UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

PROPUESTA DE GESTIÓN DE ANCHO DE BANDA PARA LA RED INALÁMBRICA DEL COLEGIO PRIVADO CHAMPAGNAT, AREQUIPA 2017

TESIS

PRESENTADA POR:

ELMER EMERSON, GUERRA MENDIVEL

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PUNO – PERÚ

2020

DEDICATORIA

Dedico el presente trabajo a mis padres Bonifacia, Elmer y a mi hermano Milton por su apoyo, consejos, comprensión y ayudarme en los recursos necesarios para estudiar.

A Rosario por su amor, compañía y apoyo para seguir adelante con nuestros proyectos.

AGRADECIMIENTOS

Agradezco a Dios por todas las oportunidades que me brinda.

Agradezco a mi presidente de tesis D.Sc. Elmer Coyla Idme y a mi asesor M.Sc. Edgar Holguin Holguin por su apoyo y motivación para hacer posible este trabajo de tesis.

Así mismo agradezco a los docentes de la escuela profesional de Ingeniería de Sistemas por las enseñanzas compartidas.

Gracias a la vida por este nuevo triunfo.

¡Gracias!

ÍNDICE GENERAL

CAPÍTULO III

MATERIALES Y MÉTODOS

TEMA: Gestión, seguridad y auditoría de sistemas de información

ÁREA: Informática

FECHA DE SUSTENTACIÓN 6 DE ENERO 2020

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ACRÓNIMOS

WEP: (Wired Equivalent Privacy o Privacidad Equivalente a Cableado)

RC4: (Rivest Cipher 4 o Cifrado rivest 4)

WPA: (Wi-Fi Protected Access o Acceso Wi-Fi Protegido)

TKIP: (Temporal Key Integrity Protocol o Protocolo de Integridad de Clave Temporal)

EAP: (Extensible Authentication Protocol o Protocolo de autenticación extensible)

AP: (Access Point o Puntos de Acceso)

AES: (Advanced Encryption Standard o Estándar de Cifrado Avanzado)

NIC: (Network Interface Controller o Tarjeta de Interfaz de Red)

TLS: (Transport Layer Security o Seguridad de la Capa de Transporte)

WLAN: (Wireles Local area network o red de área local inalámbrica)

MS-CHAP: (Microsoft Challenge Handshake Authentication Protocol o Microsoft del protocolo de autenticación de contraseñas de cifrado por desafío mutuo)

SSID: (Service Set Identifier o Identificador de servicios)

RESUMEN

Al desarrollar una red inalámbrica de área local, la propuesta de gestión de ancho de banda en la cual se direcciona la investigación de la administración del ancho de banda segura, haciendo uso de soluciones basadas en software libre, la cual nos asegura un óptimo rendimiento en el uso del ancho de banda, creando así un ambiente de seguridad para el administrador y los usuarios conectados a la red inalámbrica mediante el proceso de autenticación y control de entradas de los usuarios, que estén vinculados a un nivel de privilegios, brindándoles así una buena recepción de señal y dejar de lado la incertidumbre que en cualquier momento alguien ajeno a la red inalámbrica aprovechado su ancho de banda se conecte. Esta alternativa de solución desarrolla tres elementos importantes, la Autenticación y Autorización, la Gestión de Ancho de Banda y la Seguridad de red WLAN. Para la respectiva implementación de este modelo se apoyó, con la autenticación y autorización, incorporando el protocolo AAA y el método CHAP, los cuales identifican a los usuarios, la presente gestión de ancho de banda ha sido implementada bajo una serie de políticas de asignación de ancho de banda (niveles de privilegios, regla de número de usuarios, y restricción del ancho de banda), ya que se estableció su óptimo rendimiento del uso de ancho de banda; y la seguridad a la red WLAN, donde se interactúa con el protocolo WPA2, método EAP-PEAP y certificados que determinan un alto nivel de seguridad en el desempeño de redes inalámbricas. En el presente trabajo de tesis se realizó la investigación, con la respectiva construcción, implementación y análisis de la propuesta de gestión seguro el cual hizo uso de los procesos antes mencionados para poder brindar un entorno de red inalámbrica fácil de administrar y con un elevado nivel de seguridad, recuperando así la calidad del servicio que la red WLAN debe conseguir.

Palabras Clave: ancho de banda, WLAN, Radius, AAA

ABSTRACT

When developing a wireless network of local area, the proposal of bandwidth management in which the investigation of the administration of the safe bandwidth is directed, making use of solutions based on free software, which assures us an optimum performance in the use of bandwidth, thus creating a security environment for the administrator and users connected to the wireless network through the process of authentication and control of user inputs, which are linked to a privilege level, thus providing them with a good Signal reception and set aside the uncertainty that at any time someone outside the wireless network took advantage of your bandwidth to connect. This solution alternative develops three important elements, Authentication and Authorization, Bandwidth Management and WLAN Network Security. For the respective implementation of this model, with the authentication and authorization, it was supported by incorporating the AAA protocol and the CHAP method, which identify the users, this bandwidth management has been implemented under a series of allocation policies bandwidth (privilege levels, number of users rule, and bandwidth restriction), since its optimal bandwidth usage performance was established; and security to the WLAN network, where it interacts with the WPA2 protocol, EAP-PEAP method and certificates that determine a high level of security in the performance of wireless networks. In this thesis work, the investigation was carried out, with the respective construction, implementation and analysis of the safe management proposal which made use of the aforementioned processes to be able to provide a wireless network environment that is easy to administer and with a high level security, thus recovering the quality of service that the WLAN network must achieve.

Keywords: bandwidth, WLAN, Radius, AAA

CAPÍTULO I

INTRODUCCIÓN

El internet y las comunicaciones tienen un papel muy importante, para las empresas, instituciones educativas, así como para las personas, ya que estas necesitan estar interconectadas, para que puedan realizar diversos procesos.

La redes inalámbricas viajan por ondas y se puede hacer su uso con computadoras que no estén en un mismo lugar, estas redes pueden instalarse en diversos lugares y permitir la conexión, así mismo estas redes inalámbricas como las tradicionales necesitan aplicaciones para poder ser usadas y se requiere gestionar el ancho de banda, para mejor usabilidad de los usuarios y desempeño de la red inalámbrica.

La presente investigación se encuentra dividida en cuatro capítulos: En el CAPITULO I: Contiene la descripción, justificación del problema y los objetivos de la investigación. En el CAPITULO II: Presenta los antecedentes de la investigación, sustento teórico, glosario de términos e hipótesis de la investigación. En el CAPITULO III: Detalla el tipo, diseño, población y muestra de la investigación, también la ubicación y descripción de la población y en el CAPITULO IV: Desarrollo del análisis de la investigación, conclusiones, recomendaciones y anexos.

1.1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad va en incremento el uso de redes inalámbricas ya que en algunas universidades, colegios, instituciones esta es de libre acceso y deja a cualquier usuario que pertenezca o no acceder a ella y poder hacer uso de los servicios sin ninguna seguridad de información este es uno de los problemas en el uso de redes inalámbricas.

En la institución educativa Champagnat es un ejemplo el uso de internet; donde el uso de este recurso debería ser con fines académicos y de investigación. El uso de algunas aplicaciones puede prestarse a duda en su uso académico como las de mensajería instantánea, pues nos permite comunicarnos con otras personas en temas relacionados a proyectos, como también para comunicarse con amigos por temas más personales. La opción que tienen los usuarios para poder descargar archivos de internet es otro problema ya que estos pueden ser de temas académicos como para usos personales.

Hacer uso con fines personales de las redes inalámbricas de la institución educativa hace que disminuya el desempeño de la red y ocasione malestar a los usuarios que la usan para temas educativos.

Los usuarios que hacen uso de aplicaciones fuera del contexto educativo generan que aumente el ancho de banda y donde no hay un sistema de regulación y seguridad, que controle los servicios de la red inalámbrica va a generar malestar en los usuarios que realmente hagan uso de este servicio con fines académicos.

El problema principal encontrado en la institución educativa Champagnat, es el uso de servicios de la red sin medidas de control y seguridad, así como también no existe regulación y no se asigna el ancho de banda por niveles de usuario, lo que genera un desorden en la competencia por disponibilidad del servicio disminuyendo su calidad.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo será la gestión de ancho de banda para la red inalámbrica del colegio privado Champagnat, Arequipa 2017?

1.3. HIPÓTESIS DE LA INVESTIGACIÓN

La propuesta de asignar ancho de banda por usuario, permitirá gestionar el ancho de banda de la red inalámbrica de la institución educativa Champagnat, Arequipa 2017.

1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

El proyecto de tesis surge por la necesidad de la institución educativa Champagnat de contar con las herramientas de gestión de ancho de banda así como la seguridad en las redes inalámbricas, ya que con ellas se va a tomar decisiones para poder solucionar los problemas de administración y seguridad que genera la demanda del uso de redes inalámbricas por los usuarios de la institución educativa.

Con el desarrollo de esta propuesta se podrá solucionar los problemas de los usuarios y del personal que administra esta red y poner por niveles a los usuarios para evitar el congestionamiento y dar banda ancha según la necesidad de cada usuario conectado y generando un ambiente más seguro.

En cuanto a los beneficios económicos no generará ningún costo ya que no tienen que pagar por licencias ya que es un software libre y lo cual implica independencia y los desarrolladores pueden tener acceso al código fuente.

El aporte práctico del presente trabajo es brindar a los administradores la herramienta que gestione el ancho de banda de las redes inalámbricas y la seguridad en las diferentes instituciones y se pueda brindar el servicio a todos los usuarios de la comunidad educativa.

1.5. OBJETIVOS DE LA INVESTIGACIÓN

1.5.1. Objetivo general

- Desarrollar una propuesta de gestión de ancho de banda para la red inalámbrica del colegio privado Champagnat, Arequipa 2017

1.5.2. Objetivo específicos

- Habilitar un sistema de usuarios que utilice protocolo de autenticación y manejo de cuentas (AAA) como la seguridad en un ambiente inalámbrico del colegio privado Champagnat, Arequipa 2017
- Gestionar el ancho de banda para usuarios registrados en la red con un nivel de privilegio del colegio privado Champagnat, Arequipa 2017
- Generar conexión entre mecanismo de autenticación y administrador de ancho de banda del colegio privado Champagnat, Arequipa 2017
- Implementar mecanismos de identificación y políticas de ancho de banda en el colegio privado Champagnat, Arequipa 2017.

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Según (Pilozo Campozano & Zambrano Balladares, 2013) en su investigación titulada: "Estudio del Ancho de Banda para el tráfico de Redes WAN de los ISP, con estudiantes de la Universidad Politécnica Salesiana Sede Guayaquil carrera Ingeniería de Sistemas, mediante la implementación de una página web" concluyendo que En general muchos estudiantes utilizan su servicio de Internet para muchas aplicaciones, aunque lo más preocupante es que desconocen la velocidad que ellos tienen, parece que solo les importa recibir el servicio, más no les interesa saber en qué aspectos les beneficia las normas SVA.

Según (Chuquicondor Requena, 2017) en su investigación titulada: "Propuesta Metodológica Para La Gestión Y Administración Del Ancho De Banda D Comunicaciones En El Campus De La Universidad Nacional De Piura – 2016."Y con los resultados obtenidos se concluye que el desarrollo de la Gestión y Administración del ancho de banda de comunicaciones en el campus de la Universidad Nacional de Piura, resulta beneficioso para mejorar la conectividad dentro del campus universitario, el mismo que permitirá ingresar y trabajar más rápido en los diferentes sistemas que maneja la universidad, así como la navegación por internet y además que los usuarios puedan realizar todos sus trámites sin ningún inconveniente, ya sean administrativos y/o académicos, en un menor tiempo, con una conectividad constante y fluida, quedando demostrado que la hipótesis es correcta.

Según (Albujar Moreno, 2017)en su investigación titulada: "Diseño De Un Sistema De Seguridad De Red Basado En La Integración De Los Servidores Radius – Ldap En Linux Para Fortalecer El Acceso De La Red De La Clínica Millenium Chiclayo 2016"

concluyendo que El presente diseño de Sistema de seguridad de red, cumple con el objetivo principal del trabajo pues refuerza el control de acceso a usuarios de la Clínica Millenium – Chiclayo, a partir de herramientas de software libre para la autenticación en redes inalámbricas y a su vez se reutilizó para autenticar equipos con conexión cableada.

Según (Espinoza Arana, 2018) en su investigación titulada: "Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante RADIUS" concluyendo que Los parámetros que utilizan los procesos de Autenticación y Autorización al acceso de la red local, permiten tener un control más detallado del usuario llegando a identificar el grado de procedencia del invitado. Permitir al sistema inalámbrico el uso del protocolo RADIUS con la aplicación eduroam brinda un valor agregado a la institución catalogándola como una Institución de confianza a nivel internacional, y a su vez los usuarios dispondrán de acceso a este servicio fuera de la institución de origen. La percepción de los usuarios al hacer uso de la aplicación eduroam permitió conocer las bondades inherentes tales como el Acceso a entidades externas y sus recursos disponibles, control de tráfico para el administrador de Red de la Institución y libre de costos fuera de la institución de origen a Internet.

2.2. MARCO CONCEPTUAL

2.2.1. Redes inalámbricas

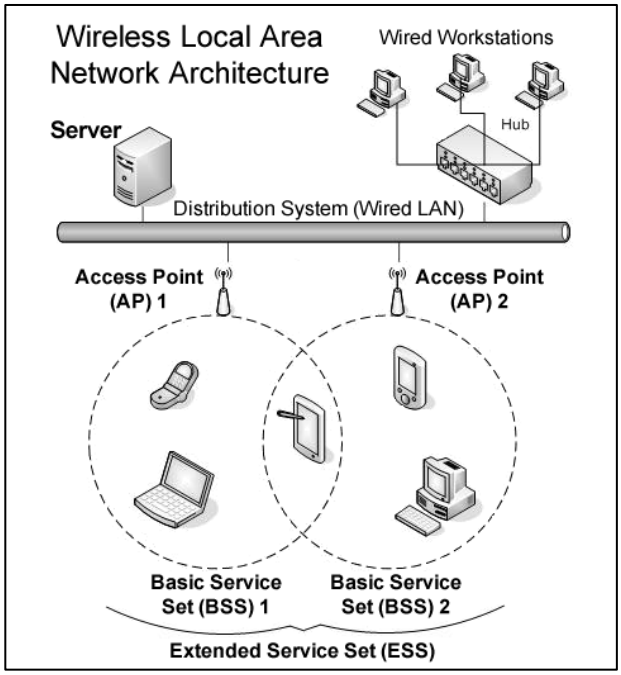
El conjunto de equipos de cómputo que están interconectados por una transmisión no guiada con ondas electromagnéticas de radio e infrarrojo en lugar de tener un cableado estándar que hace referencia a un cableado estructurado son las redes inalámbricas Wireless network (Andreu, 2011).

La transmisión y la recepción se efectúan a través de antenas. Normalmente el emisor tiene una sola antena, pero puede tener varias, ya que existen sistemas, que emplean dos,

tres e incluso hasta cuatro antenas. Unas antenas se usan para la emisión, otras para la recepción y normalmente, la mayoría de las veces, la misma antena permite actuar de ambos modos. También podemos trabajar con antenas intermedias (alcanzando distancia de pocos metros) o repetidoras (alcanzando decenas de kilómetros) (Andreu, 2011, pág. 213).

