UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA INFORMÁTICA

TESIS DE GRADO

MODELO DE GESTIÓN DE ANCHO DE BANDA PARA UNA RED INALÁMBRICA DE ÁREA LOCAL

PARA OPTAR AL TÍTULO DE LICENCIATURA EN INFORMÁTICA
MENCIÓN: INGENIERÍA EN SISTEMAS INFORMÁTICOS

POSTULANTE: UNIV. AIDA LUZ BELTRÁN CABRERA

TUTOR: LIC. NANCY ORIHUELA SEQUEIROS

REVISOR: LIC. JOSÉ LUÍS ZEBÁLLOS ABASTO

ASESOR: LIC. GABINO VARGAS MURILLO

LA PAZ - BOLIVIA
2009

RESUMEN

El desarrollo del modelo de gestión de ancho de banda para una red inalámbrica de área local, es una investigación de la administración del ancho de banda segura mediante el uso de soluciones basadas en software, que determinan, un óptimo rendimiento en el uso del ancho de banda, con un ambiente de seguridad para el administrador y los usuarios conectados a la red inalámbrica con el proceso de autenticación y control de entradas de los usuarios, asociados a un nivel de privilegios, obteniendo así, una buena recepción de la señal sin tener temor de que alguien ajeno a la red inalámbrica, se conecte aprovechando su ancho de banda.

Esta solución aplica tres elementos importantes que forman el núcleo central del diseño del modelo propuesto para consolidar el presente trabajo de investigación estos son: (1) La Autenticación y Autorización, (2) La Gestión de Ancho de Banda, y (3) La Seguridad de red WLAN.

La implementación del modelo se apoyo, con la autenticación y autorización, incorporando el protocolo AAA, el modelo tripartito y el método CHAP, donde se identifican a los usuarios; la gestión de ancho de banda fue implementada bajo las políticas de asignación de ancho de banda (niveles de privilegios, regla de número de usuarios, y restricción del ancho de banda), que establece un optimo rendimiento del uso de ancho de banda; y la seguridad a la red WLAN, donde se interactúa con el protocolo WPA, método EAP-PEAP y certificados que determinan un nivel alto de seguridad en el desempeño de redes inalámbricas.

En este trabajo de tesis se realizo la investigación, construcción, implementación y análisis del modelo de gestión seguro utilizando los procesos antes mencionados para poder ofrecer un entorno de red inalámbrica administrable y con un alto nivel de seguridad, recuperando así la calidad del servicio que la red WLAN debe conseguir.

Palabras clave: modelo, ancho de banda, administración, autenticación, seguridad, red inalámbrica, WLAN.

ÍNDICE ESPECIFICO

ÍNDICE GENERAL

- **Dedicatoria**
- **Agradecimientos**
- **Resumen**

Pág.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1 MARCO REFERENCIAL

1.1 Introducción

La globalización de la economía mundial, el Internet y las comunicaciones tienen un papel muy importante, las personas, instituciones y empresas necesitan estar interconectadas en línea para realizar diferentes procesos, y permitir el intercambio de recursos e información. Actualmente, la navegación por Internet a través de los dispositivos inalámbricos, hace que el intercambio de información por este medio, sea una práctica común para usuarios de las redes inalámbricas.

Las redes inalámbricas viaja por medio de ondas de radio luz o infrarroja, y es aplicada en situaciones donde las computadoras no se encuentran en un solo lugar y se necesite mantener conexión con una red de computadoras o Internet, estas redes son instaladas en diferentes ambientes como en oficinas, áreas de manufacturas, laboratorios de investigación, hospitales o universidades, y permite la conexión con otras terminales o dispositivos móviles.

Las redes inalámbricas, al igual que una red tradicional también cuenta, con aplicaciones que requiere un uso considerable de ancho de banda, pues las transacciones de audio y video generan muchos más paquetes que el envío de texto e imágenes, además de que, para garantizar un buen desempeño de estas aplicaciones, se necesita que el envío de paquetes sea a una taza de transferencia constante[1].

En las redes inalámbricas el ancho de banda, juega un papel muy importante en el desempeño de la red, teniendo como concepto de ancho banda, que es la cantidad de información que se transmite en un tiempo determinado a través de la red, [Cisco, 04] esto se debe a que los servicios requieren el uso de este recurso en

[1] La taza de transferencia es la medición real del ancho de banda en un momento dado y en segmento determinado de la red.

mayor o menor medida; donde la competencia se mide en términos de muchos factores como el número de usuarios de la red, la capacidad de dispositivos de la red para manejar el flujo de la información y el tipo de servicios que le soliciten a la red [Morales, 06].

El presente trabajo de tesis, plantea una solución a este problema, con el desarrollo de un modelo de gestión de ancho de banda para redes inalámbricas, con mecanismos de identificación de usuarios y políticas de asignación de ancho de banda por usuario, obteniendo así un mejor desempeño y manejo eficiente de la administración de este recurso. Este modelo, tiene como base la identificación de cada usuario, con un determinado límite del recurso, de manera, de categorizar o clasificar su uso, todo esto con el fin de que ningún usuario pueda acaparar una gran parte del ancho de banda y repercutir en los demás usuarios de la red.

1.2 Antecedentes

Las redes inalámbricas empezaron a cobrar fuerza desde que los costos de los equipos que permiten la conectividad empezaron a disminuir, y esto permitió la incursión de la tecnología inalámbrica en diferentes aspectos de nuestra vida diaria.

En el área de administración de redes inalámbricas de computadoras, el ancho de banda depende de las tecnologías que se estén implementando en la red. Para las redes inalámbricas, los equipos y tecnologías actuales nos permiten un ancho de banda limitado a velocidades entre 11 y 54 Mbps [Cissp - 07].

Algunas de las características del ancho de banda, es un recurso finito, por lo que se tiene que moderar su uso de acuerdo a las necesidades más importantes en el momento y servicios que se consideren como críticos, el ancho de banda no es gratuito, generalmente se compra de un proveedor de servicios, los cual lleva a los administradores de red a tomar decisiones sobre los equipos, servicios y políticas a establecer en la red, y traducir estos en términos de ahorro económico, su

demanda nunca deja de aumentar, a pesar de los nuevos dispositivos y tecnologías, el uso y competencia por el ancho de banda sigue en aumento debido a las aplicaciones que hacen uso de estas mayores capacidades de red [Cisco, 04].

La importancia del ancho de banda radica porque es un recurso finito y en un momento dado, la saturación de usuarios en una red y la competencia por el recurso entre aplicaciones puede generar que la transferencia de información se ajuste a velocidades por debajo de la capacidad de la red y la disponibilidad de los servicios se vea afectada, disminuyendo su nivel de calidad o la pérdida total de la calidad del servicio. Cuando un usuario se conecta a la red, el uso que este hace del ancho de banda, no es generalmente de una manera constante, debido a la diversidad de actividades que un usuario busca en los servicios de la red y sus motivos personales.

En las redes inalámbricas, el ancho de banda disponible está limitado por las características de los equipos que permiten la conectividad con la red, el cual, se encuentra más detallado en las especificaciones del estándar en el que se basa el equipo, uno de los estándares más utilizados para redes inalámbricas es el estándar 802.11[2] y sus diferentes versiones.

Lo que se puede encontrar, con respecto al presente trabajo de tesis en otras fuentes, principalmente en Internet, es de tipo comercial. Existe hardware dedicado a la administración de ancho de banda para redes de gran tamaño, esto para más de 1000 conexiones activas en una red corporativa. Algunas de estas compañías son Allot NetEnforcer y Bandwidth Controller, y proyectos Open Sourse. Las soluciones basadas en hardware se han desarrollado hasta este momento para redes cableadas y se empieza con la comercialización de equipos para ambientes inalámbricos, siendo los últimos equipos muy costosos para la implementación en oficinas o instituciones de menos de 100 usuarios [Riu, 08].

[2] Norma original IEEE de una LAN inalámbrica, sus características se especifican en la familia de 802.11, a, b, g, e, las cuatro normas utilizan el protocolo de Ethernet y CSMA/CA para compartir el camino.

En el caso de las soluciones basadas en software, el uso de un servidor que permita la regularización del ancho de banda en la red es indispensable, pero las características que debe poseer son que todos los dispositivos terminales deben tener sistema operativo Windows o otros sistemas operativos como en el caso de Linux, otro punto es que no se considero la interacción con los protocolos de seguridad (WAP)[3] y (WEP)[4] por lo que no se tienen estadísticas de desempeño en redes inalámbricas.

En la Carrera de Informática de la Facultad de Ciencias Puras y Naturales de la Universidad Mayor de San Andrés se encuentran pocas tesis de grado, que contemplen este tipo de temas. Sin embargo, la carrera cuenta con los siguientes trabajos realizados con anterioridad:

Control de seguridad y desempeño de una red Informática, Hace referencia al diseño de un modelo de administración de una red informática bajo plataforma Windows, para optimizar el desempeño, rendimiento y seguridad en redes, que contemplen diferentes tecnologías y usuarios [Marca, 04].

Control de Calidad de Servicio y rendimiento del proveedor de Internet, Hace referencia a la implementación de métricas de Internet existentes para garantizar la calidad de servicio al usuario propietario, y que se cobre un precio justo minimizando costos de inversión [Vargas, 03].

Seguridad y protección en redes LAN conectadas a Internet, Hace referencia al desarrollo de políticas y procedimientos de seguridad informática, dirigido a prevenir agresiones sobre activos informáticos que pertenecen a redes de área local, mediante las cuales se obtenga mayor control sobre las actividades de los usuarios y los recursos informáticos [Quisbert, 02].

[3] Del inglés Wireless Application Protocol, Acceso protegido a Wi-Fi
[4] Del inglés Wired Equivalent Privacy, Privacidad equivalente a cable

Herramienta para la protección de procedimientos almacenados de base de datos, Hace referencia al desarrollo de una herramienta que aplique las técnicas de encriptación y la ofuscación de código para determinar cuál es la más efectiva en la protección de procedimientos almacenados en Base de Datos [Sirpa, 07].

Administrador Proxy-Web & Proxy-Cache, Hace referencia al desarrollo e implementación de un software que permita gestionar de manera intuitiva los servicios Proxy Web y Proxy Cache para maximizar una conexión a Internet [Luna, 08].

1.3 Problemática.

El uso de las redes inalámbricas ha ido incrementando en la actualidad, ya que el hecho de que esta red sea de libre acceso en algunas instituciones y universidades deja a cualquier usuario, perteneciente o no a la institución que se puede conectar con su equipo de cómputo a la red del lugar y hacer uso de los servicios y recursos almacenados ahí, sin tener mecanismos de seguridad y regulación, esta situación es uno de los problemas de servicio que ofrece la red inalámbrica.

Un ejemplo es el uso del Internet en una institución educativa; donde el uso de dicho recurso debe ser con fines académicos y de investigación. El uso de algunas aplicaciones como las de mensajería instantánea puede prestarse a duda en su uso académico, pues permite tanto la opción de comunicarse con otras personas relacionadas a la proyecto, como para comunicarse con amigos para fines personales. La opción de descargar archivos de Internet, es otra situación que presta a dudar de las intenciones del usuario, ya que se puede bajar información necesaria para actividades académicas como para información de uso personal.

Hacer uso de la red de una institución con una conexión inalámbrica con fines personales puede disminuir el desempeño de la red, y ocasionar problemas a todos los usuarios que también utilicen dicha red.

El uso de aplicaciones con fines personales hace que la utilización del ancho de banda vaya en incremento, por lo que, con un número considerable de usuarios y un ambiente donde no se cuente con mecanismos de regulación y seguridad, la disponibilidad de los servicios de esta red puede verse afectada, además de, disminuir su capacidad de respuesta a las peticiones de servicio por parte de los usuarios que si utilicen la red con fines de la institución.

El principal problema que se encontró es el siguiente:

- El uso de los servicios de una red inalámbrica sin mecanismos de seguridad, regulación, y asignación de ancho de banda por usuario, que evite la competencia por el recurso, e incremente la calidad y disponibilidad del servicio en una red.

1.4 Hipótesis

El empleo de políticas de asignación de ancho de banda por usuario y mecanismos de identificación, permite al administrador de una red de conexión inalámbrica gestionar el ancho de banda.

La hipótesis planteada corresponde al tipo de "formulación causa y efecto".

La variable independiente es: Políticas de asignación por usuario, mecanismos de identificación.

La variable dependiente es: Gestión de ancho de banda

1.5 Objetivos

1.5.1 Objetivo General

Desarrollar un modelo de gestión de ancho de banda para una red inalámbrica de área local segura.

1.5.2 Objetivos Específicos

- Habilitar un sistema básico de identificación de usuarios que utilice el protocolo de autenticación, autorización y manejo de cuentas (AAA) como base de la seguridad en un ambiente inalámbrico.
- Gestionar el ancho de banda, para usuarios registrados en la red, asociándole un nivel de privilegio a cada determinado usuario.
- Generar la conexión entre el mecanismo de autenticación y el administrador de ancho de banda.
- Implementación de los mecanismos de identificación y las políticas de asignación de ancho de banda.

1.6Justificación

1.6.1 Técnica

El presente trabajo de tesis, se justifica técnicamente porque constituye un aporte a las técnicas de gestión y seguridad de redes inalámbricas de área local, ya que ofrece una herramienta para la toma de decisiones en cuanto a la soluciones de los problemas de administración y seguridad ocasionados por la excesiva demanda de ancho de banda, por usuario no registrado en la red.

1.6.2 Económica

Al trabajar con software libre, cualquier desarrollador puede disponer de su código fuente, lo cual implica independencia total en cuestión de licencias y de desarrollo tecnológico, un costo nulo de adquisición, garantizando sostenibilidad técnica y tecnológica en el tiempo.

1.6.3 Social

Con el desarrollo del modelo, se pretende satisfacer las necesidades de los usuarios, y administradores de red inalámbrica de área local, quienes tropiezan con el problema de administrar el ancho de banda según necesidades del usuario, con mecanismos de identificación en un ambiente seguro.

1.7 Alcances y Límites

Entre los alcances y límites que se tienen en el presente trabajo de tesis tenemos:

La construcción de un modelo, basada en software, que haga uso de un punto de acceso, que integre tecnologías de formato libre con mecanismos de seguridad y políticas de asignación de ancho de banda propuestas en el presenta trabajo de tesis para la gestión de ancho de banda en una red de conexión inalámbrica.

La integración de estos sistemas será la del servidor RADIUS[5] y el control de tráfico[6] de SQUID para la gestión, que darán un cierto nivel de confianza para el mejor desempeño en la administración del ancho de banda.

Para la implementación de la aplicación, se partirá del supuesto que no se cuenta con un mecanismo de autenticación de usuarios y los servidores y servicios tienen medidas de seguridad básicas.

Además, es importante hacer notar que el ancho de banda solo se alcanza en los casos más ideales, es decir, que no exista degradación (disminución progresiva) de la señal.

---

[5] Servidor de seguridad que autentica, autoriza, y administra las cuentas de los clientes que desean conectarse en una red de acceso remoto.

[6] Permite controlar el flujo de datos que sale hacia el servidor y lo permite redistribuir para los equipos destino.

1.8 Aportes

1.8.1 Aporte Práctico

Con el presente trabajo de tesis, se brindará a los administradores una herramienta para la gestión, asignación de ancho de banda y seguridad de su red de área local inalámbrica, ya que siendo esta una tecnología nueva, el administrador necesita información de este tipo de redes, donde el modelo de gestión de ancho de banda propuesto puede ser utilizado, y de esta manera, dar servicio a una gran comunidad de miembros.

1.8.2 Aporte Teórico

Al utilizar el servidor RADIUS y el control de tráfico del ancho de banda por SQUID, se podrá comprobar que esta tecnología también puede ser de gran ayuda para la gestión segura del ancho de banda de una red inalámbrica, de esta manera los administradores podrán realizar una mejor toma de decisiones, con respecto a la seguridad, administración y asignación de ancho de banda.

1.9 Métodos y Medios de Investigación Científica

Antes de señalar los métodos y metodologías a utilizar, es necesario conocer la diferencia entre estos dos conceptos: "El método es el procedimiento para lograr los objetivos. Metodología es el estudio del método". (Sirpa, 07)

La metodología a aplicarse en el desarrollo del presente trabajo de tesis es el método científico, que es camino de la observación, la interpretación y la comparación que sigue la ciencia para encontrarse a sí misma o mejorarse.

Como método general se utilizará el deductivo – inductivo, lo deductivo está ligado más al razonamiento que es lo abstracto, lo inductivo es más empírico - observacional, tomando en cuenta etapas de observación experimentación y

emisión de conclusiones, además de, técnicas de verificación de resultados, acumulación de datos, evaluación de datos, discusión de resultados.

Entre las herramientas a emplear como base del modelo en el aspecto tecnológico son: a) Software de base Linux, b) Software de seguridad, RADIUS, c) Software de administración, SQUID.

CAPÍTULO 2. MARCO TEÓRICO

2.1 Redes Inalámbricas

Las redes inalámbricas wireless network hacen referencia a un conjunto de equipos de cómputo interconectados por medio de transmisión no guiado mediante ondas electromagnéticas de radio e infrarrojo en lugar de cableado estándar (cableado estructurado) [Stallings, 02]. Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, para realizar el envió y la recepción de datos, a unos metros de distancia como a varios kilómetros. Asimismo, la instalación de estas redes no requiere ningún cambio significativo en la infraestructura existente, como pasa con las redes cableadas [Morales, 06].

La figura 2.1 muestra una red mixta, compuesta por la estación inalámbrica, y la red alambrica, con un punto de conexión, que se encuentra conectada a otro punto por medio de un enlace cableado, como es un segmento unido por cables de cobre o fibra óptica [Bing, 02].

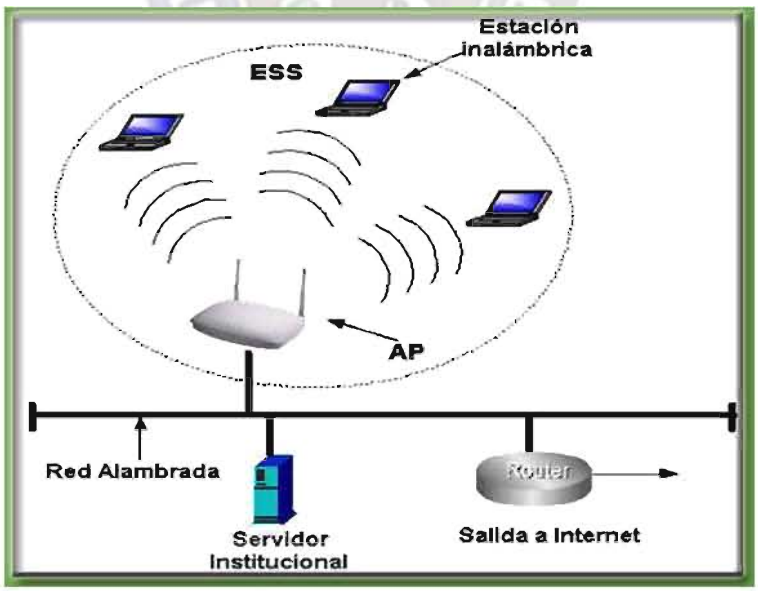

Fig. 2.1 Red mixta (inalámbrica, alambrica).
Fuente: [Telecom, 09]

Es importe comprender que la red inalámbrica es parte de una red mixta, dependiendo de si se estudia un segmento de la red o la totalidad de la misma. La interconexión de diversos medios de transmisión como las de: a) ondas de radio y b) fibra óptica, entre otros; hace que se piense en diferentes dispositivos que permiten la conectividad entre estos medios y las diferencias entre sus tecnologías; es decir, tienen diferentes consideraciones sobre instalación y desempeño los dispositivos que utilizan, fibra óptica que los medios que se comunican por ondas de radio [Morales, 06].

Las características principales de las redes inalámbricas por onda de radio es que las fuentes de interferencia existen en mayor cantidad que las fuentes para las redes cableadas. Al utilizar el aire como medio de transmisión para las ondas de radio, esta se encuentran expuestas a interferencias generales por el mismo ambiente (humedad, tormentas eléctricas, entre otras), el campo magnético de la tierra, otras ondas de radio como las antenas de radiodifusión; y la cobertura que ofrecen es directamente proporcional a la potencia de la antena, aunque los estándares IEEE[7] de transmisión juegan un papel de regulación en las potencias y frecuencias a ser utilizadas para la transmisión [Cisco, 04].

Las redes inalámbricas empezaron a cobrar fuerza desde que los costos de los equipos que permiten la conectividad empezaron a bajar, y esto permitió la incursión de la tecnología inalámbrica en diferentes aspectos de nuestra vida diaria. Muchos lugares como: a) aeropuertos, b) escuelas, c) oficinas, d) restaurantes, e) hoteles, entre otros, empiezan a instalar redes inalámbricas para sus clientes o usuarios[8] [Morales, 06].

[7] Del Inglés Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Electrónicos y Eléctricos.
[8] Se entiende por usuario a una división, un departamento, o un individuo, que satisfaga los requerimientos de acceso a la red inalámbrica.

En la figura 2.2 se observa el uso de redes inalámbricas que conectan las computadoras y todos los dispositivos electrónicos, con el fin de compartir información entre distintos puntos de conexión en cuestión de segundos, de manera, de tener todo bajo control y un mismo canal de conexión[9].

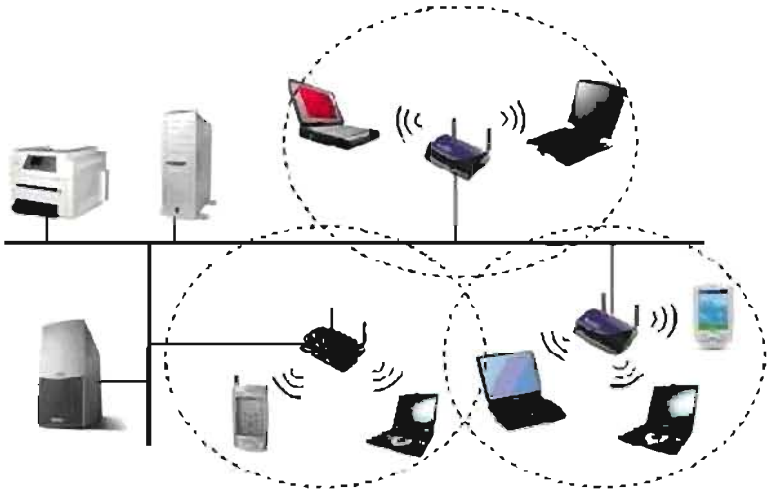

Fig. 2.2 Redes Inalámbricas
Fuente: [Telecom, 09]

Las redes inalámbricas no solo se han enfocado a lugares de área pequeña como son: a) la casa, b) oficinas, c) edificios, entre otros, también, están siendo implementadas para cubrir espacios geográficos tan grandes, con independencia de cables pero con el manejo de gran ancho de banda. Además de, ser una alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite.

