación

Fuente: (Propia)

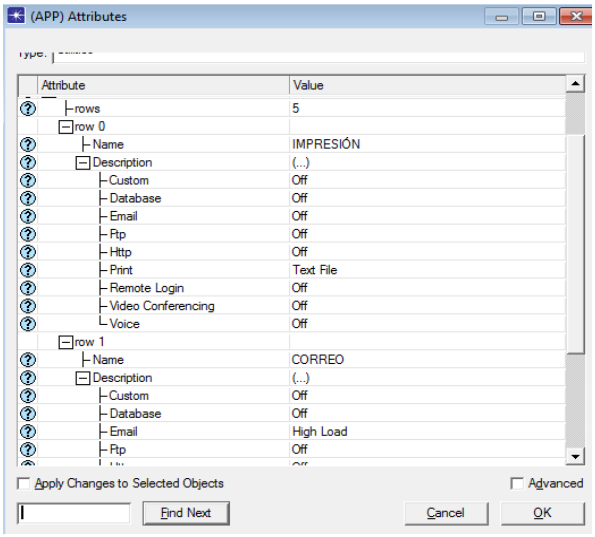

Figura 20 - Aplicaciones creadas. *Software* OPNET

Fuente: (Propia)

Además de configurar los servicios que brinda la red, se crearon perfiles para los usuarios, los cuales indicaban las aplicaciones a las cuales podía acceder cada perfil, seleccionando también la manera en la que las aplicaciones funcionan dentro de cada perfil (distribuidas por departamentos), para el análisis máximo de la red, se configuraron las aplicaciones en cada perfil (Tabla 6), de manera que se realizaran de forma aleatoria y simultánea, además de repetir hasta que finalizara la simulación; en la Figura 21, se puede apreciar la distribución de administración y facturación (ADM-

FACT) e inventario y recursos humanos (INV-RRHH), la asignación de perfiles se muestra en la Tabla 7:

PERFILES	APLICACIONES
ADM-FACT	Impresión
	Correo
	Datos
INV-RRHH	Impresión
	Correo
	Datos
	WEB
OTROS	*WEB*
ADM-RED	Correo
	Datos
	WEB
	Remoto

Tabla 7 - Distribución de las aplicaciones en los perfiles creados

Fuente: (Propia)

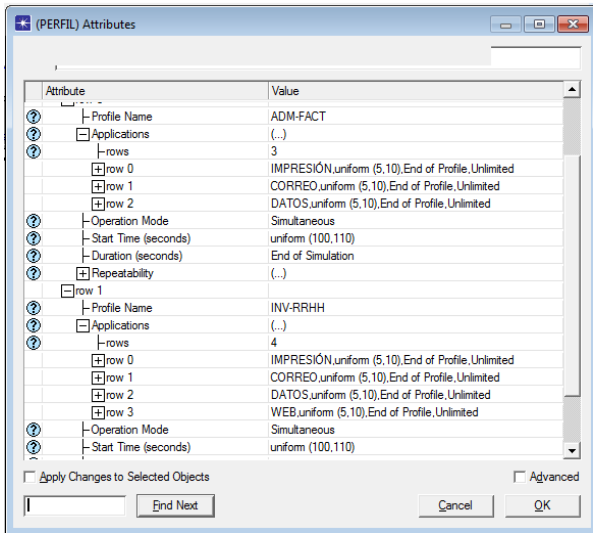

Figura 21 - Creación y configuración de los perfiles. *Software* OPNET

Fuente: (Propia)

Luego de la creación de la topología, las aplicaciones y los perfiles de la red, se configuraron los equipos que requieren un perfil (de los creados con anterioridad) para su correcto funcionamiento, estos equipos fueron las estaciones de trabajo (*PC's*) y los servidores, la configuración de las estaciones de trabajo se realizó por *subnet* lo que permitió hacer este proceso de manera más rápida, sin embargo, los servidores, se configuraron de forma individual, ya que no todos compartían los mismo perfiles (Figura 22)

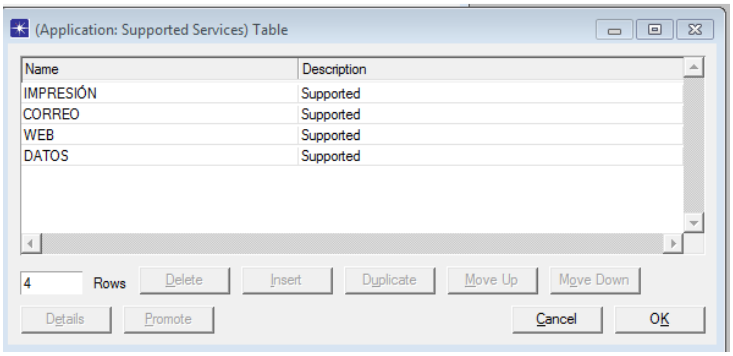

Figura 22 - Configuración de perfiles soportados por servidor INV-RRHH. Software OPNET
Fuente: (Propia)

Como estándar WLAN, se escogió 802.11n, ya que mejora considerablemente la velocidad de transmisión con respecto al estándar anterior y mantiene los protocolos de seguridad y compatibilidad; la Figura 23 ilustra el retardo comparativo, entre las redes 802.11n y Ethernet, indicando que el retardo entre las mismas es de aproximadamente 1ms (milisegundo). La Figura 24, compara el tiempo aproximado de descarga de archivos, donde muestra que entre la red Ethernet y el estándar 802.11n; es no mayor a cinco (5) segundos en archivos de tamaños considerables.

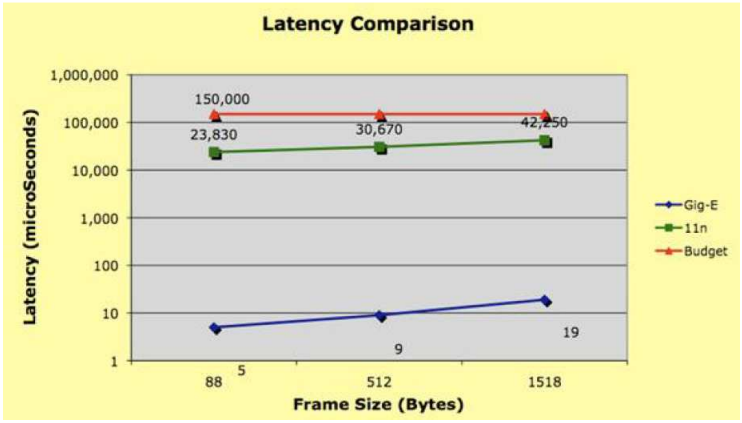

Figura 23 - Comparación de retardo entre tecnología 802.11n y Ethernet

Fuente: (DeBeasi, 2009)

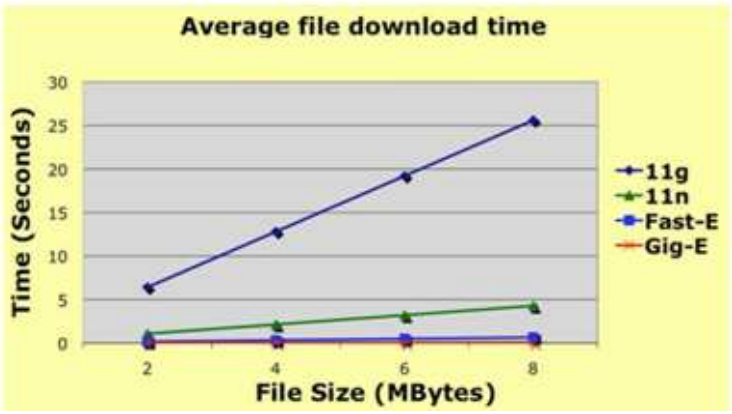

Figura 24 - Comparación de tiempo de descarga entre 802.11n y Ethernet

Fuente: (DeBeasi, 2009)

Tomando en cuenta lo mencionado anteriormente, es importante resaltar que aun cuando la red que se desea diseñar utiliza tecnología inalámbrica, las simulaciones realizadas en OPNET utilizaron conexiones alámbricas de Fast Ethernet (100Mbps); ya que el análisis lógico, en cuanto al consumo de ancho de banda y retardo en la red, es similar en ambos casos, por lo tanto, no existe diferencia relevante.

La simulación tuvo una duración de treinta (30) minutos en una situación real (la adquisición de datos se llevó a cabo en aproximadamente un minuto); en donde a

partir del segundo 110 los perfiles se activaron y los usuarios hicieron uso de las aplicaciones existentes hasta que terminó la simulación. Esto se realizó con el fin de crear el máximo tráfico de información en la red y obtener datos de tráfico en los enlaces y en la red; para analizar así el rendimiento de la red en un **punto crítico**.

Al ejecutar la simulación, se obtuvieron gráficas globales correspondientes al promedio estadístico de la red, y gráficas de enlaces específicos. Al momento de analizar las gráficas se sobrepusieron los resultados de ambas simulaciones (pequeña y mediana empresa) de forma que las comparaciones resultarán más fáciles de realizar. En todos los casos de análisis, la pequeña empresa se representa en color azul, mientras que las medianas con color rojo.

En las gráficas globales, podemos observar el tiempo de respuesta en el *download* (Figura 25) y *upload* (Figura 26) de *e-mails*; donde se observan tiempos no mayores a los 0,2 segundos, de igual manera se aprecia que existe más cantidad de peticiones de correos de parte de la red mediana, lo que es lógico por el aumento de usuarios.

El tráfico recibido por medio de correos electrónicos, se muestra en la Figura 27, donde se estima un promedio de la cantidad de información recibida por todos los usuarios en el tiempo de estudio (30 minutos), ya que el uso de las aplicaciones es el mismo para ambas redes, se observa un patrón parecido para ambas simulaciones.

