PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

TESIS DE GRADO PREVIA A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO EN SISTEMAS Y COMPUTACIÓN

TEMA

"ANÁLISIS DE LAS TÉCNICAS DE ENCRIPTACIÓN DE DATOS USADAS EN REDES WI-FI. CASO DE ESTUDIO: PUCE"

AUTOR

FRANCISCO JAVIER ZAMBRANO VALVERDE

DIRECTORA: ING. SUYANA ARCOS

QUITO 10 DE SEPTIEMBRE DE 2018

DEDICATORIA

Lo dedico a mis padres y hermanos quienes me han apoyado incondicionalmente en el trayecto de mi vida, motivándome cada día a luchar por los anhelos que me he planteado, y que a pesar de las adversidades nunca debo rendirme.

AGRADECIMIENTOS

Primeramente agradezco a dios por estar a mi lado sin importar quién soy.

Agradezco a mis maestros los cuales me guiaron a lo largo de mi carrera, aportando a mi crecimiento intelectual e inyectándome el valor de la perseverancia de alcanzar las metas.

También doy gracias a cada una de las personas que de alguna u otra manera, aportaron un granito de arena para lograr esta meta que me propuse en la vida, y que me ha permitido crecer intelectualmente como persona y ser humano.

RESUMEN

El ser humano en el transcurso de su historia ha buscado la forma de facilitar las actividades diarias que se realizan en la sociedad desde la invención de la rueda a esta el microchip que los ordenadores utilizan hoy en día. Pero en esta era, se ha impulsado agresivamente el uso de la información en todos los aspectos cotidianos por medio de conexiones por intranet o el más usado el internet. Los dispositivos se han desarrollado de tal forma que puedan ser más pequeños y potentes y su forma de conexión es a través de las redes inalámbricas, permitiendo que los dispositivos remotos puedan conectarse sin dificultad a través de señales de radiofrecuencia, permitiendo al usuario desplazarse con sus equipos portátiles dentro de un área de cobertura determinada. Accediendo a la información de cualquier parte del mundo por medio del internet, o a su vez transfiriendo o recibiendo información de un punto a otro sin la necesidad de utilizar un medio físico o cableado.

Sin embargo, los inconvenientes de conexión a las redes inalámbricas, son personas no autorizadas que puedan vulnerar las seguridades e ingresar a la información que se trasmite. Por tal motivo, encriptar la información que se trasmite de un punto a otro es actualmente indispensable con el propósito de proteger la integridad de la misma. En ese aspecto existen actualmente técnicas de encriptación WEB, WPA, WPA2 encargadas de convertir los datos en información confidencial.

ABSTRACT

The human being in the course of its history has sought to facilitate the activities that are carried out in society from the invention of the wheel to the microchip that users today. But at this time, the use of information has been aggressively promoted in all aspects of everyday life through intranet connections or the most used on the Internet.

The devices have been developed in such a way that they can be small and powerful and their form of connection is through wireless networks, allowing remote devices to access through radio frequency signals, allowing the user to move with their portable equipment inside. of a certain coverage area. Accessing information from any part of the world through the Internet, or through it transferring or receiving information from one point to another with the need to use a physical medium or wired.

However, the drawbacks of the connection to wireless networks, people without authorizations that can violate the security and enter the information that is transmitted. For this reason, encrypt the information that is transferred from one point to another is currently essential for the purpose of protecting the integrity of it. In this aspect there are currently encryption techniques WEB, WPA, WPA2 responsible for converting the data into confidential information.

INTRODUCCIÓN

El proyecto de investigación denominado "ANÁLISIS DE LAS TÉCNICAS DE ENCRIPTACIÓN DE DATOS USADAS EN REDES WI-FI. CASO DE ESTUDIO: PUCE" permitirá el lector introducirse un poco más a fondo de las técnicas de encriptación en redes inalámbricas.

Este proyecto iniciará con la explicación de los principales conceptos de técnicas de encriptación, algoritmos de cifrado, estándares de trabajo, autenticación de usuario y protocolos de autenticación para manejo seguro de la información. Esta permitirá realizar un análisis de la mejor técnica de encriptación en la que se pueda determinar las ventajas y desventajas de su uso en la "PUCE".