2.1.1 Categorías de Redes Inalámbricas.

Al igual que las redes tradicionales cableadas, las redes inalámbricas se clasifican en cuatro categorías. a) WAN Wide Area Network, Red de Área Extensa, b) MAN Metropolitan Area Network, Red de Área Metropolitana c) LAN Local Area Network, Red de Área Local, d) PAN Personal Area Network, Red de Área Personal.

[9] Modo de compartir información entre dos puntos distintos y a un corto tiempo de conexión.

La figura 2.3, muestra el cuadro comparativo (Distancia/Velocidad), de los tipos de Redes Inalámbricas; se tiene como primera y segunda categoría a WAN y MAN, redes que cubren desde decenas hasta miles de kilómetros, en la tercera categoría LAN, redes que comprenden de varios metros hasta decenas de metros, y en la última categoría PAN, las redes que comprenden desde metros hasta 30 metros [Ponce, 07].

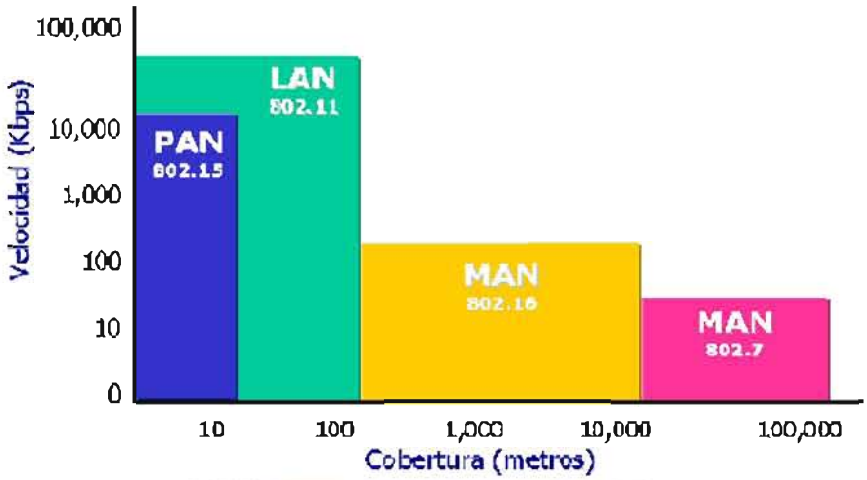

Fig. 2.3 Cuadro comparativo (Distancia /Velocidad) de las categorías de Redes Inalámbricas.
Fuente: [Ponce, 07]

2.1.1.1 Redes WWAN

Las redes WWAN, Wireless Wide Area Network o Wireless WAN, red inalámbrica de área extensa, son redes inalámbricas que cubren una amplia región geográfica, a menudo un país o un continente como se muestra en la figura 2.4. Este tipo de redes contiene maquinas que ejecutan programas de usuario llamadas hosts[10] o sistemas finales[11] [Wi-Max, 08].

[10] Nombre único que se le da a un dispositivo conectado a una red informática, este es un ordenador, un servidor de archivos, un dispositivo de almacenamiento por red, entre otros, que ayuda al administrador de la red a identificar las máquinas sin tener que memorizar una dirección IP para cada una de ellas.
[11] Los sistemas finales son conexiones a una subred de comunicaciones, la subred cumple la función de es transportar los mensajes de un host a otro.

En la mayoría de las redes inalámbricas de amplia cobertura se distinguen dos componentes. a) Las líneas de transmisión, que se conocen como circuitos, canales o trúncales, y b) Los elementos de intercambio (Conmutación), que son computadores especializados, utilizados para conectar dos o más líneas de transmisión [Wi-Max, 08].

Las características principales de las WWAN son las siguientes: a) Operan dentro de un área geográfica extensa, b) usan conexiones seriales de diversos tipos para acceder al ancho de banda, c) conectan dispositivos separados por áreas geográficas extensas; entre estos dispositivos se incluyen: routers[12], switches[13], módems[14], servidores de comunicaciones[15]; y d) la cobertura se logra a través de satélite o sistemas de radio, puesto que, las redes WWAN tienen una topología irregular [Ponce, 07].

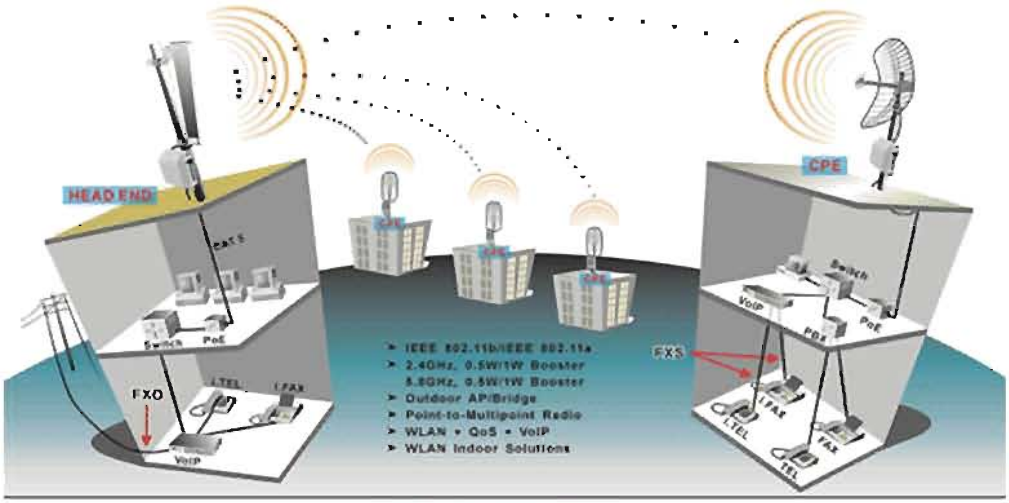

Fig. 2.4 Red inalámbrica de área extensa WWAN
Fuente: [Telecom, 09]

[12] Router, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores, este dispositivo permite asegurar el enrutamiento de paquetes entre redes.
[13] Switch, o conmutador, es un dispositivo analógico de lógica de interconexión de redes de computadoras, su función es interconectar dos o más segmentos de red, pasando datos de un segmento a otro.
[14] Un módem es un dispositivo que sirve para modular y desmodular (en amplitud, frecuencia, fase u otro sistema) una señal llamada portadora mediante otra señal de entrada llamada moduladora.
[15] Servidor de Comunicaciones es el encargado de monitorear los paneles, registrar los eventos en el sistema y enviar alarmas por correo electrónico, garantizando la seguridad e integridad del sistema.

2.1.1.2 Redes WMAN

Las redes WMAN, Wireless Metropolitan Area Network, o Wireless MAN, red inalámbrica de área metropolitana, son redes inalámbricas que cubren una distancia de 100 a 10.000 metros, ocupando una región geográfica desde manzanas y ciudades enteras, como se observa en la figura 2.5. Las redes WMAN están basadas en el gran ancho de banda al igual que las cableadas de cobre y fibra óptica que son instaladas para la transmisión de videos, voz, y otro tipo de datos [Wi.Max, 08].

Para las redes inalámbricas de área metropolitana existen tecnologías basadas en Wi-Max[16], que son implementadas para cubrir este espacio geográfico. Las velocidades, Wi-Max incluye mecanismos de calidad de servicio (QoS[17]) que ayudan a proveer grandes recursos de proceso y transferencia de información, para todos los usuarios y aplicaciones importantes que usan la red inalámbrica [Wi.Max, 08].

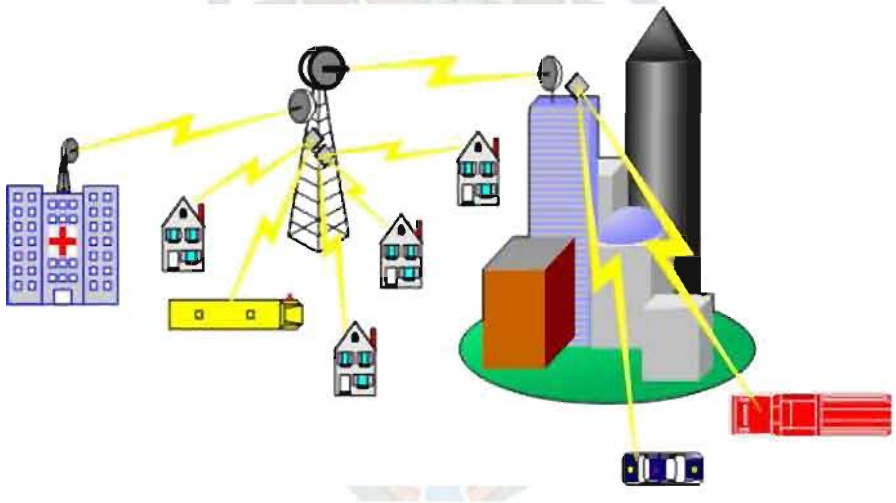

Fig. 2.5 Red Inalámbrica de Área Metropolitana WMAN
Fuente: [Telecom, 09].

[16] Del inglés, Worldwide Interoperability for Microwave Access, Interoperabilidad Mundial para acceso con Microondas – WiMax, es un protocolo parecido al Wi-Fi, pero con mas cobertura y ancho de banda.
[17] Del inglés, Quality of Service, Calidad de Servicio – QoS, son tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado, para dar un buen servicio.

2.1.1.3 Redes WLAN

Las redes WLAN Wireless Local Area Network, Red Inalámbrica de Área Local, son redes inalámbricas que cubren distancias de 10 a 100 metros, esta pequeña cobertura permite una menor potencia de transmisión, y admite el uso de bandas de frecuencia sin licencia. Este tipo de redes inalámbricas, utilizan ondas de radiofrecuencia en vez de cables para comunicarse y transmitir datos entre los clientes de la red inalámbrica y los dispositivos, es un sistema de comunicación de datos flexible que se implementa como una ampliación o una alternativa a la red local cableada [Wi-fi, 08].

La figura 2.6 muestra a las redes inalámbricas de área local, como una extensión de las redes LANs[18] convencionales, ya que permite el intercambio de información de datos en una forma transparente al usuario por medio de: a) un punto de acceso, b) un controlador de acceso, c) el gestor de servicio, y d) el proveedor de servicio.

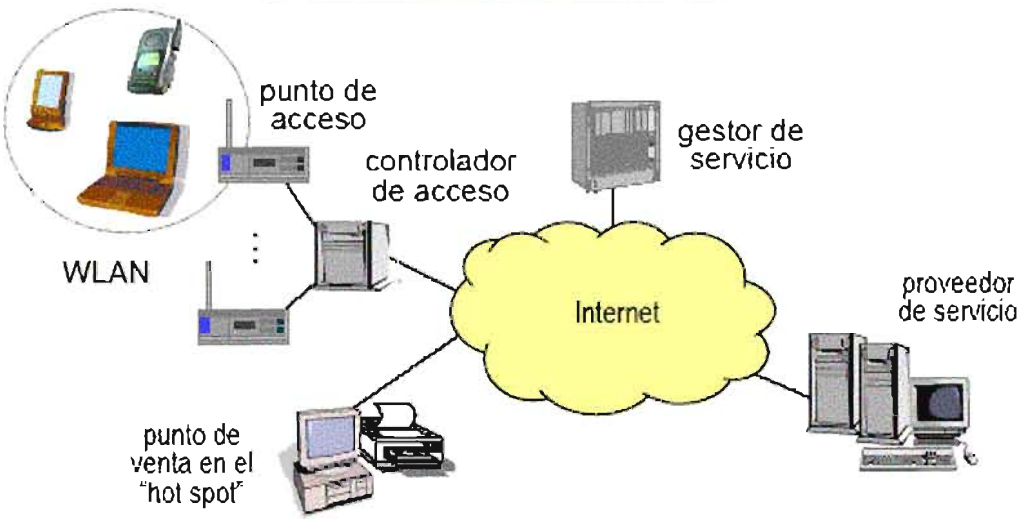

Fig. 2.6 Red Inalámbrica de Área local WLAN
Fuente: [Telecom, 09].

[18] Del ingles, Local Area Network, Red de Área Local - LAN

El objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total, donde coexistan los dos tipos de sistemas, (las inalámbricas y cableadas), que enlacen los diferentes equipos o terminales móviles asociados a la red inalámbrica. Este hecho proporciona al usuario una gran movilidad sin perder conectividad [Wi-fi, 08].

El atractivo fundamental de redes inalámbricas de área local, es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado. Aún así sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2 y los 10 Megabits por segundo, frente a los 10 y hasta los 100 Megabits por segundo ofrecidos por una red tradicional [Ponce, 07].

En la figura 2.7se muestra un ejemplo de red de área local inalámbrica sencilla, en la que los adaptadores[19] inalámbricos se instalan en los clientes, llamados también clientes inalámbricos. Estos, los clientes inalámbricos envían y reciben información mediante una conexión inalámbrica denominada canal. El cliente inalámbrico funciona en modo estructura o modo punto a punto (ordenador a ordenador).

Fig. 2.7 Red de área local inalámbrica
Fuente: [Ponce, 07]

[19] El adaptador permite que el cliente inalámbrico se comunique con la red WLAN sin cables.

La versatilidad y flexibilidad de las redes inalámbricas WLAN, permite la implementación de esta tecnología de forma variable. Esta gran variedad de configuraciones ayuda a que este tipo de redes se adapte a casi cualquier necesidad. La configuración de las redes WLAN se divide en dos grupos: a) las redes peer to peer (punto a punto) y b) las que utilizan Access Point (Puntos de Acceso) [Ponce, 07].

a) Peer to peer (punto a punto), también conocidas como redes ad-hoc, este tipo de red utiliza una configuración sencilla, ya que en ella los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas. En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles estén dentro de este rango para que la comunicación sea posible. En la figura 2.8 se muestra la configuración de este tipo de red.

Figura 2.8 Conexión peer to peer
Fuente: [Wi-Fi, 09]

b) Access Point (Punto de Acceso), es un tipo de configuración que utiliza el concepto de celda, ya utilizado en otras comunicaciones inalámbricas, como la telefonía móvil. Una celda podría entenderse como el área en el que una señal radioeléctrica es efectiva, y funcionan como repetidores, y por tanto son capaces de doblar el alcance de una red inalámbrica.

La figura 2.9 muestra un único punto de acceso que soporta un mínimo grupo de usuarios y que funciona en un rango de al menos treinta metros y hasta varios cientos de metros.

Figura 2.9 – Utilización de un Punto de acceso.
Fuente: [Wi-Fi, 09]

Los estándares para la red inalámbrica de área local, se basan en el estándar IEEE 802.11b[20] y el estándar IEEE 802.11g[21], que utiliza la banda de radio correspondiente a los 2,4 GHz, la misma frecuencia utilizada actualmente por teléfonos inalámbricos y hornos microondas. Existen también otros estándares para redes de área local inalámbricas como las tecnologías inalámbricas basadas en: a) HiperLAN[22], estándar del grupo ETSI[23], o b) tecnologías basadas en Wi-Fi[24] [Ponce, 07].

[20] 802.11b es una versión del estándar original 802.11, esta revisión del estándar original fue ratificada en 1999, con una velocidad máxima de transmisión de 11 Mbps y utilizando el mismo método de acceso CSMA/CA definido en el estándar original.
[21] Estándar IEEE, compatible con el estándar 802.11b, 802.11a, utiliza la banda de 2.4 Ghz, y opera a una velocidad real de transferencia de 22.0 Mbps, pero con una velocidad teórica máxima de 54 Mbps.
[22] Del Inglés High Performance Radio LAN, radio de alta calidad en red de área local.
[23] Del Inglés European Telecommunications Standards Institute, Instituto de niveles de telecomunicaciones europeo.
[24] Abreviatura del término Inglés Wireless Fidelity, es el término utilizado corrientemente para una red local sin cables WLAN de alta frecuencia.

2.1.1.4 Redes WPAN

Las redes WPAN Wireless Personal Area Network, red inalámbrica de área personal, son redes de cobertura personal, que comprenden desde metros hasta 30 metros de distancia, las tecnologías para este tipo de redes son basadas en: a) HomeRF; Estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparto central; b) Bluetooth Protocolo que sigue la especificación IEEE 802.15.1; c) ZigBee Basado en la especificación IEEE 802.15.4 y utilizado en aplicaciones como la domótica que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo; d) RFID sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio [Ponce, 07].

La figura 2.10 muestra una red inalámbrica de área personal WPAN, con dispositivos inalámbricos como son: a) computadora, b) impresora, c) celular, y d) cámara.

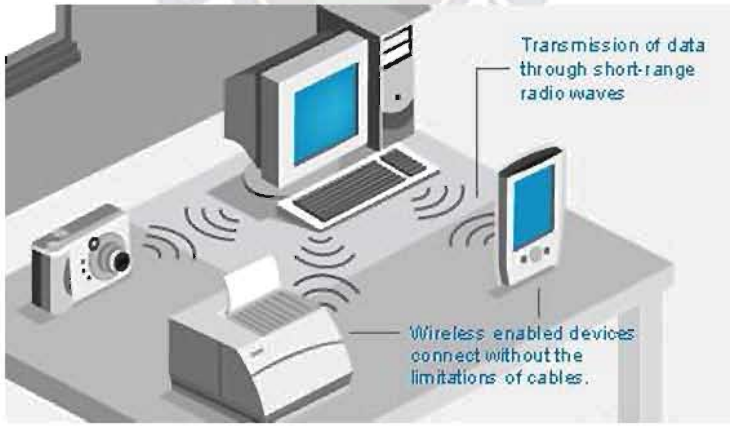

Fig. 2.10 Red Inalámbrica de Área Personal WPAN
Fuente: [Ponce, 06].

El presente trabajo de tesis abarca las redes inalámbricas de área local WLAN, por la flexibilidad y versatilidad que es tipo de redes ofrece en el ambiente inalámbrico.

2.1.2 Estándares y tecnologías Inalámbricas.

Los estándares son un conjunto de especificaciones tecnológicas establecidas por un organismo controlador, en este caso el Instituto de Ingenieros de electrónica y electricidad, conocida por sus siglas en ingles como IEEE (Institute of Electrical and Electronics Engineers), para que los productores y desarrolladores de tecnología tengan una normativa que les permita lograr que los dispositivos operaren entre si [Mantana, 06].

La figura 2.11, muestra los tipos de estándares 802 que IEEE utiliza para las redes inalámbricas, que son: a) las redes WWAN, con el estándar 802.20, b) las redes WMAN, con el estándar 802.16, c) las redes WLAN, con el estándar 802.11, y d) las redes WPAN, con el estándar 802.15.

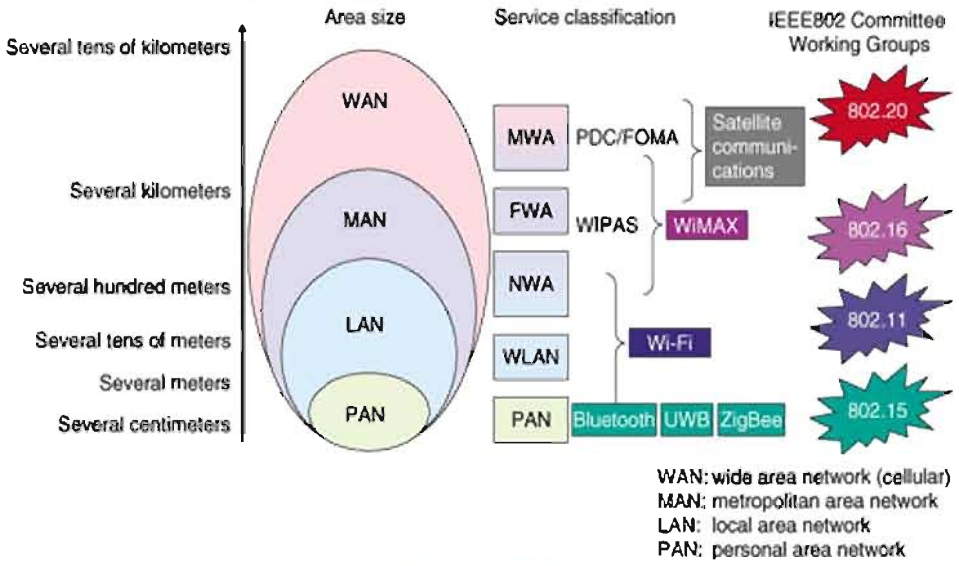

Fig. 2.11 Estándar IEEE 802 para redes Inalámbricas.
Fuente: [Ieee, 06]

El presente trabajo de tesis, toma como referencia a IEEE 802.11 en la parte del desarrollo de estándares de operación para redes inalámbricas de área local (WLAN).

2.1.2.1 Especificación 802.11

La especificación 802.11 es un miembro de la familia IEEE 802, que es una serie de especificaciones para las tecnologías de redes de área local (LAN). Esta especificación lleva a la red tradicional a un medio de comunicación inalámbrico en donde los dispositivos de este medio usan radio frecuencias en lugar de cables para establecer una conexión y comunicación entre ellas, algunos de estos estándares derivados de la 802.11 más importantes para redes WLAN son los siguientes [Mantana, 06]:

802.11a, Fue creado como uno estándar de las redes inalámbricas de área local, opera en una banda de 5Ghz con un flujo de datos de 54Mbps.

802.11b, Creado como un estándar (también conocido como (Wi-Fi), para las redes inalámbricas de área local, opera en una banda de 2.4Ghz con un flujo de datos de 11Mbps.

802.11g, Creado con una extensión de alta velocidad del estándar 802.11b, mantiene una compatibilidad con tecnologías 802.11b, opera en una banda de 2.4Ghz con un flujo de datos en un inicio de 20Mbps y ahora de 54Mbps.

2.1.2.2 Diseño y componentes del estándar 802.11.

Las redes inalámbricas 802.11 están formadas de cuatro componentes físicos principalmente: a) Estaciones, b) Puntos de Acceso, c) Medio Inalámbrico, d) Sistema de distribución, y e) Servidor, resumidos en la figura 2.12 [Sosinski, 04].

a) Estaciones, Las estaciones son componentes computacionales con interfaces de red inalámbrica. Típicamente las estaciones son: a) computadoras portátiles, b) computadoras de bolsillo, c) computadoras normales, las que se conectan de forma inalámbrica para evitar que tener que poner cableado, las redes inalámbricas están construidas para transferir datos entre estaciones.

b) Puntos de Acceso (Access Point), son equipos que tienen la principal función de hacer de puente entre la conexión por cable y la conexión inalámbrica.

c) Medio inalámbrico, para mover datos de estación a estación, el estándar utiliza un medio inalámbrico, en un principio eran numerosas las opciones que podían ser usadas para transmitir información pero las que se utilizaron en primero fue la señal de infrarrojo y el uso de radio frecuencias que con el tiempo se volvieron más populares.

d) Sistema de distribución, cuando muchos puntos de acceso están conectados para formar una gran área de cobertura, deben comunicarse entre ellos para llevar un seguimiento de todos los movimientos de las estaciones de trabajo.

e) Servidor, una computadora que realiza algunas tareas en beneficio de otras aplicaciones que se pueden efectuar en dispositivos llamados clientes. Algunos servicios habituales son: a) los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de un ordenador y b) los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final.