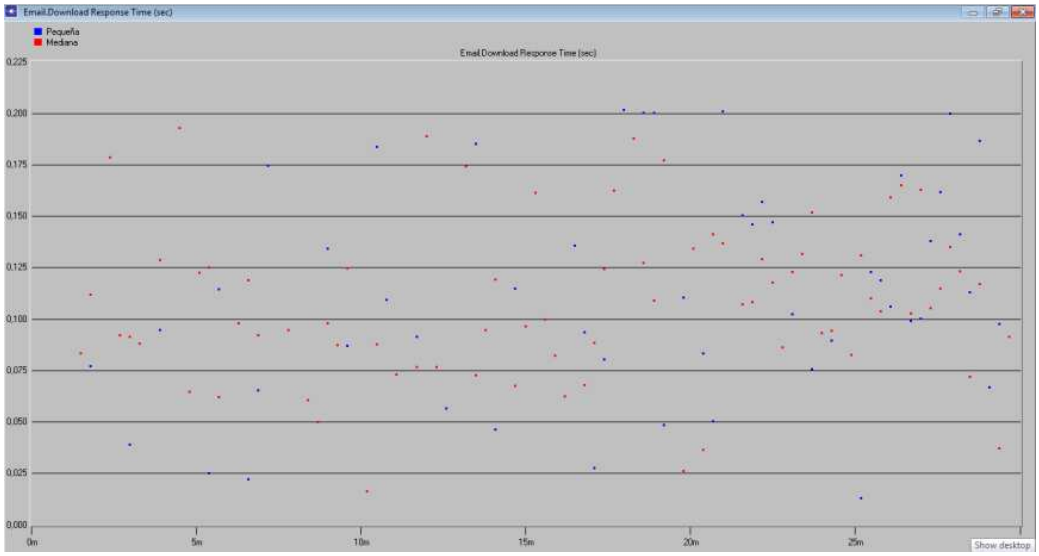

Figura 25 - Tiempo de respuesta de *download* en correos electrónicos. *Software* OPNET

Fuente: (Propia)

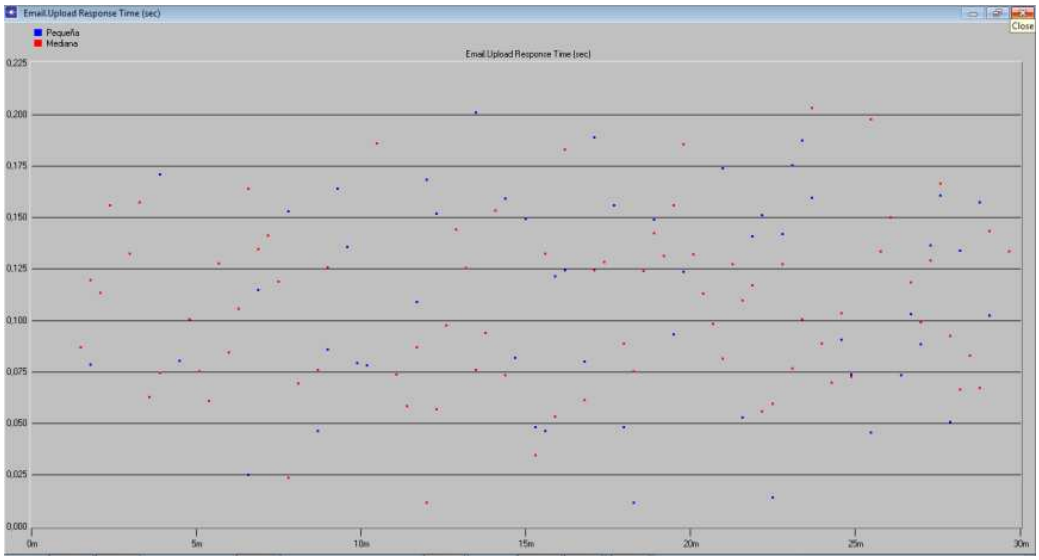

Figura 26 - Tiempo de respuesta de *upload* de correos electrónicos. *Software* OPNET

Fuente: (Propia)

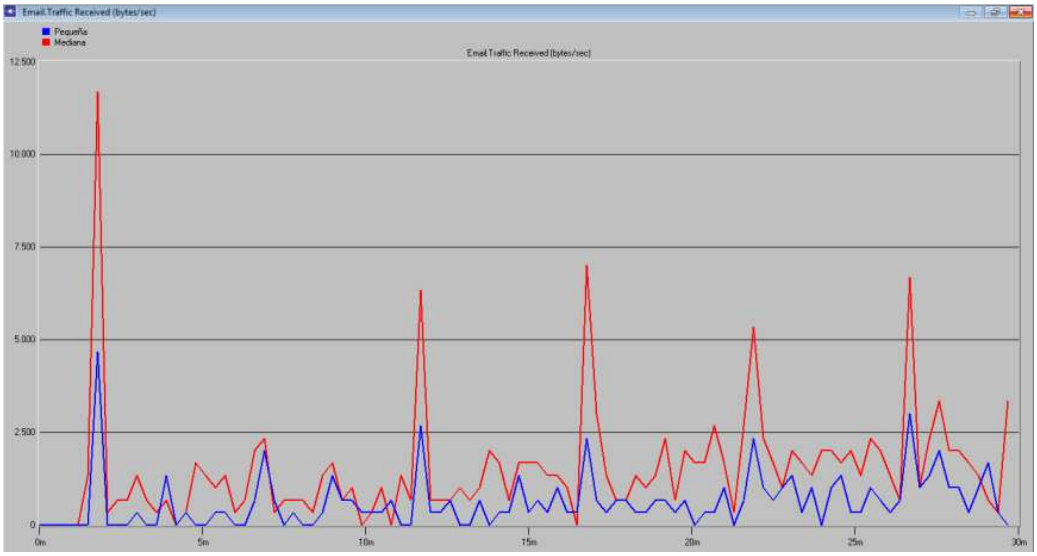

Figura 27 - Volumen de tráfico total de correo electrónico. *Software OPNET*

Fuente: (Propia)

Como resultado de las simulaciones, se obtuvieron los valores del retardo (Figura 28) que sufre la red de forma global, donde los máximos para ambas redes (pequeña y mediana empresa) se pueden observar a valores menores a 600µseg, por lo que estadísticamente brinda valores significativos y favorables con respecto al rendimiento de la red.

Seguidamente, se puede apreciar la gráfica obtenida de la cantidad de información que fue recibida (Figura 29) entre los usuarios de los departamentos y el servidor *HTTP* o *WEB*, cabe destacar que se observa un pico al comienzo que representa el impacto inicial del servidor a la cantidad de peticiones de acceso *WEB*, hasta que se estabiliza y se mantiene en equilibrio hasta el final de la simulación.

Para terminar las estadísticas globales de la red, se muestra el tiempo de respuesta de páginas *WEB* en la Figura 30, el cual no excede a los 0,2 segundos; lo cual afirmó por segunda vez el rendimiento de la red, aun cuando todos los usuarios realicen peticiones a las diferentes aplicaciones de forma simultánea.

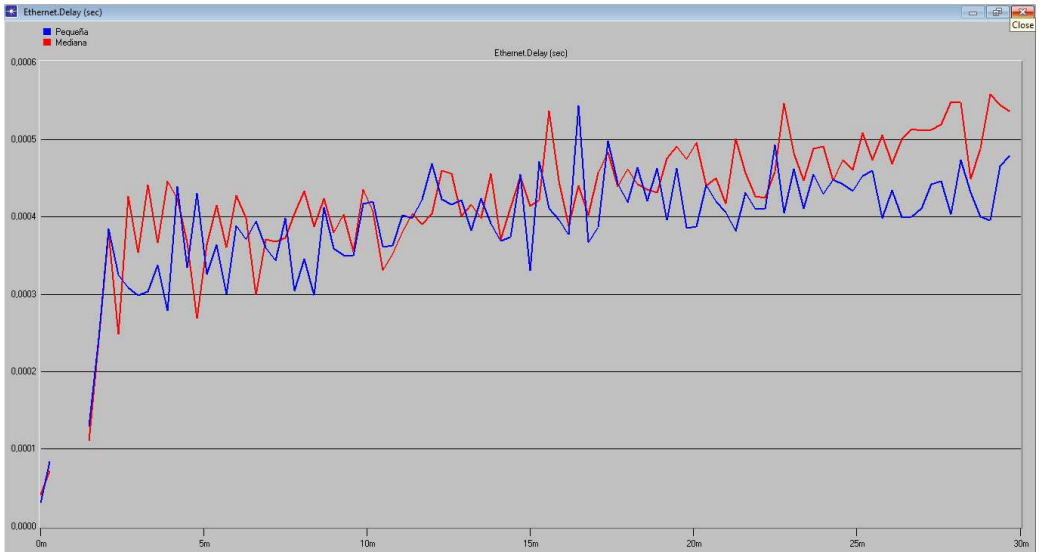

Figura 28 - Retardo de la red. *Software* OPNET

Fuente: (Propia)