Las transmisiones de las redes inalámbricas hacen que los dispositivos estén conectados sin inconvenientes para la recepción y envió de datos a una determinada distancia en metros o kilómetros, es así que la instalación de estas redes no necesita de cambios muy significativos como sucedería en el cableado convencional. La figura 1 es una red mixta, alámbrica e inalámbrica. (Andreu J. , 2011)

Figura N° 1: Red mixta



Fuente: Recuperado http://www.atc.uniovi.es

La red inalámbrica dependiendo si se estudia un segmento o su totalidad se debe entender que es parte de una red mixta los diversos medios de transmisión se interconectan como por ejemplo las ondas de radio, fibra óptica, etc. Hace suponer en considerar diversos

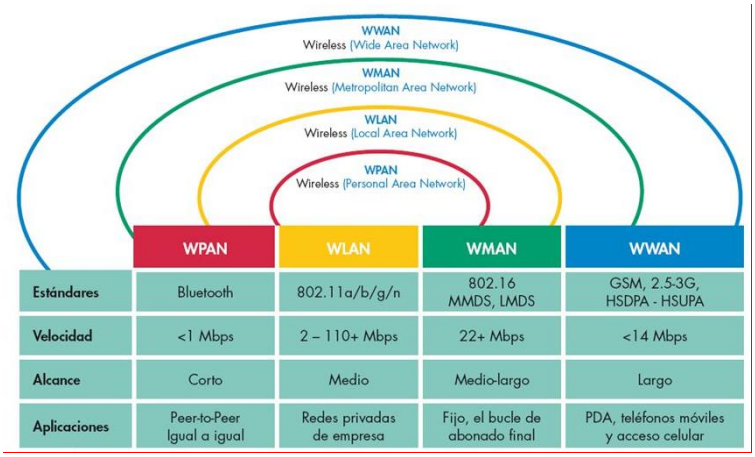
dispositivos los cuales permiten la conectividad y las posibles diferencias de sus tecnologías pero se debe tener en cuenta que la instalación y el desempeño son diferentes tanto para la fibra óptica como por ondas de radio. (Andreu, Pellejero, & Lesta, 2006)

Las diferencia principales entre las redes inalámbricas y cableadas es que hay mayor interferencia en las redes inalámbricas por onda de radio. Es por eso que al usar el aire para transmitir las ondas de radio esta se encuentra expuesta a sufrir interferencia en el ambiente por la humedad las tormentas eléctrica entre otras y la cobertura que se ofrece es proporcional a la potencia de la antena pero los estándares IEEE son muy importantes para poder regular la potencia y frecuencia que se utilizara en la transmisión. (Cabezas Granado & Gonzales Lozano, 2010)

Los costos de los equipos que nos permiten la conectividad comenzaron a disminuir esto hizo que las redes inalámbricas puedan tener más presencia en diferentes aspectos de nuestra vida como en lugares públicos como aeropuertos, escuelas restaurantes, hoteles entre otros.

Las redes inalámbricas son una alternativa para aquellos lugares donde no se puede tener acceso a estas redes de forma cableada, también esta implementada para espacios geográficos grandes pero con un gran ancho de banda y no solo estar enfocada en áreas pequeñas.

Figura N° 2: Comparación de redes



	WPAN	WLAN	WMAN	WWAN
Estándares	Bluetooth	802.11a/b/g/n	802.16 MMDS, LMDS	GSM, 2.5-3G, HSDPA - HSUPA
Velocidad	<1 Mbps	2 – 110+ Mbps	22+ Mbps	<14 Mbps
Alcance	Corto	Medio	Medio-largo	Largo
Aplicaciones	Peer-to-Peer Igual a igual	Redes privadas de empresa	Fijo, el bucle de abonado final	PDA, teléfonos móviles y acceso celular

Fuente: Recuperado https://slideplayer.es/slide/5473520/

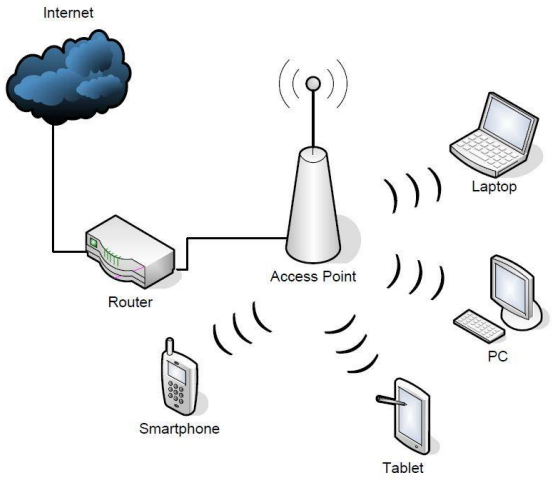
2.2.1.1.1. Redes WLAN

Las redes WLAN Wireless Local Área Network, Red Inalámbrica de Área Local, estas redes inalámbricas cubren distancias de 10 a 100 metros, hay una menor potencia de transmisión por ser de cobertura pequeña, y se puede utilizar bandas de frecuencia sin licencias. Este tipo de redes inalámbricas, Se distinguen distintas tecnologías inalámbricas en función del área de cobertura de la red, de esta manera la tecnología WLAN es aquella con área de cobertura en entorno local. (Andreu J. , 2011).

Esta red inalámbrica para poder comunicarse entre los dispositivos utiliza ondas de radiofrecuencia y es un sistema más flexible y puede ser una mejor alternativa que las redes cableadas.

La figura 3 muestra la red WLAN

Figura N° 3: Red WLAN



Fuente: Recuperado https://pdfs.semanticscholar.org/

Las redes WLAN se han incorporado rápido en el mercado por sus ventajas como la movilidad, la flexibilidad, se solucionan con un bajo costo, instalación sencilla y permite a los usuarios acceder con rapidez y sencillez. (Garbarino, 2012)

El objetivo de las redes inalámbricas WLAN es dar la facilidad que no podemos tener con el sistema cableado, también pueden ser un buen complemento para las redes cableadas y brindar al usuario mayor movilidad y poder estar conectado en distintos lugares.

2.2.1.1.2. Topología de la red WLAN

Punto de acceso: Es un elemento que gestiona las estaciones inalámbricas y puede comunicarse con otras redes. Es un bridge de dos puertos que comunica los equipos de su celda de cobertura entre sí y con otras redes que estén conectadas haciendo de puente entre las redes.

Estaciones inalámbricas STA: Son dispositivos de usuarios que cuentan con adaptadores que realizan las funciones de las tarjetas de Ethernet, adaptando las tramas Ethernet que

genera el dispositivo a las tramas del estándar inalámbrico y viceversa, posibilitando la transmisión transparente de la información. (Andreu, Pellejero, & Lesta, 2006)

2.2.1.1.3. Modos de funcionamiento de una red WLAN

Modo IBSS: Permite interconexión entre dispositivos de usuario sin necesidad de un punto de acceso, cada estación inalámbrica se conecta directamente con las otras estaciones de red, las funciones de coordinación se asumen de forma aleatoria, el tráfico de información se lleva a cabo entre los equipos conectados. (Andreu, Pellejero, & Lesta, 2006)

Modo BSS: Permite conexiones de las estaciones inalámbricas de un punto de acceso que gestiona las conexiones, todo el tráfico desde y hacia las estaciones inalámbricas, se ve que hay una clara perdida de eficiencia cuando dos estaciones dentro de un mismo BSS quieren comunicarse entre sí. (Andreu, Pellejero, & Lesta, 2006)

Modo ESS: Está formado por un conjunto de BSS asociados mediante un sistema de distribución formando una sub red única. Teniendo en cuenta que la mayoría de las redes WLAN tendrán la necesidad de conectarse a las redes LAN cableadas y este será el modo de operación de las redes WLAN con más de un AP. (Andreu, Pellejero, & Lesta, 2006)

2.2.1.2.Estándares de capa física y de enlace

A continuación se describen los distintos estándares de capa física y de enlace, que componen la familia IEEE 802.11.

IEEE 802.11: Estándar que fue ratificado en julio de 1997. Funciona en la banda 2,4 GHz con velocidades de transmisión máxima de 2Mbps. Incluye velocidades de transmisión de 1 Mbps y 2 Mbps, dependiendo de la distancia entre el punto de acceso y la estación inalámbrica y de las condiciones de utilización del canal, utiliza las modulaciones FHSS

(Frecuency Hoping Spread Spectrum) y DSSS (Direct Spread Spectrum) en la capa de enlace y DBPSK (Differential Binary PKeying), DQPSK (Diferencial Quadrature Phase Shift Keying) y GFSK (Frequency Shift Keying) en la capa física. Este estándar utiliza el protocolo CSMA/CA como método de acceso, la primera barrera que s eencontro en este estándar fue la baja velocidad en la transmisión de datos en consecuencia se trabajó un nuevo estándar. (Andreu J. , 2011)

IEEE 802.11b: Estándar que se ratificó en 1999 y de momento es el más utilizado en la redes WLAN europeas, este estándar extiende el uso del DSSS del IEEE 802.11 hasta obtener velocidades máximas de transmisión de datos de 11 Mbps. Únicamente utiliza modulación DSSS en la capa enlace y CCK (Complementary Code Keying) en la capa física. Tiene el mismo método de acceso CSMA/CA. (Andreu J. , 2011)

IEEE 802.11a: Una de sus características es que llega a alcanzar velocidades de hasta 54 Mbps gracias a la utilización de OFMD (Orthogonal Frequency-division multiplexing) con 52 subportadoras, este estándar opera en la banda 5GHz. (Andreu J. , 2011)

IEEE 802.11g: Este estándar garantiza la compatibilidad con los dispositivos IEEE 802.11b y ofrece una velocidad de hasta 54 Mbps al igual que el estándar IEEE 802.11a funciona dentro de la banda de frecuencias de 2,4 GHz con modulación DSSS y OFDM, el esquema de modulación es CCK. (Andreu J. , 2011)

Figura N° 4: Estándares

	IEEE 802.11	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g
Fecha	1997	1999	2000	2003
Banda	2,4 GHz	2,4 GHz	5,8 GHz	2,4 GHz
Velocidad de transmisión	1, 2 Mbps	1, 2, 5.5 y 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Modulación	DHSS, FHSS	DHSS	OFDM	OFDM
Compatibilidad		Compatible con IEEE 802.11	No es compatible con ningún otro estándar	Compatible con IEEE 802.11 y IEEE 802.11b

Fuente: (Andreu J. , 2011)

IEEE 802.11n: Este estándar es una propuesta de mejora del estándar IEEE 802.11b, su principal objetivo es ofrecer una mayor velocidad de transmisión de la redes WLAN con un objetivo inicial de alcanzar los 100 Mbps. (Andreu J. , 2011)

IEEE802.11c: Este estándar provee información necesaria para asegurar el correcto funcionamiento de las operaciones en modo bridge en los dispositivos inalámbricos. (Andreu J. , 2011)

IEEE 802.11d: Este estándar es un complemento del estándar IEEE 802.11 para promocionar el uso a escala mundial, de las redes WLAN, permite a los puntos de acceso comunicar información sobre los canales radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios sus especificaciones son importantes en banda de 5GHz ya que esta banda varia en países. (Andreu J. , 2011)

IEEE 802.11e: Su objetivo es proporcionar QoS (Calidad de servicio) en redes WLAN, es un estándar con modificaciones en el sub nivel MAC de la capa enlace, y es de aplicación a los estándares físicos IEEE 802.11a, b y g su finalidad es proporcionar clases de servicios con niveles gestionados para aplicaciones de datos, voz y video. Este estándar ha sido aprobado en el 2005 y define hasta 8 clases de servicios los cuales se pueden conseguir mediante uno de los mecanismos de acceso al medio que permiten priorizar el tráfico de la red WLAN. (Andreu J. , 2011)

IEEE 802.11f: Este estándar nace con el objetivo de lograr la interoperabilidad de puntos de acceso IEEE 802.11b/g dentro de una red WLAN con puntos de acceso de diferentes fabricantes dentro de la misma red. El estándar define un protocolo para la comunicación entre puntos de acceso que permite la transferencia de usuarios entre puntos de acceso El protocolo IAPP (Inter Access Points Protocol) es el encargado de transferir la información

de contexto para permitir el traspaso de ususarios entre punto de acceso. (Andreu J. , 2011)

IEEE 802.11h: El principal objetivo de este estándar es cumplir los reglamentos europeos para redes WLAN que emplean la banda de frecuencias de 5GHz y que son compatibles con los estándares IEEE 802.11a. Los reglamentos europeos para la banda 5GHz requieren que los productos tengan control de la potencia de transmisión (TPC) y selección de la frecuencia dinámica (DFS). (Andreu J. , 2011)

IEEE802.11i: Este estándar se centra en cubrir aspectos de seguridad en redes WLAN basadas en alguno de los estándares IEEE 802.11 a, b y g. Proporciona una alternativa al mecanismo WEP original disponible para ofrecer seguridad en este tipo de redes, ofreciendo nuevos métodos de cifrado y procedimiento de autenticación. (Andreu J. , 2011)

2.2.1.3.Componentes de una red WLAN (dispositivos).

Los componentes de una red WLAN, son similares a los de una red cableada y se describen cada uno de ellos:

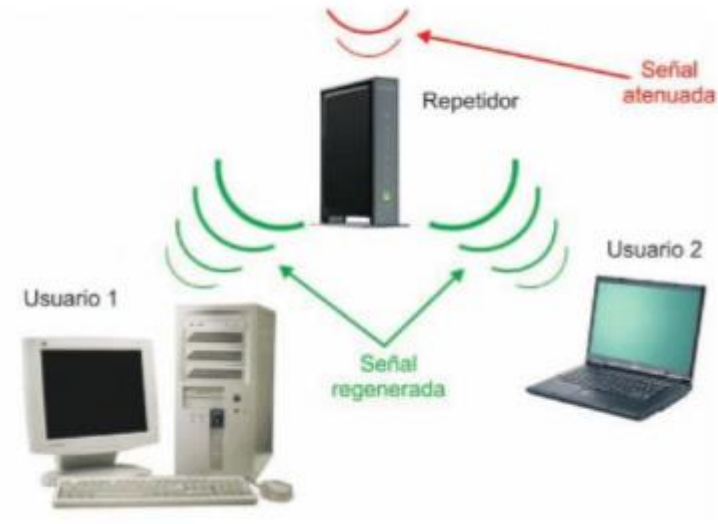
Adaptadores de red: También llamado NIC, se instalan en los sistemas informáticos que quieren conectarse a la red inalámbrica, disponen de una pequeña antena, puede instalarse mediante una tarjeta en una de las ranuras de expansión de la placa base o mediante un dispositivo USB. (Valdivia Miranda, 2005)

Figura N° 5: Adaptador de red

Fuente: (Valdivia Miranda, 2005)

Repetidores: Estos dispositivos permiten que se extienda el área de cobertura de una red inalámbrica ya que las ondas que viajan por aire van perdiendo potencia, y la señal puede no llegar a los dispositivos alejados del punto de acceso con los repetidores se regenera y amplifica la señal. (Valdivia Miranda, 2005).

Figura N° 6: Repetidor de red



Fuente: (Valdivia Miranda, 2005)

Puntos de acceso (Access Point): Son el centro neurálgico de las redes, permite conectar los dispositivos inalámbricos entre sí y con la red cableada, actúan como concentradores inalámbricos, que están en el mercado como enrutadores que tienen varios interfaces,

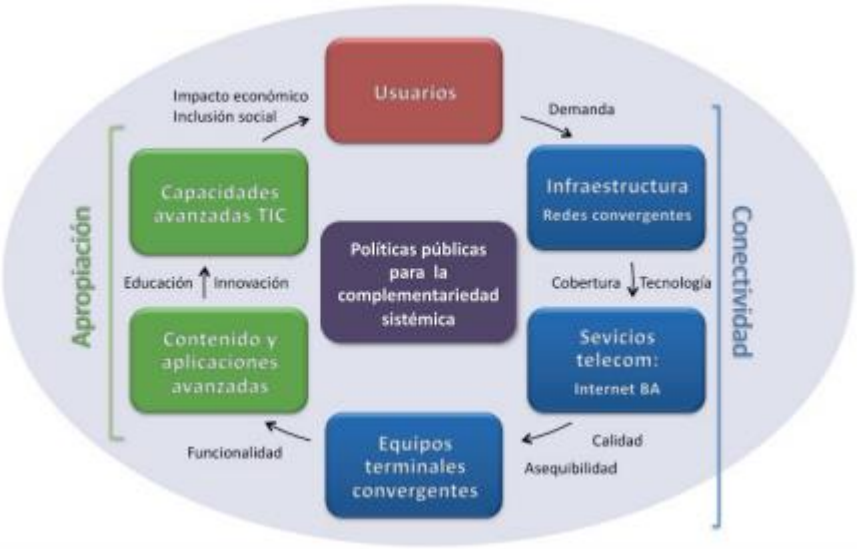
entre los cuales uno de ellos es el interfaz inalámbrico que hace punto de acceso a todos los dispositivos inalámbricos que quieran conectarse en la red. (Valdivia Miranda, 2005).

Puentes inalámbricos: Son elementos software o hardware que permiten la interconexión de dos redes que pueden usar distinta arquitectura de red o distinto protocolo, el puente hace de intermediario entre las redes que conecta. (Valdivia Miranda, 2005).