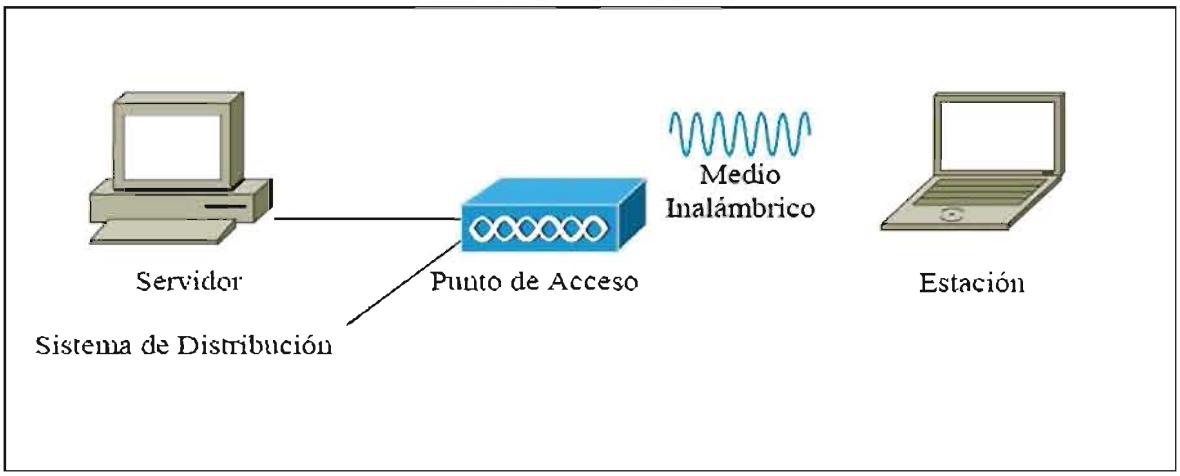

Fig. 2.12 Componentes de una red WLAN
Fuente [Mantana, 06]

2.1.3 Tipos de Redes Inalámbricas Comunitarias.

Entre los tipos de redes inalámbricas comunitarias tenemos [Randall, 04]:

a) Redes Inalámbricas Ad Hoc, también llamada red de punto a punto (peer to peer), se crea de forma temporal ante la necesidad de tener una conexión rápida con otra computadora ya sea para compartir información o para aprovechar algún servicio de la computadora como el Internet, para formar este tipo de red no se usan puntos de acceso sino que se usan las tarjetas inalámbricas de cada computadora para conectarse entre si. La conexión se realiza en red abierta sin ninguna autenticación, y las computadoras comparten el mismo ancho de banda. Las redes inalámbricas Ad Hoc, tienen como desventaja el que su ancho de banda se vea disminuido cuando comparten archivos muy grandes de información, adicionalmente no tienen una buena seguridad
b) Portales cautivos, un portal cautivo es cuando se da un servicio de red inalámbrico por medio de un punto de acceso inalámbrico, o ruteador que autentica y administrar a los recursos individualmente con el objetivo especifico de ofrecerles un servicio de red, principalmente Internet, y restringe el uso de otros servicios que el administrador del portal no quiera que los otros usuarios usen.
c) Redes extendidas, una red extendida es cuando se otorgan privilegios de dominio a todo usuario que quiera disponer de servicios, a los cuales no pueda acceder por la red normal. Formar una red extendida implica que se tienen que crear cuentas para cada uno de los usuarios y además se tienen que definir políticas para cada uno de ellos.
d) Redes inalámbricas de acoplamiento, es una red que comúnmente se usa para cubrir un área extensa, sin la necesidad de usar varios puntos de acceso y tener que administrar direcciones para cada uno

de ellos. En las redes inalámbricas de acoplamiento, se usa un solo uso punto de acceso central que conecta una serie de repetidores que extienden el área de cobertura, como si fuese un solo punto de acceso.

2.1.4 Dispositivos de Red Inalámbrica

El equipo de computación necesita una forma de conectarse a la red ethernet, si la red es inalámbrica o alámbrica, o ambas. Se hace la conexión a través de un adaptador de red, un equipo que provee interfaz de la computadora a la red. La mayoría de las computadoras se venden con el adaptador para redes inalámbricas ya preinstalado en la fábrica, y estos adaptadores se construyen cada vez más sobre la tarjeta madre. Es común que las computadoras portátiles vengan con adaptadores inalámbricos instalados. Las personas, para conectar la computadora portátil o la de escritorio, necesitan comprar e instalar adaptadores de red inalámbrica por separado. Los adaptadores vienen en tres configuraciones: a) Pc Cards, b) USB, c) PCI, y recientemente han aparecido en Compact Flash y usando tecnología Bluethoot [Randall, 06]. En la siguiente figura 2.13 se puede ver una tarjeta inalámbrica para computadoras portátiles.

Fig. 2.13 Tarjeta de red PC-Card
Fuente: [Telecom, 09]

Los puntos de acceso desempeñan muchas funciones importantes, además de, ser las interfaces entre la red normal y el medio inalámbrico, una de sus principales funciones es la de ser estación de camino del tráfico inalámbrico de la red. Muchas redes inalámbricas usan múltiples puntos de acceso, cada uno actuando precisamente como una estación de camino, extendiendo el alcance de la red local de acceso inalámbrico, ofreciendo puntos físicos adicionales para la conexión. En redes más pequeñas, un solo punto de acceso provee un transmisor y receptor central para todas las computadoras en la red, ruteando tráfico de y hacia varios adaptadores inalámbricos mientras proporciona acceso a los clientes a una o varias redes inalámbricas [Randall, 06].

Los puntos de acceso inalámbricos incluyen la tecnología y características de los routers, implícitamente los vendedores de equipo inalámbrico ofrecen equipos que combinan un punto de acceso con un router, resultando en una caja pequeña con tres o cuatro puertos para cables ethernet, otro para el cable modem, y los componentes inalámbricos requeridos por el punto de acceso, incluyendo la antena El router es el que, conecta dos o más redes pasando datos entre o a través de ellas, y los switchs son los que proveen información entre computadoras en una sola red aislando el tráfico de cada uno, de tal manera que la señal viaja del origen al destino sin que otra computadora tenga acceso a ellas [Randall, 06]. En la figura 2.14 se puede observar como es un router inalámbrico.

Fig. 2.14 Router Inalámbrico.
Fuente: [Randall, 06]

2.1.5 Ancho de banda

El ancho de banda es definido como la cantidad de información que puede pasar por un segmento de red en un momento determinado [Cisco, 04]. La figura 2.15 muestra al ancho de banda como una representación de los tubos de cañería, para su mejor visión.

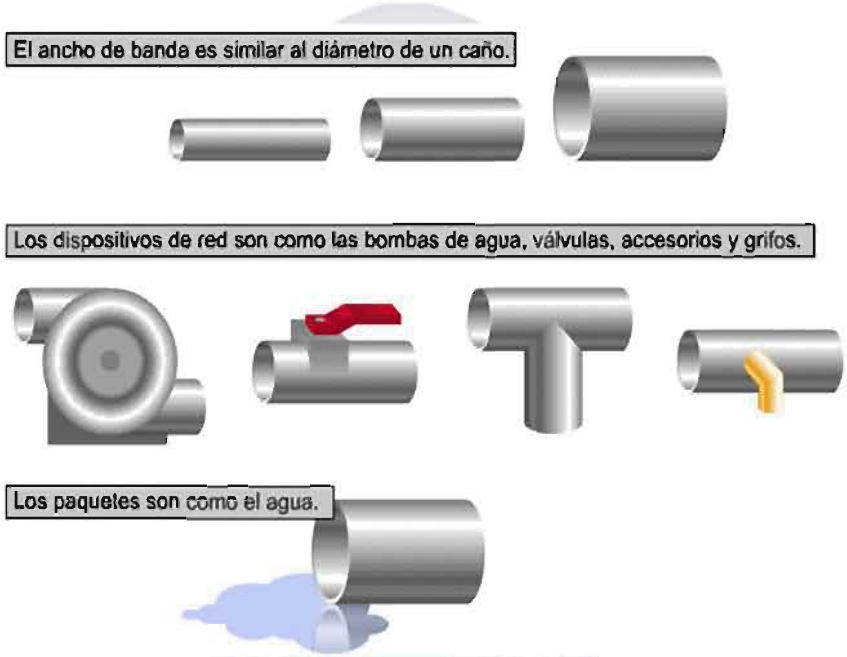

Fig. 2.15 Ancho de Banda
Fuente: [Randall, 06]

Existen ciertas características fundamentales del ancho de banda [Cisco, 04]:

- El ancho de banda es finito, por lo que se limita su uso de acuerdo a las necesidades y los servicios que se consideran como críticos. La principal limitación es el medio físico aunque las tecnologías han permitido grandes velocidades de transferencias, no se aprovecha al máximo el ancho de banda.

- El ancho de banda no es gratuito, generalmente se compra a un proveedor de servicios ISP[25], lo cual lleva a los administradores de la red a la toma de decisiones sobre los equipos, servicios y políticas a establecer en la red, y traducir estos en términos de ahorro económico.
- La demanda de ancho de banda nunca deja de aumentar, a pesar de los nuevos dispositivos y tecnologías, el uso y competencia por el ancho de banda sigue en aumento debido a las aplicaciones que hacen uso de estas mayores capacidades de la red.

En las redes inalámbricas, el ancho de banda está limitado por las características de los equipos que permiten la conectividad con la red, el cual, se encuentra más detallado en las especificaciones del estándar en el que se basa el equipo, uno de los estándares utilizados para redes inalámbricas es el estándar 802.11a, 802.11b y 802.11g [Riu, 08].

Por otra parte, el ancho de banda tiene una relación directa con la potencia de la señal. La señal de los dispositivos se va debilitando conforme se aleja del origen, ya sea obstáculos o por la atenuación de la señal debido a la pérdida de potencia con la distancia recorrida [Wi-Fi, 09].

Es importante recordar que el ancho de banda solo se alcanza en casos ideales, es decir, que no exista degradación de la señal y que la asignación del ancho de banda sea equitativa entre todos los usuarios, generando un equilibrio en la competencia por el recurso. El concepto de entre más ancho de banda en una red inalámbrica, mayor su desempeño, es una proposición no necesariamente cierta, la decisión de incrementar el ancho de banda en una red inalámbrica existente recae sobre el administrador de la red cuando se determina que las capacidades de transferencia de la red inalámbrica comprometen la disponibilidad de los servicios de la red, es decir, cuando el flujo de datos es muy grande, ocupa todo el

[25] ISP, Acrónimo de Internet Service Provider (Proveedor de servicios de Internet). Es una compañía, persona natural o jurídica que proporciona acceso a Internet a particulares y empresas.

ancho de banda disponible y compromete el envío del resto de la información en la red inalámbrica proveniente de todos los usuarios [Morales, 06].

La tasa de transferencia es la medición real del ancho de banda en un momento dado y en un segmento determinado de la red [Cisco04]. En el mundo real se trabaja con la tasa de transferencia y esta resulta ser menor al ancho de banda; esto se genera por diversas situaciones como: a) la latencia de los dispositivos de red, b) la topología de la red, c) el número de usuarios en un momento determinado, d) el tipo de datos a transferir, e) las características y capacidades de los equipos terminales y servidores. La tasa de transferencia se presentara en tres valores, máximo, promedio y mínimo [Morales, 06].

La definición de buenas tasas de transferencia está determinada principalmente por las características propias de una red como: 1) el número de usuarios, 2) el ancho de banda disponible y 3) los servicios ofrecidos por la red. No existe una técnica ampliamente aceptada para determinar estas tasas, por lo que proponen formalizar prácticas recomendables, que pueden ser implementadas en la mayoría de las redes para tratar de obtener de una manera eficiente estas tasas de transferencia ideales [Riu, 08].

Las empresas proveedoras de este servicio en Bolivia son: a) AXS, b) Viva, c) Tigo entre otras, que debido a la alta demanda y el rápido crecimiento de las principales ciudades de nuestro país, han permitido llegar con sus redes de banda ancha a todos aquellos lugares donde es requerido este servicio, brindando servicios integrales de telecomunicaciones para permitir la instalación de una red inalámbrica de banda ancha capaz de satisfacer todas las necesidades de sus clientes, con planes distintos en los cuales se detallan los pagos, cantidad de ancho de banda y cantidad de computadoras optimas para el servicio [Nic, 09]. (Ver Tabla 2.1).

Tabla 2.1. Plan de servicio del ISP, y cantidades de computadoras optimas para cada uno de ellos.

Plan	Equivalente a:	Cantidad de Computadoras Optimas
128 Kbps	→	De 1 a 5
192 Kbps	→	De 5 a 8
256 Kbps	→	De 8 a 10
320 Kbps	→	De 10 a 14
512 Kbps	→	De 14 a 25
1024 Kbps	→	De 25 a 43
2028 Kbps	→	De 43 a 86

Fuente: [Axs, 09].

2.2Identificación y Autenticación

La identificación y autenticación son las claves de los sistemas de control de acceso en la red inalámbrica. La identificación es el acto de ejercer una identidad de usuario en el sistema, normalmente, es un identificador en el registro del sistema. La autenticación es la comprobación que válida la identidad del usuario, y se lleva a cabo a través de una contraseña de usuario en el momento del registro [Cissp, 03]. La identidad del usuario son todos aquellos datos que nos permitan identificar a la persona en el mundo real, así como sus intenciones en el momento de utilizar la red; cuando se verifica la identidad del usuario, es ahí, donde se le permitirá o deniega el acceso a la red [Mantana, 06].

Antes de permitir a las entidades a acceder a la red inalámbrica y sus recursos asociados, el procedimiento general es autenticar la entidad, esta entidad puede ser: a) un dispositivo ó b) un usuario; después de identificar a la entidad, se aprueba la autorización basándose en el tipo de entidad que requiere la autorización. Este proceso se inicia cuando el cliente envía una trama de petición de autenticación al AP y éste acepta o rechaza la trama, el cliente recibe una respuesta por medio de una trama de respuesta de autenticación [Cissp, 03].

La asociación que se realiza después de la autenticación es el estado que permite que un cliente use los servicios del AP para transferir datos, entre los tipos de autenticación y asociación tenemos: a) No autenticado y no asociado; el nodo está desconectado de la red y no está asociado a un punto de acceso, b) Autenticado y no asociado; el nodo ha sido autenticado en la red pero todavía no ha sido asociado al punto de acceso, c) Autenticado y asociado; el nodo está conectado a la red y puede transmitir y recibir datos a través del punto de acceso [Cwls, 09].

El uso de la autorización en operaciones, es idéntico a la de autenticación. Sin embargo, el uso más exacto describe la autenticación como el proceso de verificar la identidad de una persona, a diferencia de la autorización que es el proceso de verificación, que una persona conocida tiene la autoridad para realizar una cierta operación, por tanto la autenticación, debe preceder de la autorización [Seri, 07].

2.2.1 El modelo tripartito.

La autenticación está basada en un modelo tripartito: 1) el cliente que requiere acceso; 2) el autenticador, que permite el acceso; y 3) el servidor de autenticación que da los permisos [Cwls, 04].

La figura 2.16 describe el modelo tripartito con el cliente que tiene una identidad y algunas credenciales para probar que es el que dice ser. El cliente está conectado a la red inalámbrica por medio del puerto del autenticador que es controlado por el punto de acceso. El autenticador por sí mismo no sabe si se le puede prohibir el acceso a la entidad, esta función la realiza el servidor de autenticación. Un autenticador puede ser: a) un servidor de acceso a la red, y b) un servicio de llamada de direcciones de usuarios remotos. Es importante comprender que el rol de autenticador y el servidor de autenticación pueden ser desempeñados por un solo dispositivo [Cwls, 04].

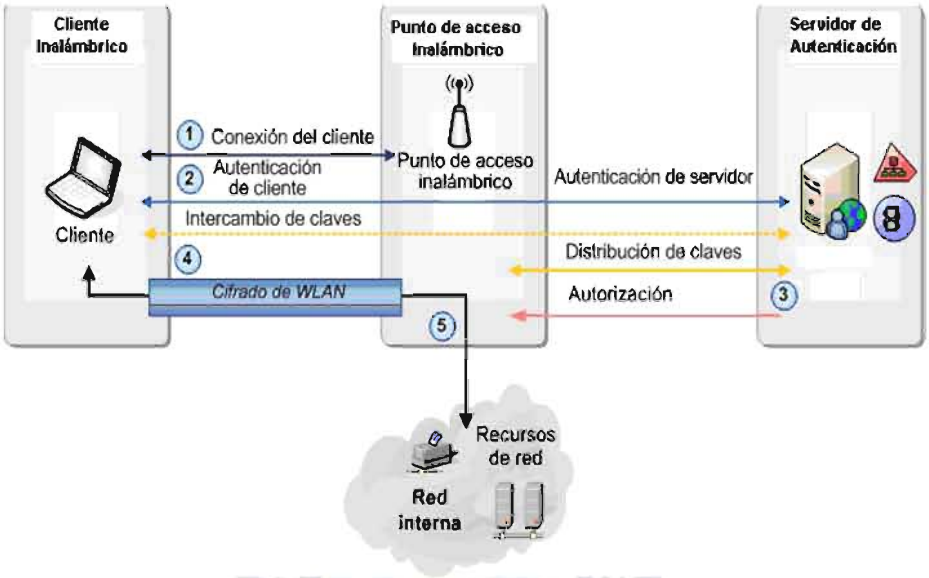

Fig.2.16 Modelo Tripartito de autenticación
Fuente: [Telecom, 09]

2.2.2 Métodos de Autenticación.

Los métodos de autenticación son procedimientos que cumplen la función de verificación, estos se dividen en tres categorías: a) Sistemas basados en algo conocido, como un identificador personal, password, o passphrase b) Sistemas basados en algo poseído, como una tarjeta de identidad, una tarjeta inteligente (smartcard), dispositivo usb, c) Sistemas basados en una característica física del usuario o un acto involuntario del mismo, como, verificación de voz, de escritura, de huella digital, de patrones oculares [Cissp, 03].

Cualquier sistema de identificación mencionado anteriormente posee determinadas características para ser viable, estas son: 1) Ser fiable con una probabilidad muy elevada (se habla de tasas de fallo en los sistemas menos seguros), 2) Económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto), 3) Soportar con éxito cierto tipo de ataques, 4) Ser aceptable para los usuarios, que serán al fin y al cabo quienes lo utilicen [Cissp, 03].

2.2.2.1 Protocolos de Autenticación

Los protocolos de autenticación para redes inalámbricas, son los protocolos de seguridad PAP, Password Authentication Protocol (Protocolo de autenticación de contraseña) Y CHAP, Challenge Handshake Authentication Protocol (Protocolo de autenticación por desafió de apretón de manos), protocolos de seguridad de nodo remoto que utilizan métodos de autenticación usados por servidores accesibles por el protocolo punto a punto (PPP) [Cissp, 03].

a) PAP, Password Authentication Protocol (Protocolo de autenticación de contraseña), es un protocolo de seguridad remoto que proporciona la identificación y autenticación del nodo que intenta comenzar la sesión remota. PAP usa la contraseña estática para su autenticación que se considera un proceso débil, además, no encripta al ID o contraseña del usuario durante la comunicación [Morales, 06].

b) CHAP, Challenge Handshake Authentication Protocol (Protocolo de autenticación por desafió de apretón de manos), es un método de autenticación remota o inalámbrica más fuerte, que verifica la identidad del nodo que intenta comenzar la sesión remota con un dialogo de desafío CHAP es la evolución de PAP, que usa un proceso de la autenticación más fuerte, es uno de los últimos protocolos de autenticación, CHAP verifica periódicamente la identidad del cliente remoto usando un intercambio de información de tres etapas también llamado modelo tripartito. Esto ocurre cuando se establece el enlace inicial y puede pasar de nuevo en cualquier momento de la comunicación, la verificación se basa en un secreto compartido (como una contraseña), CHAP se usa para habilitar comunicaciones de red-a-red y normalmente es utilizado por los servidores de acceso remoto [Cissp, 03].

2.2.3 Mecanismos de Autenticación.

En las redes inalámbricas se mantiene de uno u otro modo una relación de identidades personales (usuarios) asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación de usuarios permite a estos sistemas asumir con una seguridad razonable de quien se está conectando es quien dice ser para que las acciones que se ejecuten en el sistema puedan ser referidas a esa identidad y aplicar los mecanismos de autorización y/o auditoría [Mantana, 06].

El primer elemento necesario para la autenticación es la existencia de identidades bi-unívocamente identificadas con un identificador único. Los identificadores de usuarios tienen distintas formas de identificación, siendo la más común una sucesión de caracteres conocida comúnmente como login [Mantana, 06].

El mecanismo utilizado para la autenticación en redes WLAN, es la del protocolo AAA (autenticación, autorización, y auditoria), modelo que es utilizado en ambientes inalámbricos, y consiste en autenticar, autorizar y el manejo de cuentas, cada uno de ellos, es considerado uno de los tres pasos fundamentales para la seguridad de red WLAN, y que se detallan en forma ordenada [Seri, 07]:

a) Autenticación, en la seguridad del ordenador, la autenticación es el proceso de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado es: a) una persona que usa un ordenador, b) un ordenador por sí mismo ó c) un programa. En la web la autenticación, es el modo de asegurar que los usuarios son quién ellos dicen que son, es decir, que el usuario que intenta realizar funciones en el sistema es de hecho el usuario que tiene la autenticación para hacer así autorización.

b) Autorización, es el proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.

c) Auditoria, es el proceso de manejo de cuentas, mediante la cual la red o sistemas asociados registran todos y cada uno de los accesos a los recursos que realiza el usuario autorizado o no.

Este mecanismo para el proceso general de autenticación en redes WLAN, hace referencia a los sistemas basados en algo conocido, descrita en la figura 2.17, y que consta de los siguientes pasos: 1) El usuario solicita acceso al sistema, 2) El sistema solicita al usuario que se autentique, 3) El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación, el sistema valida según sus reglas si las credenciales aportadas son suficientes para dar acceso al usuario o no.