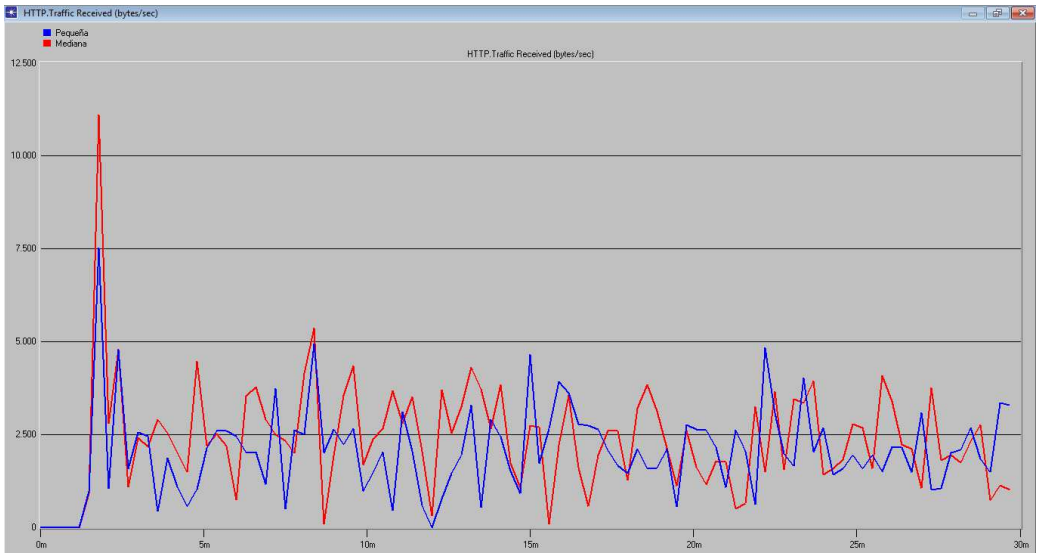

Figura 29 - Tráfico recibido por páginas *WEB. Software* OPNET

Fuente: (Propia)

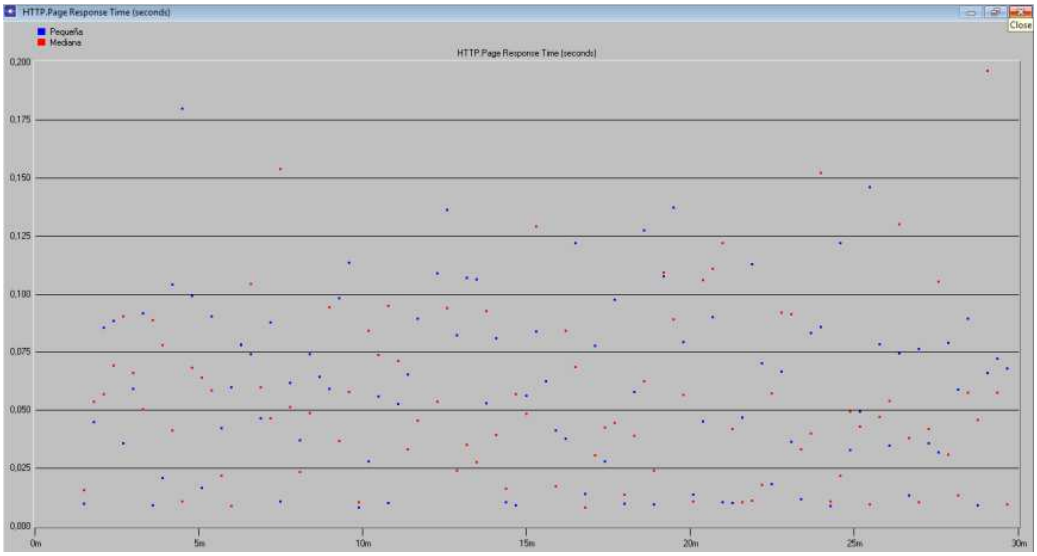

Figura 30 - Tiempo de respuesta en páginas *WEB. Software* OPNET

Fuente: (Propia)

Al analizar un enlace especifico, se tomó como ejemplo, un enlace entre el *switch* de los departamentos (S1) y el *switch* de los servidores (*CORE*), ya que es el enlace que contiene el tráfico de todas las peticiones que puedan realizarse de los usuarios a los servidores, de forma que es el más ocupado en la simulación, y por lo tanto, el que sería de más utilidad para calcular el **punto crítico**.

Inicialmente, se obtuvo la gráfica de utilización de bajada del enlace, donde el tráfico que fluye desde **CORE** hacia **S1**, es decir, desde los diversos servidores hacia los distintos departamentos. La Figura 31, muestra en una escala porcentual el uso del enlace, dando como resultado aproximadamente 1,2% y 0,75% para las redes mediana y pequeña, respectivamente.

Para ambos casos se utilizó una conexión cableada de Base100-T, lo que conllevo a concluir que el ancho de banda necesario para ambos sistemas es de 1,2Mbps para medianas empresas y 750Kbps para pequeñas. Conocidos estos requerimientos, se estima que una conexión de INTERNET de 2Mbps cumplirá los requerimientos básicos de cualquiera de estas dos redes. Es importante destacar, que

estos cálculos fueron realizados en un contexto "improbable", ya que todos los usuarios usaban todos los servicios disponibles en la red, al momento de la simulación.

Por último, en la Figura 32, se muestra el *throughput* (cantidad de información) en el enlace, en donde se puede apreciar que el tráfico máximo del enlace; en el caso de pequeñas empresas, el valor máximo fue 750Kbps, mientras que en las empresas medianas fue de un poco mas de 1,25Mbps. Estos datos coinciden perfectamente con el análisis de utilización de la red, por lo que se reafirma el uso de un plan de INTERNET que ofrezca como mínimo 2Mbps de velocidad de transmisión.

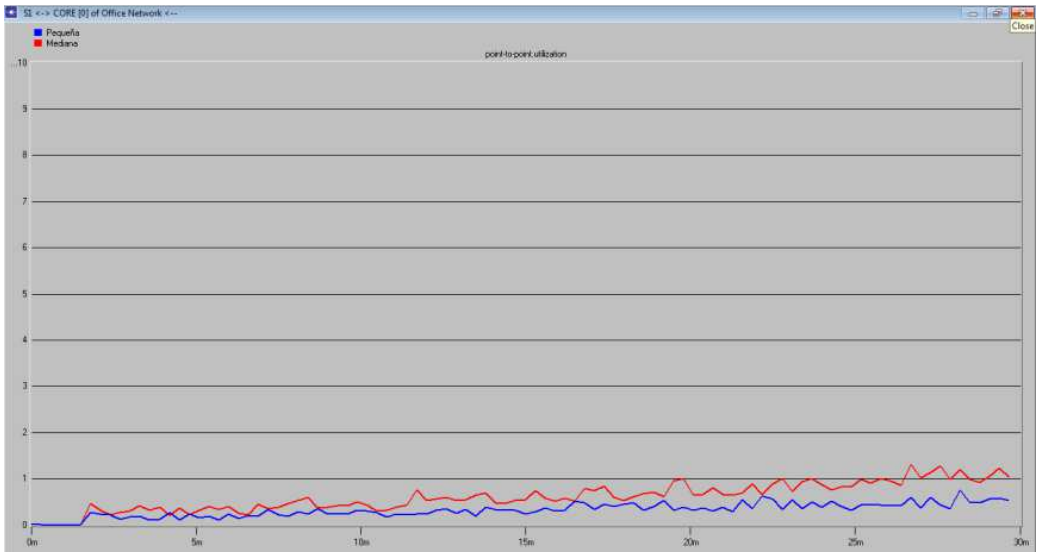

Figura 31 - Utilización de enlace CORE --> S1 (*downlink*). *Software* OPNET

Fuente: (Propia)

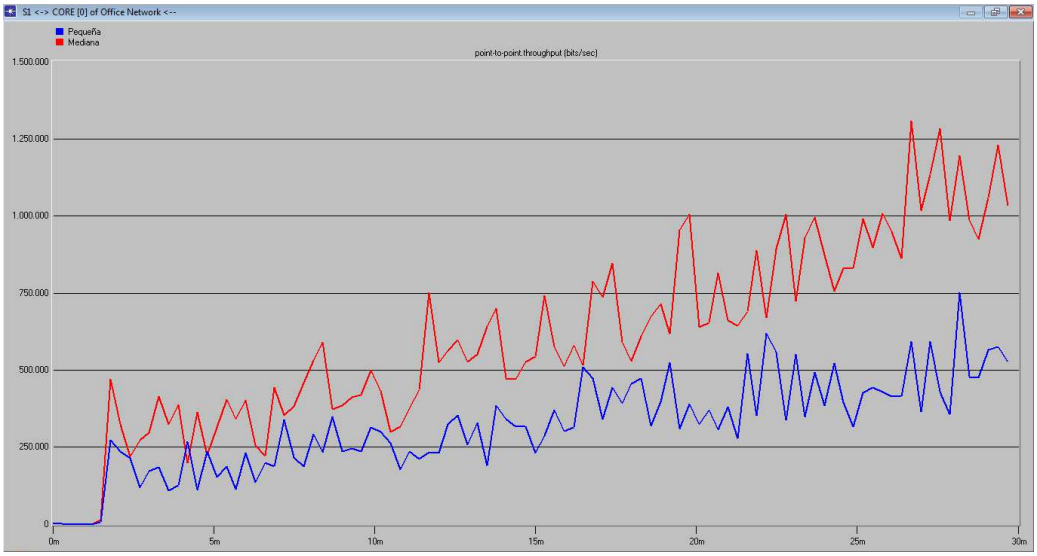

Figura 32 - *Throughput* (bps) del enlace CORE --> S1. *Software* OPNET

Fuente: (Propia)

Para finalizar el análisis de los diseños efectuados se realizó un modelo estructural en PACKET TRACER de CISCO de lo que será la red inalámbrica para ambos modelos de empresas; con el cual se demostró la conectividad entre todos los equipos y la implementación de medidas de seguridad que debe considerar el administrador de la red para el buen funcionamiento de la misma.

Como se explicó con anterioridad, se conectaron los servidores para cada departamento (cada uno con una *VLAN* establecida), un (1) equipo por departamento, tres (3) *switchs*, tres (3) *routers* inalámbricos, dos (2) enrutadores principales y 2 servidores externos, recordando que esta simulaciones es sólo para comprobar conectividad y correcto funcionamiento de posibles configuraciones de red.