2.2.1.4.Ancho de banda

El progreso tecnológico en el acceso de banda ancha está transformando significativamente el paradigma digital. Por su capacidad de transmitir grandes volúmenes de datos y viabilizar el uso de aplicaciones más avanzadas, la banda ancha materializa las potencialidades de crecimiento económico y desarrollo social de la revolución digital, dando origen a un sistema en el que sus componentes se desarrollan en un ambiente sustentado en esta tecnología. El progreso técnico asociado es vertiginoso y transforma a los componentes del sistema, agregando múltiples dimensiones y complejidad a la brecha digital. (Jordan, Galperin, & Peres, 2010)

Figura N° 7: Brecha digital de banda ancha



Fuente: (Dordoigne, 2018)

En infraestructura, el progreso técnico plantea desafíos en términos de cobertura y tecnología de redes. La convergencia de redes y servicios y el crecimiento de tráfico en Internet impulsan el despliegue de tecnologías de última generación con mayor capacidad de transmisión, que demandan más recursos de red y una gestión más inteligente del tráfico. Estas redes soportan la prestación de múltiples servicios mediante banda ancha, lo que plantea la necesidad de mejorar tanto el acceso al abonado como las redes de distribución (backhaul). (Jordan, Galperin, & Peres, 2010)

La existencia de diversas tecnologías de acceso a banda ancha con un amplio diferencial de velocidades de conexión (entre 256 kbps y 100 Mbps) es un nuevo aspecto a considerar en la brecha digital además del tradicional problema de la cobertura. (Jordan, Galperin, & Peres, 2010)

Para un mejor uso del ancho de banda se debe desarrollar contenidos en línea que se adapten a los dispositivos que tienen acceso y den mayor valor a la red inalámbrica, en la actualidad hay mayor innovación en el ámbito de diversión, pero disminuye en otras áreas como en educación, en el mundo laboral.

2.2.1.4.1. Características del ancho de banda

- Finito, ya que su uso es de acuerdo a las necesidades del usuario.
- El ancho de banda no es gratis ya que se tiene que obtener de algún proveedor, para los cual la administración de este recurso debe ser optimo, por eso se deben establecer las políticas adecuadas.
- Siempre existe demanda por su uso ya que en la actualidad hay mayor cantidad de aplicaciones y la competencia por el ancho de banda cada vez es mayor.

El ancho de banda está relacionado directamente con la potencia, cada vez que los dispositivos se alejan hay menor señal, ya que disminuye la potencia.

El ancho de banda alcanza un nivel ideal cuando hay buena señal, cuando las políticas de distribución son adecuadas ya que hay un equilibrio de los usuarios que usan el recurso, puede haber necesidad de aumentar el ancho de banda por la gran cantidad de información de datos que se transmiten, para un mejor desempeño.

Cuando se habla de ancho de banda, también se debe tomar en cuenta las tasas de transferencia, para eso debemos tomar en cuenta la cantidad de usuarios de la red, saber el ancho de banda disponible y conocer que servicios ofrece la red.

Tabla N° 1: Tasas de transferencia

PLAN	EQUIVALENTE	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

Elaboración propia

2.2.2. Protocolos de seguridad de red AAA

El aumento de los servicios en internet, exige que los routers y los servidores de acceso a red (NAS) tengan una gestión más sofisticada, la mayor parte de estos servicios, necesitan un protocolo AAA, para poder facilitar la descarga de información.

Se ha hecho uso del protocolo RADIUS para poder proporcionar servicios AAA en PPP conmutado (point-to-point Protocol), localizado en el nivel de enlace de datos de la pila TCP/IP y en el acceso de servidores a terminal. (Areitio Bertolín, 2008)

2.2.2.1.Componentes del protocolo AAA

Uno o más servidores AAA. Por razones de tolerancia a fallos, se suele utilizar más de uno, que se conectan a la red y sirven como un lugar de almacenamiento central para guardar y distribuir información de AAA.

El dispositivo que funciona como el punto de entrada a la red, que generalmente es una NAS, aunque puede ser un router, un servidor de terminales una pasarela de seguridad multifuncional o una máquina de computación que contiene un cliente AAA. (Areitio Bertolín, 2008)

2.2.2.2.Servicios de un protocolo AAA

Autenticación: Este servicio implica que se debe validar al usuario, antes de permitirle que acceda a la red, este proceso es importante al probar que el usuario posee una pieza única de información una combinación de nombre de usuario, contraseña y una clave secreta PIN (Personal Identification Number) que va asociado a una tarjeta inteligente, una llave USB criptográfica por tanto una identificación no ambigua. (Areitio Bertolín, 2008)

Autorización: Este procedimiento es proporcionar una dirección IP o un filtro para determinar las aplicaciones o protocolos que se necesitan, la autenticación y la autorización se realizan de forma conjunta en un entorno de gestión AAA. (Areitio Bertolín, 2008)

Contabilidad o accouting: Nos brinda la metodología para recoger información acerca del uso del recurso del usuario final, la auditoria para saber las operaciones realizadas, la capacidad de planificación, gestión de abusos y así monitorizar y actuar contra usuarios maliciosos en base a la información registrada. (Areitio Bertolín, 2008)

2.2.2.3.Funcionalidades de RADIUS

RADIUS (Remote Acces Dial-In User Service), es actualmente el protocolo AAA más utilizado en el mundo, en competencia con Kerberos (de Merit), es un sistema de autenticación y contabilidad, que se activa cuando un usuario se conecta vía ISP. Cuando el usuario pone su nombre y contraseña RADIUS comprueba la información y concede o deniega el acceso. (Areitio Bertolín, 2008)

Las Funcionalidades son:

Operaciones basadas en cliente-servidor: Un cliente RADIUS reside en el NAS y se comunica por la red con otro servidor RADIUS, que se ejecuta en una máquina de computo, además el servidor RADIUS puede servir como cliente proxy para otro RADIUS. (Areitio Bertolín, 2008)

Seguridad de red: Las comunicaciones entre un cliente RADIUS y el servidor están autenticadas, en base a una clave secreta compartida que no se envía por la red, además las contraseñas de usuarios contenidos en los mensajes RADIUS están cifradas. (Areitio Bertolín, 2008)

Autenticación Flexible: RADIUS puede soportar múltiples mecanismos de autenticación como por ejemplo CHAP, EAP, PAP. (Areitio Bertolín, 2008)

Pares atributo/valor: Los mensajes RADIUS transportan la información AAA codificada, en campos de tipo longitudinal y valor denominados atributos o pares

atributos/ valor ejemplo de dichos atributos son el nombre de usuario, contraseña de usuario, protocolo trama PPP, dirección IP final de usuario o el número de puerto del proceso final destino. (Areitio Bertolín, 2008).

2.2.2.4.Criterios de evaluación de protocolos AAA

Los criterios más importantes son los siguientes:

Funcionalidad: Para comprobar si se puede trabajar con cortafuegos y en que situaciones da una mejor utilización, según el tipo de red, el tamaño y el número de peticiones simultaneas sin congestión. (Areitio Bertolín, 2008).

Grado de gestión: Permite saber si las claves pueden enviarse por correo o distribuirse de una forma confiable fuera de línea. (Areitio Bertolín, 2008)

Seguridad: Para cifrar la información de autenticación o todo el mensaje, dependiendo del grado de simplicidad para utilizar cifrado extra, de identificar la parte del protocolo que es segura, independientemente del uso, del esfuerzo necesario para romper el cifrado. (Areitio Bertolín, 2008)

Economía: Valora la ventajas e inconvenientes económicos para utilizar dicho protocolo AAA. (Areitio Bertolín, 2008)

Participación en el mercado: De saber en dónde existen en la actualidad dichos protocolos AAA, saber si su uso se incrementa o disminuye en la actualidad. (Areitio Bertolín, 2008)

2.2.3. Seguridad

Uno de los factores importantes al momento de implementar o utilizar una red inalámbrica es la seguridad, ya que los datos que se transfieren a través de las redes inalámbricas tienen un medio de comunicación que no están restringidas, a diferencia de las redes

cableadas, nuestros datos viajan por un medio de comunicación accesible a cualquier dispositivo externo a la red, pero con la capacidad de capitación de la señal radioeléctrica. El mecanismo de seguridad estándar en WI-FI incluye la autenticación como el cifrado de los datos, actualmente los dispositivos se pueden configurar con varios mecanismos de seguridad.

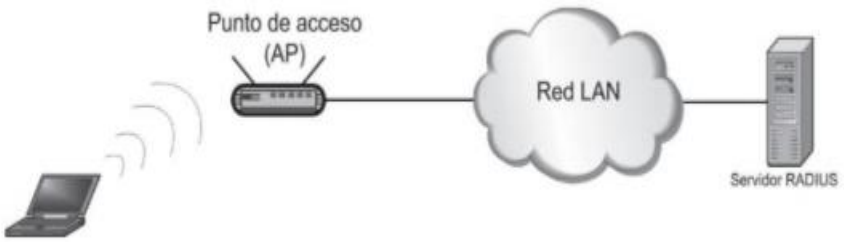
2.2.3.1.WEP

Este mecanismo esta inicialmente especificado en el estándar 802.11 es WEP, en la actualidad este mecanismo es considerado como poco robusto y fácil de romper por lo que hoy en día no se aconseja su uso. Se basa en utilización de claves simétricas con las que se lleva a cabo la encriptación de los datos basándose en un algoritmo llamado RC4.

2.2.3.2.WPA

Debido a las debilidades del WEP se desarrolló un formato más robusto por lo que se desarrolla una nueva especificación de seguridad para los dispositivos Wi-fi conocida como WPA, esta utiliza un nuevo protocolo llamado TKIP que es el mismo que se utiliza en el estándar IEEE 802.11i, una ventaja es que se puede usar en el mismo hardware que WEP, es decir que no se necesita cambiar los dispositivos inalámbricos, solo se cambiaría el firmware de los dispositivos, también utiliza claves simétricas con el algoritmo RC4, pero para mayor seguridad genera claves temporales que se cambian de forma dinámica, corrige fallos de seguridad y algunas mejoras respecto al WEP.

Figura N° 8: Conexión WPA



Fuente: (Andreu J. , 2011)

2.2.3.3.WPA2

También conocido como el estándar IEEE 802.11i, uno de los cambios es la utilización de AES que es un estándar de encriptación avanzado en lugar de un RC4.

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. TIPO Y DISEÑO DE INVESTIGACIÓN

3.1.1. Tipo

Descriptiva por que describe las etapas de análisis, diseño e implementación de la propuesta.

3.1.2. Diseño de investigación

El Diseño de investigación es cuasi experimental porque permite establecer una relación causal entre una o más variables denominada dependiente (Y) y otras variables independiente (X) en una situación estrictamente controlada.

3.2. LOCALIZACIÓN

El presente trabajo se realizó en el área de informática del colegio privado CHAMPAGNAT con los docentes de la institución educativa que se encuentra ubicado en la ciudad de Arequipa.

3.3. POBLACIÓN

La población para la implementación de la propuesta estará conformada por la totalidad de docentes de la institución educativa que son 30.

Figura N° 9: Página Web del colegio Champagnat

Fuente: Recuperado http://www.champagnataqp.edu.pe/

3.4. MUESTRA

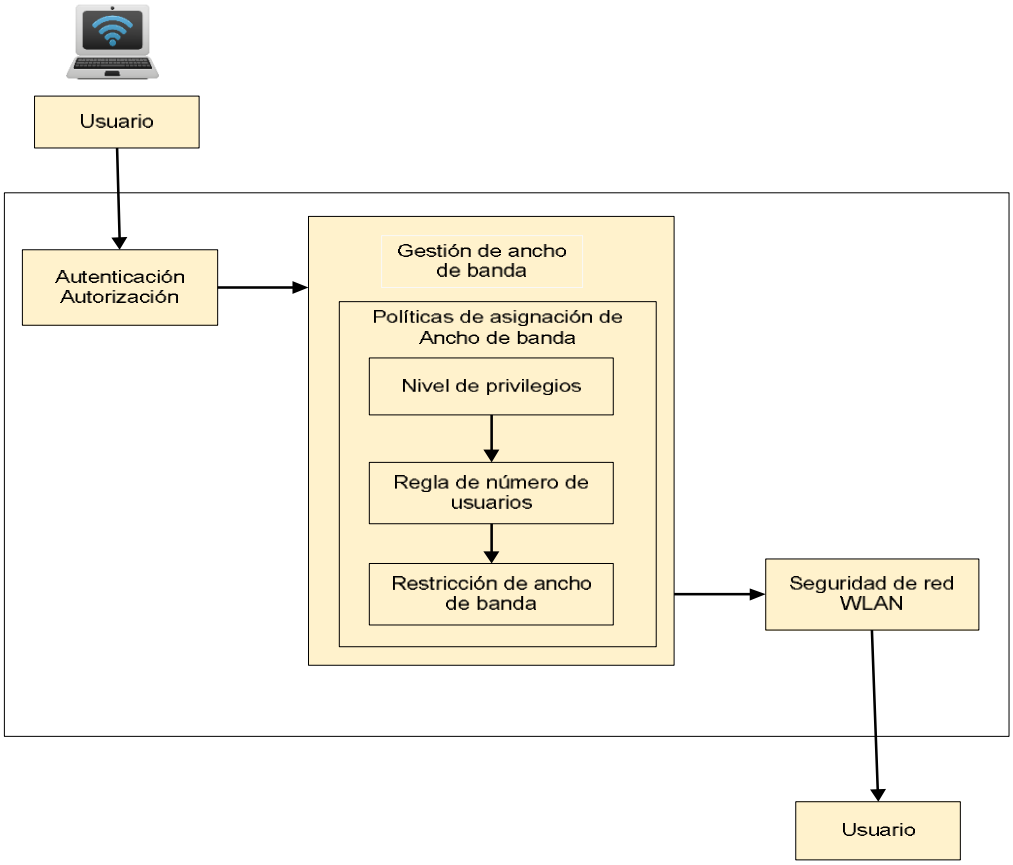
La muestra estará conformada por 30 docentes de la institución educativa que accedan a la red.

3.5. METODOLOGÍA DE DESARROLLO

3.5.1. Descripción de la propuesta

Para poder describir la propuesta de gestión de ancho de banda, en la figura 10 se ha desarrollado un diseño general, donde se muestra los tres componentes principales que dará solución al planteamiento de nuestro problema.

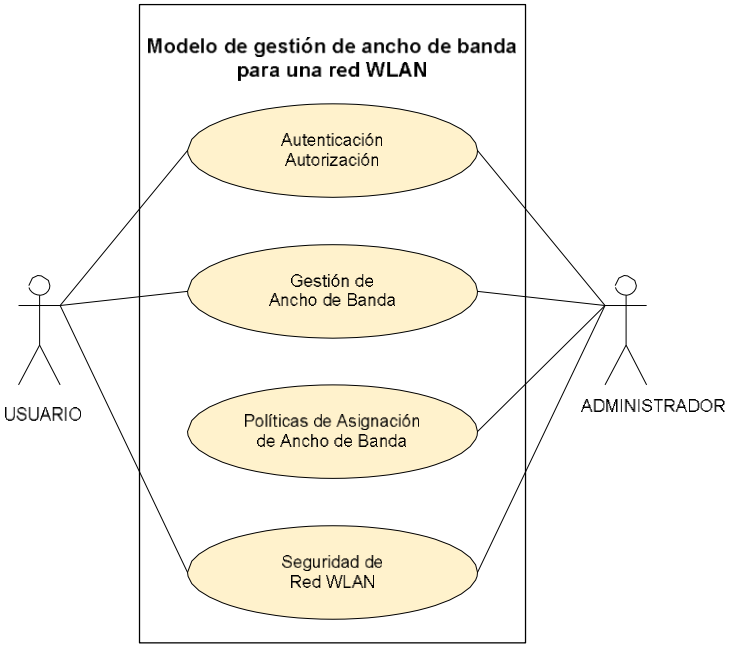
Figura N° 10: Propuesta de ancho de banda en la red WLAN



Elaboración propia

En la figura 11 se hace una representación de la propuesta utilizando el diagrama de casos de uso, donde: El usuario al conectarse a nuestra red WLAN, solicita al sistema la autenticación, aceptada la autenticación, el administrador permitirá según las políticas de la propuesta asignar el ancho de banda para el usuario.