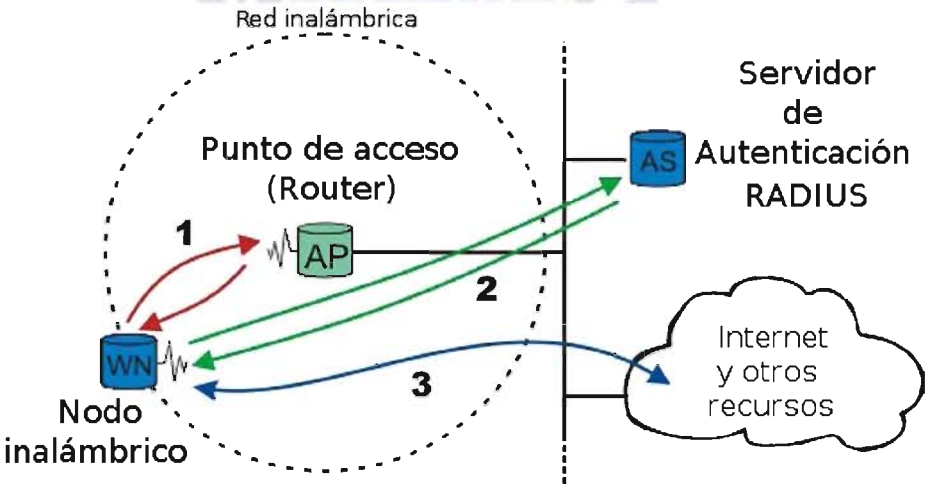

Fig. 2.17 Proceso general de autenticación
Fuente: [Peña, 08]

2.3 Gestión de Redes de área local

En el área de la gestión de redes inalámbricas de área local, se considera a la gestión de red como el trabajo de administración, supervisión y control de una red, además que, el administrador de una red inalámbrica es el encargado de la configuración, fallas, y seguridad de la red [Cwna, 07].

El comportamiento de la red inalámbrica incluye situaciones como monitoreo de la taza de transferencia y ejecutar acciones que garanticen la disponibilidad de los servicios, las políticas establecidas por el gestor de la red, ayudan a que el desempeño de la red se aproxime a lo óptimo en cualquier momento [Morales, 06].

En la gestión de redes WLAN, para que el ancho de banda sea aprovechado eficientemente para todos los usuarios, se han creado soluciones basadas en hardware y software para crear una distribución de este recurso. Si la solución se basa en hardware, el dispositivo físico tiene configurado en su memoria interna un schedules[26] para hacer la administración del ancho de banda basados en la regulación de la velocidad de transferencia entre un usuario en particular y un punto de acceso a la red o un equipo responsable de la administración. Si la solución es software, este se instala en un servidor quien será quien procese todas las peticiones de conexión y transferencia de datos [Morales, 06].

Un gestor de red, opta por alguna de estas dos opciones cuando desee aplicar restricciones sobre el uso del ancho de banda y acceso a la red. La decisión que tome el gestor se basa tanto en cuestiones: a) técnicas, b) económicas y c) de planeación, el futuro y crecimiento de una red también son factores que intervienen en la teoría de decisiones [Morales, 06].

2.3.1 Gestión de ancho de banda

La gestión de ancho de banda, es una técnica eficiente cuando no suceden muchos cambios en la topología de la red y sobre todo para conservar un óptimo desempeño de todas las funciones de la red, las características de la gestión de ancho de banda son: a) realiza la asignación de ancho de banda una vez que se conoce la identidad de los usuarios, b) le asigna una dirección IP, c) cumple la función de regulación, cuando los usuarios realizan muchos movimientos de

[26] Calendarios de trabajo basados en probabilidad, turnos, prioridad y otras técnicas para hacer más justa la distribución.

entrada, salida, alta, baja en la red, y d) la creación de niveles de privilegios donde se agrupa a los usuarios, entre otras [Morales, 06].

2.3.1.1 Nivel de Privilegios

El ancho de banda con privilegios, son normas que permiten establecer los privilegios y prioridades de las solicitudes del usuario, respecto al ancho de banda y que se configuran especificando una serie de elementos como: a) protocolos de definiciones, b) direcciones IP, c) tipo de usuarios, d) programas, e) tipos de contenido, y f) capacidad de ancho de banda, entre otros [Isa, 09].

El privilegio del ancho de banda también es, un elemento que se utiliza para establecer los valores para el ancho de banda, que una vez definidos, se aplica a: a) las prioridades específicas de ancho de banda, b) a las conexiones a Internet de banda ancha a través de normas, c) a la creación de reglas de ancho de banda, y d) al ancho de banda efectivo de la conexión a Internet que debe ser especificado [Isa, 09].

El uso de niveles de privilegios, en la gestión de ancho de banda, se da con la necesidad de que se reconozca la prioridad que tienen los usuarios con mayor nivel de privilegios en el momento que se conectan a la red inalámbrica [Ponce, 07].

Los niveles de privilegios son considerados para que el administrador empiece a asignar el ancho de banda en base a dos criterios: a) utilizar un ancho de banda fijo para usuarios con privilegios ya determinados y b) una distribución en base a los usuarios que estén registrados en la red inalámbrica; ya que el ancho de banda es un recurso limitado [Ponce, 07].

La tabla 2.2 muestra un ejemplo de la interpretación de los niveles de privilegios para usuarios en una red con un ancho de banda disponible de 2048 Kbps pero que no hace referencia al máximo número de usuarios en la red [Morales, 06].

Tabla 2.2. Ejemplo de anchos de banda interpretado por nivel de privilegios.

Nivel de Privilegio	Ancho de Banda Reservado
Menor uso de la red	30 Kbps
Uso promedio de la red	100 Kbps
Uso fuerte de la red	300 Kbps

Fuente: [Morales, 06].

2.3.1.2 Políticas de Gestión de Redes de área local.

Política es uno de esos términos que puede significar varias cosas. Por ejemplo, hay políticas de gestión de redes de área local con normas, procedimientos, y directrices que son la base de una buena implementación de sistemas de administración y que garantizan la disponibilidad de los servicios ofrecidos por la red [Isa, 09].

Una buena política es más que un ejercicio creado en papel en blanco, es un elemento esencial y fundamental de una buena práctica de gestión de redes de área local [CWNA, 08].

2.4 Seguridad de Redes inalámbricas de área local.

Las redes inalámbricas, usan ondas electromagnéticas como medio de conmutación, las mismas ondas que utilizan: a) los radios, b) los teléfonos, c) los radios de intercomunicación, entre otros. Estas ondas son fácilmente captadas por dispositivos ajenos al entorno, que acceden a los servicios y a la información de la red, lo cual pone en riesgo la privacidad y la seguridad de la entidad, es así, que las redes inalámbricas tiene un canal de comunicación peculiarmente inseguro, para tratar de atenuar este defecto, con el fin de resguardar la información y protegerlas de ataques al entorno inalámbrico, se pone en práctica mecanismos de

seguridad que garanticen la seguridad computacional, con el fin de poder resguardar la información y protegerlas de ataques al entorno inalámbrico [Seri, 08].

2.4.1 Mecanismos de seguridad.

Los mecanismos básicos de seguridad para la red WLAN son: a) confidencialidad, b) integridad, c) viabilidad, d) autenticación, e) autorización, f) control de acceso, g) encriptación y h) administración de llaves [Cwls, 04].

a) Confidencialidad, es la capacidad de mandar (y recibir) datos sin divulgar ninguna parte a las entidades no autorizadas durante la transmisión de los datos. Los mecanismos para lograrlo son la encriptación-simétrica y la asimétrica [Cwls, 04].

b) Integridad, es la capacidad de mandar y recibir datos de tal manera que las entidades no autorizadas no puedan cambiar ninguna parte de los datos intercambiados sin que el que lo envió y el que lo recibió no hayan detectado los cambios. Como mecanismos usa firmas digitales usando una función hash[27] de un solo camino [Cwls, 04].

c) Viabilidad, está definida como la capacidad de recibir y enviar datos. Es decir, si un sistema está sobre ataque, este no será capaz de recibir o enviar datos. Los mecanismos de viabilidad son, en su mayoría, mecanismos de defensa que detectan varias formas de ataque y protegen contra ellos [Cwls, 04].

d) Autenticación, establece la identidad del que envía o recibe la información. Cualquier revisión de la integridad de la información privada no tiene sentido si la identidad del que envía o recibe no está establecida correctamente. Los mecanismos usados son protocolos de nivel múltiple como: 802.11x, RADIUS, PAP/CHAP, entre otros [Cwls, 04].

[27] hash se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo

e) Autorización, establece que es lo que se permite hacer después de que uno se ha identificado. (También es llamada control de acceso, capacidades y permisos). La autorización y la autenticación van juntas en la mayoría de los requisitos de acceso a red. Los mecanismos son los niveles múltiples y protocolos [Cwls, 04].

f) Control de acceso, es la capacidad de controlar el acceso de entidades y recursos basándose en varias propiedades: a) atributos, b) autenticación, c) políticas, entre otros. Los mecanismos son la autenticación o el conocimiento de la llave WEP en el punto de acceso (AP) [Cwls, 04].

g) Encriptación, es la capacidad de transformar datos (texto plano) en bytes sin sentido (texto cifrado) basándose en algún algoritmo. Desencriptar es el acto de convertir los datos sin sentido en datos significativos de nuevo. El punto principal relacionado con la autenticación y la autorización en el medio inalámbrico es la robustez de los métodos usados para verificar la identidad de la entidad [Cwls, 04].

h) Administración de llaves.- Una llave es un código digital que puede ser usado para encriptar, desencriptar y firmar información. Algunas llaves se guardan en privado, y otras son compartidas y deben ser distribuidas de una manera segura. La administración de llaves se refiere al proceso de distribuir llaves para los procesos previamente mencionados. El desafío en el área inalámbrica es la distribución de las llaves de una forma segura, escalable y en forma automática [Cwls, 04].

2.4.2 WEP

Wired Equivalent Privacy, privacidad equivalente a cable, WEP. Es una de las soluciones a la seguridad inalámbrica, parte del estándar IEEE 802.11 original, de 1999, el propósito de WEP es brindar, a las redes inalámbricas, un nivel de seguridad comparable al de las redes alambradas tradicionales. La necesidad de

un protocolo como WEP fue obvio, las redes inalámbricas usan ondas de radio y son más susceptibles de ser interceptadas [Mantana, 06].

Sin embargo, la vida de WEP fue muy corta; un diseño malo y poco transparente condujo ataques muy efectivos a su implantación, algunos meses después de que el WEP fuera publicado, el protocolo fue considerado obsoleto. Aunque la llave tenía una longitud limitada debido a restricciones de exportación, se probó que el protocolo era débil independientemente de ese hecho [Mantana, 06].

WEP aunque no cumple con las expectativas se sigue utilizando, en muchos casos, éste es el único protocolo de seguridad presente en un dispositivo en particular. El diseño de WEP es muy fácil de implementar, debido a su sencillez no consume mucho poder computacional, por lo que es una buena opción para dispositivos chicos como computadoras de bolsillo [Bing, 07].

2.4.3 Protocolo de integridad de llave temporal.

Temporal Key Integrity Protocol (TKIP), protocolo de integridad de llave temporal, es un nuevo protocolo de encriptación ampliamente implementado, fue concebido como una actualización de WEP, retiene la arquitectura básica y operaciones de WEP añadiendo nuevas características. Entre sus nuevas características que lo hacen mucho más seguro encontramos: a) Jerarquía de Llaves y su administración automática de llaves, b) Generación de llaves por cada paquete, c) Contador de secuencia, d) Chequeo de integridad de los mensajes, e) Contramedidas por fallo de chequeo de la integridad del mensaje [Mantana, 06].

TKIP también es usado en conjunto con protocolos de administración de llaves basados en el estándar 802.1x, en donde se habilita la llave maestra de TKIP para ser derivadas de una transacción de autenticación [Bing, 07].

2.4.4 Encriptación AES.

AES (Advanced Encryption Standard), Algoritmo Estándar de Cifrado Avanzado, es un bloque cifrado de operaciones lógicas y matemáticas, el método combina una llave y un bloque de datos de 128-bit (sin encriptar) para producir un bloque de datos diferentes (encriptados). Para todo propósito práctico, es imposible de realizar esta transformación si no se tiene la llave. AES es reversible (esto es, que puedes convertir los datos a su forma original usando una decriptación), lo cual es útil, pero no esencial para todos los protocolos de seguridad. Los bloques encriptados y sin encriptar son del mismo tamaño. La conversión de un solo bloque de 128 bits de datos es lo único que hace AES, pero de una forma eficiente y extremadamente segura [7]. AES está basado en el algoritmo de Rijindael, inventado por Joan Daemen y Vicent Rijmen. Este algoritmo está muy bien documentado, incluyendo los detalles del algoritmo y la puesta en práctica [Edney, 03].

2.4.5 WPA

WPA Wireless Application Protocol, Acceso Protegido a Wi-Fi, este es un estándar de comercialización puesto por la alianza Wi-Fi en 2003, que fue implementado para acelerar el desarrollo de TKIP, llegando al mercado con una versión previa de TKIP y después con la versión final y que queda certificado como parte del estándar IEEE 802.11.

WPA es una nueva tecnología de seguridad de redes inalámbricas desarrollada por Wi-Fi Allince, Acceso Protegido Wi-Fi refuerza las limitaciones de cifrado existentes de WEP e introduce un método para generar y distribuir claves de cifrado automáticamente. La solución también introduce una comprobación de integridad sobre los datos para que un atacante no pueda modificar paquetes de información que se están comunicando. Para mejorar la autenticación de usuarios a nivel empresarial.

Algunas características de WPA son: a) autentica a cada usuario de la red, b) impide que se unan usuarios de redes maliciosas, c) presenta una respuesta práctica para tratar las limitaciones de WEP, basándose en las tecnologías disponibles y ofreciendo compatibilidad con versiones posteriores como 802.11 y compatibilidad con versiones anteriores con las soluciones 802.11 existentes, d) está diseñado para trabajar con y sin un servidor de manejo de llaves; si no se usa un servidor de llaves, todas las estaciones de la red usan una llave previamente compartida. [Wilac, 07].

En las últimas implementaciones de WPA también se maneja el uso de la encriptación AES como una opción diferente a TKIP.

2.4.6 EAP

EAP es un protocolo de autenticación que opera con el protocolo desafió-respuesta (CHAP); que es extendido para funcionar en cualquier mecanismo de transporte y usar cualquier sistema de encriptación para manejar la verificación. Este protocolo puede ser usado con el servicio de autenticación RADIUS (servicio de autenticación de llamado a direcciones de usuarios remotos), y con el transporte en la capa de seguridad (TLS) mediante EAP-TLS protegido PEAP [Mantana, 06].

Por definición, los medios de red inalámbrica LAN deberían de verse sin ninguna protección, por desgracia esto no es recomendado. Cualquier envió de datos enviados por la red inalámbrica debe de ser protegido si quiere mantenerse seguro. La mayoría de los métodos EAP diseñados para las redes inalámbricas usan seguridad en la capa de transporte para proveer protección criptográfica en sus credenciales, entre los métodos criptográficos, se cuenta con EAP- TLS, este método de Seguridad de la capa de transporte (TLS) provee autenticación mutua promedio de intercambio de certificados, el usuario es requerido para enviar un certificado digital para que el servidor de autenticación lo valide, pero este también debe proporcionar un certificado. Al validarlo en una lista de certificados

autorizados, el cliente puede estar seguro de que se está conectando a una red que está certificada [Mantana, 06].

Existen dos métodos EAP propuestos para habilitar el uso de los supuestos "métodos de autenticación legados" que son: a) TLS Entubado (TTLS) y b) EAP protegido (PEAP), ambos TTLS y PEAP trabajan en una forma similar. En el primer paso del protocolo, se debe establecer un túnel TLS usando rutinas similares a EAP-TLS. Certificados digitales en el servidor de autenticación son usados para validar que la red es confiable antes de proseguir, en el segundo paso, el túnel TLS es usado para encriptar un protocolo de autenticación ampliamente usado como CHAP, que autentifica el usuario en la red, el primer paso comúnmente se refiere como autenticación "externa", puesto que es un túnel el que protege la segunda autenticación o "interna" [Bod, 06].

PEAP, Protected Extensible Authentication Protocol (PEAP) es un método para transmitir de manera segura información de autenticación, incluyendo contraseñas, sobre redes cableadas e inalámbricas. Hay que tener en cuenta que PEAP no es un protocolo de encriptación, sino que como otros tipos EAP solo autentica un cliente a una red [Peña, 08].

2.4.7 PROTOCOLO RADIUS.

RADIUS permite la autentificación de usuarios cuando estos intentan acceder al servidor. Utilizan el protocolo AAA (autentificación, autorización y manejo de cuentas) lo cual permite un manejo de todos los clientes que hacen uso del servidor. Cuando el usuario intenta acceder a la red misma, necesita identificarse por medio de un nombre de usuario y una contraseña. Esta información es recibida por el servidor RADIUS el cual valida una petición de autentificación contra la información almacenada en su base de datos. Si la petición fue aceptada, el servidor se encargará de asignar una dirección IP y los demás parámetros necesarios para la conexión y manejo de la cuenta. Los mecanismos de autentificación pueden ser diversos como PAP, CHAP o EAP, según lo soporte el

servidor. RADIUS fue creado originalmente por Livingston Enterprises y en 1997, se convirtió en un estándar. RADIUS es un protocolo usado ampliamente en ambientes de red. Se aplica usualmente con dispositivos de red incrustados como ruteadores, servidores, y switches [Hill,01] . Algunas razones de su uso son:

a) Los sistemas incrustados generalmente no pueden manejar información de autentificación de los usuarios cuando el número de estos es muy grande. Dicho proceso requiere mayor espacio de almacenamiento que el que los sistemas incrustados poseen [Mantana, 06].
b) RADIUS facilita una administración centralizada. Esto representa una ventaja cuando los usuarios son agregados y retirados durante el día, y la información de autentificación cambia constantemente [Mantana, 06].
c) Se provee un alto nivel de protección contra ataques activos de escucha de la red o sniffing [Mantana, 06].

CAPÍTULO 3 MARCO APLICATIVO

3.1 Descripción del Modelo.

La representación del modelo, se presenta con el desarrollo de un diseño general del modelo de gestión de ancho de banda para una red inalámbrica de área local, con características esenciales relacionadas al modelo para así encontrar la solución al problema planteado en el presenta trabajo de tesis, este se compone por 3 elementos (figura 3.1) los cuales forman el núcleo central del mismo.

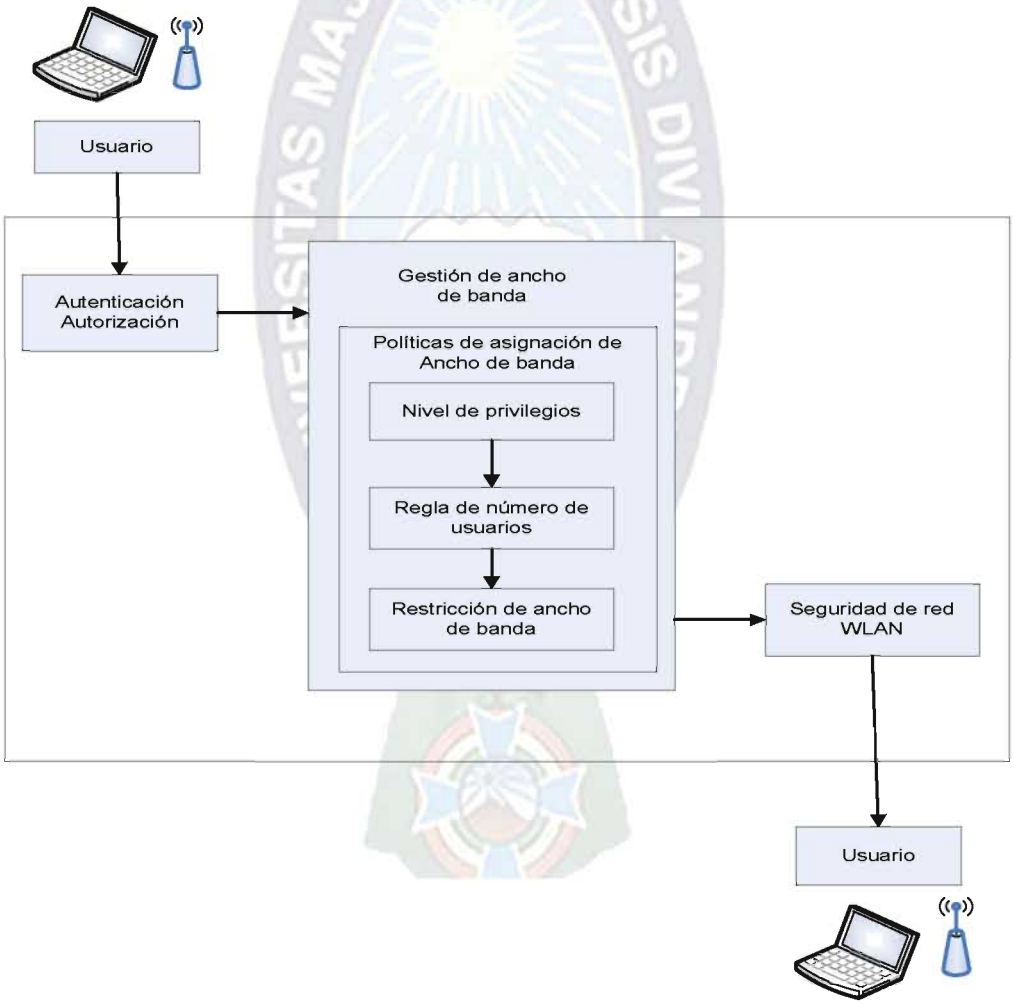

Figura 3.1. Modelo de gestión de ancho de banda para una red WLAN
Fuente: Elaboración Propia.

Para su mejor comprensión la figura 3.2, muestra a dicho modelo como una representación de diagrama de caso de uso, el cual se explica a continuación:

El usuario solicita al sistema autenticación, una vez realizada la autenticación, el administrador autoriza la gestión de ancho de banda para el usuario, incluyendo en el las políticas de asignación de ancho de banda propuestas por el modelo, todos estos procesos toman en cuenta la seguridad de red WLAN, los actores de la figura representan al usuario y al administrador de la red inalámbrica WLAN.