Las simulaciones realizadas son un modelo que comprobaron la conectividad y funcionamiento de ciertas aplicaciones, este no sería el modelo definitivo de los modelos de las empresa, ya que, en la realidad se conectarían muchos más equipos por cada *router* inalámbrico en funcionamiento. Cabe destacar que al añadir más usuarios a la red no varía el funcionamiento de estas simulaciones.

El modelo es funcional para pequeñas y medianas empresas, ya que los servicios implementados son los mismos en ambos casos, la diferencia radica únicamente en la cantidad de usuarios y, por lo tanto, los *routers* inalámbricos, ya que, al aumentar el número de usuarios a gran escala, la cantidad de *routers* aumentará progresivamente para poder mantener el área de cobertura y la capacidad de conexión para todos los equipos.

Las simulaciones demuestran conectividad solo entre equipos conectados a la misma *VLAN*, seguridad por servidor *AAA Radius*, activación de *firewall* para permitir tráfico *HTTP, SMTP Y POP3*, activación de seguridad *WAP-2* en cada uno de los *routers* y finalmente, el filtrado *MAC* de los equipos.

Las *VLAN's* (redes de área local virtual) es una red de área local que permite interconectar equipos de manera lógica; fueron implementadas de nivel 1, ya que su administración será a través de los puertos de conexión del conmutador, a su vez fueron configuradas de forma estática, es decir, se asignaron manualmente los puertos del conmutador a las respectivas *VLAN's*.

La implementación de este tipo de red permite tener una mayor flexibilidad y administración de la red, proporciona mayor seguridad ya que la información se encapsula en un nivel adicional y además este tipo de conexión garantiza disminución en la transmisión de tráfico de la red. Se configuraron de forma tal que cada sector o departamento solo pueda conectarse específicamente con su servidor, para ello es necesaria la configuración de sub-interfaces para poder controlar el tráfico en la red.

Además, a cada servidor se le activó la aplicación *DHCP* para proporcionar la dirección IP de cada *VLAN* de forma dinámica, esta aplicación permite que se asignen las direcciones de forma automática a todos los equipos que pertenezcan a una *VLAN* especifica, por tanto en momentos que la red escale, solo se configuran las

VLAN a la cual se desea conectar y este automáticamente distribuirá las direcciones IP pertinentes.

El diseño interno (Figura 33) está integrado por cuatro (4) servidores, cada uno cumplirá con funciones específicas que dependerán exclusivamente de los requerimientos de la empresa, lo que conlleva a la implementación de una VLAN (Anexos F y G) por servidor, distribuidas como se muestra en la Tabla 8:

VLAN	DEPARTAMENTO
10	INV-RRHH
20	ADM-FACT
30	OTROS
50	Administrador de red

Tabla 8 - Distribución de *VLAN's* según departamento

Fuente: (Propia)

Se debe considerar, que en una situación real cada *VLAN*, estará compuesta por varios usuarios, los cuales, estarán conectados a través de routers inalámbricos para permitir a la empresa tener varios empleados conectados a la red.

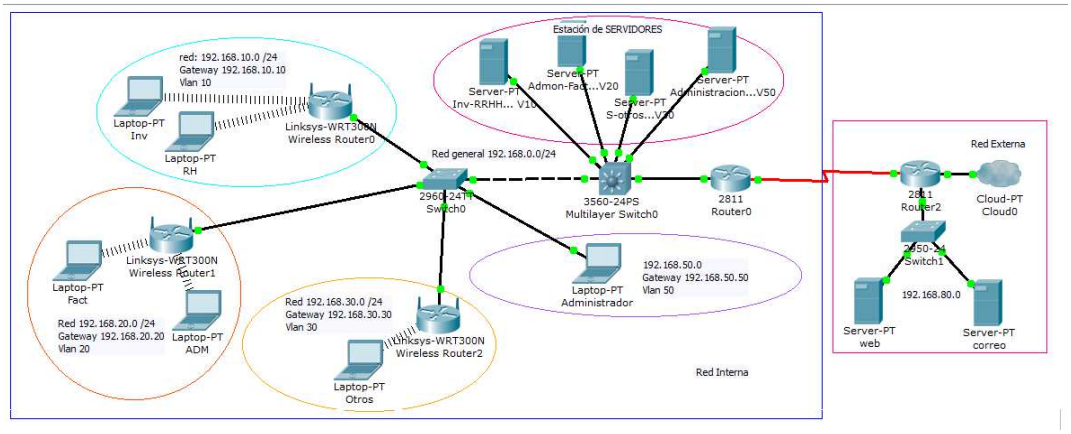

Figura 33 - Topología diseñada. *Software* PACKET TRACER

Fuente: (Propia)

Una vez establecida la configuración seleccionada, se realizaron pruebas de conectividad entre equipos de la misma *VLAN* y entre equipos integrantes de otras VLAN. En la Figura 34, se observa la ejecución de un *ping* desde la *VLAN*-10 Inv (192.168.10.11) a su respectivo servidor cuya dirección IP es 192.168.10.1, el cual se realiza satisfactoriamente (*Successful*), por contrario si realizamos un ping de Inv (192.168.10.11) al servidor de la *VLAN*-20 192.168.20.1 el ping es denegado (*Failed*).

Para comprobar que existe la comunicación entre diversos equipos de la red, aun cuando pertenecen a distintas *VLAN's*, se obtiene la Figura 35, la cual refleja la conexión satisfactoria entre un equipo perteneciente a la *VLAN*-20 (ADM) y otro perteneciente a la *VLAN*-10 (Inv). También muestra el intento de ADM de entrar al servidor de la *VLAN*-10, lo cual da como resultado una comunicación fallida. Esta prueba demuestra que la comunicación entre equipos pertenecientes a la red es exitosa y que para entrar a cada servidor se tienen que pertenecer a la *VLAN* respectiva.

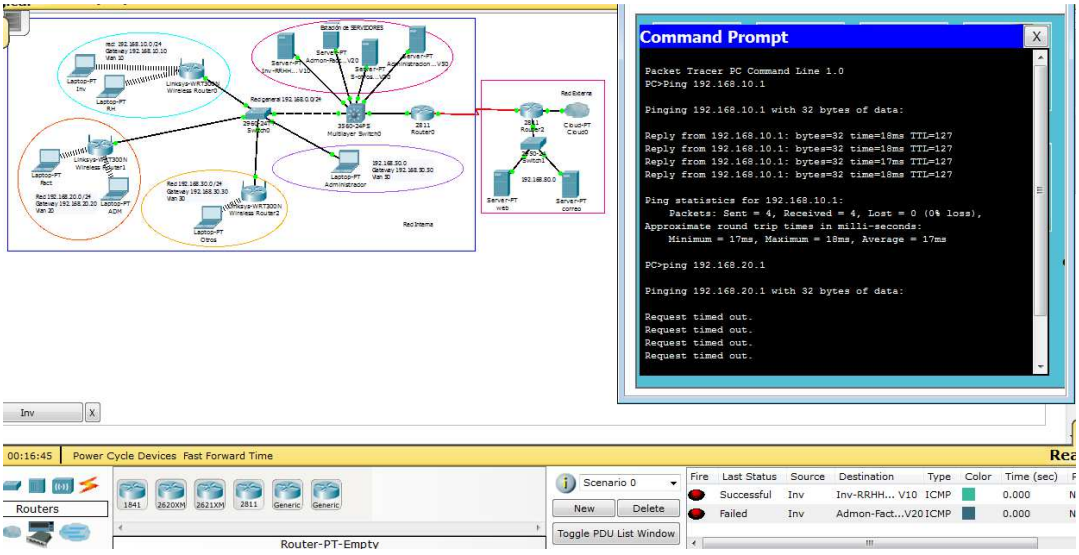

Figura 34 - Conectividad entre *VLAN's*. *Software* PACKET TRACER

Fuente: (Propia)

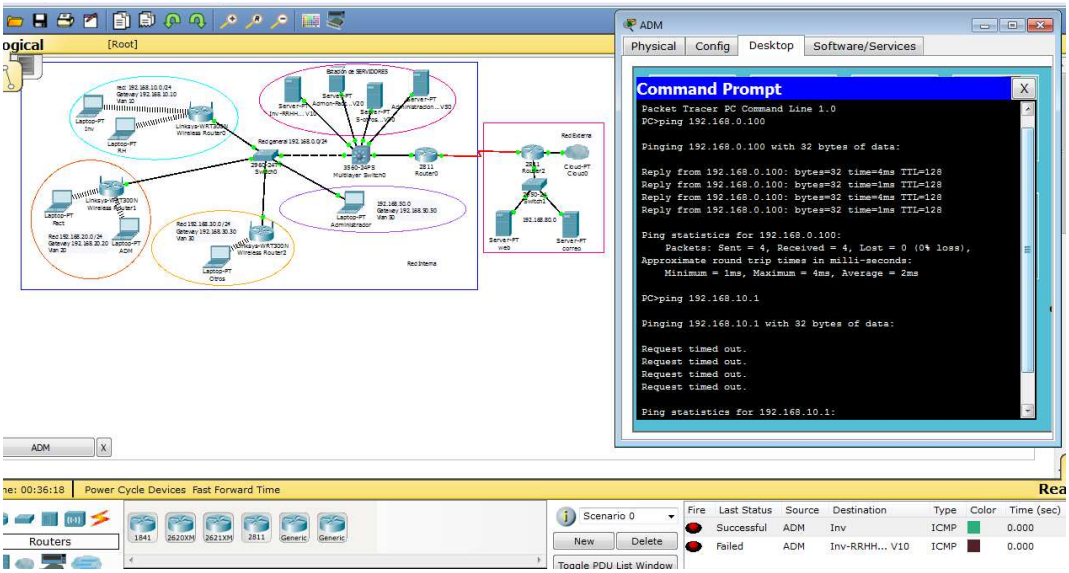

Figura 35 - Conectividad entre equipos. *Software* PACKET TRACER

Fuente: (Propia)

Seguidamente, se implementó el *firewall*, configurado a nivel de *software* para permitir o limitar el tráfico de información a la red interna, y se habilitaron los protocolos *HTTP* y *SMTP* en los servidores que deben permanecer accesibles desde la red exterior. Esta configuración bloquea la comunicación directa con los servidores externos desde el interior de la red, más sin embargo, permite la comunicación de forma gráfica, es decir, los usuarios pertenecientes a la red interna no podrán realizar *ping* al servidor *WEB* ni al servidor de correo, pero podrán acceder a través del *BROWSER*.