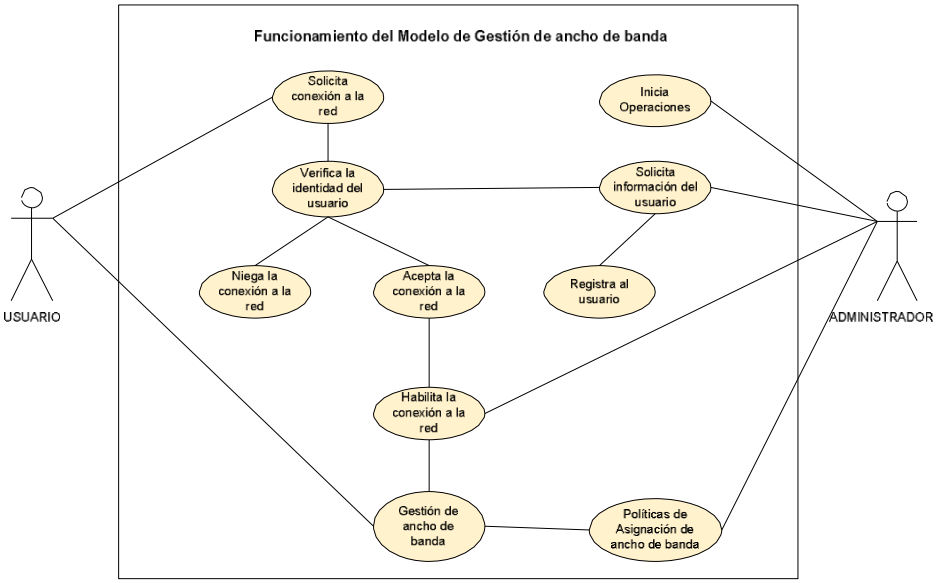
Figura N° 11: Gestión de ancho de banda para una red WLAN



Elaboración propia

La figura 12 se detalla el funcionamiento de la propuesta de gestión de ancho de banda de la red WLAN

Figura N° 12: Propuesta de ancho de banda función



Elaboración propia

3.5.2. Componentes de la propuesta

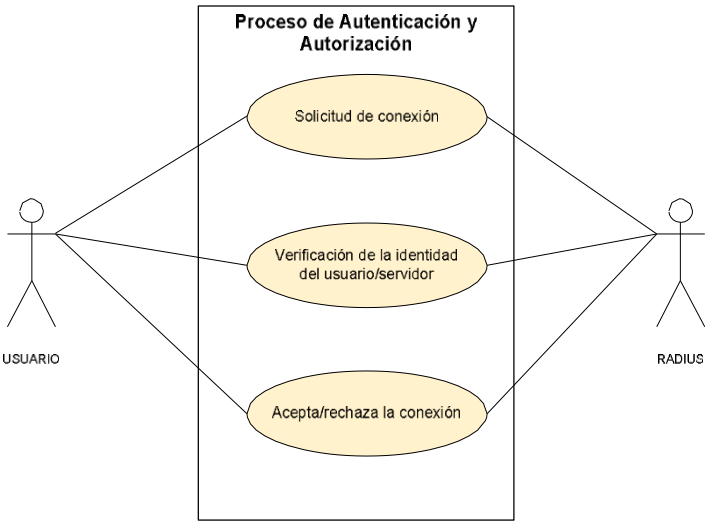
- Autenticación y Autorización.
- Gestión de ancho de banda.
- Seguridad de red WLAN.

3.5.2.1.Autenticación y autorización

Con este componente se identifica a cada usuario que ingresa a la red WLAN que previamente haya sido autenticada utilizando el protocolo AAA para poder otorgarle los permisos propuestos por la propuesta, que también nos permite obtener datos del ingreso y tiempo de uso de la red WLAN.

En la figura 13 se representa el diagrama de caso de uso del proceso de autenticación y autorización, donde el usuario solicita conectarse a la red WLAN, se verifica su identidad mediante RADIUS que toma en consideración el protocolo CHAP.

Figura N° 13: Propuesta para una red WLAN

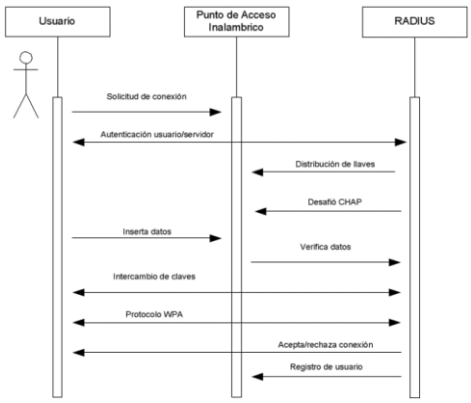


Elaboración propia

La figura 14 muestra el diagrama de secuencia donde nuestro usuario pide conexión para tener acceso a la red inalámbrica, después de este proceso de autentificación con RADIUS (distribución de llaves y desafío CHAP), el usuario inserta la contraseña que será

autenticada, RADIUS acepta o rechaza la conexión a la red WLAN, en caso de ser aceptado se asigna su ancho de banda de acuerdo al nivel de privilegios de la propuesta.

Figura N° 14: Diagrama de secuencia



Elaboración propia

3.5.2.2.Gestión de ancho de banda

Políticas de la propuesta:

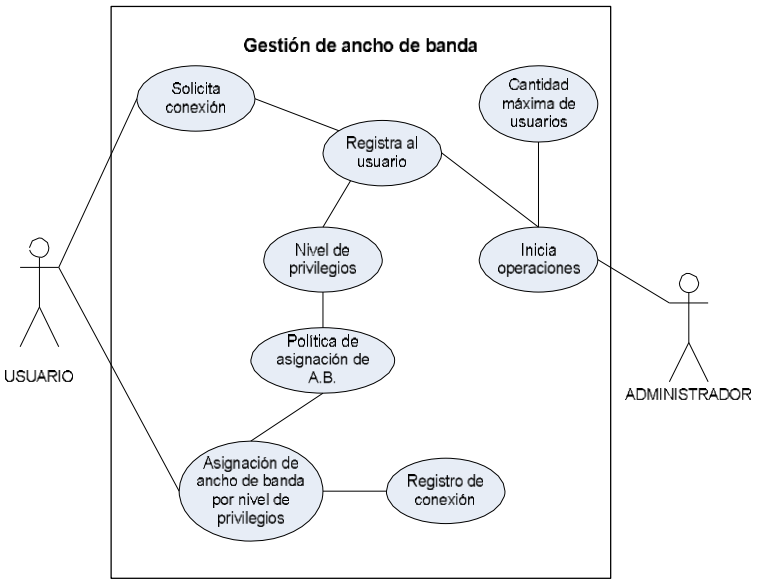
Nivel de privilegio: Se toma en consideración la cantidad de usuarios y el administrador asigna el ancho de banda para cada nivel.

Cantidad de usuarios: Se optimiza la calidad para un mejor desempeño de la red mediante la administración del ancho de banda.

Ancho de banda: Restringiendo puertos, dominios (red) de acuerdo a cada nivel.

La figura 15 muestra cómo funciona nuestro modelo de gestión, entre el usuario y el administrador, este último es encargado del inicio del proceso para calcular el número de usuarios que soporta la red, haciendo el registro del usuario según el nivel de privilegio asociado a un ancho de banda.

Figura N° 15: Propuesta de gestión de ancho de banda



Elaboración propia

3.5.2.2.1. Niveles de privilegios

En el siguiente modelo se considera 3 niveles de privilegio (Banda mínima, Banda media y Banda máxima) según asignación de ancho de banda.

a) Banda mínima denominada “X”, su ancho de banda es mínimo para la red.

b) Banda media denominado “Y”, su ancho de banda es mayor y tiene la capacidad de transferencia de archivos por la red.

c) Banda máxima denominada “Z”, no tiene limitación del ancho de banda en la red.

Para cada nivel de privilegio se debe tener un registro de los usuarios, el administrador asignara un ancho de banda según la necesidad de cada usuario.

3.5.2.2.2. Reglas de numero de usuario

La cantidad de usuarios es importante para determinar la capacidad de nuestra red en la distribución de niveles de privilegio de ancho de banda.

El modelo de ancho de banda está distribuida en 3 niveles de privilegios X, Y, Z que nos dará un cálculo aproximado de cuantos usuarios soportara la red WLAN asignando un porcentaje a cada nivel que el total de estos nos dará un 100%.

X+Y+Z=100%

Dónde: X = Banda minina X

Y = Banda media Y

Z = Banda máxima Z

Nuestras variables (X, Y, Z) cumplen la ecuación donde cada una tiene un porcentaje, este porcentaje es el mismo pero la cantidad de usuarios por cada nivel puede variar.

El ancho de banda es un recurso limitado que soporta una cantidad de usuarios en la red, al igual que los equipos como los puntos de acceso, los switches también admiten un número determinado de usuarios, en el modelo de gestión de ancho de banda la cantidad de usuarios estará determinada por el ISP de la red inalámbrica.

La red inalámbrica soporta una cantidad determinada de usuarios, si hay mayor cantidad de usuarios, el ancho de banda no aumenta lo que ocasiona que la asignación por nivel de privilegios disminuya.

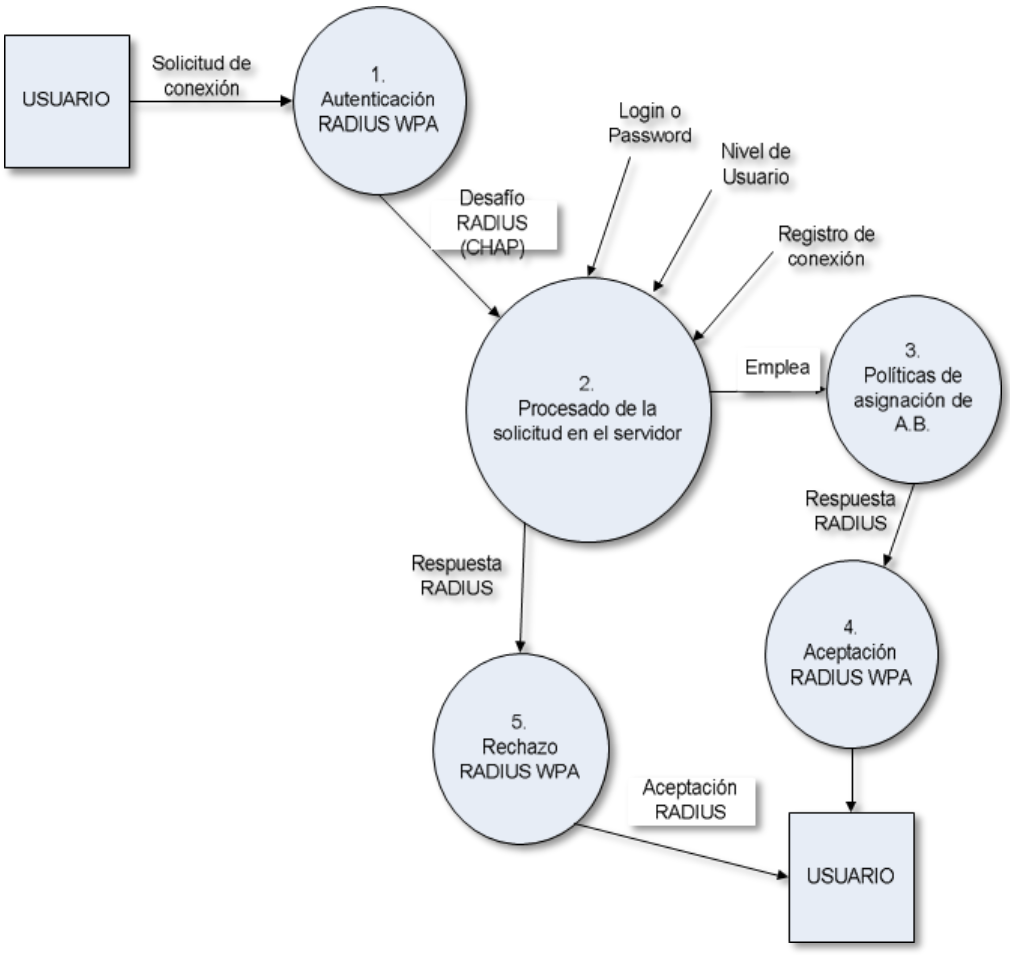
El diagrama de contexto 16, da una descripción simple del funcionamiento de la propuesta de gestión de ancho de banda donde los usuarios envían una petición para poder conectarse a la red inalámbrica y el sistema envía una respuesta a la petición.

Figura N° 16: Diagrama de ancho de banda

Elaboración propia

La figura 17 muestra cómo se procesa la petición, el usuario hace una solicitud de conexión RADIUS mediante la Autenticación y el servidor se encargara de la validación del usuario, si esta es aceptada accederá a un nivel de privilegio, caso contrario si el usuario no cuenta con un password, un registro de conexión se le negara el acceso.

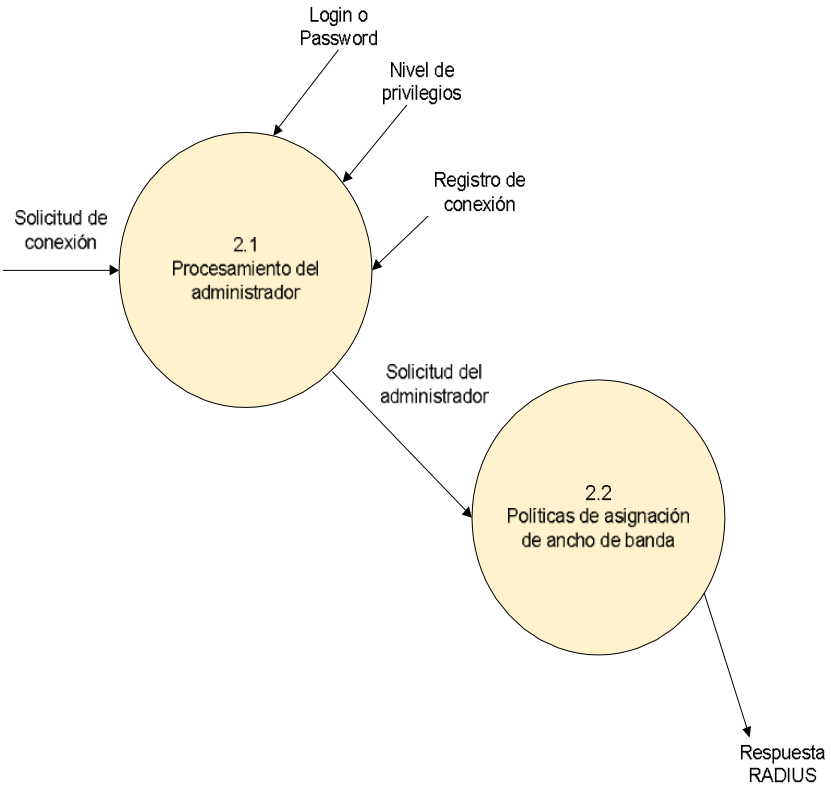
Figura N° 17: Flujo de datos



Elaboración propia

En la figura 18 muestra el procesamiento que hace el administrador con la información del usuario al registrarse, para poder validar su identidad. Y asignarle el ancho de banda según el nivel de privilegio, después de ejecutar el proceso se acepta o se rechaza al usuario.

Figura N° 18: Solitud del adiestrador



Elaboración propia

3.5.2.2.3. Restricción de ancho de banda

Para restringir el ancho de banda se aplican las políticas y los niveles de privilegio, para el usuario con banda minina se le restringen sitios web, o dominios de red que requieren un mayor ancho de banda, para el usuario de banda media la restricción será personalizada y podrá acceder a sitios web donde pueda hacer descarga de archivos y para el usuario con banda máxima podrá acceder a distintos sitios y dominios la única restricción es la cantidad de ancho de banda que se le asigne.

Hay políticas adicionales que el administrador debe considerar según su modelo de gestión: acceder a sitios web que no estén dentro de su nivel de privilegio le reducirá su ancho de banda y si el usuario persiste en las faltas se le negara el acceso a la red.

El administrador es el único que realiza el registro del usuario y asigna el nivel de privilegio para distribuir el ancho de banda.

El administrador es quien determina la cantidad de usuarios la restricción y los niveles de privilegio de acuerdo a la gestión de ancho de banda.