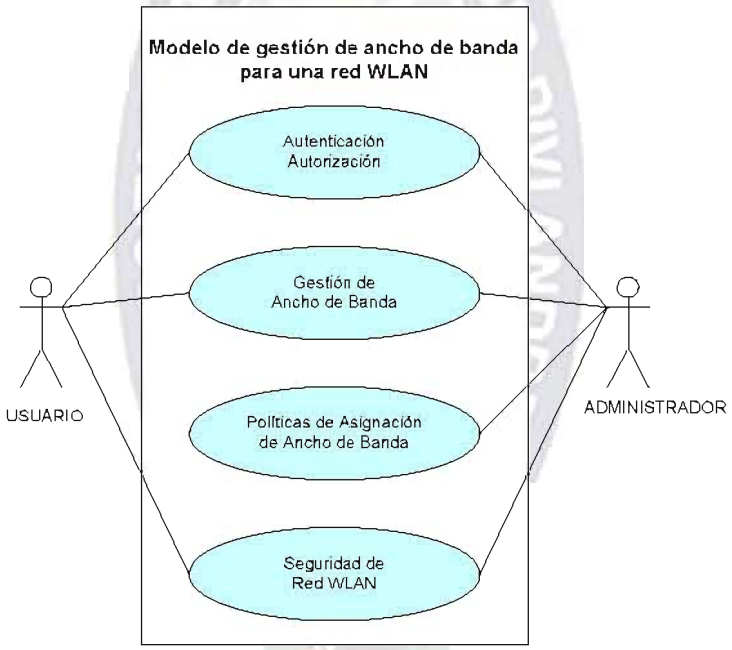

Figura 3.2 Diagrama de Caso de Uso.
Modelo de gestión de ancho de banda para una red WLAN
Fuente: Elaboración Propia.

La figura 3.3, muestra el funcionamiento general del modelo de gestión de ancho de banda para una red WLAN, con esta figura se quiere demostrar el flujo de información que existe entre uno proceso y otro, los actores de la figura representan al usuario y al administrador de la red inalámbrica WLAN.

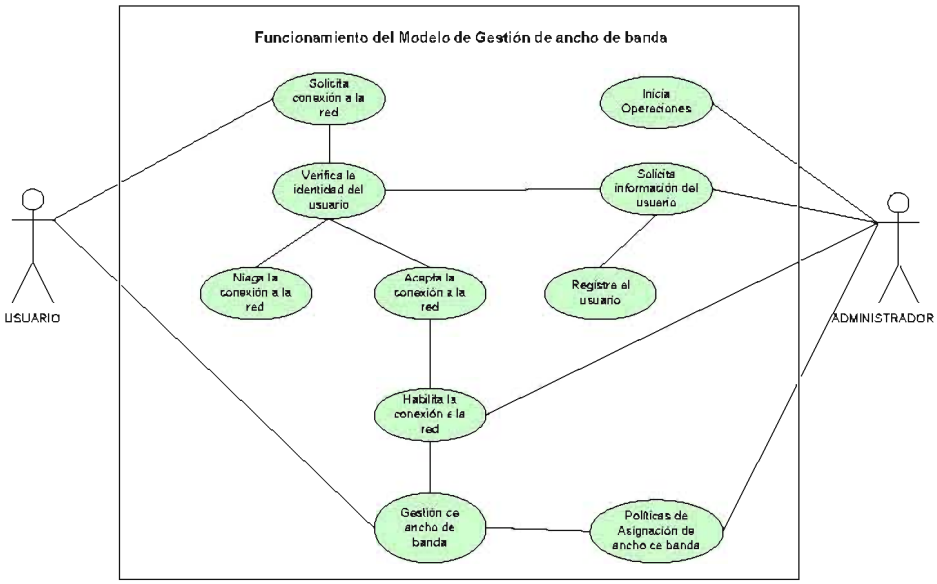

Figura 3.3 Diagrama de Caso de Uso.
Funcionamiento del Modelo de gestión de ancho de banda para una red WLAN
Fuente: Elaboración Propia.

3.2 Componentes del Modelo.

El modelo se compone por los siguientes componentes: (1) Autenticación y Autorización, (2) Gestión de ancho de banda, y (3) Seguridad de red WLAN.

3.2.1 Autenticación y Autorización.

El presente trabajo de tesis propone identificar al usuario que está ingresando a la red, con un proceso de autenticación, para posteriormente otorgar privilegios asociados a cada usuario, los cuales, indicarán el ancho de banda asignado por usuario, la autenticación incorpora el protocolo AAA (Autenticación, Autorización, Auditoria), que permite la implementación del servicio de autenticación y control de sesión. Con este control de acceso se obtiene datos estadísticos del ingreso de los usuarios y el tiempo de utilización a la red WLAN.

La autenticación se ejecuta en base a dos conceptos: a) modelo tripartito mencionado en el punto 2.2.1, y b) el método de autenticación CHAP mencionado en el punto 2.2.2.1; de esta forma, cuando se haya verificado la identidad del

usuario se le permite o deniega el acceso a la red, esto funciona como una medida básica de seguridad del modelo propuesto ver (Fig. 3.4). Con respecto de la confidencialidad de la identidad del usuario, estas conservan cierto grado de privacidad, pues la información almacenada en el sistema no se interpreta sin las normas de seguridad tomadas por el administrador de la red, como se indica en el punto 2.4.1, el cual explica que la confidencialidad, es la capacidad de mandar (y recibir) datos sin divulgar ninguna parte a las entidades no autorizadas durante la transmisión de los datos. Los mecanismos para lograrlo son la encriptación-simétrica y la asimétrica, los cuales son considerados en la seguridad de red.

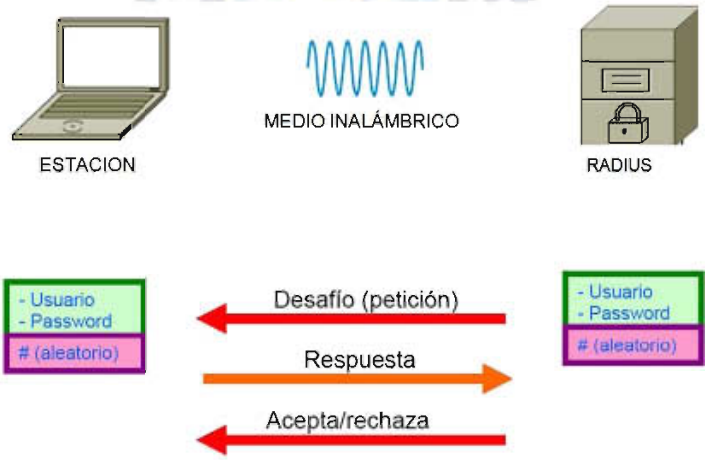

Figura 3.4. Representación del proceso de Autenticación y Autorización
Fuente: Elaboración Propia.

De la figura 3.4, se observa la representación del proceso de autenticación y autorización, que presta atención en tres puntos importantes: (1) la estación o usuario, (2) el medio inalámbrico o punto de acceso, y (3) El servidor de autenticación, las flechas rojas representan el esquema de autenticación del proceso de autenticación que está basado en el protocolo CHAP, el cual utiliza un saludo de tres vías, este se observa en la figura 3.4 (El servidor realiza un desafío al usuario que intenta conectarse a la red, el usuario responde al desafío, finalmente el servidor acepta o rechaza al usuario que intenta conectarse a la red); el servidor verifica periódicamente la identidad del anfitrión o usuario final.

La autenticación CHAP se realiza en el establecimiento de la primera conexión y puede ser repetido en cualquier tiempo después de que la conexión se ha establecido, CHAP toma en cuenta características importantes como: a) Imponer seguridad en la red al requerir que los extremos compartan un secreto en texto simple, b) El secreto nunca es enviado a través de la conexión, sólo se envía la respuesta del desafío como un valor hash, c) Las contraseñas secretas deben ser idénticas en los equipos locales y remotos, y d) Los secretos deben de estar de acuerdo en ser generados e intercambiados fuera de la banda en una manera segura, de esta manera, debido a que el secreto nunca se transmite, otros equipos son prevenidos de no robarlo y ganar acceso ilegal al sistema (ver punto 2.2.2.1).

La figura 3.5 muestra el diagrama de caso de uso general del proceso de autenticación y autorización, donde el usuario solicita la conexión a la red WLAN, RADIUS verifica la identidad del usuario que solicita acceso a la red (mediante el protocolo CHAP el cual toma en cuenta la encriptación de datos), finalmente RADIUS acepta o rechaza la conexión al usuario.

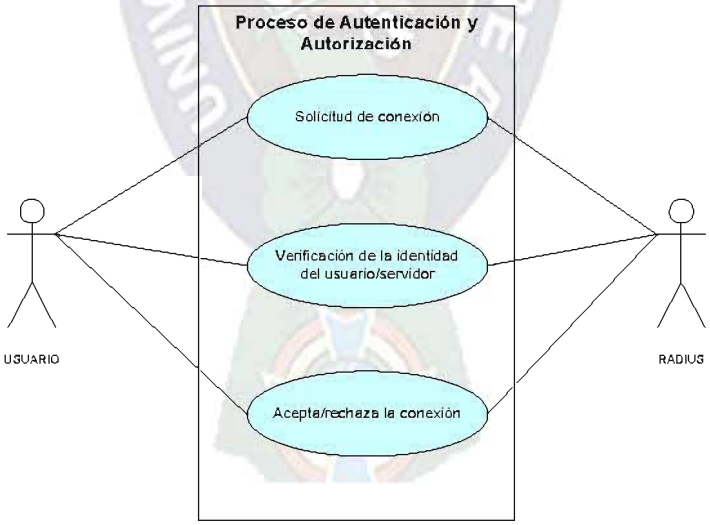

Figura 3.5 Diagrama de Caso de Uso.
Proceso de Autenticación y Autorización
Fuente: Elaboración Propia.

La figura 3.6 diagrama de secuencia, muestra el proceso de autenticación y autorización de forma más detallada en base al modelo tripartito ((1) el usuario, (2) punto de acceso inalámbrico, y (3) RADIUS); y el método de autenticación CHAP, los cuales se describen a continuación:

El usuario solicita conexión al punto de acceso inalámbrico, este a su vez sirve de puente en la solicitud de autenticación del servidor y el usuario, RADIUS realiza la distribución de llaves y envía el desafío CHAP para la autenticación y autorización del usuario, este a su vez inserta datos como ser un login o password, que deben ser verificados por el autenticador, este intercambio de claves lo realiza el usuario y RADIUS por medio del punto de acceso, después de este proceso RADIUS envía la respuesta de aceptación o rechazo de la conexión a la red WLAN al que quiere acceder el usuario, finalmente se realiza el registro del usuario conectado a la red WLAN, para su posterior designación de ancho de banda por nivel de privilegios.

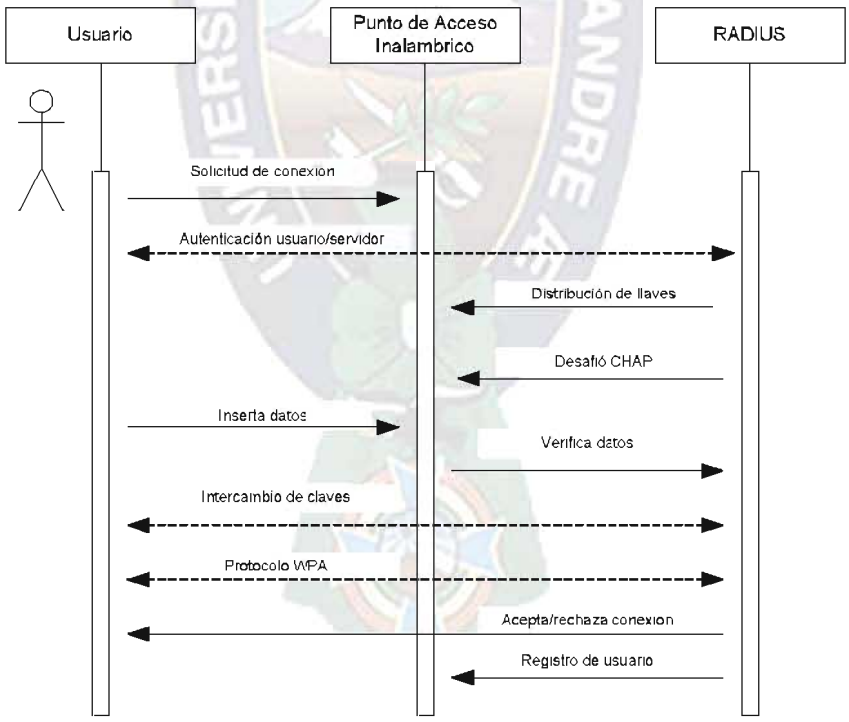

Figura 3.6 Diagrama de Secuencia
Proceso de Autenticación y Autorización
Fuente: Elaboración Propia.

También, es importante mencionar que el ancho de banda asignado, tiene una relación directa con la identidad del usuario, dentro de las características de la identidad del usuario, los privilegios estarán determinados por el administrador de la red, el cual debe determinar un ancho de banda necesario para las necesidades de dicho usuario.

3.2.2 Gestión de ancho de banda.

El proceso de gestión se basa en políticas de asignación de ancho de banda el cual considera como política del modelo propuesto:

(1) La creación de niveles de privilegios; recomendados, en el punto 2.3.1; donde se agrupa a los usuarios, el administrador de red configura el procedimiento necesario para asignar el ancho de banda.

(2) Regla de cantidad de usuarios, la cual se realiza para optimizar la calidad del desempeño de la red en la administración del ancho de banda.

(3) La restricción de ancho de banda de: sitios, puertos, y dominios de red, por nivel de privilegios.

La figura 3.7 muestra el funcionamiento general del proceso de gestión de ancho de banda donde los actores principales son el usuario, y el administrador, el cual, es el encargado del inicio de operaciones donde se realiza el proceso de calcular la cantidad de número de usuarios que soporta la red y el registro de usuarios por nivel de privilegios, asociados a las restricciones de ancho de banda de cada nivel.

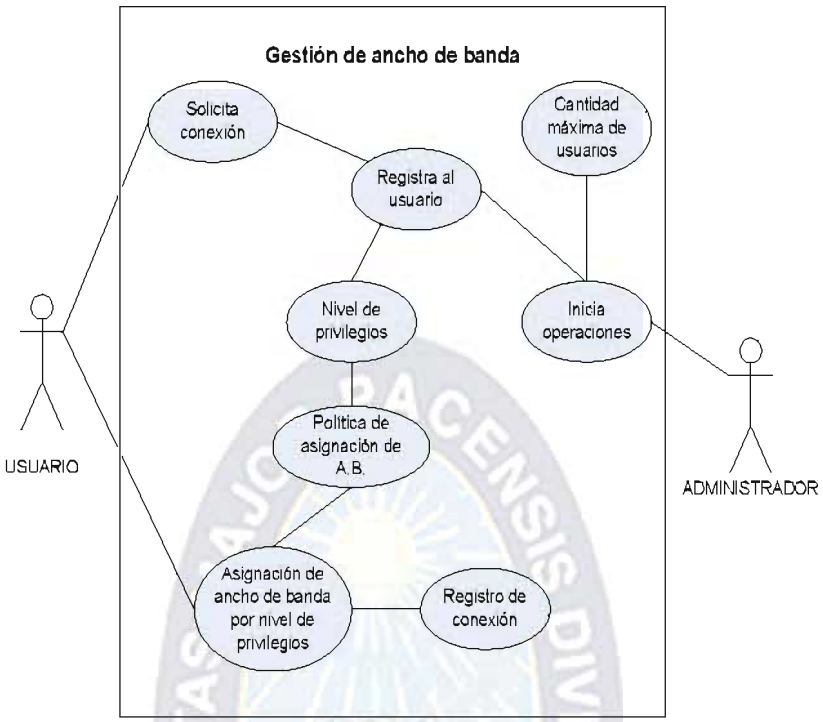

Figura 3.7 Diagrama de Caso de Uso
Proceso de gestión de ancho de banda
Fuente: Elaboración Propia.

3.2.2.1 Niveles de privilegios.

El presente trabajo de tesis considera 3 niveles de privilegios que forman la base de las políticas de asignación de ancho de banda:

a) El primer nivel es básico denominado "A", y solo se asigna un ancho de banda mínimo para el uso de servicios en la red.

b) El segundo nivel, es intermedio denominado "B", se le asigna un mayor porcentaje de ancho de banda, además permite realizar transferencias de archivos de la red.

c) El tercer nivel, denominado "C", no tiene restricciones en la asignación de ancho de banda de ningún tipo.

Para crear los diversos niveles de privilegios en la asignación del ancho de banda, se propone manejar un registro de usuarios con su información y con el identificador de privilegios, que el administrador particulariza dependiendo de las necesidades de la red. La postura general es crear niveles de privilegios donde a cada uno de estos, se le asigne un cierto ancho de banda. La idea de crear niveles de privilegios se base en dos criterios: a) utilizar un ancho de banda fijo, y b) distribución en base a los tipos de usuarios registrados en la red, esto, con el fin de garantizar la disponibilidad del servicio para los usuarios, que hacen uso de servicios que requieren mayor ancho de banda y que son los que requieren una mejor calidad del servicio de la red.

3.2.2.2 Reglas de número de usuario.

Las reglas para el número de usuarios por nivel de privilegios es una técnica de estimación determinado por el administrador, el cual realiza cálculos sobre cuántos usuarios puede tolerar la red en base a la cantidad de ancho de banda disponible, el número de usuarios es importante, pues sirve como base para los cálculos de repartición del ancho de banda.

La distribución del ancho de banda está dada por la división del ancho de banda total entre los 3 niveles de privilegios A, B, C el cual nos brinda una estimación del número de usuario soportados por la red WLAN, el presente trabajo de tesis propone la creación de una regla para determinar el número máximo de usuarios de acuerdo al ancho de banda que se le solicite al proveedor de servicios de Internet. La regla del número de usuarios se determina por la repartición de porcentajes entre los tres niveles de privilegios representados por la suma de estos:

$$A + B + C = 100\% \qquad \text{ecuación 3.1}$$

Donde:
A = Nivel de privilegio básico A
B = Nivel de privilegio intermedio B
C = Nivel de privilegio irrestricto C

Cada variable (A, B, C) representa un porcentaje que cumple la ecuación establecida con una igualdad de repartición de usuarios, en otras palabras, el porcentaje de usuarios de cada nivel de privilegios, debe ser igual al 33.3%, lo que nos da como resultado un 99.9% del total de usuarios en la red. Aunque los porcentajes sean iguales, el número de usuarios por nivel no es necesariamente el mismo. Por ejemplo, si se dispone de ancho de banda de 1024 Kbps la distribución se realiza de la siguiente manera: A = 10 kbps, B = 50 Kbps y C = 100 Kbps.

Entonces se tiene que al ejecutar las operaciones descritas anteriormente, y suponiendo que todos pertenecen a un mismo nivel, se divide el 100% del ancho de banda 1024 Kbps sobre el nivel de privilegio, se tiene el número máximo de usuarios en la red: para el nivel A se tiene 102 usuarios, el nivel B tiene 20 usuarios y el nivel C tiene 10 usuarios. Esto con el fin de que no se exceda ningún nivel con la capacidad de usuarios. (Ver Tabla 3.1)

Tabla 3.1. Distribución Independiente del ancho de banda por nivel de privilegios.

AB	N	ABP	ADAB	U
1024 Kb	A	100%	10 Kb	102
1024 Kb	B	100%	50 Kb	20
1024 Kb	C	100%	100 Kb	10

Fuente: Elaboración Propia.

Donde: AB = Ancho de banda disponible.
N = Niveles de privilegios.
ABP = Ancho de banda porcentual.
ADAB = Asignación de ancho de banda.
U = Cantidad de usuarios soportados por la red.

Ahora ejecutando la regla del número de usuarios para la red con un 33.3% para cada nivel, se obtiene la distribución del ancho porcentualmente:

$$ABP = (1024\ Kb * 33\%) / 100\% = 341Kb \qquad \text{ecuación 3.2}$$

Tabla 3.2. Cantidad de usuarios por nivel de privilegios.

AB	N	DPAB	ABNP	ADAB	U
1024 Kb	A	33%	341 Kb	10 Kb	34
1024 Kb	B	33%	341 Kb	50 Kb	7
1024 Kb	C	33%	341 Kb	100 Kb	3
TOTAL		99%	1024 Kb		44

Fuente: Elaboración Propia

Donde:
AB = Ancho de banda disponible.
N = Niveles de privilegios.
DPAB = Distribución porcentual de ancho de banda por nivel de privilegios.
ABNP = Ancho de banda por nivel de privilegios
ADAB = Asignación de ancho de banda.
U = Cantidad de usuarios soportados por la red.

De la tabla 3.2 se observa que A = 34, B = 7 y C = 3, como cantidades de usuarios. El cual tiene sentido, ya que, el número de usuarios para el nivel con mayor ancho de banda requerido (C) es menor que el número de usuarios requerido en el primer nivel (A), cumpliendo además con las recomendaciones mencionadas, vistas en el punto 2.1.5 y en la tabla 2.2.

El crear un número tope de usuarios que soporta la red se basa en el principio de que el ancho de banda es un recurso limitado, además de que, los dispositivos físicos que tienen conexión directa con los clientes como: a) los puntos de acceso,

b) los switches y c) hubs, soportan un número determinado de usuarios, según las especificaciones del producto. Estableciendo así, que el número de usuarios para el modelo de gestión de ancho de banda para una red WLAN, se encuentra determinado por el ancho de banda provisto por el ISP de la red.

También se debe tomar en cuenta, que si el número de usuarios en la red crece, sin tomar en cuenta el soporte de la red, es decir la cantidad máxima de usuarios; y el ancho de banda no se incrementa, las asignaciones por nivel llegan a ser pequeñas, e inclusive ridículas ya que la regla del número de usuarios en la red propuesta, sirve como una limitante en la asignación de ancho de banda, siempre y cuando se practiquen con valores adecuados para realzar el modelo de gestión de ancho de banda para una red WLAN.

El diagrama de contexto 3.8, da una descripción a grandes rasgos del funcionamiento del modelo de gestión, siendo una descripción del sistema que recibe los usuarios que se conectan a la red al enviar una petición de conexión a la red, el sistema le regresa al usuario la respuesta de la petición de conexión, junto con los detalles de conexión, si es necesario.

Figura 3.8. Diagrama de Contexto
Descripción de la gestión de ancho de banda para una red WLAN
Fuente: Elaboración Propia.