La implementación del *firewall*¸ se realiza con la finalidad de bloquear el acceso no autorizado a la red interna y, a su vez, permite que en la red no existan congestiones de tráfico a causa de ráfagas de *ping*. Se permitió el paso de información a través de los puertos ochenta (80) y cuatrocientos cuarenta y tres (443) para *HTTP* y veinticinco (25) y ciento diez (110) para *SMTP* y *POP3* respectivamente. Esta configuración se realizó en las interfaces pertenecientes al *router* más inmediato a la red interna.

En la Figura 36, se muestra que al realizar un *ping* hacia la red externa es fallido; esta prueba se realizó desde el equipo Fact al servidor *WEB* y la falla ocurre debido a que el protocolo *icmp* está bloqueado, aunque si realiza la comunicación a través del buscador *WEB* del equipo Fact y se puede visualizar la página del servidor 192.168.80.2, ya que si se permitió el tráfico *HTTP*.

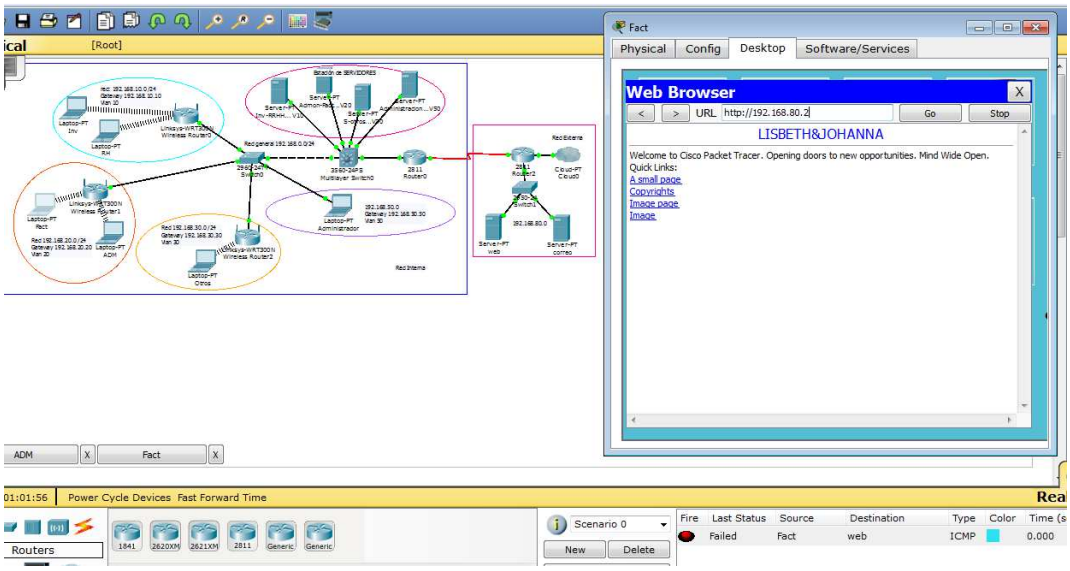

Figura 36 - Prueba de *Firewall. Software* PACKET TRACER

Fuente: (Propia)

Como se espera que las empresas administren el acceso a páginas *WEB*, para colocar información relevante, se configuró el protocolo *DNS* (Sistema de Nombre de Dominios), el cual, permite el seguimiento de las páginas *WEB* a las cuales sus empleados tienen permitido el acceso, es decir, traduce nombres asociados a equipos dentro de la red para localizar servidores, este proceso es realizado a través de direcciones IP.

La Figura 37 refleja cómo se configuró el sistema *DNS* para cuando algún usuario introduzca una página *WEB*, este sea dirigido directamente a la dirección IP configurada y acceder a la respectiva página, en este caso la página **www.lijoha.com**

está relacionada a la dirección IP del servidor *WEB* y por ende se direcciona al *HTTP* configurado en este servidor (Figura 38)

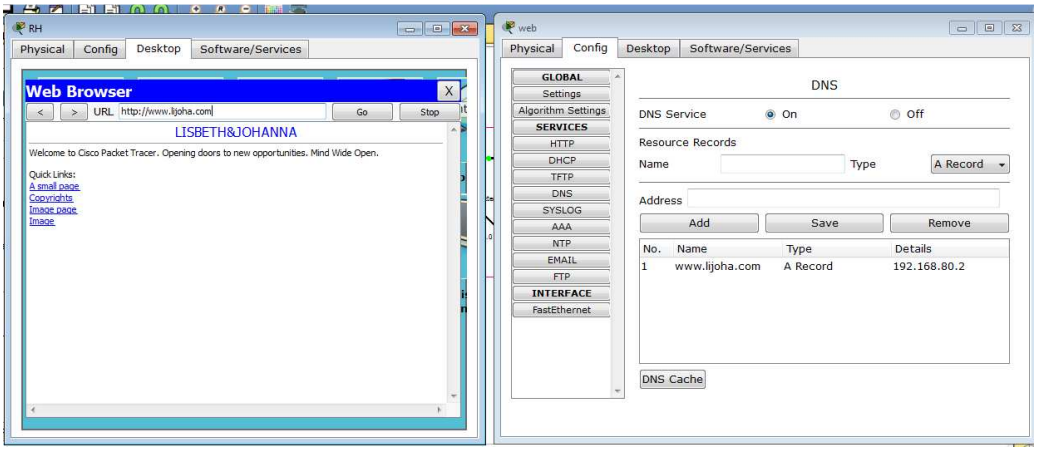

Figura 37 - Configuración *DNS. Software* PACKET TRACER

Fuente: (Propia)

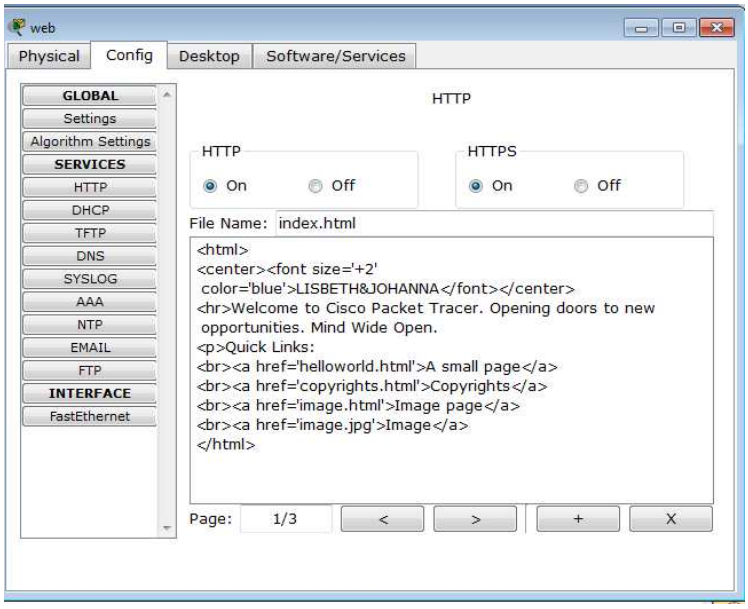

Figura 38 - Configuración *HTTP. Software* PACKET TRACER

Fuente: (Propia)

Otro de los servicios implementados fue el de correo electrónico, por ende se configura el servidor de correo con los posibles usuarios y se habilita el tráfico *SMTP*

y *POP3* (Figura 39); a continuación, se establecen cuentas de *e-mail* en cada uno de los equipos a manejar, en este caso fueron las máquinas Inv y RH asignando la dirección del servidor de correo como entrada y salida de las peticiones. (Figura 40). Por último, se comprobó el envío de un *e-mail* desde Inv con usuario **lili@lijoha.com** hacia RH con usuario **joha@lijoha.com** de manera satisfactoria (Figura 41), lo que permitió demostrar que el tráfico *SMTP* y *POP3* se encontraban configurados y activados en el *firewall* correctamente.