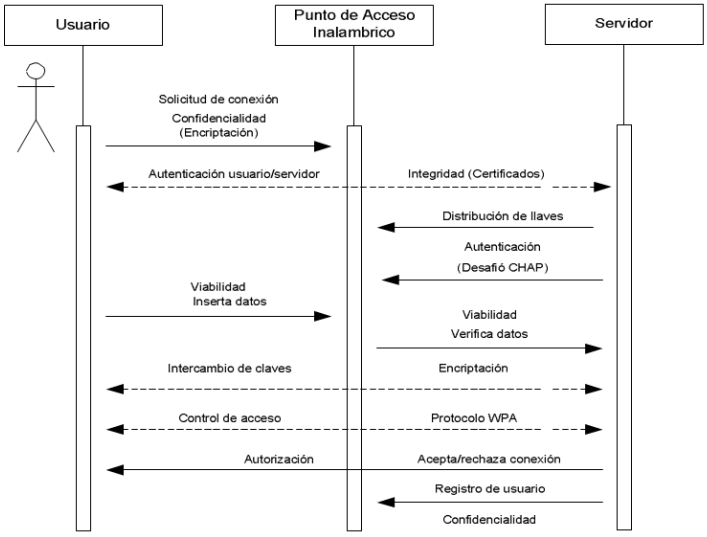
3.5.2.3.Seguridad de la red WLAN

La red WLAN utiliza un medio abierto para la transmisión de la información para lo cual tiene un mecanismo para proteger la información de manera que evita cualquier peligro en la red.

En la propuesta de gestión de ancho de banda, se aplico medidas de seguridad en la instalación del servidor Linux para el monitoreo de la información de los usuarios, aplicado servidor RADIUS.

En la figura 19 se detalla las medidas de seguridad de la gestión de ancho de banda y el control de acceso tiene el protocolo WPA2 que cuenta con un mecanismo de seguridad.

Figura N° 19: Seguridad del ancho de banda



Elaboración propia

Se utilizó el método de autenticación EAP-TLS para que la red sea confiable.

3.5.3. Límites de la propuesta

La propuesta de gestión de ancho de banda es únicamente para redes WLAN.

3.5.4. Construcción de la propuesta

Para el desarrollo de la propuesta de la tesis, interactúan tres elementos (clientes, punto de acceso (AP) y el servidor).

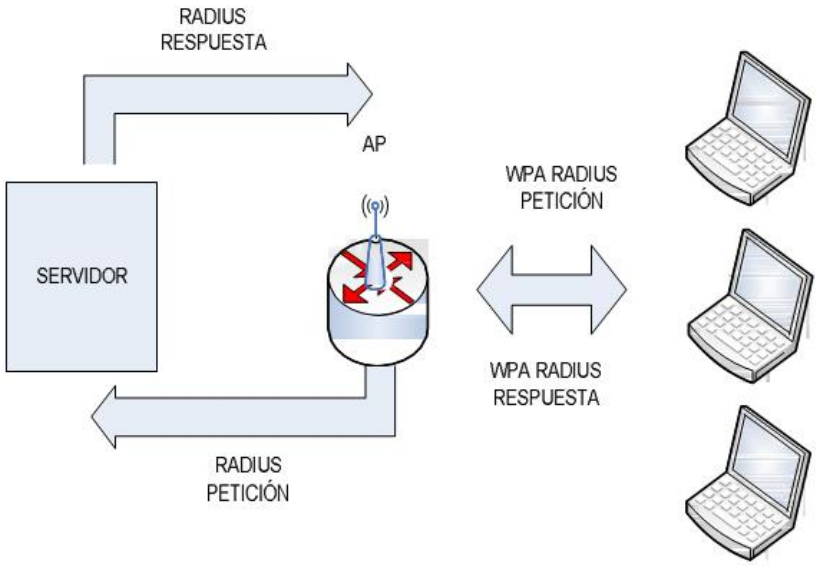
- Clientes: Son equipos de cómputo que puedan conectarse a una red inalámbrica.
- Punto de acceso: Trabajara como router, admitiendo el protocolo WPA2 con RADIUS, el punto de acceso soporta el estándar 802.11b/g.
- Servidor: Es una aplicación que atiende las peticiones de los usuarios de la red.

La propuesta utiliza el servicio RADIUS (freeRADIUS) es un servidor de código abierto, para la seguridad en la red se usa la autenticación CHAP (MS-CHAPV2).

3.5.5. Arquitectura de red utilizada en la propuesta

La propuesta de gestión de ancho de banda de la red WLAN tiene una arquitectura básica con un punto de acceso a internet, un servidor y varios clientes.

Figura N° 20: Modelo de gestión



Elaboración propia

3.5.5.1.Equipos para la implementación de la propuesta

Relación de dispositivos utilizados:

- Computadora con función de servidor que autenticara y administrara el ancho de banda, montada con el sistema operativo Linux Ubuntu Server.
- Router inalámbrico Sagemcom F@ast 3284u que servirá de punto de acceso.
- Laptop Portátil HP 14-cm0004la con sistema operativo Windows 10.
- Laptop Portátil HP 14-cm0004la con sistema operativo Windows 10.

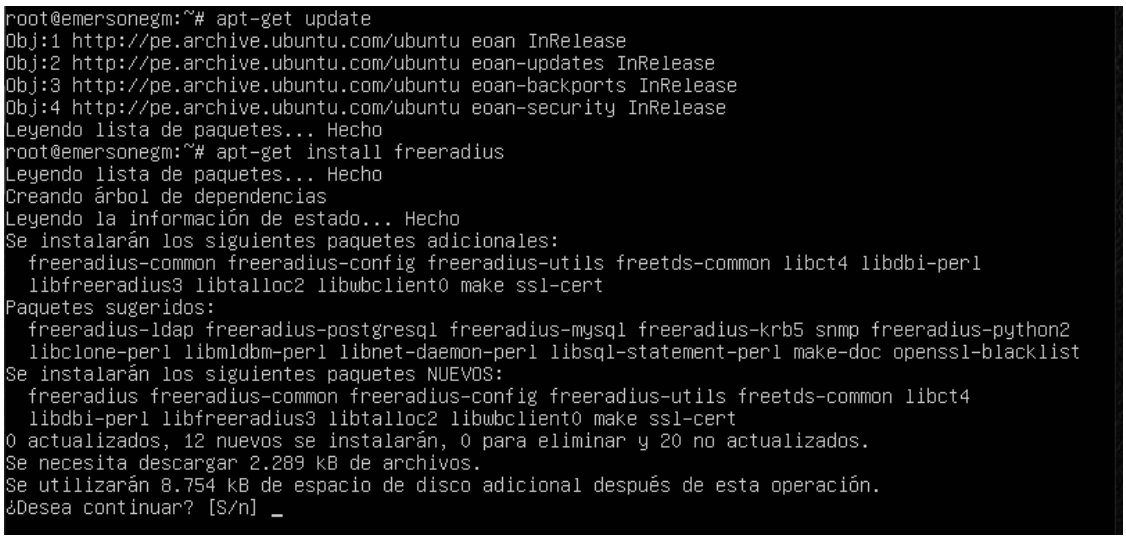
3.5.6. Instalación del servidor FreeRADIUS en Ubuntu Server 19.10

Para la implementación del servidor de seguridad utilizaremos FreeRADIUS, en Ubuntu Server.

En la figura 21, ingresamos a la consola de Linux de Ubuntu Server, para actualizar los paquetes de actualización con el comando:

apt-get update

Figura N° 21: Paquetes de actualización

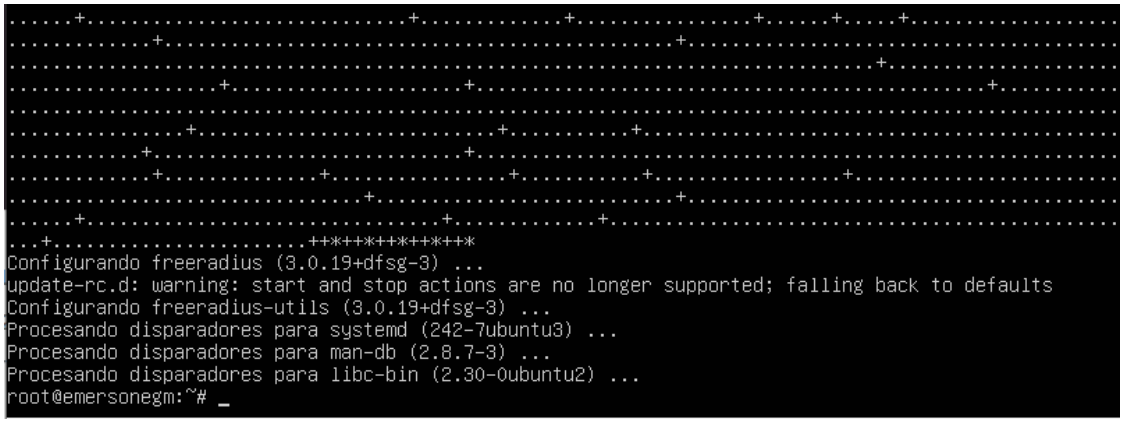


Elaboración propia

En la figura 22, instalamos el servicio con el siguiente comando:

apt-get install freeradius

Figura N° 22: Instalación servicio FREERADIUS

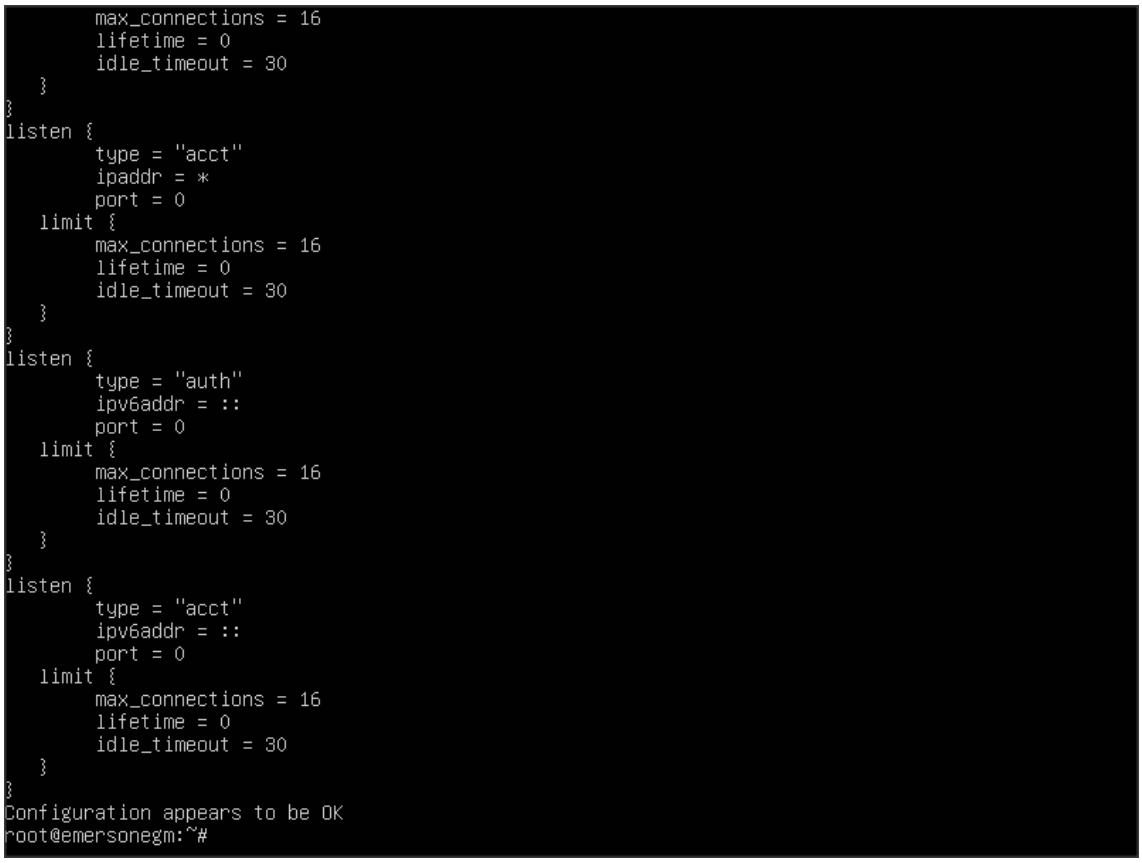


Elaboración propia

En la figura 23, comprobamos que el servicio este correctamente instalado, con el comando:

freeradius –CX

Figura N° 23: Comprobación del servicio instalado



Elaboración propia

En la figura 24 mostramos los directorios de FreeRADIUS con el comando:

sudo ls /etc/freeradius/3.0/

Figura N° 24: directorios de FreeRADIUS

Elaboración propia

Después de la instalación del servidor editaremos los archivos de configuración:

- client.conf (AP interfaces)
- users (información de clientes)
- EAP.conf (método a utilizar)

3.5.6.1.Configuración del módulo de usuarios

En la figura 25, los usuarios que se conectaran a la red inalámbrica estarán especificados en el archivo “users”, creando un usuario con los comandos:

vi /etc/freeradius/3.0/users

Figura N° 25: Configuración modulo usuarios

```
root@emersonegm:~# sudo ls /etc/freeradius/3.0
certs         experimental.conf  mods-available  panic.gdb   radiusd.conf     sites-enabled   users
clients.conf  hints              mods-config     policy.d    README.rst       templates.conf
dictionary    huntgroups         mods-enabled    proxy.conf  sites-available  trigger.conf
root@emersonegm:~# vi /etc/freeradius/3.0/users
```

Elaboración propia

En la figura 26, editando con VI agregamos el usuario:

eguerra Cleartext-Password := "eguerra"

Figura N° 26: Editando el archivo users

```
#
DEFAULT Hint == "CSLIP"
        Framed-Protocol = SLIP,
        Framed-Compression = Van-Jacobson-TCP-IP

#
# Default for SLIP: dynamic IP address, SLIP mode.
#
DEFAULT Hint == "SLIP"
        Framed-Protocol = SLIP

#
# Last default: rlogin to our main server.
#
#DEFAULT
#       Service-Type = Login-User,
#       Login-Service = Rlogin,
#       Login-IP-Host = shellbox.ispdomain.com

# #
# # Last default: shell on the local terminal server.
# #
# DEFAULT
#       Service-Type = Administrative-User


# On no match, the user is denied access.


############################################################
# You should add test accounts to the TOP of this file! #
# See the example user "bob" above.                      #
############################################################
elmer Cleartext-Password :="eguerra"
~
-- INSERTAR --                                    220,27      Final
```

Elaboración propia

3.5.6.2.Configuración del módulo cliente

En la figura 27, ingresamos la dirección IP que se utiliza del punto de acceso, agregando la contraseña, editando el archivo clients.conf con el comando:

vi /etc/freeradius/3.0/clients.conf

Figura N° 27: Configuración modulo Clientes

Elaboración propia

En la figura 28, editando con VI agregamos el siguiente código al archivo clients.conf:

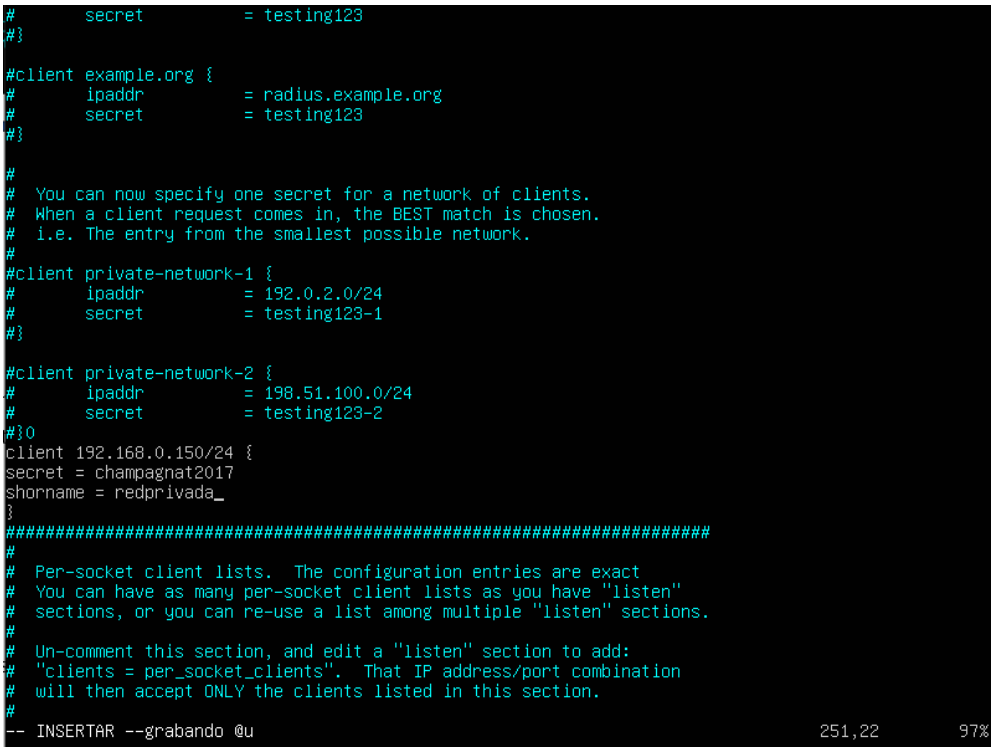
client 192.168.0.50/24 {

secret = champagnat2017

shortname = redprivada

}

Figura N° 28: Configurando el archivo clientes



Elaboración propia

3.5.6.3.Configuración del módulo EAP

En la figura 29, FreeRADIUS soporta el método EAP, que está en el archivo eap.conf editamos el archivo con el comando:

vi /etc/freeradius/3.0/eap.conf

Figura N° 29: Accediendo al archivo EAP.CONF

Elaboración propia

En la figura 30, editando con VI agregamos el siguiente código al archivo eap.conf:

eap {

default_eap_type = peap

...}

Figura N° 30: Agregando el método EAP

Elaboración propia

En la propuesta se utiliza el método EAP-TLS, con una ubicación específica de los certificados, contraseñas y otros archivos para su correcto funcionamiento, editando el archivo eap.conf con el contenido:

tls {

certdir = ${confdir}/certs cadir = ${confdir}/certs

private_key_password = champagnat2017

private_key_file = ${certdir}/server.pem

certificate_file = ${certdir}/server.pem

CA_file = ${cadir}/ca.pem

dh_file = ${certdir}/dh

random_file = ${certdir}/random

...