Por lo tanto, se realizará un ejemplo práctica para demostrar cuán importante son las técnicas de encriptación para mantener la seguridad e integridad de la información que circula por la red, además mediante el uso de la herramienta Wireshark encargada del análisis del tráfico de la red, se capturará los paquetes y determinará el nombre de usuario y contraseña de una determinada página WEB que no maneja las seguridades pertinentes, permitiendo identificar la importancia del uso de las técnicas de encriptación en las redes inalámbricas para garantizar la confidencialidad e integridad de los datos.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

CAPITULO I

1. Marco Teórico

1.1 Redes inalámbricas

Es la transmisión realizada por señales de radiofrecuencia, que se propagan por el aire y pueden cubrir áreas de centenares de metros cuadrados. En otras palabras podríamos decir que una red Wi-Fi (red inalámbrica) es aquella que nos permite transferir datos de un punto a otro sin la necesidad de utilizar un medio físico, como es el caso del cable de cobre o la fibra óptica por este motivo es muy atractivo para los usuarios finales. Las redes inalámbricas se catalogan de acuerdo a tres categorías como son PAN (Red de área personal), LAN (Red de Área Local), y WAN (Red de Área Amplia).

Figura: 1. 1 Red Inalámbrica

Fuente: (Gómez, 2010)

1.1.1 Tipos de redes Inalámbricas

1.1.1.1. Red de Área Personal (PAN)

Son redes inalámbricas que utilizan la tecnología bluetooth, permite la trasmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia a 2.4 GHz ofreciendo la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales como son impresoras, teléfonos celulares con tecnología bluetooth, mouse, teclado , computadoras, cámaras digitales etc. (Dominguez, 2002)

Figura: 1. 2 Red de Área Personal (PAN)

Fuente: https://sites.google.com/site/kiryaherrs/home/010-redes

1.1.1.2. Red de Área Local (LAN):

Son redes pequeñas que proporcionan servicio a usuarios dentro de una estructura común, que suelen ser una empresa, un centro, una casa, etc. (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015). Habría que decir también que este tipo de red es la más conocida, por su uso doméstico como en el entorno empresarial, además cabe señalar que cuando este tipo de red utiliza dispositivos inalámbricos se la conoce como WLAN.

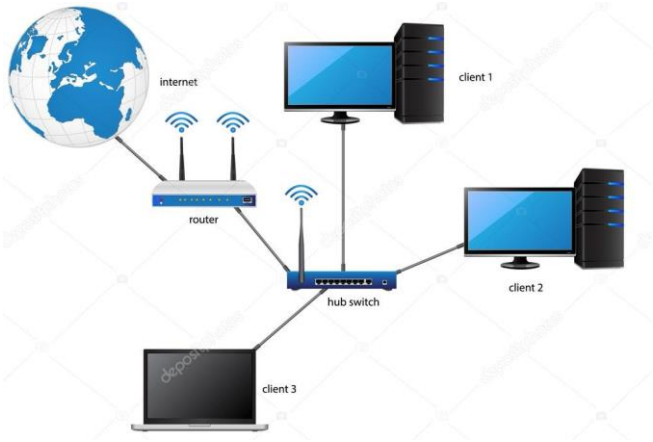

Figura: 1. 3 Red de Área Local (LAN)

Fuente: https://sp.depositphotos.com/49511103/stock-illustration-lan-network-diagram.html

1.1.1.3. Red de Área Extensa (WAN):

Las redes inalámbricas de área extensa tienen el alcance más amplio de todas las redes inalámbricas. Las tecnologías WAN permiten a los usuarios establecer conexiones inalámbricas a través de redes remotas públicas o privadas. Estas conexiones pueden mantenerse a través de áreas geográficas extensas, como ciudades o países. (Dominguez, 2002).