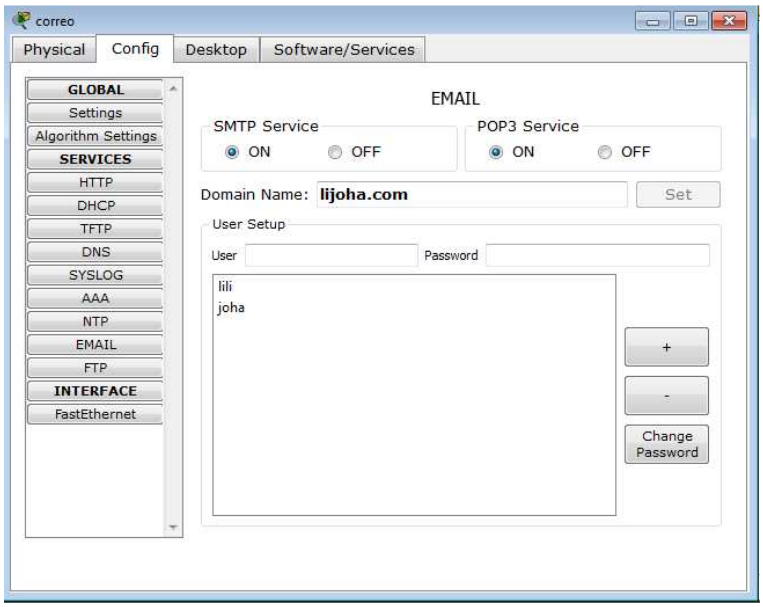

Figura 39 - Configuración de *e-mail* en el servidor. *Software* PACKET TRACER

Fuente: (Propia)

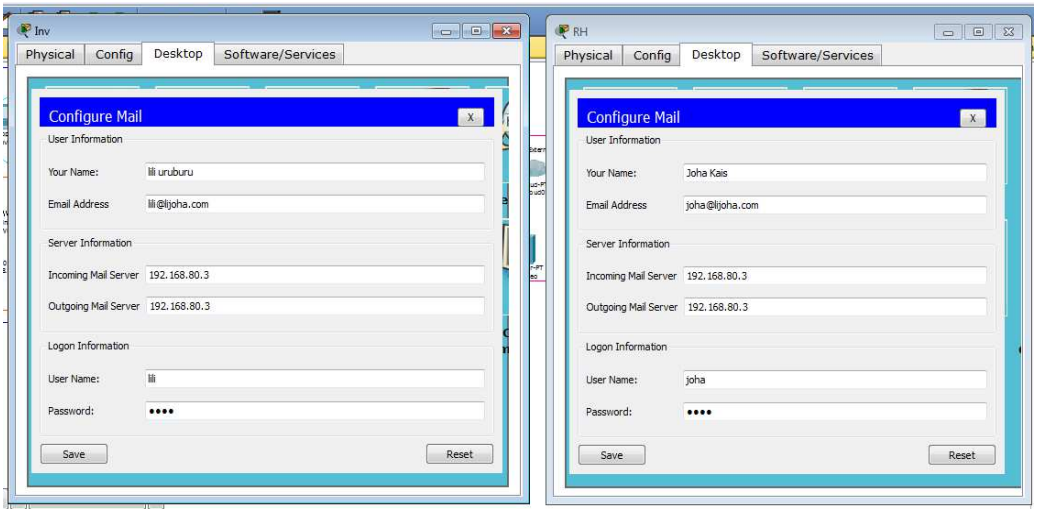

Figura 40 - Configuración de correo electrónico en los equipos. *Software* PACKET TRACER

Fuente: (Propia)

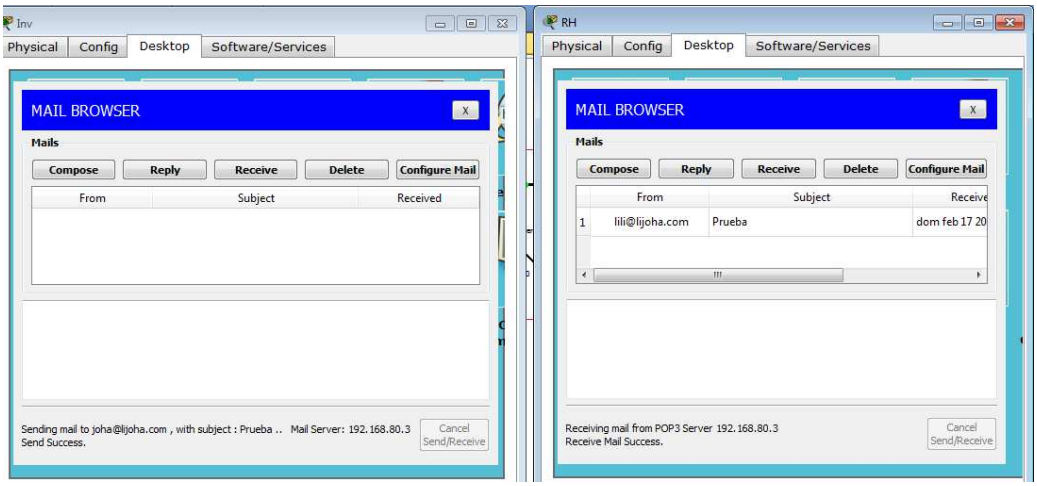

Figura 41 - Prueba de recepción de correo. *Software* PACKET TRACER

Fuente: (Propia)

Una vez comprobada la correcta configuración del *firewall*, se procedió a la activación de otros servicios de seguridad como son: el filtrado por listado *MAC* y la activación de un servidor *AAA Radius* para la administración de los *routers*, este servidor corresponde a un tipo de protocolo que realiza funciones de autenticación, autorización y contabilización; en este caso se realizó con el fin de poder asignar una

cantidad de usuarios determinada con acceso al *router* principal de la empresa para su posible administración.

El acceso al enrutador principal es de suma importancia, ya que en él se configuran los accesos a la red, los servicios que se permiten, así como otros requerimientos de enrutamiento, debido a esto es importante establecer parámetros de seguridad para el mismo; se establece como servidor *AAA Radius*, al servidor de administración en el cual se introducen los posibles usuarios con sus respectivas claves y configuraciones previas.

La activación de este servidor (Figura 42) garantiza que las únicas personas con acceso a los parámetros de configuración y administración de la red estén previamente registradas en el servidor. Una vez realizadas las configuraciones, para verificar su funcionamiento se demuestra que para poder acceder a la configuración del *router* principal, este solicita el usuario y su clave para luego verificar con el servidor y de esta manera, autentificar los datos introducidos, si este procedimiento es satisfactorio entonces es cuando el servidor autoriza el acceso del usuario al *router* (Figura 43).

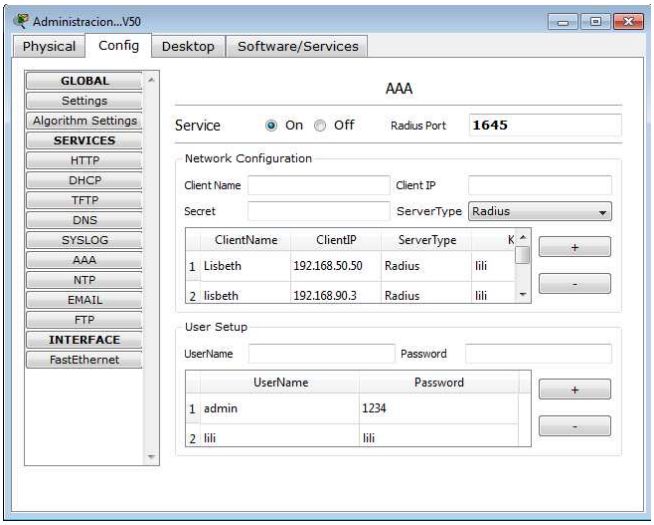

Figura 42 - Configuración Servidor *AAA-Radius*. *Software* PACKET TRACER

Fuente: (Propia)

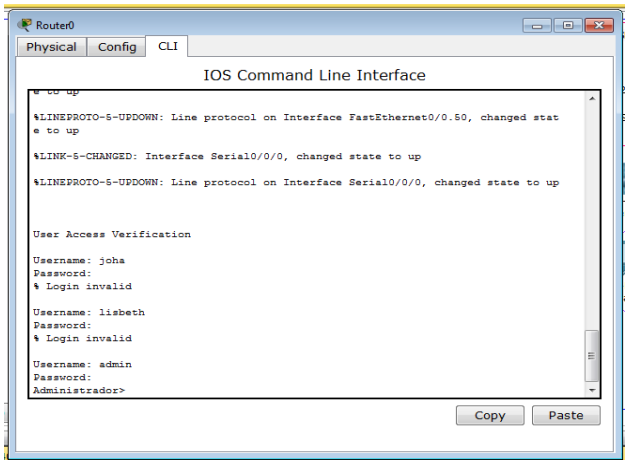

Figura 43 - Comprobación de funcionamiento *AAA-Radius* en *Router0*. *Software* PACKET TRACER
Fuente: (Propia)

Para terminar con la fase de comprobación de las características de seguridad de la red, se configuró el filtrado *MAC*, el cual se realiza debido a que los equipos deben estar conectados inalámbricamente a los *routers* correspondientes, por lo que es necesario sincronizar la conexión entre cada conjunto de enrutador y sus usuarios; para evitar que algún equipo se conecte a un enrutador perteneciente a otra *VLAN* y por ende obtener información de otros servidores.

Para obtener acceso al *router*, se cuenta con una clave previamente establecida (Figura 44) por el administrador de la red, por tanto solo él será quien pueda llevar un registro de las direcciones *MAC* registradas en cada *router* (Figura 45).