}

Autenticación con CHAP (versión MSCHAPV2)

peap {default_eap_type = mschapv2

...

}

mschap { use_mppe = yes

require_encryption = yes require_strong = yes

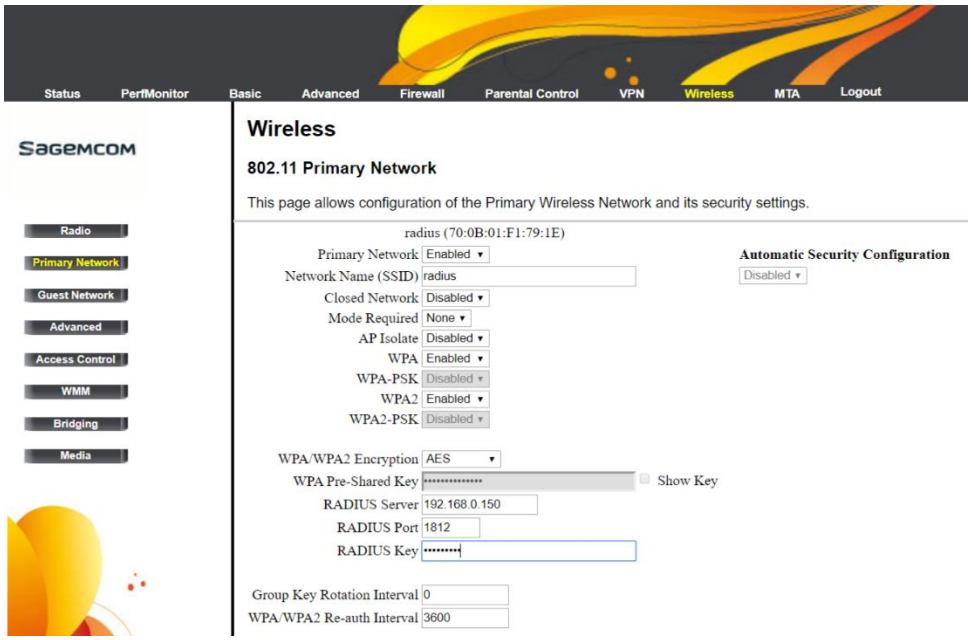
...

}

3.5.6.4.Configuración del punto de acceso

La figura 31 muestra la configuración del punto de acceso (AP)

Figura N° 31: Configuración AP



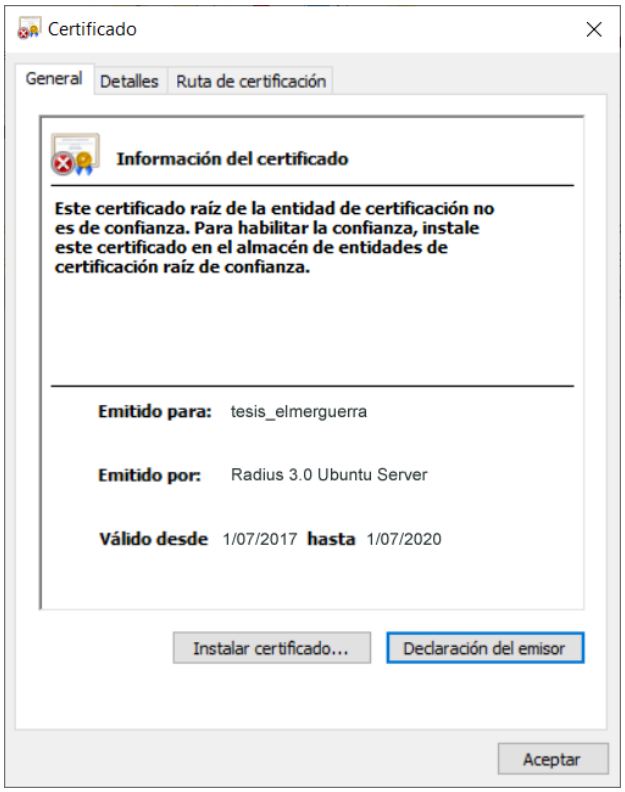
Elaboración propia

3.5.6.5.Configuración del cliente

El cliente debe instalar el certificado

En la figura 32 muestra el certificado EAP/PEAP

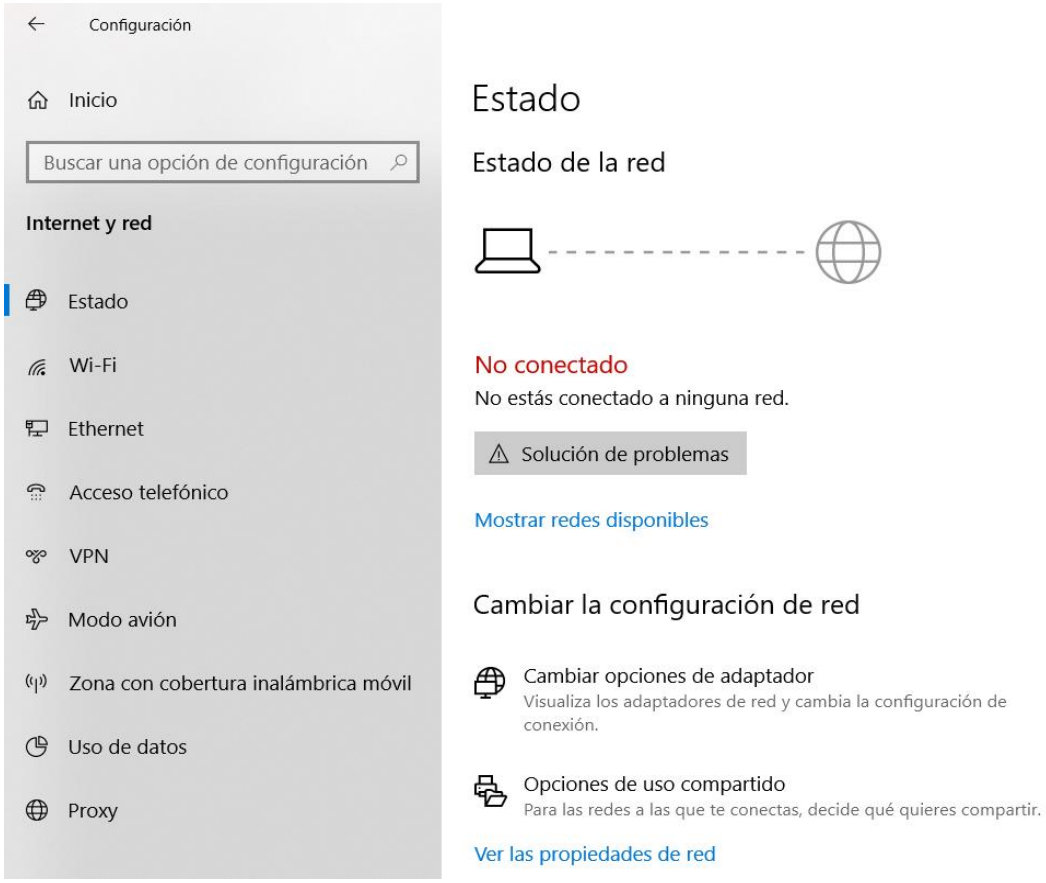
Figura N° 32: Certificado de la propuesta



Elaboración propia

Culminada la instalación se accede a las redes inalámbricas, para utilizar el cliente RADIUS y conectarse a la red. Ver Figura 33

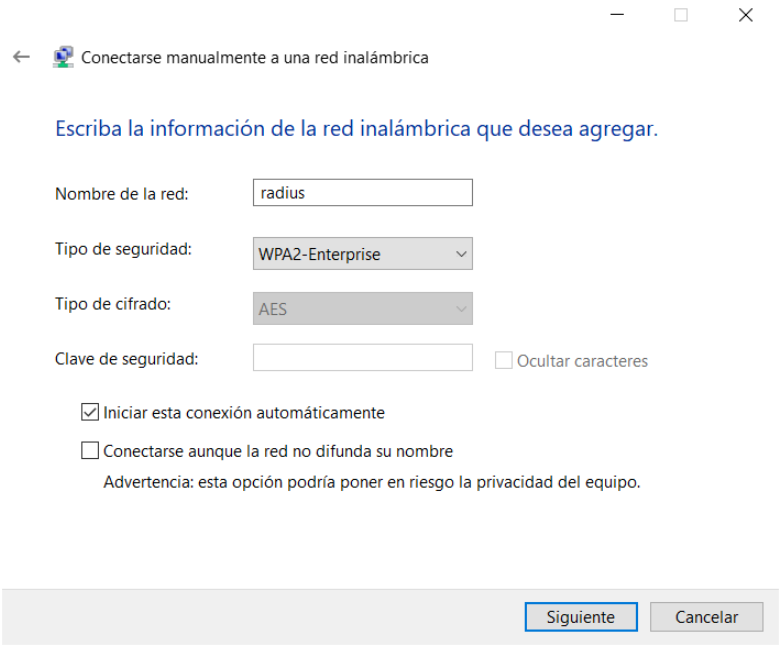
Figura N° 33: Configuración de cliente RADIUS



Elaboración propia

Agregamos la red inalámbrica llamada “radius” seleccionando la seguridad “WPA2-Enterprise” y descifrado “AES”.

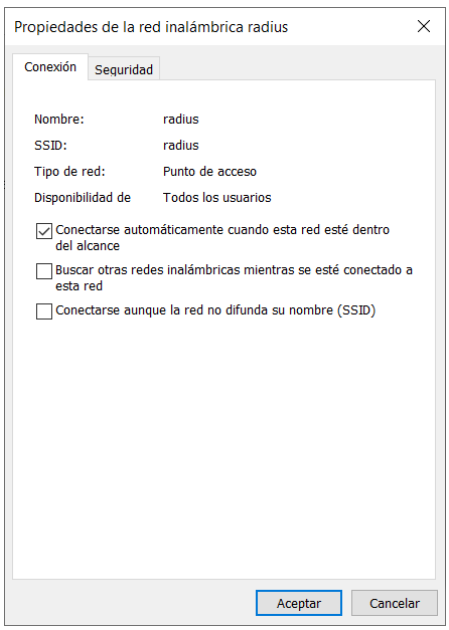
Figura N° 34: Configuración de la red RADIUS



Elaboración propia

Al estar conectado en la red, hacemos clic derecho sobre la red “radius” y hacemos clic sobre “Propiedades”

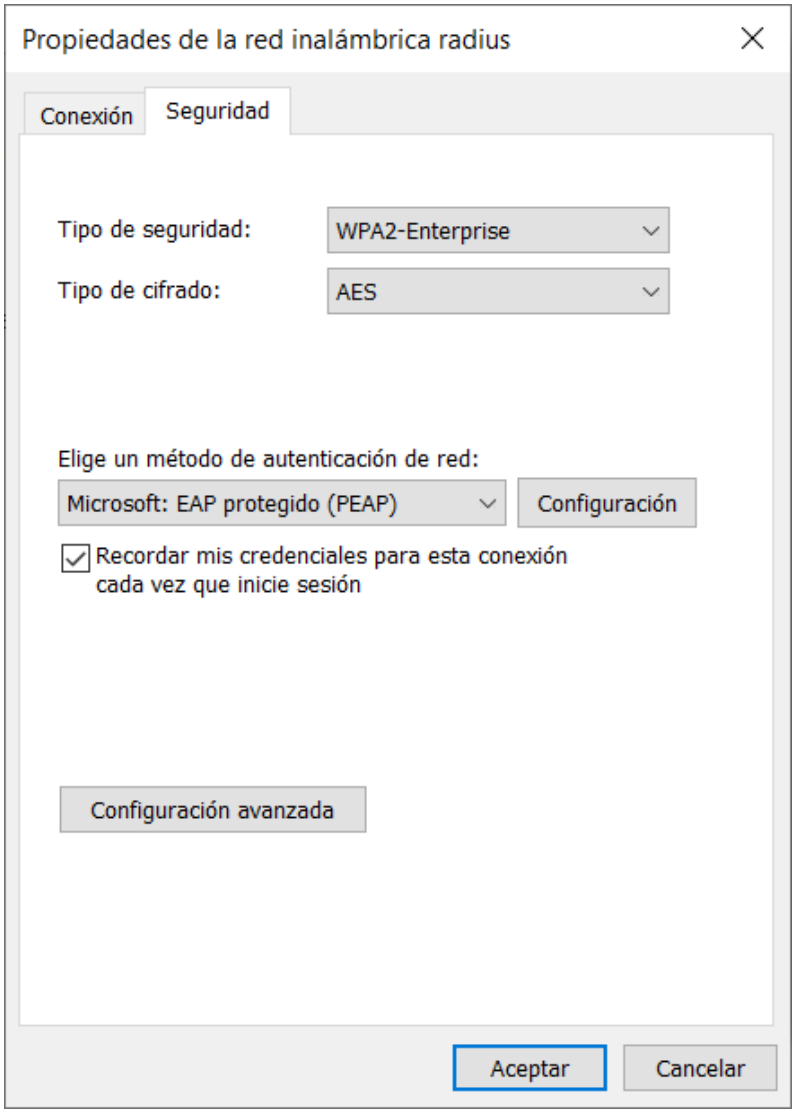
Figura N° 35: Propiedades de la red RADIUS



Elaboración propia

En la pestaña “Seguridad” realizamos clic en configuración para elegir el método de autenticación.

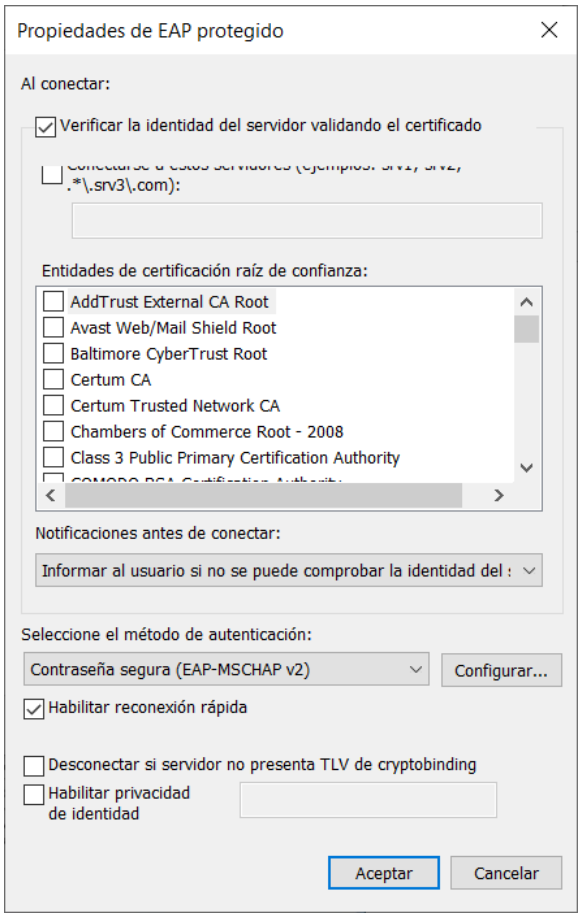
Figura N° 36: Seguridad de red RADIUS



Elaboración propia

Quitar la selección de “Validar un certificado de servidor”, seleccionamos el método EAP-MSCHAPV2 y clic en “aceptar’’.