La figura 3.9, muestra como es procesada la petición de conexión descrita en el diagrama de contexto (fig.3.8). La solicitud de conexión es una petición RADIUS que es tomada por el punto de acceso en el proceso 1 (Autenticación), esta petición se reenvía como un desafío al servidor el cual se encargará de validar la identidad del usuario enviada en el desafío. Si la petición es aceptada, el proceso 3 (Políticas de asignación de A.B.) es asociado al nivel de privilegio que corresponde al usuario, y proceso 4 (Aceptación RADIUS), se encarga de responder positivamente al usuario. En caso contrario el proceso 5 (Rechazo RADIUS), niega el acceso a la red al usuario.

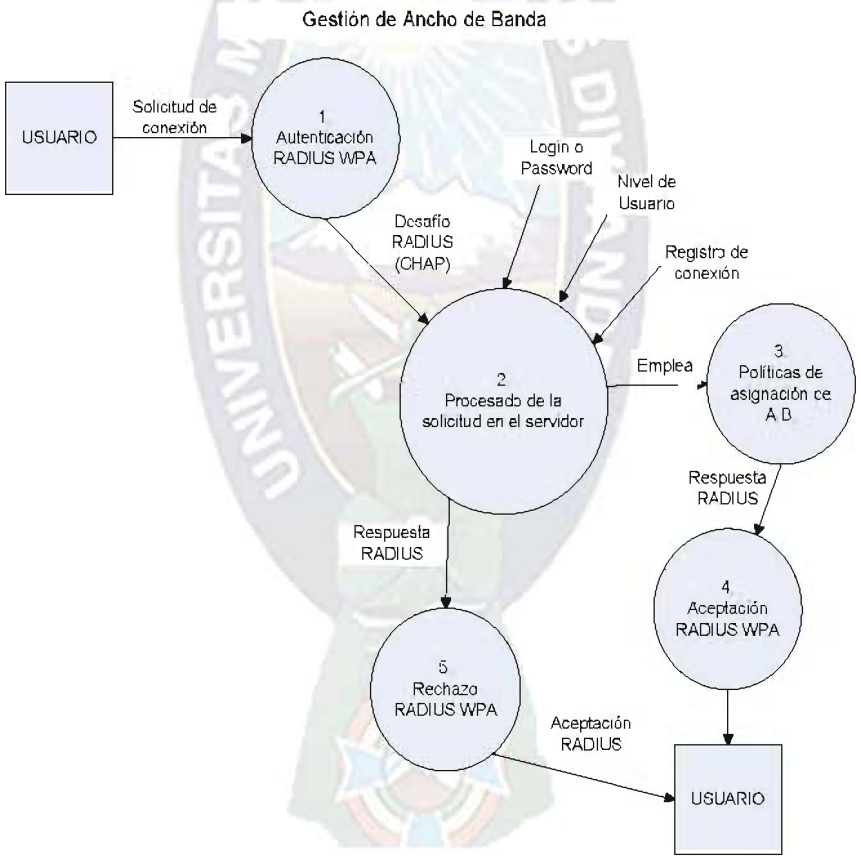

Figura 3.9 Diagrama de flujo de datos para la Gestión de ancho de banda de una red WLAN
Fuente: Elaboración Propia

La siguiente figura 3.10, muestra como el servidor 2.1 (Procesamiento del administrador) hace conexión con el registro de usuarios para obtener su información y así validar su identidad. Después se genera una asociación 2.2 (de las políticas de asignación de ancho de banda por nivel de privilegios), solamente con los usuarios validos por el sistema, y se ejecuta dicho proceso, después de la ejecución del proceso se envía una respuesta de aceptación o rechazo del usuario.

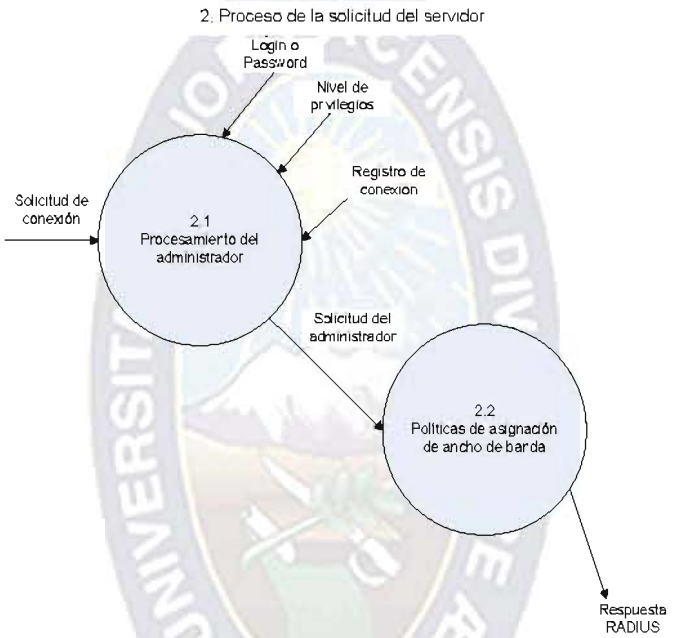

Figura 3.10 Diagrama de flujo de datos.
Descripción del Proceso de solicitud del administrador.
Fuente: Elaboración Propia.

3.2.2.3 Restricción de ancho de banda.

Para la restricción de ancho de banda se le asocia el empleo de políticas de uso de ancho de banda, con la clasificación de los niveles de privilegios, se considera los siguientes puntos:

a) El usuario correspondiente al nivel de privilegios "A", tiene restricción sitios, puertos, y dominios de red, que ocupan un mayor ancho de banda, este accederá a sitios web específicos.

b) El usuario correspondiente a nivel de privilegios "B", tiene una restricción personalizada a sitios, puertos, y dominios de la red; este accederá a sitios web donde se admitan descargas de archivos.

c) El usuario corresponde a nivel de privilegios "C", tendrá acceso a distintos sitios, puertos y dominios de red, la única limitación de este tipo de usuarios es la cantidad de ancho de banda que se le asigne.

Otras políticas que el administrador deberá considerar para particularizar el modelo según las necesidades de su institución son:

a) El incumplimiento de las anteriores políticas y el acceso a sitios web ajenos al nivel de privilegios reduce la asignación del ancho de banda al usuario con previa notificación, el incurrir frecuentemente en estas faltas por un periodo de tiempo prolongado tendrá penalizaciones como el negar el acceso a la red por un periodo de tiempo determinado.

b) El proceso de registro de usuarios por nivel de privilegios, y los cambios de preferencias de un usuario, lo realiza el administrador por medio de una configuración, además es el punto de inicio para determinar cuánto ancho de banda asignar.

c) El número de usuarios en el sistema, la restricción y sus privilegios lo determina el administrador en base al proceso de gestión propuesto (punto 3.2.2, gestión de ancho de banda).

3.2.3 Seguridad de red WLAN.

La seguridad de red WLAN se caracteriza por efectuar mecanismos de protección a los paquetes de información, que emplea un medio abierto para transmitir la información, y de esta manera, evitar cualquier peligro, y protegerse en contra de agentes externos a la red intercepten la señal y así obtener datos seguros.

Por los alcances del presente trabajo de tesis, las medidas de seguridad se incorporan a la seguridad del servidor; en este caso Linux, el uso del servidor para

el monitoreo de los usuarios en la red presenta un punto de atención para la seguridad que se tomará en cuenta; el cual, se aplica en el momento de instalar el servidor RADIUS.

Estas medidas de seguridad se concentran cuándo: 1) el nodo inalámbrico (suplicante) intenta conectarse a la red inalámbrica y el punto de acceso (autenticador) se encarga de pedirle al suplicante sus credenciales, 2) Luego de recibirlas, se las envía a nuestro servidor de autenticación, que se encarga validar su identidad y de acuerdo a eso permitirle o negarle el ingreso a la red, y 3) Ya con el suplicante validado, éste puede acceder a la red y utilizar todos los recursos que ésta tenga disponible (ej. Internet), la figura 3.11 muestra como intervienen los medidas de seguridad a) confidencialidad, b) integridad, c) viabilidad, d) autenticación, e) autorización, f) control de acceso, g) encriptación y h) administración de llaves, que son indispensables para la obtención de un sistema robusto.

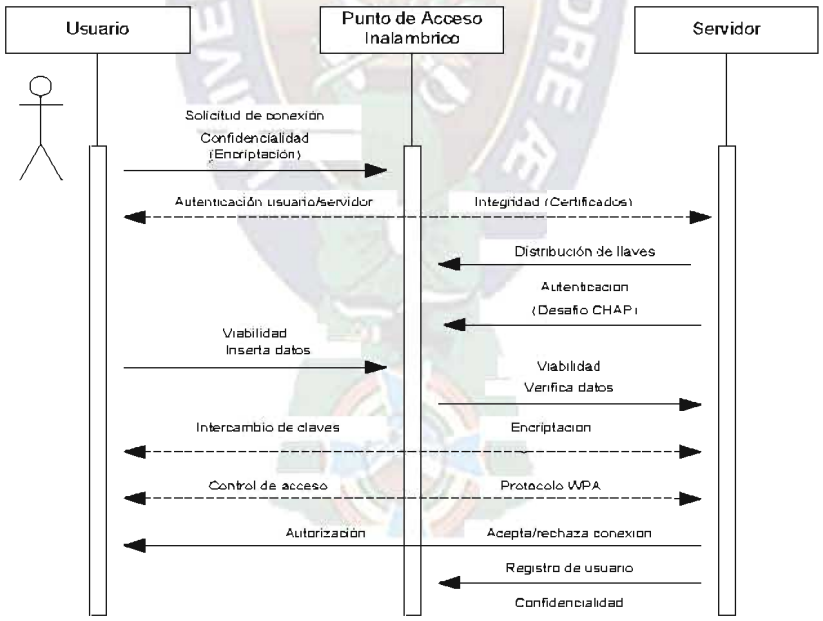

Figura 3.11 Diagrama de secuencia.
Descripción de las medidas de seguridad.
Fuente: Elaboración Propia.

En la figura 3.11, también se puede observar que para la implementación del control de acceso se utiliza el protocolo WPA, el cual, es uno de los últimos protocolos de seguridad para redes inalámbricas, que cuenta con un mecanismo de seguridad robusto para la conexión (ver punto 2.4.5).

Para el mecanismo de identificación se utiliza el método EAP protegido (PEAP). PEAP trabaja de la siguiente manera: a) como primer paso del protocolo, se establece un túnel TLS usando rutinas similares a EAP-TLS es decir, certificados digitales en el servidor de autenticación son usados para validar que la red es confiable antes de proseguir, b) en el segundo paso, el túnel TLS es usado para encriptar un protocolo de autenticación ampliamente usado como CHAP, que autentifica el usuario en la red. El primer paso comúnmente se refiere como autenticación "externa", puesto que es un túnel el que protege la segunda autenticación o "interna". En la figura 3.12 se puede observar la ideología implementada en PEAP.

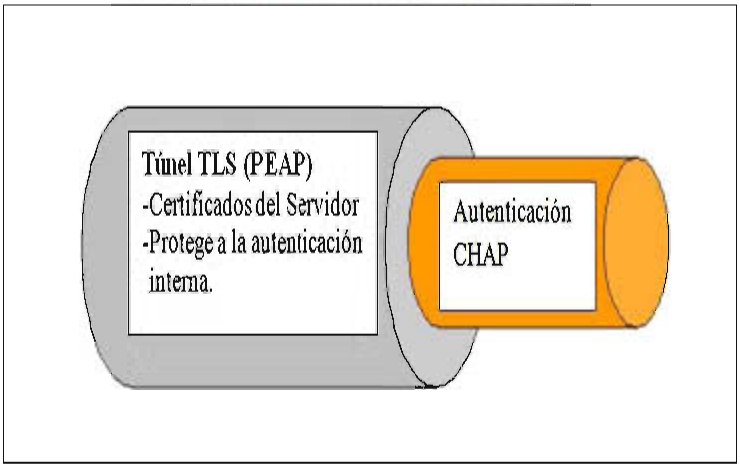

Figura 3.12 Representación de EAP protegido PEAP.
Fuente: Elaboración Propia.

3.3 Formalización del Modelo.

Sea la descripción del modelo de gestión de ancho de banda variables **(V)** los cuales pertenecen a una red **(R)** WLAN con servicio de internet ADSL[28]

Donde:

V_A = Variable de Autenticación

V_{AAB} = Variable de gestión de ancho de banda

V_{PAAB} = Variable de políticas de asignación de ancho de banda

V_S = Variable de seguridad

V_N = Variable de nivel de privilegios

V_{RU} = Variable de regla de número de usuarios soportados por la red

y $$V_{AAB} = (V_N + V_{RU}) \in R_{WLAN}$$

Del punto 3.2.2.1 Nivel de privilegios, se tiene:

$$V_N = (V_{N1} + V_{N2} + V_{N3}) \in R_{WLAN}$$

V_1 = nivel de privilegios A

V_2 = nivel de privilegios B

V_3 = nivel de privilegios C

En la tabla 3,2 Distribución independiente del ancho de banda por privilegios, se tiene:

$$V_{RU} = (V_{AB} \cap V_N \cap V_{DPAB} \cap V_{ABNP} \cap V_{ADAB} \cap V_U) \in R_{WLAN}$$

V_{AB} = Variable de ancho de banda disponible

V_N = Niveles de Privilegios

V_{DPAB} = distribución porcentual de ancho de banda por nivel de privilegios

[28] Del inglés Asymmetric Digital Subscriber Line – Línea de Abonado Digital Asimétrica – ADSL

V_{ABNP} = Ancho de banda por nivel de privilegios

V_{ADAB} = Asignación de ancho de banda

V_U = Cantidad de usuarios soportados por la red

Sea ***GAB*** la función de gestión de ancho de banda, por lo tanto el modelo se formaliza de la siguiente manera:

$$V_{GAB} = (V_A \cap V_{AAB} \cap V_{PAAB} \cap V_S) \quad \in R_{WLAN}$$

3.4 Límites del Modelo.

El modelo de gestión de ancho de banda trabaja en redes WLAN con servicio del Proveedor de Internet ADSL y no así otros servicios de internet (DSL, Dial-up), el modelo no considera redes WWAN, WMAN, WPAN.

CAPÍTULO 4. IMPLEMENTACIÓN

4.1 Construcción del Modelo

El desarrollo del modelo se realiza con la construcción e implementación del entorno de mecanismos de seguridad y políticas de gestión de ancho de banda propuesto en la introducción de este trabajo de tesis.

El modelo consta de tres elementos fundamentales: a) los clientes, b) el punto de acceso (AP), y c) el servidor. La interacción de los tres elementos es primordial para el desempeño de la solución propuesta.

a) Para establecer el modelo se ha contemplado que los clientes sean equipos de computación laptops con capacidad de conexión a una red inalámbrica. Los clientes del modelo no necesitarían alguna característica especial como instalar algún software extra salvo, certificados de seguridad necesarios para manejar el protocolo WPA.

b) El segundo elemento importante es el punto de acceso, que trabajará con un routeador, dicho equipo cuenta con la característica de soportar el protocolo WPA con RADIUS y así lograr un canal de conectividad con el servidor. Otra característica que vale la pena mencionares que el AP soporta tanto el estándar 802.11b como el 80211.g, lo que permite que diversidad de tarjetas de red inalámbrica puedan hacer uso de este dispositivo, y considerando que el 802.11g soporta comunicación tanto con el 802.11b y 802.11a, existe un gran rango de compatibilidad de frecuencia para que equipos recientes y los no tanto, pueden hacer uso del modelo sin ningún problema.

c) El tercer elemento es el servidor que atenderá las peticiones de la red, tiene varios elementos importantes: a) se necesita que tenga instalado el servicio RADIUS con protocolo AAA; b) una configuración de datos para que el protocolo RADIUS almacene la información necesaria; c) el sistema

operativo Linux; d) y el servicio de asignación de ancho de banda, para la configuración de las políticas propuestas. Todos estos elementos son los necesarios para establecer el servidor de servicio para la gestión de ancho de banda.

El servicio RADIUS utilizado para la implementación es el freeRADIUS de libre distribución bajo la licencia GNU (General Public License), incluyendo su instalación y configuración previa, y las distintas configuraciones de los elementos principales restantes, como el punto de acceso inalámbrico y el cliente RADIUS, y para establecer el entorno de seguridad se usa el método de autenticación CHAP en su versión MS-CHAPV2.

FreeRADIUS es elegido por ser uno de los mejores servidores de distribución gratuita, con referencia de la publicidad y las recomendaciones, además de que puede instalarse sobre Linux y cuenta con el manejo del protocolo AAA.

El sistema operativo Linux instalado en el servidor es la versión de Suse 10 distribuida por Red Hat Enterprises, esta versión se eligió por recomendaciones acerca de la seguridad que ofrece el sistema operativo con respecto a otras distribuciones de Linux [rad, 09].

4.2Arquitectura de red utilizada

La construcción del modelo se presenta a continuación en un gráfico tomando en cuenta los puntos mencionados con anterioridad haciendo uso de una arquitectura de red para su mejor comprensión.

La Figura 4.1. Modelo de gestión de ancho de banda para una red inalámbrica WLAN, muestra el funcionamiento del modelo utilizando, una arquitectura de red simple compuesta por un punto de acceso inalámbrico, un cable ethernet para el acceso a Internet, un servidor, y uno o varios clientes con tarjeta de red inalámbrica.

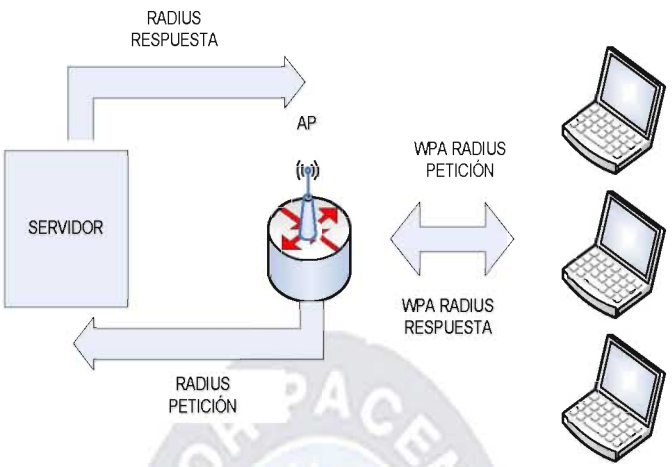

Figura 4.1. Modelo de gestión de ancho de banda para una red WLAN
Fuente: Elaboración Propia.

4.2.1 Equipo usado

En la implementación del esquema de red anterior se utiliza los siguientes dispositivos: (ver anexo "C" costos de implementación)

- Una Computadora con ambiente Linux, como servidor de autenticación y administrador de ancho de banda.
- Un Ruteador inalámbrico especificación D-Link DIR-300, como punto de acceso.
- Computadora Laptop HP compaq con sistema operativo Windows Vista como nodo inalámbrico o suplicante.
- Computadora Laptop DELL con sistema operativo Windows XP SP2, como nodo inalámbrico o suplicante.

4.3 Instalación del servidor de seguridad

Para la instalación y configuración de FreeRADIUS, se busca el archivo de instalación específico al sistema operativo, la versión utilizada es la 2.1.4, a continuación se mostrara un ejemplo de cómo bajar el código fuente, descomprimir el archivo, configurar las opciones de compilación:

• Descarga el archivo comprimido de instalación de la página www.freeradius.org y como root se ejecuta los siguientes comandos:

```
# tar xvf freeradius-server-2.1.4.tar // extrae el contenido
# cd freeradius-server-2.1.4
# ./configure        //directorio que contiene los archivos de instalación
# make              // para compilar
# make install
```

Los archivos de configuración quedan instalados en /usr/local/etc/raddb/, que es la ruta por defecto. Si la instalación fue exitosa, se prueba que el servidor FreeRadius esté funcionando correctamente con el siguiente comando:

```
# radiusd -X
```

Si todo está configurado correctamente, luego de presionar Enter se muestra la pantalla siguiente:

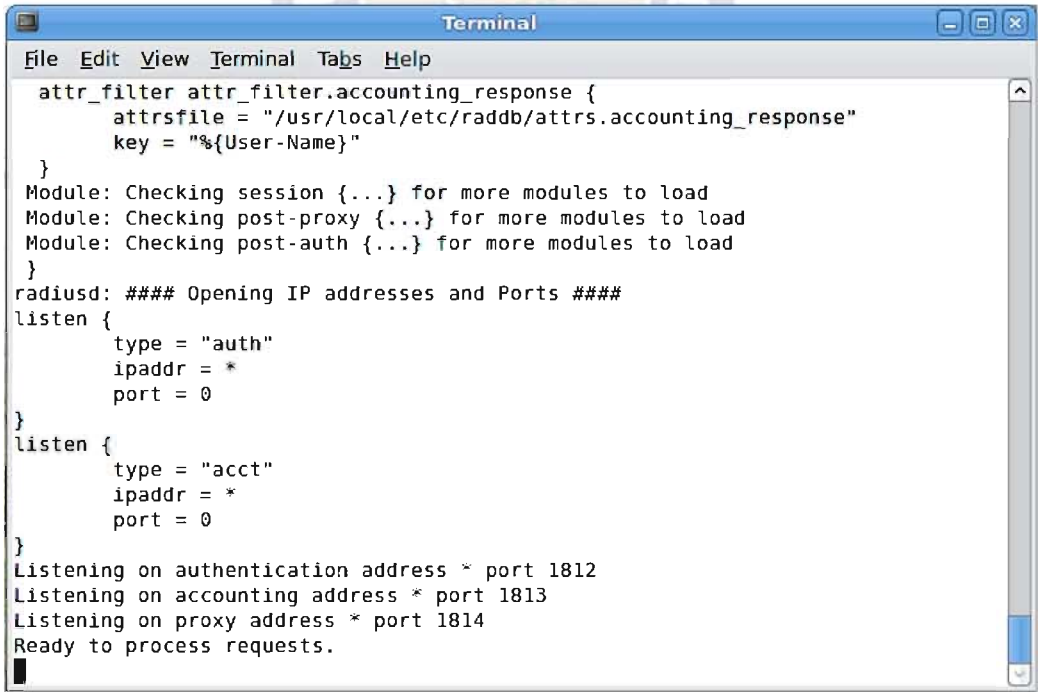

Figura 4.2. Habilitación del servidor freeradius
Fuente: Elaboración Propia

Una vez compilado e instalado el servidor a continuación se muestran las configuraciones necesarias, donde se editan los archivos de configuración de la carpeta principal del software llamada raddb, los archivos de configuración son: client.conf (Como su nombre lo indica es donde se configura la interface del AP), users (Aquí se establece la información del o los clientes), EAP.conf (es el archivo donde se establece el método EAP a utilizar).