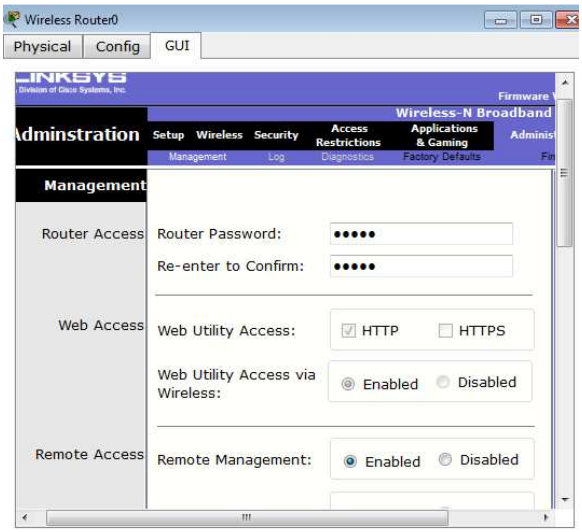

Figura 44 - Administración de *router* inalámbrico. *Software* PACKET TRACER

Fuente: (Propia)

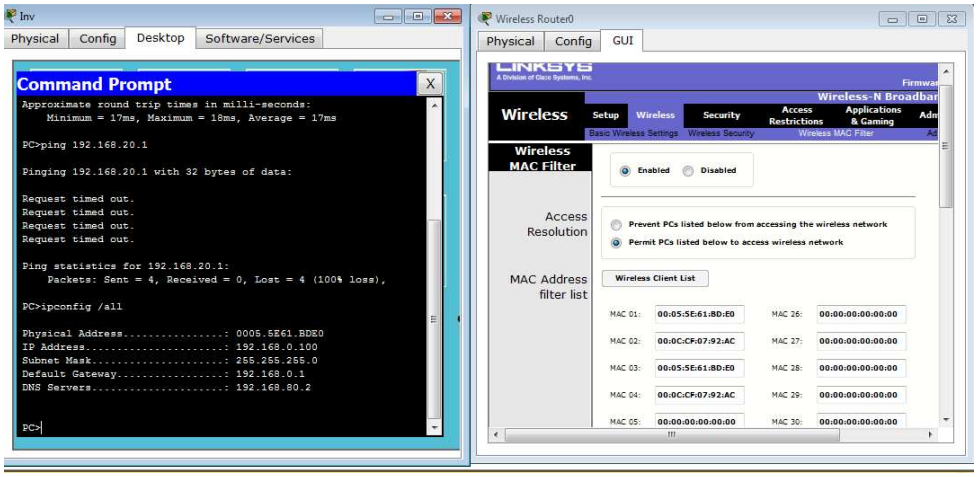

Figura 45 - Configuración y comprobación de filtrado *MAC*. *Software* PACKET TRACER

Fuente: (Propia)

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

Conclusiones

El último censo económico realizado en Venezuela, indica que las pequeñas y medianas empresas (PYMES) abarcan aproximadamente un 93% del total de la actividad económica del país. En la actualidad, estas empresas no poseen un patrón de conexión establecido, lo que conlleva a que enfrenten diferentes desafíos con respecto a la movilidad y la seguridad en sus redes internas.

Este trabajo demuestra los beneficios de utilizar las redes inalámbricas en PYMES, ya que garantizan accesibilidad, productividad, fácil configuración, y escalabilidad, además de reducir costos de implementación y establecer protocolos de seguridad en el tráfico de la información.

La realización de este proyecto, determinó que para la implementación de una red inalámbrica, se deben considerar diversos parámetros para su correcto desempeño y funcionamiento, como son: cantidad de usuarios que se desean manejar, tipo de información que se va a traficar en la red y por último, los servicios que requieran mayor importancia; lo que conllevó a realizar un estudio exhaustivo de la ubicación de los equipos, con el fin de garantizar una mejor aplicación y utilización de los recursos, como se demostró con el uso del *software* RPS.

Se demostró que, para el desarrollo de redes inalámbricas en PYMES, se debe utilizar el estándar 802.11n, que aunque esta tecnología reduce el rango de cobertura, permite mejorar la velocidad y la tasa de transmisión de los equipos, por lo tanto mejora el rendimiento de la red, además de ser compatible con versiones anteriores.

En el desarrollo de una red inalámbrica, se debe considerar que la cobertura de la red es limitada, ya que se ve afectada por obstáculos como paredes y puertas, cantidad de usuarios conectados y la distancia entre los *AP's* y las máquinas correspondientes a cada uno; sin embargo hay conexiones que necesariamente tienen que ser cableadas, como las conexiones entre switches y servidores, por lo tanto la red sería una red hibrida (inalámbrica-cableada), bajo estas condiciones, se utilizó el estándar *WiFi* mencionado y cableado Fast-Ethernet (100Mbps)

Luego de realizar los estudios pertinentes para la ejecución de este proyecto, se determinó que la seguridad de una red inalámbrica se garantiza utilizando diversas técnicas; como son: el cifrado de la información, la autenticación de usuarios y los sistemas de control, como se comprobó utilizando el *software* de simulación de conectividad y seguridad PACKET TRACER de CISCO.

Después del estudio de los modelos establecidos, se estableció que los mismos podrán ser utilizados en empresas pequeñas, hasta un máximo de diecisiete (17) usuarios por turno de trabajo y, hasta cuarenta y un (41) usuarios en las empresas medianas, por turno.

El estudio global de la red, con respecto a su rendimiento, conectividad y seguridad, por medio de los *softwares* utilizados, demuestra que ambos modelos son proyectos factibles, si se implementan bajo condiciones similares a las simuladas y analizadas en el desarrollo de esta investigación, garantizando una conexión fiable a todos los usuarios, aún en el punto crítico de congestión.

Recomendaciones

La ubicación de los equipos es de vital importancia ya que de ello depende el mejor aprovechamiento de la red, en cuanto a cobertura de la misma. Los equipos tienen que estar ubicados a alturas significativas ya que esto garantiza una mejor distribución de las ondas y por seguridad evita el fácil reinicio de los mismos.

Hay que considerar las condiciones físicas de las estructuras donde se desea implementar la red, ya que los mismos pueden generar algunos cambios con respecto a la propagación de las ondas y rango de cobertura de los equipos. Por ende es necesario contar con los planos detallados de la estructura que se va a manipular.

Para futuros trabajos se sugiere el estudio de la virtualización de los diferentes servidores en uno solo, lo que permita manejar las diferentes aplicaciones necesarias según sean los requerimientos de la empresa y de esta manera reducir costos de implementación y optimizar la red.

También es posible, utilizar un único servidor que provea todos los servicios y contenga diferentes puertos, donde cada puerto utilizará los recursos que necesita cada servicio, para su correcto funcionamiento.

BIBLIOGRAFÍA

Andreu, F., Pellejero, I., & Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad, Redes WLAN*. Barcelona: Marcombo.

Ariganello, E. (19 de Junio de 2006). *Las tres capas del modelo jerárquico de Cisco.* Recuperado el 24 de Enero de 2013, de http://aprenderedes.com/2006/06/las-tres-capas-del-modelo-jerarquico-de-cisco/

ArticlesBase. (20 de Diciembre de 2012). *Actix releases free RF modeling software for student use*. Recuperado el 2 de Septiembre de 2012, de http://www.articlesbase.com/art-articles/actix-releases-free-rf-modeling-software-for-student-use-3880436.html

Cisco. (s.f.). *Course Catalog*. Recuperado el 1 de Septiembre de 2012, de Packet Tracer: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html

Cisco. (s.f.). *Lo que usted necesita saber de redes inálambricas*. Recuperado el 6 de Diciembre de 2012, de http://www.cisco.com/web/solutions/smb/espanol/productos/inalambrica/wireless_primer.html

Cooper, K. (14 de Agosto de 2011). *Tecnical Talk*. Recuperado el 14 de Febrero de 2013, de Firewall: http://www.technicaltalk.net/index.php?topic=3966.0

DeBeasi, P. (14 de Septiembre de 2009). *Aruba Networks.* Recuperado el 17 de Febrero de 2013, de 802.11n: The end of Ethernet?: http://www.arubanetworks.com/pdf/technology/whitepapers/wp_Burton_End_of_Ethernet.pdf

Decreto N° 6.215, Ley de promoción y desarrollo de la pequeña y mediana industria (Gaceta Oficial 15 de Julio de 2008).

MercadoLibre. (Agosto de 2010). *Computación*. Recuperado el 15 de Febrero de 2013, de http://home.mercadolibre.com.ve/computacion/

Molina, J. (2012). *Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y*

seguridad de la red LAN en la Empresa Editora El Comercio - Planta Norte. Chiclayo: Universidad Católica Santo Toribio de Mogrovejo.

Monachesi, E., Frenzel, A. M., Chaile, G., Carrasco, A., & Gómez, F. (2011). *Conceptos Generales de Antenas.* Tucumán: edUTecNe.

OPNET. (2012). *University Program*. Recuperado el 28 de Noviembre de 2012, de http://www.opnet.com/university_program/

Pahlavan, K., & Krishnamurthy, P. (2002). *Principles of Wireless Networks.* New Jersey: Prentice Hall.

Peinado, V., & Prado, R. (2008). *Propuesta de una guía general de acción para la aplicación del Marketing digital en las Pequeñas y Medianas Empresas (PYMES), en la ciudad de Cumaná, Estado Sucre.* Cumaná: Universidad de Oriente. Escuela de Administración.

Peredo, S. (2004). *Estudio de la propagación de ondas electromagnéticas.* Cholula: Universidad de las Américas Puebla.

Pérez, C., Zamanillo, J. M., & Casanueva, A. (2007). *Sistemas de Telecomunicación.* Cantabria: Santander.

Roman, F. (2005). *Introducción a WiFi redes inalámbricas*. Recuperado el 1 de Marzo de 2013, de http://www.chw.net/2005/08/introduccion-a-wi-fi-redes-inalambricas/

Ruíz, J. (Agosto de 2004). *Seguridad en Redes Inálambricas*. Recuperado el 11 de Diciembre de 2012, de http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridad_en_redes_inalambricas_WiFi.shtml

Sánchez, S. (2010). *Evaluación de factores determinantes para la participación de las PYMES del estado Lara en el mercado de capitales venezolano.* Barquisimeto, Venezuela: Universidad Centroccidental Lisandro Alvarado, Facultad de Ciencias Económicas.

Seoane, E. (2005). *Estrategia para implantación de nuevas tecnologías en PYMES.* España: Ideaspropias.

Tanenbaum, A. (2003). *Redes de Computadoras.* México: Pearson Education.