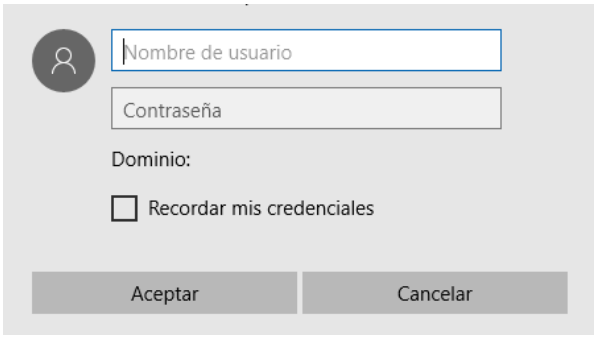
Figura N° 37: Selección del método EAP-MSCHAPV2



Elaboración propia

Realizado todos los pasos anteriores, nos mostrara la figura x donde nos solicitara las credenciales y clic en “aceptar’’.

Figura N° 38: Solicitud de credenciales



Elaboración propia

3.5.7. Descripción del servidor de gestión

SQUID es un servidor proxy de Linux, de gran utilidad ya que funciona con una licencia pública (GPL).

La figura 39 muestra la estructura del servidor de gestión.

Figura N° 39: Estructura de servidor de gestión

Elaboración propia

3.5.8. Instalación del servidor de gestión

Para la instalación de SQUID (ver figura 40) ejecutamos el comando:

sudo apt-get update

sudo apt-get install squid

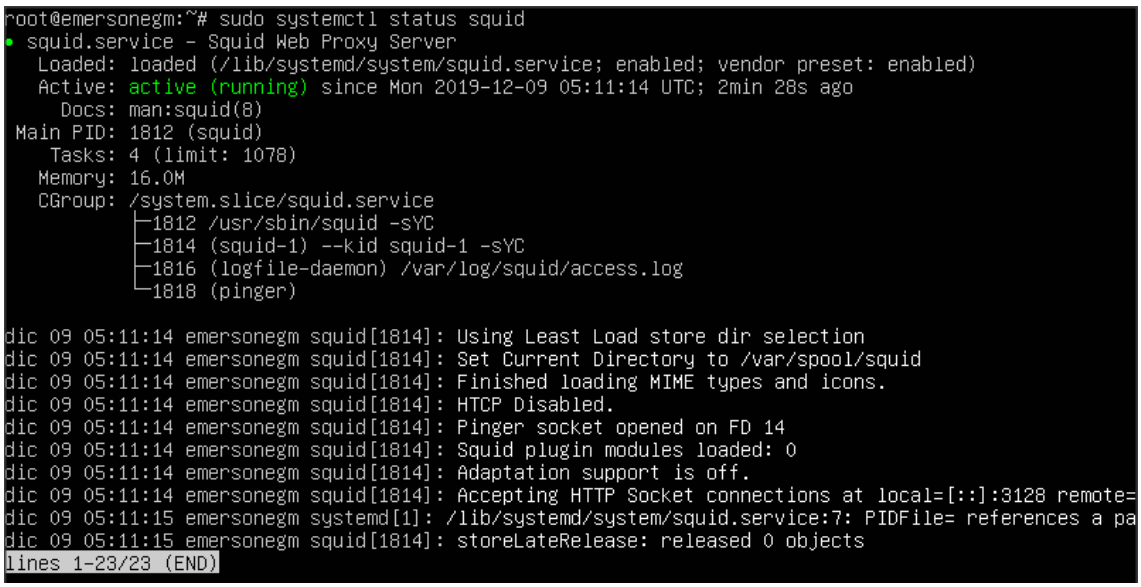
Figura N° 40: Instalación de SQUID

```
root@emersonegm:~# sudo apt-get update
Obj:1 http://pe.archive.ubuntu.com/ubuntu eoan InRelease
Des:2 http://pe.archive.ubuntu.com/ubuntu eoan-updates InRelease [97,5 kB]
Des:3 http://pe.archive.ubuntu.com/ubuntu eoan-backports InRelease [88,8 kB]
Des:4 http://pe.archive.ubuntu.com/ubuntu eoan-security InRelease [97,5 kB]
Descargados 284 kB en 3s (98,7 kB/s)
Leyendo lista de paquetes... Hecho
root@emersonegm:~# sudo apt-get install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libecap3 libltdl7 squid-common squid-langpack
Paquetes sugeridos:
  squidclient squid-cgi squid-purge resolvconf smbclient winbind
Se instalarán los siguientes paquetes NUEVOS:
  libecap3 libltdl7 squid squid-common squid-langpack
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 20 no actualizados.
Se necesita descargar 2.974 kB de archivos.
Se utilizarán 13,9 MB de espacio de disco adicional después de esta operación.
```

Elaboración propia.

En la figura 41 verificamos el estado de SQUID

Figura N° 41: Verificación del SQUID



Elaboración propia

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

Para que nuestros usuarios pasen, será a través de las MAC’s

acl cpcham01 arp 00:01:12:AC:60:83

acl cpcham02 arp 00:00:40:E6:D8:20

acl cpcham03 arp 00:0B:15:40:D2:C2

http_access allow cpcham01

http_access allow cpcham02

http_access allow cpcham03

http_access deny all

3.5.8.1.Configuración de las políticas de asignación de ancho de banda por nivel de privilegios

La configuración se realiza en el fichero squid.conf editando con el siguiente código:

```
acl all src 0.0.0.0/0.0.0.0

acl nivel_X src 10.0.0.200/24

acl nivel_Y src 10.0.0.203/24

delay_pools 3

#Transferencia ilimitada dentro de la WLAN

delay_class 1 1

delay_parameters 1 -1/-1

delay_access 1 allow all

#Nivel Y: Navegarán a 50 Kbs

delay_class 2 2

delay_parameters 65536/1024 10240/1024

delay_access 2 allow nivel_Y

#Nivel X: navegarán a 10 Kbs

delay_class 3 2

delay_parameters 32678/1024 26624/1024

delay_access 3 allow nivel_X
```

Asignado la cantidad de ancho de banda, se prohíbe otro puerto que no esté definido en safe-ports, para los usuarios de banda minima X.

http_access deny !Safe_ports

Permite el acceso al localhost

http_access allow manager localhost

http_access deny manager.

Configurando el archivo acl url_deny, permite a los usuarios de nivel de privilegio Y puedan ver páginas denegadas

http_access allow horario_almuerzo all peapLimitado url_deny

http_access allow peapTotal all !cont_palabras

Los usuarios de nivel de privilegio Z tienen acceso a todas las páginas.

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

Se configura el usuario y el grupo que utilizara squid, e indica donde se guaradara en cache.

cache_effective_user proxy

cache_effective_group proxy

coredump_dir /var/spool/squid

El SQUID se configura para la asignación de ancho de banda por nivel de privilegio y a la vez se configura el navegador de cada usuario con la dirección IP y el puerto del proxy.

3.5.9. Pruebas y resultados

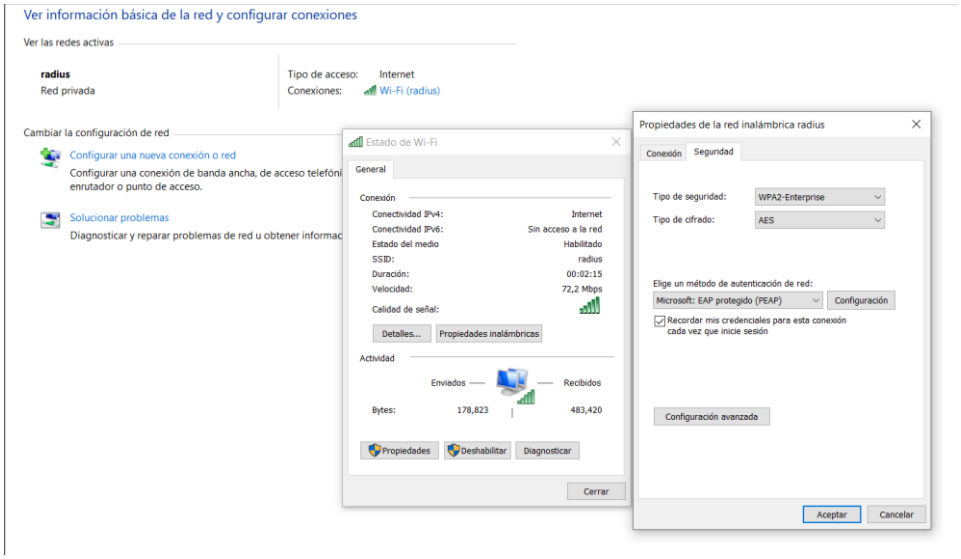
Para comprobar la propuesta se tomó en consideración los componentes de la red.

Cada componente debe estar en el mismo protocolo de autenticación, según el ancho de banda.

Una vez autenticado el cliente es autorizado.

En la figura 42 se logró realizar la autenticación mediante el protocolo CHAP versión MS-CHAPV2 por el protocolo TLS (PEAP).

Figura N° 42: Acceso a la red de la propuesta



Elaboración propia

Revisión del servidor de seguridad y comprobar autenticación

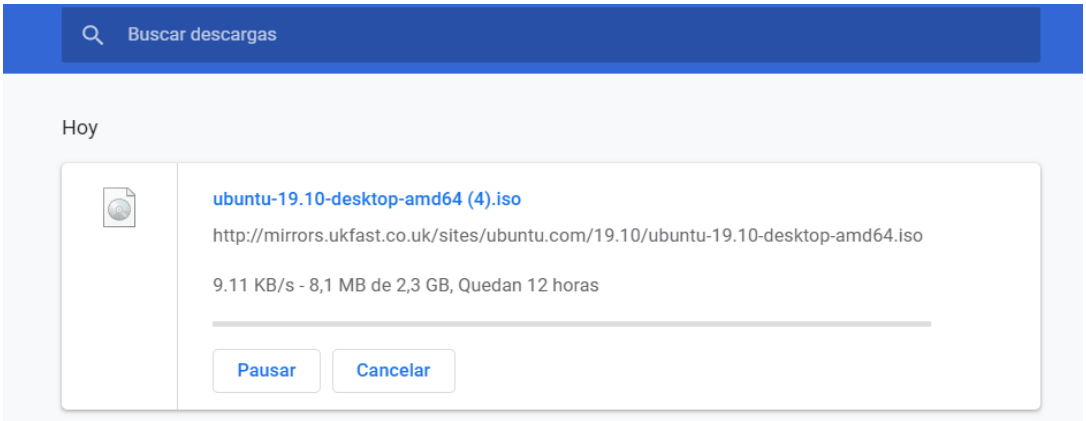
Figura N° 43: Autenticación CHAP

```
[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
```

Elaboración propia

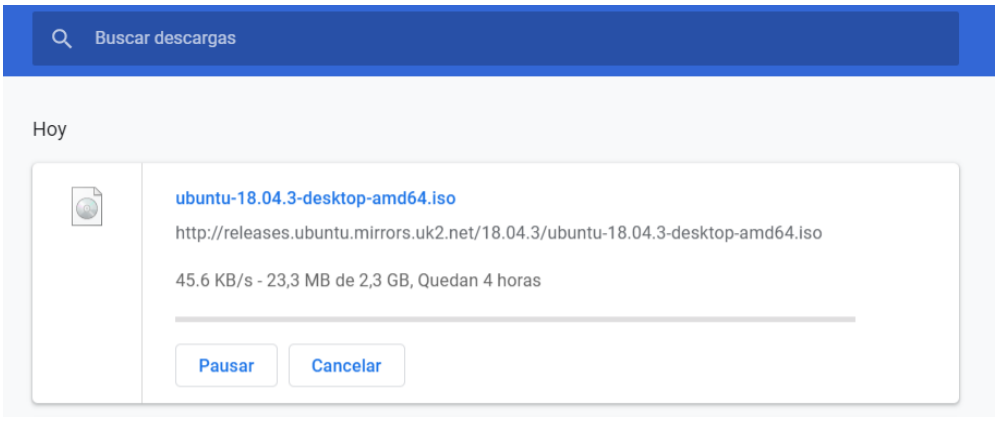
Se comprobó la transferencia de archivos en usuarios de privilegios X, Y, Z según ancho de banda.

Figura N° 44: Control de nivel de privilegio X 10KB



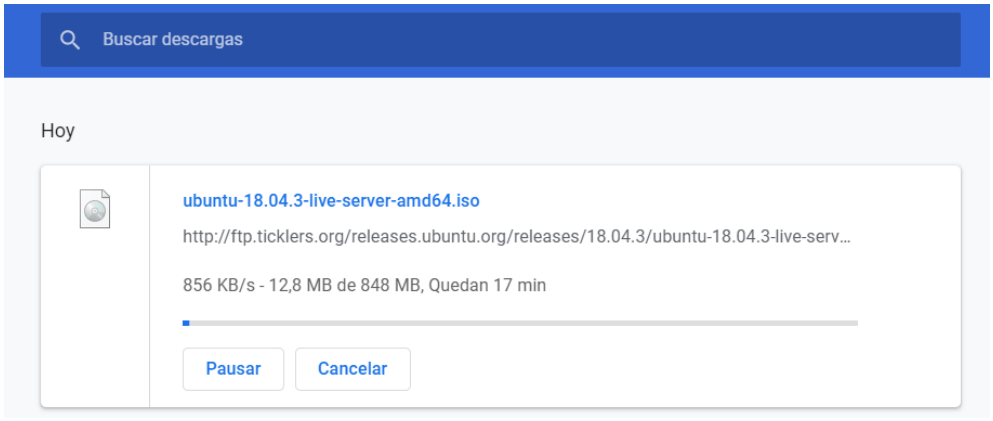
Elaboración propia

Figura N° 45: Control de nivel de privilegio Y 50KB



Elaboración propia

Figura N° 46: Control de nivel de privilegio Z Ilimitado



Elaboración propia

3.6. EVALUACIÓN ECONÓMICA Y FINANCIERA DE LA SOLUCIÓN

Tabla N° 2: Presupuesto de propuesta

Descripción	Costo
• **Computadora con función de servidor que autenticara y administrara el ancho de banda, montada con el sistema operativo Linux Ubuntu Server.** **Placa base lubin** **Velocidad de CPU: 3,0 GHz (máx. turbo boost: 3,5 GHz)**	S/. 1800.00

Cantidad: 8 GB **Velocidad: PC4-19200 MB/s** **Tipo: DDR4-2400** **Interfaz: M.2** **Estándares de transmisión: 802.11 a/b/g/n/ac** **Doble banda: 2,4 GHz y 5,0 GHz** **Tamaño: 1 TB** **Interfaz: SATA** **Velocidad de rotación: 7200 RPM** **Lector de DVD**	
• **Router inalámbrico Sagemcom F@ast 3284u que servirá de punto de acceso.**	S/. 130.00
• **Laptop Portátil HP 14-cm0004la con Sistema operativo Windows 10.**	S/. 1000.00
• **Laptop Portátil HP 14-cm0004la con Sistema operativo Windows 10.**	S/. 1000.00
• **Laptop Portátil HP 14-cm0004la con Sistema operativo Windows 10.**	S/. 1000.00
• **Servicio de internet**	S/. 79.00
TOTAL	**S/. 5009.00**

Elaboración propia

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

- Se implementó satisfactoriamente la propuesta de ancho de banda donde se permitió el acceso a usuarios que estaban registrados en la red según su nivel de privilegios.
- Cada usuario logro autenticarse en la red con su respectiva contraseña y poder acceder.