4.3.1 Configuración del módulo de usuarios

En el archivo "users" se especifica la información de validación para los usuarios que tienen permiso a conectarse al servidor de seguridad, se crea un usuario para probar la autenticación con FreeRadius, los comandos necesarios se muestran a continuación:

```
"luz"     Cleartext-Password := "luz"
```

4.3.2 Configuración del módulo Cliente

En el módulo del cliente se especifica la dirección IP del punto de acceso que se va a utilizar, también se especifica la contraseña, el identificador o nombre que se le asigna al punto de acceso.

```
client 192.168.0.1/24 {
secret      = testing123
shortname   = linksys
}
```

4.3.3 Configuración del módulo EAP

En el archivo EAP.conf se encuentra los métodos EAP soportados por FreeRADIUS, los módulos que no están en funcionamiento se documentan colocándoles un signo de número antes de empezarla línea, uno de los módulos que está en funcionamiento y por lo tanto no está documentado es el que hace

referencia al método eap que el servidor utiliza por defecto, se asegura que los parámetros siguientes tengan los valores que se muestran a continuación:

```
eap {
default_eap_type = peap
...}
```

En el módulo eap se establece el tipo de método eap por defecto que se utiliza. Para el presente trabajo de tesis, el método eap que se utiliza es EAP-TLS.

```
tls {
certdir = ${confdir}/certs
cadir = ${confdir}/certs
private_key_password = testing123
private_key_file = ${certdir}/server.pem
certificate_file = ${certdir}/server.pem
CA_file = ${cadir}/ca.pem
dh_file = ${certdir}/dh
random_file = ${certdir}/random
...
}
```

En este fragmento de código anterior se especifica el password, la ubicación de los certificados del servidor y otros archivos necesarios para que el módulo pueda funcionar. El módulo tls requiere para usar la protección de autenticación peap para la transmisión de los paquetes, además en el módulo tls se especifica los certificados del servidor los cuales son necesarios para que el cliente los verifique si así lo desea.

```
peap {
default_eap_type = mschapv2
...
}
```

En el fragmento anterior se describe la autenticación que se realiza, está autenticación está establecida por (chap) con su versión MSCHAPV2, el cual, se edita los parámetros siguientes:

```
mschap {
use_mppe = yes
require_encryption = yes
require_strong = yes
...
}
```

4.3.4 Configuración del punto de acceso

El punto de acceso se configura con la dirección IP del servidor de seguridad para que este lo identifique, también debe quedar libre cada uno de los puertos usados en la autenticación, en el caso de que se utilice firewall del lado del servidor, y de los clientes inalámbricos.

A continuación se muestra la figura 4.2 configuración del punto de acceso.

Figura 4.3. Configuración del punto de acceso
Fuente: Elaboración Propia.

En la figura 4.2 se muestra el menú de configuración para el servidor de seguridad, en éste se destaca la técnica de encriptación para la conexión, la dirección IP del servidor RADIUS y el puerto de comunicación usado, también se muestra la llave que debe compartir con los clientes para que puedan conectarse, y el intervalo de envió de la llave.

4.3.6 Configuración del cliente

Para que el usuario pueda conectarse al entorno de red inalámbrico de seguridad necesita clientes de autenticación RADIUS. Para instalar el cliente se debe ejecutar el certificado EAP/PEAP y seguir las instrucciones del programa de instalación con detenimiento. (Ver figura 4.3)

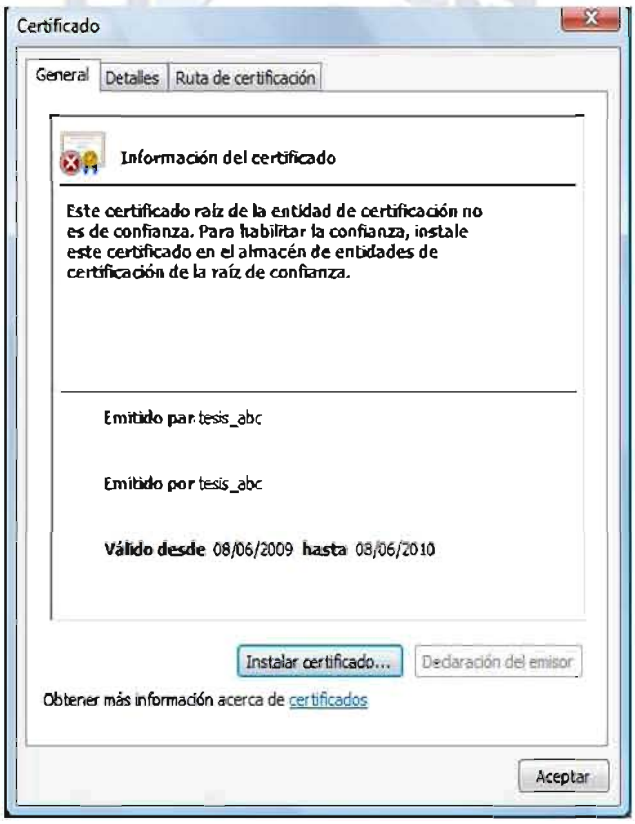

Figura 4.4. Certificado CA para cliente RADIUS
Fuente: Elaboración Propia.

Después de terminado el proceso de instalación, se tiene que acceder al cliente de redes inalámbricas de Windows para poder usar el cliente RADIUS y poder conectarse al entorno de seguridad de la red inalámbrica (ver figura 4.3).

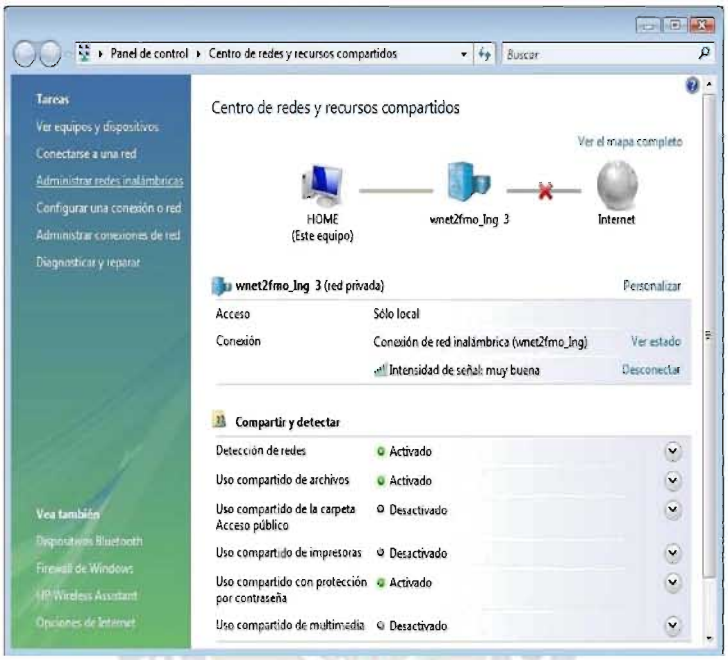

Figura 4.5. Configuración del cliente
Fuente: Elaboración Propia

El cliente soporta un mismo protocolo o método de autenticación para que puedan trabajar entre sí al validar o restringir el acceso a la red. Un entorno inalámbrico de seguridad como el presentado no funciona con tan solo instalar cada componente, es necesaria una configuración y/o programación de cada elemento sobretodo del cliente y el servidor.

Para agregar a la red inalámbrica se ingresa a: "Agregar" perfil de red y seleccionamos la opción "Crear un perfil de red manualmente", Se introduce la información de la red inalámbrica, en este caso le llamamos "radius", seleccionamos el tipo de seguridad "WPA-Enterprise" y el tipo decifrado "TKIP".

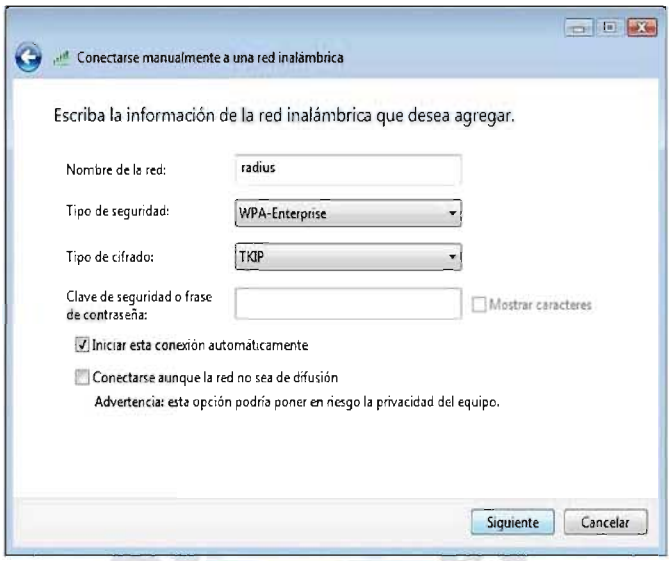

Figura 4.6.Menu de asociación para el punto de acceso
Fuente: Elaboración Propia

En el Administrador de redes inalámbricas podemos ver nuestro nuevo perfil de red. Ahí seleccionamos el perfil y hacemos clic secundario sobre éste para luego hacer clic sobre "Propiedades" y configurar algunos aspectos de seguridad del perfil.

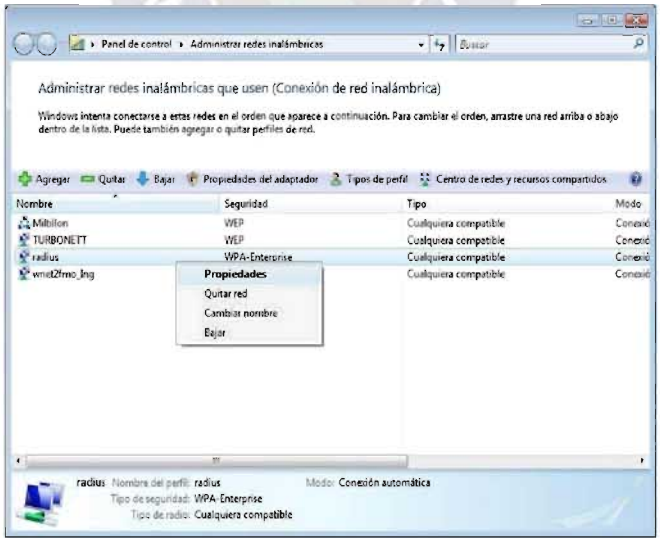

Figura 4.7. Menú de administración de redes inalámbricas
Fuente: Elaboración Propia

En la pestaña de “Seguridad configuramos el método de autenticación de red haciendo clic sobre el botón “Configuración”.

Figura 4.8. Menú de propiedades de redes inalámbricas
Fuente: Elaboración Propia

Una vez estemos en las propiedades del método de autenticación de la red, indicamos que al conectarnos valide un certificado de servidor por lo que quitamos la selección en “Validar un certificado de servidor”.

Figura 4.9. Menú de propiedades EAP protegido
Fuente: Elaboración Propia

Luego de realizar toda la configuración en cada uno de los formularios abiertos. El cliente solicitará una credencial para conectarse a la red. Escribimos el nombre de usuario y la contraseña que nos ha sido asignada. Hacemos clic en “Aceptar”.

Figura 4.10. Menú de credenciales
Fuente: Elaboración Propia

4.4 Descripción del servidor de gestión.

El servidor de gestión se configura en base a la previa configuración del servidor RADIUS que viene detallado en el punto 4.3 El servidor SQUID es configurado para el administrador de la red por medio de una interfaz que permitirá alterar los valores con los que trabaja este módulo, para la implementación de las políticas de asignación de ancho de banda. Los valores que se cambian son: a) el ancho de banda disponible en la red, b) el ancho de banda por nivel de privilegios que se registra directamente en SQUID, y c) la restricción de sitios, puertos o dominios de red.

Con Squid se implementa un servidor proxy y un dominio para caché de páginas web, ya que tiene una amplia variedad de utilidades, está especialmente diseñado para ejecutarse bajo entornos tipo Linux y ha sido desarrollado durante muchos

años lo que lo hace completo y robusto. SQUID, es distribuido bajo los términos de Licencia Pública General de GNU o más conocida por su nombre en inglés GNU General Public License (GPL).

La figura 4.9 muestra de manera gráfica la estructura del servidor con la interacción de estos servicios, que se encuentren sobre un mismo equipo, dado que se busca que el procesamiento recaiga solo sobre un dispositivo y no se involucre la adquisición de nuevos equipos.

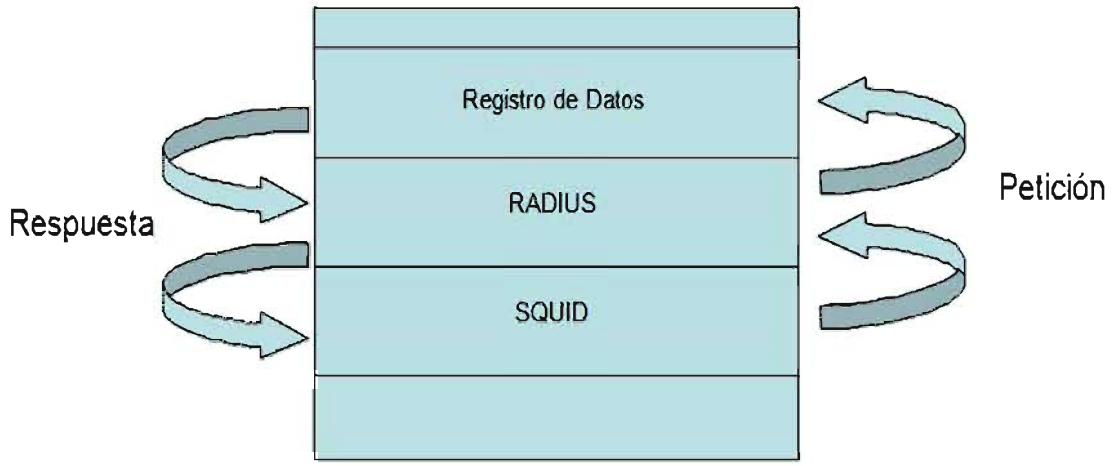

Figura 4.11. Descripción del servidor de gestión
Fuente: Elaboración Propia

4.5 Instalación del servidor de gestión.

Para la instalación y configuración de Squid, se busca el archivo de instalación específico al sistema operativo, a continuación se mostrara un ejemplo de cómo bajar el código fuente, descomprimir el archivo, configurar las opciones de compilación:

• Descarga el archivo comprimido de instalación de la página http://www.squid-cache.org y como root se ejecuta los siguientes comandos:

Extraer el contenido del archivo tar.bz2:

```
tar xvf nombre_del_archivo.tar.bz2
```

Por consola, ingresar al directorio extraído y ejecutar los siguientes comandos:

```
./configure
make
make install
```

Una vez instalado con este soporte la forma de dejar pasar a los usuarios es atreves de las MAC's:

```
acl usuario01 arp 00:01:02:BF:55:63
acl usuario02 arp 00:00:39:E6:D0:08
acl usuario03 arp 00:0B:6A:54:2B:B2

http_access allow usuario01
http_access allow usuario02
http_access allow usuario03
http_access deny all
```

4.5.1 Configuración de las Políticas de asignación de ancho de banda por nivel de privilegios.

Para la asignación de ancho de banda "X" por nivel de privilegios, se adiciona las líneas en el archivo de configuración de squid, para esta configuración se edita en el fichero squid.conf el siguiente código:

```
acl all src 0.0.0.0/0.0.0.0

acl nivel_A src 10.0.0.200/24
acl nivel_B src 10.0.0.203/24

delay_pools 3
#Trasnferencia ilimitada dentro de la WLAN
delay_class 1 1
delay_parameters 1 -1/-1
delay_access 1 allow all

#Nivel B: Para 7 equipos y navegarán a 50 Kbs
delay_class 2 2
delay_parameters 65536/1024 10240/1024
delay_access 2 allow nivel_B

#Nivel A: Para 33 equipos y navegarán a 10 Kbs
delay_class 3 2
delay_parameters 32678/1024 26624/1024
delay_access 3 allow nivel_A
```

Una vez restricto la cantidad de ancho de banda. Se deniega el acceso a cualquier puerto diferente a los definidos en Safe_ports, para los usuarios de nivel de privilegios A.

```
http_access deny !Safe_ports
```

Ningún usuario que pertenezca el grupo al nivel de privilegio “A” limitado puede acceder al contenido establecido dentro de las acl’s archivos mime_types url_denycont_palabras.

```
http_access allow manager localhost

http_access deny manager
```

Se permite que todos los usuarios RADIUS de nivel de privilegios "B" limitado consigan ver el contenido de la paginas denegadas dentro del archivo acl url_deny.

```
http_access allow horario_almuerzo all peapLimitado url_deny

http_access allow peapTotal all !cont_palabras
```

Todos los usuarios del grupo de nivel de privilegios C Total tienen acceso a todas las páginas definidas por el servidor.

```
http_access allow peapnoLimitado all !archivos !mime_types
!url_deny !cont_palabras
```

Se permite solo el acceso a cachemgr desde localhost.

```
http_access allow localhost
```

Para que se registre los cambios se realiza la siguiente configuración del usuario y el grupo que utilizara squid:

```
cache_effective_user proxy

cache_effective_group proxy

coredump_dir /var/spool/squid
```

La última línea indica a SQUID donde guardar la cache.

Hasta aquí se realizan todas las líneas para la asignación y restricción de ancho de banda por nivel de privilegios, donde se configura todas las líneas del archivo de configuración de SQUID, asegurando añadir a los usuarios en los niveles de privilegios correspondientes de los Active Directory delay ports, y configurar el navegador de los usuarios con la dirección IP y el puerto del proxy.

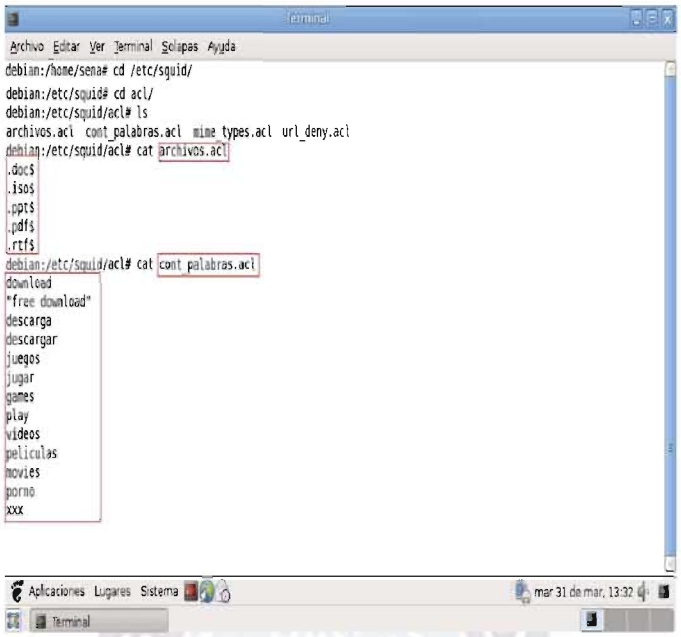

Figura 4.12. Configuración del servidor de gestión por nivel de privilegios
Fuente: Elaboración Propia

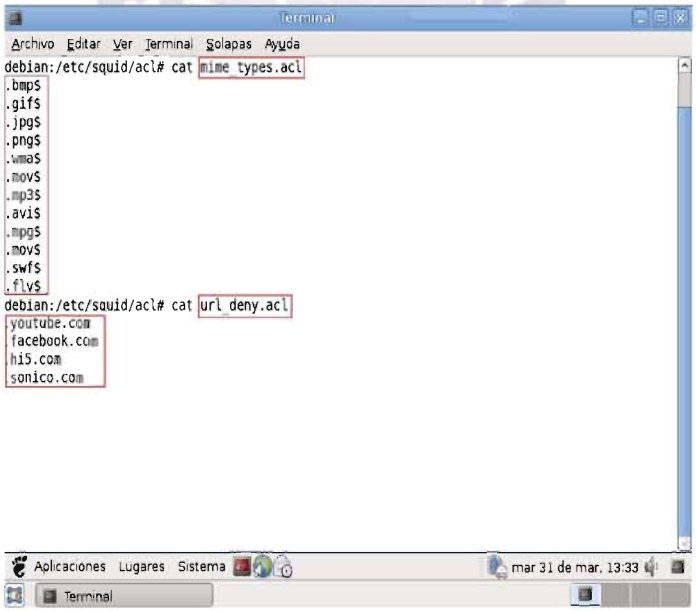

Figura 4.31. Tipos de acceso del servidor de gestión
Fuente: Elaboración Propia

4.6 Pruebas y resultados

La prueba de funcionamiento del modelo se realizó con los distintos componentes de la red, empezando por el servidor de seguridad y gestión, el punto de acceso, y por último los clientes computadoras portátiles con interface inalámbrica.

Para la instalación del servidor se requirió previo conocimiento de los recursos de software y hardware necesarios para configurar el sistema de seguridad inalámbrico de alto nivel, debido a que la implementación de la propuesta de esta tesis es una tecnología nueva.

Cada una de las partes usadas como el servidor, el punto de acceso y el cliente deben soportar un mismo protocolo y/o método de autenticación para que puedan trabajar entre sí al validar o restringir el acceso a la red, asignándole un ancho de banda. El segundo elemento, el punto de acceso inalámbrico fue configurado para ofrecer la autenticación WPA con servidor RADIUS; por último, las computadoras portátiles fueron instaladas y configuradas para efectuar la conexión.