Figura: 1. 4 Red de Área Extensa (WAN)

Fuente: http://www.servervoip.com/blog/bs/red-voip-introduccion/

1.1.1.4. Red de Área Metropolitana (MAN):

Son varias redes LAN interconectadas en distancias cortas (unos pocos kilómetros). Por ejemplo las sucursales de una empresa en la misma ciudad o ciudades próximas. (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015). También permite la conexión de computadoras en varias localidades de una ciudad, país o escala mundial. Internet es una Red de Área Metropolitana que permite la comunicación entre varios puntos del mundo a través de distintas redes de computadoras.

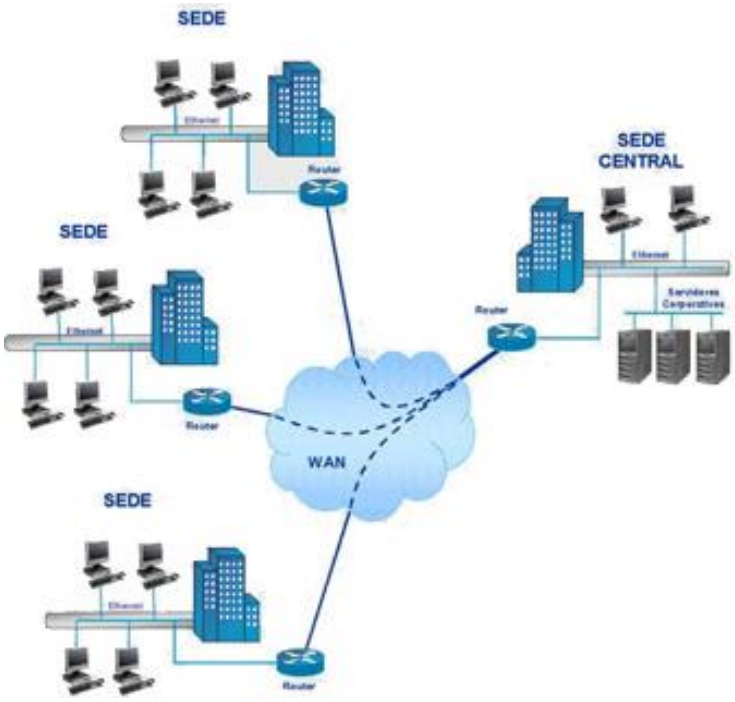

Figura: 1. 5 Red de Área Metropolitana (MAN)

Fuente: https://sites.google.com/a/galileo.edu/proyectofinal8203/redes-de-computadoras/redes-wan

1.1.2 Modos de operación de las redes inalámbricas

Hay dos modos de operación, uno ad-hoc, en el que las estaciones se comunican Entre sí directamente, y otro de Infraestructura, en el que las estaciones acceden a la red a través de uno o varios puntos de acceso. (Dominguez, 2002).

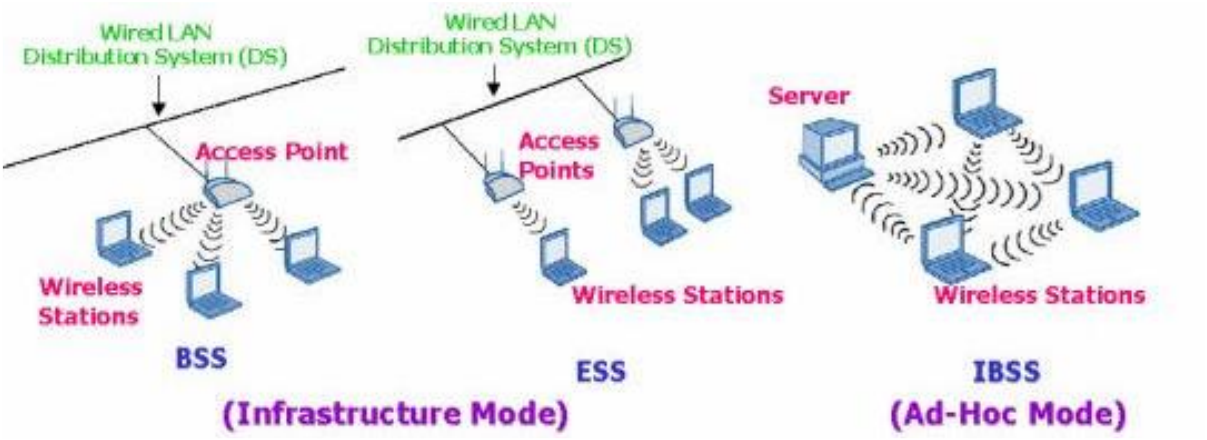

Figura: 1. 6 Modos de operación de redes inalámbricas

Fuente: (Dominguez, 2002)