Discusión:

Nuestra propuesta de ancho de banda, permite al usuario acceder a la red según el nivel de privilegio.

Haciendo mención a la tesis de (Pilozo Campozano & Zambrano Balladares, 2013) titulada: "Estudio del Ancho de Banda para el tráfico de Redes WAN de los ISP, con estudiantes de la Universidad Politécnica Salesiana Sede Guayaquil carrera Ingeniería de Sistemas, mediante la implementación de una página web" donde concluye que los estudiantes usan muchas aplicaciones y desconocen la velocidad del servicio , en nuestra propuesta de ancho de banda cada usuario sabe el nivel de privilegio o de banda que le corresponde y las actividades que puede realizar con la velocidad del nivel de privilegio de la red.

En el presente trabajo se recomienda el uso del servidor RADIUS para tener mayor control de los usuarios y que cada uno de estos pueda realizar las actividades dentro de la institución sin ninguna dificultad el cual concuerda con la tesis de (Chuquicondor Requena, 2017) titulada "Propuesta Metodológica Para La Gestión Y Administración Del Ancho De Banda de Comunicaciones En El Campus De La Universidad Nacional De

Piura – 2016.” Donde se concluye que al desarrollar la implementación de gestión de ancho de banda en la universidad de Piura beneficia la conectividad dentro del campus, así como los usuarios puedan realizar sus actividades sin ningún inconveniente, que es lo mismo que se logró en el colegio particular Champagnat.

V. CONCLUSIONES

- Se habilito el sistema de usuarios para que puedan ingresar a la red mediante el protocolo AAA, generando un ambiente de seguridad en el colegio privado Champagnat Arequipa.
- Se gestionó el ancho de banda para los usuarios del colegio privado, asignándoles el nivel de privilegio que les corresponde, observando que la tasa de transferencia se cumplió para cada nivel de usuario, cumpliendo con el objetivo planteado para este trabajo de investigación.
- Se generó la conexión con los usuarios registrados en la red, logrando un entorno seguro y administrable, brindando un servicio de calidad en la red WLAN del colegio privado.
- Se implementó mecanismos de identificación para asignarles el ancho de banda a los usuarios autenticados según el nivel de privilegio que le corresponde.

VI. RECOMENDACIONES

- En base al diseño de la propuesta se recomienda desarrollar una base de datos en MYSQL así administrar la creación, borrado y modificación de usuarios que acceden a la red.
- Para mayor facilidad en la configuración de usuarios que accedan a la red se recomienda instalar un servidor RADIUS, ya que hay varias entidades donde se encuentra gran cantidad de routers, con el servidor Radius hay mayor facilidad de administración de usuarios dentro de toda la red.
- Se recomienda evitar la difusión del identificador de red o SSID, también segmentar zonas de seguridad administrado por un firewall creando una red privada virtual.
- Crear políticas de uso, para la utilización de los equipos de cómputo en el área de informática, así mantener la integridad del servicio de la gestión de ancho de banda.

VII. REFERENCIAS

Albujar Moreno, O. R. (2017). *"Diseño De Un Sistema De Seguridad De Red Basado En La Integración De Los Servidores Radius - Ldap En Linux Para Fortalecer El Acceso De La Red De La Clínica Millenium Chiclayo 2016".* Lambayeque.

Andreu, F., Pellejero, i., & Lesta, A. (2006). *Fundamentos y Aplicaciones de Seguridad en Redes WLAN.* Barcelona: Marcombo S.A.

Andreu, J. (2011). *Redes inalambricas (Servicios en red).* Madrid: Editex, S.A.

Areitio Bertolín, J. (2008). *Redes Informatica y sistemas de información.* Paraninfo.

Cabezas Granado, L., & Gonzales Lozano, F. (2010). *Redes Inalambricas.* España: Anaya multimedia.

Chuquicondor Requena, Y. D. (2017). *"Propuesta Metodológica Para La Gestión Y Administración Del "Propuesta Metodológica Para La Gestión Y Administración Del Universidad Nacional De Piura – 2016.".* Piura.

Delgado Ortiz, H. H. (2009). *Redes Inalambricas* . Macro empresa editora.

Dordoigne, J. (2018). *Redes informaticas nociones fundamentales.* Ediciones ENI.

Espinoza Arana, E. D. (2018). *"Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante RADIUS".* Lima.

Garbarino, J. (2012). *Protocolos Para Redes Inalámbricas de Sensores.* United States: EAE.

Jordan, V., Galperin, H., & Peres, W. (2010). *Acelerando la revolución digital: banda ancha para América Latina y el Caribe.* Chile.

Pilozo Campozano, D. A., & Zambrano Balladares, G. B. (2013). *"Estudio del Ancho de Banda para el tráfico de Redes WAN de los ISP, con estudiantes de la Universidad Politécnica*

Salesiana Sede Guayaquil carrera Ingeniería de Sistemas, mediante la implementación de una página web" (tesis de grado). Universidad politecnica salesiana, Guayaquil.

Valdivia Miranda, C. (2005). *Sistemas informáticos y redes locales*. Ediciones Paraninfo S.A. .

ANEXOS

Anexo N° 1: Laboratorio del Colegio privado Champagnat

Elaboración propia

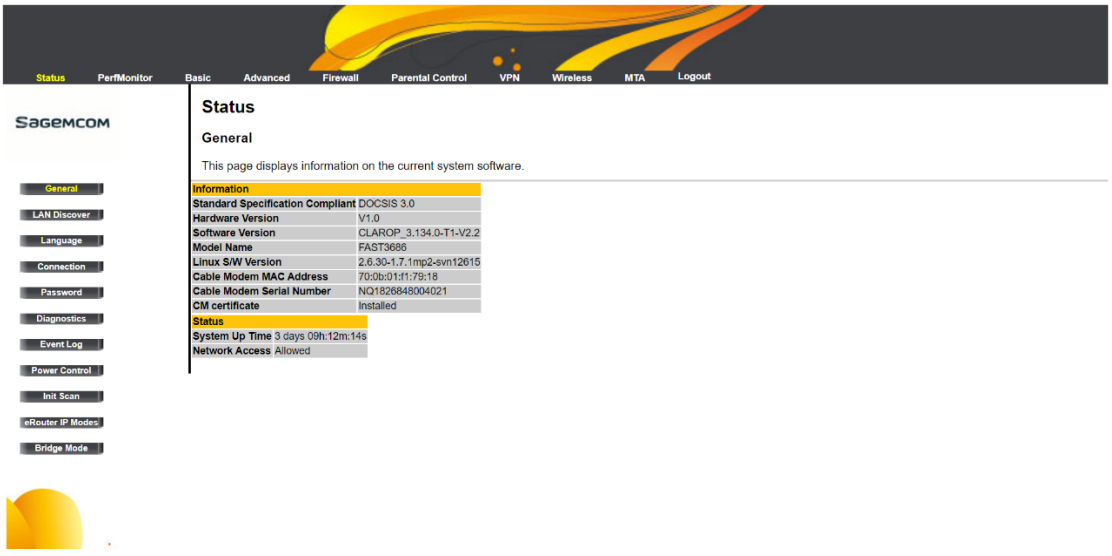
Anexo N° 2: Laboratorio del Colegio privado Champagnat

Elaboración propia

Anexo N° 3: Router inalámbrico SagecomF@ast 3284 u

Elaboración propia

Anexo N° 4: Configuración inicial del Router



Elaboración propia

Anexo N° 5: Paquetes de actualización

```
root@emersonegm:~# apt-get update
Obj:1 http://pe.archive.ubuntu.com/ubuntu eoan InRelease
Obj:2 http://pe.archive.ubuntu.com/ubuntu eoan-updates InRelease
Obj:3 http://pe.archive.ubuntu.com/ubuntu eoan-backports InRelease
Obj:4 http://pe.archive.ubuntu.com/ubuntu eoan-security InRelease
Leyendo lista de paquetes... Hecho
root@emersonegm:~# apt-get install freeradius
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  freeradius-common freeradius-config freeradius-utils freetds-common libct4 libdbi-perl
  libfreeradius3 libtalloc2 libwbclient0 make ssl-cert
Paquetes sugeridos:
  freeradius-ldap freeradius-postgresql freeradius-mysql freeradius-krb5 snmp freeradius-python2
  libclone-perl libmldbm-perl libnet-daemon-perl libsql-statement-perl make-doc openssl-blacklist
Se instalarán los siguientes paquetes NUEVOS:
  freeradius freeradius-common freeradius-config freeradius-utils freetds-common libct4
  libdbi-perl libfreeradius3 libtalloc2 libwbclient0 make ssl-cert
0 actualizados, 12 nuevos se instalarán, 0 para eliminar y 20 no actualizados.
Se necesita descargar 2.289 kB de archivos.
Se utilizarán 8.754 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] _
```

Elaboración Propia

apt-get update

apt-get install freeradius

Anexo N° 6: Comprobación del servicio instalado

```
        max_connections = 16
        lifetime = 0
        idle_timeout = 30
    }
}
listen {
        type = "acct"
        ipaddr = *
        port = 0
    limit {
        max_connections = 16
        lifetime = 0
        idle_timeout = 30
    }
}
listen {
        type = "auth"
        ipv6addr = ::
        port = 0
    limit {
        max_connections = 16
        lifetime = 0
        idle_timeout = 30
    }
}
listen {
        type = "acct"
        ipv6addr = ::
        port = 0
    limit {
        max_connections = 16
        lifetime = 0
        idle_timeout = 30
    }
}
Configuration appears to be OK
root@emersonegm:~#
```

Elaboración propia

Anexo N° 7: Configuración modulo usuarios

```
root@emersonegm:~# sudo ls /etc/freeradius/3.0
certs         experimental.conf  mods-available  panic.gdb   radiusd.conf     sites-enabled   users
clients.conf  hints              mods-config     policy.d    README.rst       templates.conf
dictionary    huntgroups         mods-enabled    proxy.conf  sites-available  trigger.conf
root@emersonegm:~# vi /etc/freeradius/3.0/users
```

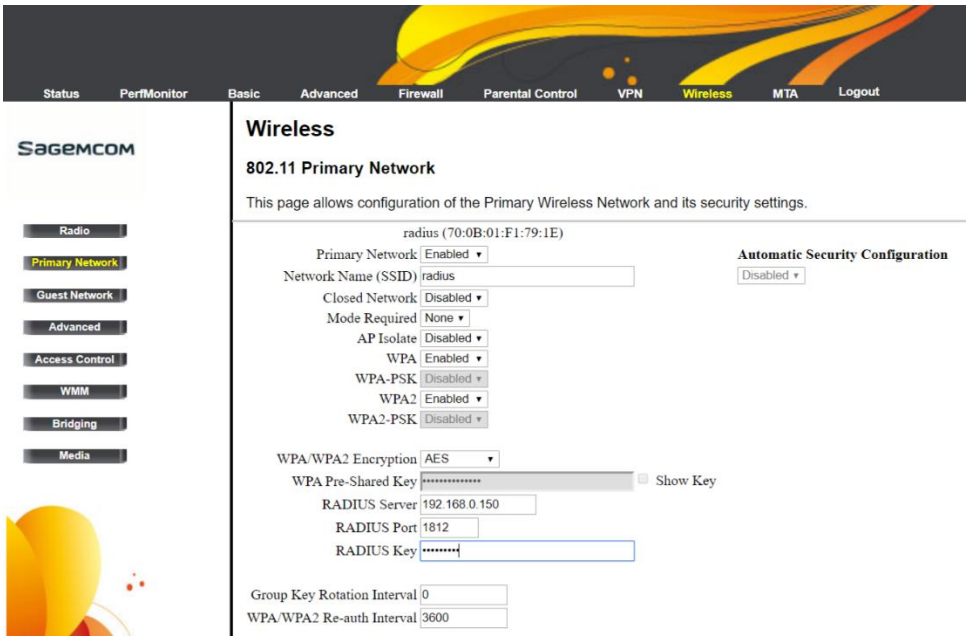
Elaboración propia

Anexo N° 8: Configurando el archivo clientes

```
#       secret          = testing123
#}

#client example.org {
#       ipaddr          = radius.example.org
#       secret          = testing123
#}

#
#  You can now specify one secret for a network of clients.
#  When a client request comes in, the BEST match is chosen.
#  i.e. The entry from the smallest possible network.
#
#client private-network-1 {
#       ipaddr          = 192.0.2.0/24
#       secret          = testing123-1
#}

#client private-network-2 {
#       ipaddr          = 198.51.100.0/24
#       secret          = testing123-2
#}0
client 192.168.0.150/24 {
secret = champagnat2017
shorname = redprivada_
}
######################################################################
#
#  Per-socket client lists.  The configuration entries are exact
#  You can have as many per-socket client lists as you have "listen"
#  sections, or you can re-use a list among multiple "listen" sections.
#
#  Un-comment this section, and edit a "listen" section to add:
#  "clients = per_socket_clients".  That IP address/port combination
#  will then accept ONLY the clients listed in this section.
#
-- INSERTAR --grabando @u                                          251,22        97%
```

Elaboración propia

Anexo N° 9: Configuración AP



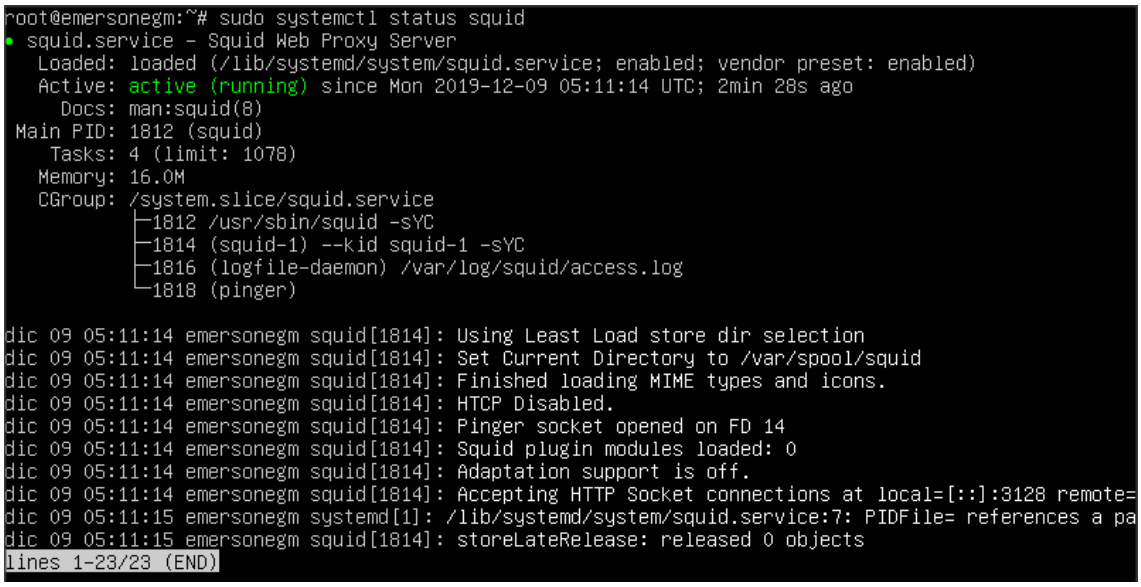
Elaboración propia

Anexo N° 10: Instalación de SQUID

```
root@emersonegm:~# sudo apt-get update
Obj:1 http://pe.archive.ubuntu.com/ubuntu eoan InRelease
Des:2 http://pe.archive.ubuntu.com/ubuntu eoan-updates InRelease [97,5 kB]
Des:3 http://pe.archive.ubuntu.com/ubuntu eoan-backports InRelease [88,8 kB]
Des:4 http://pe.archive.ubuntu.com/ubuntu eoan-security InRelease [97,5 kB]
Descargados 284 kB en 3s (98,7 kB/s)
Leyendo lista de paquetes... Hecho
root@emersonegm:~# sudo apt-get install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libecap3 libltdl7 squid-common squid-langpack
Paquetes sugeridos:
  squidclient squid-cgi squid-purge resolvconf smbclient winbind
Se instalarán los siguientes paquetes NUEVOS:
  libecap3 libltdl7 squid squid-common squid-langpack
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 20 no actualizados.
Se necesita descargar 2.974 kB de archivos.
Se utilizarán 13,9 MB de espacio de disco adicional después de esta operación.
```

Elaboración propia

Anexo N° 11: Verificación del SQUID



Elaboración propia