Las primeras pruebas se realizaron con éxito, ver tabla 4.1resumen de pruebas, el cliente RADIUS de la computadora portátil logró ser autorizado y autenticado por la combinación del punto de acceso y el servidor de seguridad. La autenticación del protocoló CHAP versión MS-CHAPV2 por medio de un protocolo de túnel TLS (PEAP) logró realizarse como se puede observar en las figuras siguientes:

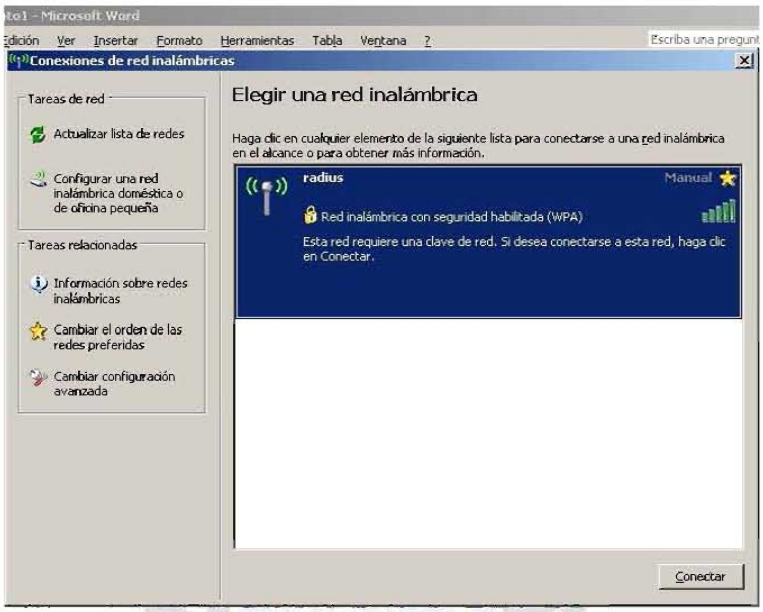

Figura 4.14. Prueba de conexión
Fuente: Elaboración Propia

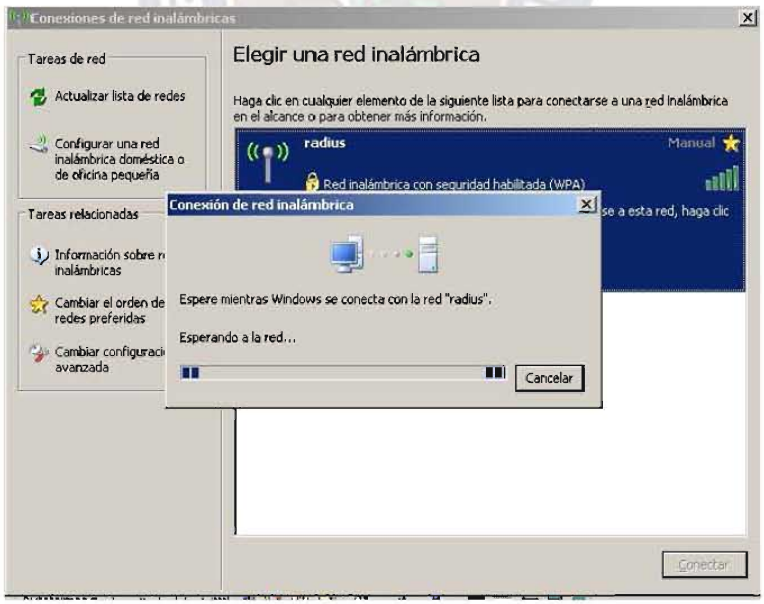

Figura 4.15. Conectándose al servidor radius
Fuente: Elaboración Propia

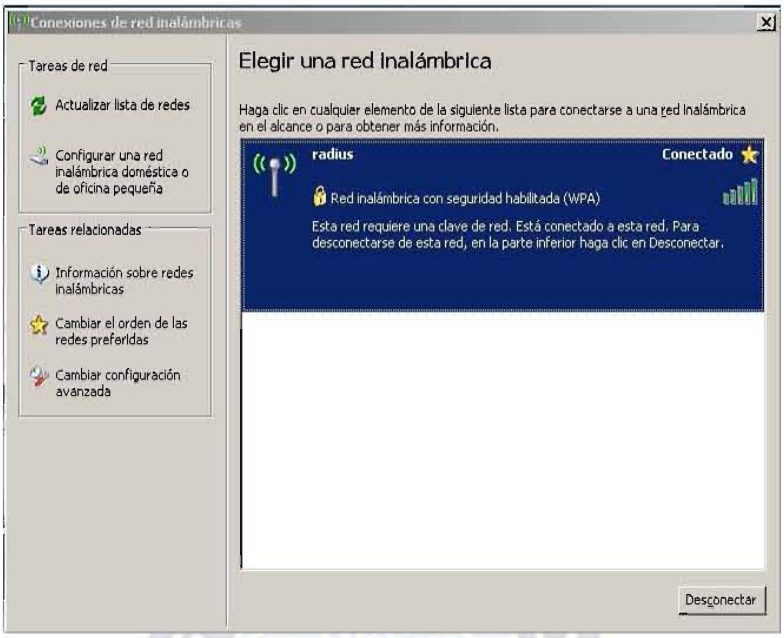

Figura 4.16. Conexión aceptada
Fuente: Elaboración Propia

Una forma de corroborar que se logró hacer la autenticación CHAP es revisando el servidor de seguridad. El servidor de seguridad maneja un registro de las peticiones de acceso que los clientes hacen a éste. Observando la ventana de comando en donde se ejecuto el servidor Freeradius se puede ver como se realizó la autenticación PEAP (CHAP) como se puede observar en la figura 4.15.

```
[peap] <<< TLS 1.0 Handshake [length 0106], ClientKeyExchange
[peap]     TLS_accept: SSLv3 read client key exchange A
[peap] <<< TLS 1.0 ChangeCipherSpec [length 0001]
[peap] <<< TLS 1.0 Handshake [length 0010], Finished
[peap]     TLS_accept: SSLv3 read finished A
[peap] >>> TLS 1.0 ChangeCipherSpec [length 0001]
[peap]     TLS_accept: SSLv3 write change cipher spec A
[peap] >>> TLS 1.0 Handshake [length 0010], Finished
[peap]     TLS_accept: SSLv3 write finished A
[peap]     TLS_accept: SSLv3 flush data
[peap]     (other): SSL negotiation finished successfully
SSL Connection Established
```

Figura 4.17. Conexión del servidor
Fuente: Elaboración Propia

Se explica a continuación el fragmento anterior para una mayor claridad.

Primera línea:

```
[peap] <<< TLS 1.0 Handshake [length 0106], ClientKeyExchange
[peap]     TLS_accept: SSLv3 read client key exchange A
```

Esta línea describe un fragmento de mensaje *Secure Socket Layer* versión 3 (SSLv3) con una longitud 0106 bytes fue que enviado del cliente al servidor, en este mensaje se comparte una llave del cliente que fue previamente solicitada por el servidor. Se puede hacer una correspondencia de este mensaje con el segundo saludo del protocolo que se realiza del cliente al servidor.

Segunda y tercera línea:

```
[peap] <<< TLS 1.0 ChangeCipherSpec [length 0001]
[peap] <<< TLS 1.0 Handshake [length 0010], Finished
[peap]     TLS_accept: SSLv3 read finished A
```

En estas líneas se puede ver que un paquete de 0001 bytes y de 0010 bytes del tipo SSLv3 fueron enviados del cliente al servidor, la primera línea envía un mensaje especial que consiste en una indicación de la técnica de cifrado utilizada y la segunda línea envía notifica al servidor que el saludo del cliente ha terminado.

Cuarta línea:

```
[peap] >>> TLS 1.0 ChangeCipherSpec [length 0001]
[peap]     TLS_accept: SSLv3 write change cipher spec A
```

Aquí se puede ver que el sentido de las flechas ha cambiado esto indicando que un paquete SSLv3, enviado del servidor al cliente corresponde a la contestación de la técnica de cifrado utilizada.

Quinta línea:

```
[peap] >>> TLS 1.0 Handshake [length 0010], Finished
[peap]     TLS_accept: SSLv3 write finished A
[peap]     TLS_accept: SSLv3 flush data
[peap]     (other): SSL negotiation finished successfully
SSL Connection Established
```

Aquí se indica que el tercer saludo del protocolo ha terminado.

Las pruebas de la gestión de ancho de banda se realizó con el control de tasas de transferencia basadas en los registros de datos de los usuarios, el punto de acceso y el servidor RADIUS que tienen un buen funcionamiento, ya que para realizar la gestión se debe contar con mecanismos de identificación indispensablemente, para la obtención de una red WLAN administrable y segura.

La prueba de gestión de ancho de banda, consistió en realizar el control durante la transferencia de archivos, el cual no rebasa de la cantidad de ancho de banda otorgado por nivel de privilegios entre equipos cuyo ancho de banda es regulado por el servidor de gestión, se descarga archivos de internet, la cantidad máxima de descarga es predeterminado por cada nivel de privilegios, los archivos se descargan a una velocidad de 10 Kb, 50Kb, y sin límite de velocidad respectivamente como se observa en las siguientes figuras:

Figura 4.18. Control de Gestión de la velocidad de internet nivel de privilegio "A"
Fuente: Elaboración Propia

Figura 4.19. Control de Gestión de la velocidad de internet nivel de privilegio "A"
Fuente: Elaboración Propia

Los resultados fueron exitosos ya que el nivel de privilegios "A" además de las restricciones de sitios, puertos o dominios no rebasó el ancho de banda otorgado por el servidor 10 Kb, el nivel de privilegios "B" logró la descarga de archivos sin sobre pasar su ancho de banda además de, algunas restricciones de sitios, puertos y dominios predispuestos por el administrador de 50 Kb, y el nivel de privilegios "C" no tubo restricción alguna.

La siguiente tabla describe como fue la conexión de algunas de las pruebas que se realizo para el sistema.

Tabla 3.2. Cantidad de usuarios por nivel de privilegios.

Resumen de Pruebas			
Equipo	**Descripción**	**Capacidad**	**Evaluación**
Primera computadora Laptop DELL s.o. Windows XP SP2 usuario1	Uso menor de red	El servidor acepto la conexión con 10 Kb de ancho de banda	Se trató de romper la seguridad del sistema con el programa Aircrack para redes WLAN, **sin éxito.,** por lo que se puede concluir que la primera prueba se logró con éxito.
Segunda Computadora Laptop DELL s.o. Windows XP SP2 usuario 2	Uso menor de red	El servidor acepto la conexión con 9 Kb de ancho de banda	Se trató de romper la seguridad del sistema con el programa Aircrack para redes WLAN, **sin éxito.,** por lo que se puede concluir que la primera prueba se logró con éxito.

Resumen de Pruebas			
Equipo	**Descripción**	**Capacidad**	**Evaluación**
Segunda Computadora Laptop HP compaq s.o. Windows Vista usuario 3	Uso promedio de red	El servidor acepto la conexión con 50 Kb de ancho de banda	Se trató de romper la seguridad del sistema con el programa Aircrack para redes WLAN, **sin éxito.,** por lo que se puede concluir que está prueba se logro con éxito, con respecto al ancho de banda se realizó la transferencia de información con éxito la cual se observa en el momento de descarga de archivos.
Segunda Computadora Laptop HP compaq s.o. Windows Vista usuario 4	Uso fuerte de red	El servidor acepto la conexión sin límite de ancho de banda	Se trató de romper la seguridad del sistema con el programa Aircrack para redes WLAN, **sin éxito.,** por lo que se puede concluir que está prueba se logró con éxito, con respecto al ancho de banda el inconveniente fue la restricción de sitios, este usuario podía acaparar una gran cantidad de ancho de banda.

Fuente: Elaboración Propia

4.7 Demostración de Hipótesis

El análisis de la hipótesis persigue una descripción de dos tipos la causal y la tautológica esta división se observa de la siguiente manera:
La forma causal se basa en la propuesta de tesis de maestría del autor García Escalante Elizabeth, 2007, misma que sigue los siguientes pasos:

Paso 1. El empleo de políticas de asignación de ancho de banda por usuario, mismo que corresponde al cap. 2 en el punto 2.3.1.2 políticas de gestión de redes de área local, y el cap. 3 en el punto 3.2.2 gestión de ancho de banda (políticas: (3.2.2.1) nivel de privilegios, (3.2.2.2.) regla de número de usuarios, (3.2.2.3) restricción de ancho de banda) respectivamente.

Paso 2. y mecanismos de identificación, responde al cap. 2 en el punto 2.2 Identificación y autenticación, y en el cap. 3.2.1 Autenticación y autorización

Paso 3. permite al administrador de una red de conexión inalámbrica gestionar el ancho de banda, responde al cap. 2 en el punto 2.3 Gestión de redes de área local, y en el cap. 3 y en punto 3.2.2 Gestión de ancho de banda.

Realizando el proceso de síntesis de los pasos analizados, la hipótesis planteada en el capítulo 1 menciona: "El empleo de políticas de asignación de ancho de banda por usuario y mecanismos de identificación, permite al administrador de una red de conexión inalámbrica gestionar el ancho de banda", está apoyado en un buen sustento teórico, que han sido plasmadas en el análisis y desarrollo del modelo de gestión de ancho de banda para una red WLAN (capítulo 4), por lo que es posible afirmar el valor tautológico de la hipótesis planteadas en el capítulo 1.

La forma tautológica se basa en:

Se tiene como notación de las premisas:

P_1: Políticas de asignación de ancho de banda.

P_2: Gestión de ancho de banda en una red de conexión inalámbrica.

Donde:

$$(P_1 \wedge P_2) \in P$$

Q: Mecanismos de identificación

Se tiene que:

$$P \wedge Q \rightarrow P$$

Este razonamiento es válido, desarrollando la tabla de verdad correspondiente:

P	Q	[(P ^ Q) → P]
1	1	1 **1** 1
1	0	0 **1** 1
0	1	0 **1** 0
0	0	0 **1** 0

Donde:

1 = [V] y 0 = [F]

Por lo tanto se concluye que la Hipótesis planteada es verdadera al obtener una tautología como resultado de la demostración.

CAPÍTULO 5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones recomendaciones.

Después de las pruebas realizadas, se puede concluir que el modelo presentó un comportamiento normal y satisfactorio ante los eventos de conexión y desconexión de usuarios en la red. La prueba del control de la tasa de transferencia, indica que el modelo está logrando el objetivo de regular el ancho de banda en una red de acuerdo al nivel de privilegio de cada usuario. Se observó que las pruebas realizadas sobre el modelo propuesto fueron exitosas y se obtuvo un comportamiento deseado, logrando los objetivos planteados en la presente tesis de grado.

Se pudo comprobar que se puede realizar la interacción entre el mecanismo de seguridad y el de gestión, ya que no se tienen estadísticas sobre la interacción de este tipo de procesos de identificación de usuarios asociados a una asignación de ancho de banda.

El empleo de los tres elementos importantes que forman diseño del modelo propuesto: (1) La Autenticación y Autorización, (2) La Gestión de Ancho de Banda, y (3) La Seguridad de red WLAN, consiguió un entorno de red inalámbrica administrable y con un alto nivel de seguridad, recuperando así la calidad del servicio que la red WLAN debe conseguir.

Además, de lograr los objetivos planteados, también se logro abarcar más sobre las tecnologías de seguridad inalámbrica y su empleo en una red inalámbrica sin mecanismos de seguridad ya que este tipo de tecnologías, no son conocidos y probados para su implementación lo cual también se logro en la presente tesis de grado.

Una vez realizada la investigación se pudo observar que muchos usuarios y administradores de redes carecen de conocimiento acerca de alguna gestión segura para redes inalámbricas de área local.

El desarrollo de esta nueva tecnología exige una mayor difusión de información para el conocimiento, ya que es insuficiente, lo cual ha generado una falta de conocimiento en la sociedad al no conocer acerca de este tipo de redes que a larga será indispensable en nuestros ambientes de trabajo como: universidades, instituciones, empresas, y colegios, donde se debería aplicar este modelo.

5.2 Trabajos futuros

Una buena aportación a este proyecto de tesis sería el diseño y la implementación de una interface en el lado del servidor de seguridad que ofrezca a los usuarios de los clientes inalámbricos la posibilidad de descargar la aplicación cliente, cuando intenten conectarse al entorno de red de seguridad.

Una recomendación es la de crear un programa que interactué con el servidor, para la asignación dinámica de ancho de banda.

REFERENCIAS BIBLIOGRÁFICAS

[KRUTZ & DIAN - 2007] Krutz, L. & Dian, Vines, The CISSP Prep Guide, Gold edition, Telecomunications and network segurity, Canada.

[KRUTZ & DIAN - 2003] Krutz, L. & Dian, Vines, The CISSP Prep Guide, Gold edition, Access Control Systems, Canada.

[CARPENTER & BARRETT - 2007] Carpenter, Tom, & Barrett, Joel, CWNA Prep Guide, Gold edition, Canada.

[BARTEN - 1998] Barten, A.P., Metodological Aspects of macroeconomic model construction, Cabay, Jezierski

[KEMPF - 2008] Kempf, James, Wireless Internet Segurity, USA.

[HERBAS – 2000] Herbas, Isaac, Metodologia de aplicación Teórica y practica en el campo del procemiento electrónico de datos, La Paz – Bolivia.

[ALCALDE & GARCIA – 2003], Alcalde, Eduardo, & Garcia, Jesús, introduccuión a la Teleinformatica, España.

[AMATO - 2000] Amato, Vito, Academia de Networking de Cisco Systems, ediciones Cisco Systems Cisco Press, Brasil.

[BAVARESCO - 1988] Bavaresco, A., Las técnicas de la investigación, Scout, Foresman and Co.

[MORALES - 2006], Morales, S.P. Administración de ancho de banda en redes, Mexico.

[NAVIA - 1997] Navia, Carlos, Elaboración científica del perfil de tesis, La Paz – Bolivia.

[SABINO - 1994] Sabino, Carlos, Como hacer una tesis, Caracas – Venezuela.

Sitios WEB consultados.

[IEEE – 2008] IEEE, norma IEEE 802.11 estandar,
http: //www. ieee.org/11
Pagina consultada el 10 septiembre de 2008

[KIOSK- 2008] WIFI, norma 802.1x,
http: //www. kiosk.com
Pagina consultada el 18 septiembre de 2008

[UMSA - 2008] Guía de tesis,
http://www.postgradoinformatica.edu.bo/
Pagina consultada el 25 septiembre de 2008

[RIU - 2008] Universidad de México, Implementación de Redes inalámbricas,
https://www.riu.unam.mx/
Pagina consultada el 06 octubre de 2008

[ENTERATE - 2008] Artículos de ancho de Banda en una red inalámbrica,
http://www.enterate.unam.mx/Articulos/2004/Abril/redes.htm
Pagina consultada el 20 octubre de 2008

[WLANA - 2008] Cobertura de una red inalámbrica de área local,
http://www.wlana.org/learn/educate.htm
Pagina consultada el 20 octubre de 2008

[WIKI - 2008] Ancho de banda,
http://es.wikipedia.org/wiki/Categor/ADa:Redes_inform
Pagina consultada el 04 noviembre de 2008

[NEO - 2008] Administración del ancho de banda en Bolivia,
http://www.neomedia.es/
Pagina consultada el 05 noviembre de 2008

[VPT – 2008] Artículos de redes inalámbricas,
http://www.virusprot.com/Redes-Inalambricas-Wifi/articulos-wireless-wifi/wifi-red-seguridad-errores.htm.
Pagina consultada el 10 noviembre de 2008

[WIFI - 2008] Las redes inalámbricas seguridad, cobertura, ancho de banda,
http://www.wi-fi.org/
Pagina consultada el 20 noviembre de 2008

[MANTANA - 2006], Mantana, C. Seguridad en redes WLAN, Mexico.

[Sandlin - 2003], Morales, Kevin. Certified Wireless Network Administrator. Segunda Edición. Estados Unidos: McGraw-Hill/Osborne,.

[Matthew - 2005], Gast, 802.11 Wireless Networks: The Definitive Guide. Estados Unidos: O'Reilly.

[Randall & Sosinski - 2004], Neil, y Barrie, Wireless Solutions. Estados Unidos: Pc Magazine, 2004.

[Hassell - 2008], Jonathan. RADIUS. Estados Unidos: O'Reilly. and 802.11i. Estados Unidos: Pearson Education, Inc.

[Fleck & Potter - 2005], Bob, y Bruce. 802.11 Security. Estados Unidos: O'Reilly,

[MARCA – 2004], Mariela, Control de seguridad y desempeño de una red Informática, La Paz Bolivia.

[VARGAS – 2003], Gabino, Control de Calidad de Servicio y rendimiento del proveedor de Internet, La Paz Bolivia.

[LUNA – 2008], Gonzalo, Administrador Proxy-Web & Proxy-Cache, La Paz Bolivia.

[SIRPA – 2007], Beatriz, Herramienta para la protección de procedimientos almacenados de base de datos, La Paz Bolivia.

[QUISBERTH – 2002], Roberto, Seguridad y protección en redes LAN conectadas a Internet, La Paz Bolivia.

ABREVIATURAS

WLAN	**Red inalámbrica de área local**
IP	**Protocolo de Internet**
VoIP	**Voz sobre el protocolo de Internet**
AAA	**Protocolo de autentificación, autorización y manejo de cuentas**
WAP	*Wireless Application Protocol*
WEP	*Wired Equivalent Privacy*
WiMAX	*Worldwide Interoperability for Microwave Access*
IEEE	*Institute of Electric and Electronic Engineers*
AP	**Punto de Acceso**
FTP	*File Transfer Protocol*
P2P	*Peer to peer*
RADIUS	*Remote authentication dial-in user service*
PAP	**Protocolo de autentificación por contraseña**
CHAP	**Protocolo de autentificación por desafío de saludo**
EAP	**Protocolo de autentificación extensible**
RFC	*Request for comment*
QoS	**Calidad del servicio**
TC	**Control de tráfico**
CCNA	*Cisco Certified Network Asociate*
WPA	*Wi-fi Protected Access*
SSID	*Service Set IDentifier*
GNU	*General Public License*
MAC	*Media Access Control*

GLOSARIO

- ***Administrador de Red***

Uso de sistemas o acciones para mantener, características o detectar los fallos de una red.

- ***Internet***

La Internetwork más grande del mundo, que conecta docenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real.

- ***Usuario de Internet***

Usuario Persona natural o jurídica que a través de los servicios de un ISP accede a la red.

- ***ISP***

Acrónimo de "Internet Service Provider" (Proveedor de servicios de Internet). Se trata de una compañía, persona natural o jurídica que proporciona acceso a Internet a particulares y empresas permitiéndoles navegar por la red, así como enviar y recibir correos electrónicos.

- ***Ancho de Banda***

Cantidad de información que se transmite en un tiempo determinado, de los recursos de una red.

- ***Red inalámbrica***

Permiten la conexión por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas, la transmisión y la recepción se realiza a través de antenas.

ANEXO C

COSTOS DE IMPLEMENTACIÓN

Descripción	Costo
Una Computadora con ambiente Linux, como servidor de autenticación y administrador de ancho de banda, con accesorios como: Microprocesador (2.8 Ghz.) Pentium IV (2.8 Ghz) Monitor (15") Memoria RAM (512 Mb.) Disco Duro (120 GB.) Tarjeta Madre (integrada ASROK) Tarjeta de Red Lectora de DVD"s Corta Picos Cables de red Otros accesorios	500 $us
Un Ruteador inalámbrico especificación D-Link DIR-300, como punto de acceso.	60 $us
Una tarjeta de red inalámbrica especificación D-Link IEEE e, b, a	30 $us
Computadora Laptop HP compaq con sistema operativo Windows Vista como nodo inalámbrico o suplicante	800 $us
Computadora Laptop DELL con sistema operativo Windows XP SP2, como nodo inalámbrico o suplicante	450 $us
Servicio de Internet del proveedor de Servicio ISP mes	30 $us
Total	1870 $us