1.1.3 Ventajas de las redes inalámbricas

- **Flexibilidad:** *Dentro de la zona de cobertura de la red inalámbrica los nodos se podrán comunicar sin necesidad de usar cables permitiendo al usuario tener movilidad.* (Dominguez, 2002)

- **Poca planificación:** *las redes inalámbricas gozan de gran popularidad debido a la facilidad de instalación y comodidad de uso*. (Marañón, 2009).La idea es que no se necesita pensar mucho en una distribución física de los equipos, Por lo contrario solo bastaría dentro del área de cobertura de la red inalámbrica.

- **Diseño y Robustez:** Los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo. Ante eventos inesperados como pueden ser usuarios que tropiezan con el cables hasta desastres naturales, una red cableada podría llegar a quedar completamente inutilizada, mientras que una red inalámbrica puede aguantar bastante mejor este tipo de percances.

- **Menos costes de mantenimiento:** las redes inalámbricas al no tener cable los costes de mantenimiento se reducen.

- **Accesibilidad:** la mayoría de equipos como son PDA, portátiles teléfonos celulares ya integran tecnología inalámbrica, la misma que permite conectarse a una red Wi-Fi

1.1.4 Estado actual de las redes Wireless

Actualmente esta tecnología se está expandiendo rápidamente por todo el mundo permitiéndonos que los dispositivos remotos se conecten sin dificultad, accediendo al internet y a toda la información que esta ofrece.

Una de las grandes ventajas de las redes inalámbricas que se puede destacar es la facilidad , robustez y costo de su instalación, permitiendo que los usuarios puedan desplazarse con sus equipos portátiles dentro de una área geográfica determinada, ya que las redes inalámbricas nos permiten llegar a lugares donde el cableado sea inaccesible. Por estas razones las redes inalámbricas se convierten en una implementación más sencilla. Asimismo, la instalación de estas redes no necesita de ningún cambio significativo de la infraestructura y el costo es mínimo. Sin embargo se debe tener en cuenta las desventajas que esta tecnología posee como son: velocidad limitada, área de cobertura, rangos de frecuencia y la más importante de todas la seguridad con las que están diseñadas, es bastante sencillo que personas no autorizadas puedan acceder a este tipo de redes, ya que estas se propaga a través del aire, dando posibilidad de que accedan a nuestra información.

Gracias a los avances tecnológicos y años de investigación se ha podido mejorar la seguridad e inalterabilidad de nuestra información, como son nuevos protocolos, métodos de protección, restricciones de direcciones MAC, autenticación y métodos de encriptación.

1.1.5 Importancia de las redes Wireless en la actualidad

En la actualidad vivimos en un mundo donde la tecnología es imprescindible para el trabajo, el estudio, y el hogar. Facilitando la vida diaria de cada una de las personas. Se ha vuelto indispensable para la mayoría de la sociedad, debido a que vamos a la par con la tecnología y los beneficios que esta nos ofrece.

Las redes inalámbricas tienen una gran importancia en el mundo ya que nos ha facilitado el acceso al internet de una forma rápida, sencilla y a través de cualquier dispositivo inalámbrico, ofreciéndonos el acceso a gran cantidad de información de cualquier pare del mundo. Una de las grandes ventajas que nos ofrece las redes inalámbricas es la movilidad con la que el usuario cuenta, puede estar en un lugar público o privado permitiendo tener interacción con otros usuarios. En la actualidad se ha convertido en una red muy solicitada mundialmente.