Técnicas Profesionales. (21 de Abri de 2012). *Comunicaciones para empresas*. Recuperado el 2 de Febrero de 2013, de Redes inalámbricas WiFi: http://foro.tecnicasprofesionales.com/index.php?topic=788.msg818#msg818

Viloria, A. (2007). Modelos socioeconómicos para las PYMES. *Economía; n° 42* , 12-14.

WiFi Alliance. (2012). *Discover and Learn*. Recuperado el 17 de Enero de 2013, de http://www.wi-fi.org/discover-and-learn

WiMax. (2012). *WiMax.com*. Recuperado el 14 de Noviembre de 2012, de 4G Wireless Broadband Solutions: http://www.wimax.com/general/what-is-wimax

ANEXOS

Anexo A: Características de *Router* inalámbrico N Lvbp1

Modelo	WRT120N
Estándares	IEEE 802.3u, 802.11g, 802.11b, versión 802.11n
Luces	Alimentación, internet, conexión inalámbrica, *WiFi Protected Setup*™ (*WiFi* protegido), Ethernet (1-4)
Puertos	Internet, Ethernet (1-4), alimentación
Botones	Reinicio, *WiFi Protected Setup*™ (*WiFi* protegido)
Tipo de cableado	Categoría 5
Número de antenas	Dos (2) internas
Modulaciones	802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAN, 64-QAM
Potencia transmitida en dBm	802.11b: 16,5 ± 1,5 dBm 802.11g: 13,5 ± 1,5 dBm 802.11n: 13,5 ± 1,5 dBm
Sensibilidad de recepción en dBm	-94 dBm a 1Mbps -90 dBm a 11Mbps -75dBm a 54 Mbps
Seguridad inalámbrica	*WiFi Protected Access*™ 2 o *WPA2* (acceso *WiFi* protegido), *WEP*, filtrado de direcciones *MAC* inalámbrico
Ganancia en dBi	2,0 (máx)
Bits de clave de encriptación	Encriptación hasta de 128 bits
Sistemas operativos compatibles	Edición Windows XP, Vista o Vista de 64 bits actualizada (para Network Magic y el asistente de configuración), Windows 7, Mac OS X 10.4 o superior (para el asistente de configuración)
Características claves	Cumple con los estándares IEEE 802.11n versión 2.0, 802.11g y 802.11b Certificación *WiFi* basada en IEEE 802.11g y 802.11b, garantizando interoperabilidad Encriptación inalámbrica *WPA2*™ para garantizar la seguridad Asistente de configuración de uso sencillo Incorpora puertos Ethernet con cruzado automático (MDI/MDI-X) 10/100, por lo que no se necesitan cables de conexión cruzada El dispositivo puede colocarse en horizontal, o bien se puede fijar en la pared

Anexo 1 - Características de *Router* inalámbrico WRT120N

Fuente: (Propia)

Anexo B: Características de *Router* CISCO 2801

Modelo	Router CISCO 2801, factor de forma externo - modular - IU
Dimensiones	Ancho: 43,8 cm Alto: 4,5 cm Profundidad: 41,7 cm Peso: 6,4 kg
Memoria	RAM 128Mb (instalada)/384Mb (máx) Flash 64Mb (instalada)/128Mb (máx)
Conexión de redes	Tecnología de conectividad cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Red/Protocolo de transporte IPSec, protocolo de gestión remota SNMP 3
Expansión/Conectividad	Dos (2) x HWIC Dos (2) x AIM Dos (2) x PDVM Un (1) x WIC Un (1) x VIC Una (1) memoria Una (1) tarjeta CompactFlash0 Dos (2) interfaces de red Ethernet 10BaseT/100BaseTX/RJ-45 Un (1) x USB Un (1) x gestión de consola Un (1) x red-auxiliar
Algoritmo de cifrado	DES, Triple DES, AES
Voltaje necesario	CA 120/230 V (47-63Hz)
Sistemas operativos	OS proporcionada CISCO IOS 12.3 T Sistema operativo requerido Microsoft windows
Normas	Cumplimiento de las normas IEEE 802.3af Cumplimiento de las normas CISPR 22 Class A, CISPR 24, EN 61000-3-2, VCCI Class A ITE, IEC 60950, EN 61000-3-3, EN55024, EN55022 Class A, UL 60950, EN50082-1, CSA 22.2 No. 60950, AS/NZ 3548 Class A, JATE, FCC Part 15, ICES-003 Class A, CS-03, EN 61000-6-2
Características	Protección firewall, cifrado de hardware, alimentación mediante Ethernet (PoE), asistencia técnica VPN, soporte de MPLS, filtrado de URL, plegable a la pared

Anexo 2 - Características de *Router* CISCO 2801

Fuente: (Propia)

Anexo C: Características de *Switch* Catalyst

Modelo	CAT2960S WS-C2960S-24TS-L stack 24 Gige-4 x SFP LAN Base
Tipo de producto	Switch Ethernet
Dimensiones	4,5 cm Alto 44,5 cm Ancho 29,9 Profundidad 4,5 Kg
Interfaz	24 puertos RJ-45 10/100/1000 Base-T *Network* LAN
Memoria	128 MB Flash 64MB
Voltaje	100-240 V (CA)
Sistema Operativo	Sistema CISCO IOS
Protocolos	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2C, HTTP Ethernet, Fast Ethernet, Gigabit Ethernet
Red	Adición de vínculos Jumbo Frames, soporte Control de transmisión de tormentas DHCP: Cliente y servidor IGMP
Seguridad	*MAC*, Filtro de direcciones Soporte SSH/SSL

Anexo 3 - Características de Switch Catalyst

Fuente: (Propia)

Anexo D: Equipos

Anexo 4 - Router inalámbrico Linksys N Lvbp1

Fuente: (MercadoLibre, 2010)

Anexo 5 - Router CISCO 2801

Fuente: (MercadoLibre, 2010)

Anexo 6 - *Switch* Catalyst CISCO

Fuente: (MercadoLibre, 2010)

Anexo E: Configuración de equipos en PACKET TRACER

EQUIPO	IP	VLAN's	Configuraciones
Servidor INV-RRHH	192.168.10.1	10	DHCP
Router Wireless 0	192.168.10.11	10	WPA2-PSK/MAC
Servidor ADM-FACT	192.168.20.1	20	DHCP
Router Wireless 1	192.168.20.10	20	WPA2-PSK/MAC
Servidor S-OTROS	192.168.30.1	30	DHCP
Router Wireless 2	192.168.30.11	30	WPA2-PSK/MAC
Servidor Administración	192.168.50.1	50	DHCP
Computadora Administrador	192.168.50.11	50	
Router 0 (Cliente)	Sub-interfaces 192.168.10.10 192.168.20.20 192.168.30.30 192.168.50.50 192.168.90.1		*Firewall* (HTTP-SMTP-POP3-ICMP) *AAA-Radius*
Router 2 (Externo)	192.168.90.3 192.168.80.1		
Servidor Web	192.168.80.2		HTTP-DNS
Servidor Correo	192.168.80.3		EMAIL

Anexo 7 - Configuración de equipos en PACKET TRACER

Fuente: (Propia)

Anexo F: Código de configuración *Switch0* (PACKET TRACER)

```
Building configuration...

Current configuration : 1374 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$nEGq.JBoaSmQZg297paTH/
!
!
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/6
!
.
.
.
!
interface Vlan1
```

```
 no ip address
 shutdown
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

Anexo G: Código de configuración *Switch CORE* (PACKET TRACER)

```
Building configuration...

Current configuration : 1842 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
ip routing
!
!
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

```
interface FastEthernet0/7
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/8
!
!
.
.
.
!
interface Vlan1
 no ip address
 shutdown

ip classless
!
!
!
line con 0
line vty 0 4
 login
!
!
!
end
```

Anexo H: Configuración *Router0* - Cliente (PACKET TRACER)

```
Building configuration...

Current configuration : 1865 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Administrador
!
!
enable secret 5 $1$mERr$4dpRATIgxQacPVK0CfNV4/
!
!
aaa new-model
!
aaa authentication login default group radius local
!
!
username admin secret 5 $1$mERr$4dpRATIgxQacPVK0CfNV4/
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 no ip address
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.10 255.255.255.0
 ip access-group 101 in
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.20 255.255.255.0
 ip access-group 101 in
```

```
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.30 255.255.255.0
 ip access-group 101 in
!
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 192.168.50.50 255.255.255.0
 ip access-group 101 in
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 192.168.90.1 255.255.255.0
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 network 192.168.0.0
 network 192.168.1.0
 network 192.168.10.0
 network 192.168.32.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
!
ip access-list extended Pyme

access-list 101 deny icmp any any host-unreachable
access-list 101 permit tcp any any eq www
access-list 101 permit tcp any any eq smtp
access-list 101 permit tcp any any eq pop3
```

```
!
!
radius-server host 192.168.50.1 auth-port 1645
radius-server key lili
!
!
!
line con 0
 login authentication default
line vty 0 4
!
!
End
```

Anexo I: Configuración de *Router* externo (PACKET TRACER)

```
Building configuration...

Current configuration : 1095 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname RouterExterno
!
!
enable secret 5 $1$mERr$RchIbJiXmCXFtFBZll50l/
!
!
aaa new-model
!
aaa authentication login default group radius local
!
!
username admin secret 5 $1$mERr$RchIbJiXmCXFtFBZll50l/
!
!
interface FastEthernet0/0
 ip address 192.168.80.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/2/0
 ip address 192.168.90.3 255.255.255.0
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 network 10.0.0.0
 network 192.168.0.0
 network 192.168.1.0
 network 192.168.10.0
 network 192.168.32.0
```

```
 network 192.169.0.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/2/0
!
!
radius-server host 192.168.50.1 auth-port 1645
radius-server key lili
!
!
line con 0
 login authentication default
line vty 0 4
!
!
end
```