1.1.6 Vulnerabilidades en las redes WI-FI

1.1.6.1. Mac Spoofing:

Esto ocurre cuando alguna persona obtiene una dirección MAC de una red haciéndose pasar por un cliente autorizado. Este ataque se puede dar porque las placas de redes en general permiten cambiar el número MAC por otro. (Bautista, 2013)

1.1.6.2. Denial of Service:

Consiste en negar algún tipo de recurso o servicio. Puede ser usado para saturar una red con pedidos de disociación haciendo que sea imposible el acceso a otros usuarios, ya que los componentes de la red se asocian y desasocian una y otra vez. (Bautista, 2013)

1.1.6.3. Access Point Spoofing:

En este caso el atacante crea un punto de acceso falso y se hace pasar por él, el cliente piensa que se está conectado a una red WLAN verdadera cuando en realidad se está conectado directamente al atacante. (Bautista, 2013).

1.1.6.4. Man in the Middle (Hombre Del Medio):

En este caso el atacante es capaz de leer, escribir y modificar a voluntad todos los mensajes entre dos víctimas sin que ninguna de ellas lo reconozca, actuando así de conexión entre las dos (Hombre del Medio). (Bautista, 2013).

Ninguna red Wi-Fi es íntegramente segura. Sin embargo para reducir las posibilidades vulnerabilidades se toman medidas con el fin de evitar la posibilidad de intromisión de un tercero, generando seguridad en la transmisión de información.

1.1.7 Estándares en las redes inalámbricas

- 802.11.
  Estándar de Red Inalámbrica de Área Local original. Soporta de 1 Mbps a 2Mbps. (Dahua Tenazoa, 2011).

- 802.11a
  Estándar de Red Inalámbrica de Área Local de alta velocidad para banda de 5GHz Soporta 54 Mbps. (Dahua Tenazoa, 2011).

- 802.11b.
  Estándar de Red Inalámbrica de Área Local para banda de 2.4 GHz Soporta 11Mbps. (Dahua Tenazoa, 2011).

- 802.11e.

  Dirige los requerimientos de calidad de servicio para todas las interfaces de radio de Red Inalámbrica de Área Local. (Dahua Tenazoa, 2011).

- 802.11g.

  Establece una técnica de modulación adicional para banda de 2.4 GHz Propuesta para ofrecer velocidades hasta 54 Mbps y 108 Mbps. (Dahua Tenazoa, 2011).

- 802.11i.

  Dirige las actuales debilidades de seguridad para los protocolos de autenticación y encriptación. El estándar comprende los protocolos 802.1X, WPA-2 y AES. (Dahua Tenazoa, 2011).

1.1.8 Elementos básicos para una red inalámbrica

1.1.8.1. Punto de acceso:

El punto de acceso es el intermediario de la comunicación entre el emisor y el receptor en una red inalámbrica con topología de tipo infraestructura, que permite la comunicación a través de ondas electromagnéticas, es decir que actúa como un puente.

El AP puede comunicarse con cualquier dispositivo que se encuentre en su área de cobertura siendo el centro de las comunicaciones.

Figura: 1. 7 Punto de Acceso (AP)

Fuente: (Gómez, 2010)

Debo agregar que El punto de acceso puede llevar puertos de red cableados RJ45, como si se tratara de un hub o un Switch, actuando de intermediario entre la red cableada y la red inalámbrica. (Gómez, 2010).

1.1.8.1. Adaptador de red inalámbrica

Un adaptador de red es un dispositivo que conecta el equipo a una red. Para conectar el equipo portátil o el equipo de escritorio a una red inalámbrica, el equipo debe disponer de un adaptador de red inalámbrica. La mayoría de los equipos portátiles ya tienen instalado un adaptador de red inalámbrica.

Figura: 1. 8 Adaptador de Red Inalámbrica

Fuente: http://www.cavsi.com/preguntasrespuestas/cuantos-tipos-de-adaptadores-de-red-hay/

1.2Encriptación

La seguridad de la información es importante al momento en que se transmiten datos, así se puede evitar que terceros puedan acceder de forma maliciosa a la información. Por este motivo se utiliza técnicas de cifrado que permitirá que la información se mantenga segura desde el emisor hasta el receptor. *"Para convertir esta información en confidencial, se cifra por codificación, se somete al cifrado. De esta manera, solo el emisor y el receptor pueden leerlos"* (Dordoigne, 2006)

Por otro lado, las redes inalámbricas se han convertido en el medio preferencial usado por los usuarios para trasmitir información de un lugar a otro. Sin embargo; por el hecho de utilizar el aire como medio de transmisión es mucho más vulnerable que una red cableada. *"Para evitar este problema los datos que se transmiten se encriptan. Los algoritmos de encriptación más utilizados hoy en día son WEB, WPA, WPA2".* (Picón, 2014)

Para asegurar cualquier red inalámbrica sea WLAN, WWAN, WPAN es recomendable configurar la autentificación y cifrado que permitirá identificar a los usuarios que han ingresado a la red inalámbrica, mientras que; “…*los mecanismos cifrados aseguran que no sea posible decodificar el tráfico de usuario. Los protocolos de seguridad para las redes WLAN deben, por lo tanto, proteger estos dos puntos vulnerables ante posibles ataques. Con ese objetivo, desde las aparición de las redes WLAN los protocolos del nivel de enlace desarrollados específicamente para dotarlas de seguridad han sido WEP, WPA; IEEE 802.11i y WPA2.”* (Izaskun Pellejero F. A., 2006)

1.2.1 Técnicas de encriptación

“Corresponden a las tecnologías que permite la transmisión segura de información, Las redes Wi-Fi incorporan la posibilidad de encriptar la comunicación. Es una práctica recomendable ya que al ser un medio inalámbrico, de no hacerlo sería muy simple capturar el tráfico que por ella circula y por tanto la captura, por personas no deseadas, de datos sensibles. A lo largo del desarrollo de las redes Wi-Fi han ido surgiendo diferentes métodos de encriptación de las comunicaciones, evolución necesaria pues los distintos métodos han resultado ser vulnerables y ha sido necesario implementar algoritmos más seguros que solventaran los problemas de los anteriores. Estos, a su vez, van demandando más recursos de los equipos que los implementan por lo que la solución adoptada será siempre un compromiso entre rendimiento y seguridad. Se establecerá tres tipos de encriptaciones: WEB, WPA, WPA/WPA2**.**

1.2.2 Tipos de Técnicas de encriptación

- **Abierta y encriptación (WEB)**

Con la encriptación abierta, no existe ningún tipo de seguridad en la red inalámbrica, por tal motivo es vulnerable y está expuesta a posibles ataques de seguridad, por terceras personas. Por tal motivo si tenemos este tipo de encriptación nuestra información prácticamente está expuesta.

- **La encriptación (WPA)**

Esta técnica de encriptación es mucho más segura que la WEP, debido a que autentica al usuario, con esto quiero decir que el usuario para acceder a los recursos de la red necesariamente tiene que tener un nombre de usuario y contraseña que se encuentran almacenados en un servidor RADIUS. Este método es más difícil de configurar, ya que se tiene que crear el servidor y las credenciales de acceso.

- **La encriptación (WPA/WPA2)**

Este tipo de encriptación es la más recomendada para entornos empresariales. Trabaja conjuntamente con estándares, protocolos de autenticación y servidor de autenticación proporcionando una mayor seguridad en los datos, debido a que los entornos empresariales manejan gran cantidad de información.

1.2.3 Mecanismos de seguridad de redes inalámbricas

1.2.3.1 WEB (Wired Equivalent Privacy)

WEP (Wired Equivalent Privacy) fue el primer protocolo de encriptación introducido en el primer estándar IEEE 802.11 allá por 1999. Está basado en el algoritmo de encriptación RC4, con una clave secreta de 40 o 104 bits, combinada con un Vector de Inicialización (IV) de 24 bits para encriptar el mensaje de texto M y su checksum – el ICV (Integrity Check Value). El mensaje encriptado C se determinaba utilizando la siguiente fórmula: (Lehembre, 2006)

$$C = [\ M \parallel \mathrm{ICV}(M)\ ] + [\ \mathrm{RC4}(K \parallel \mathrm{IV})\ ]$$

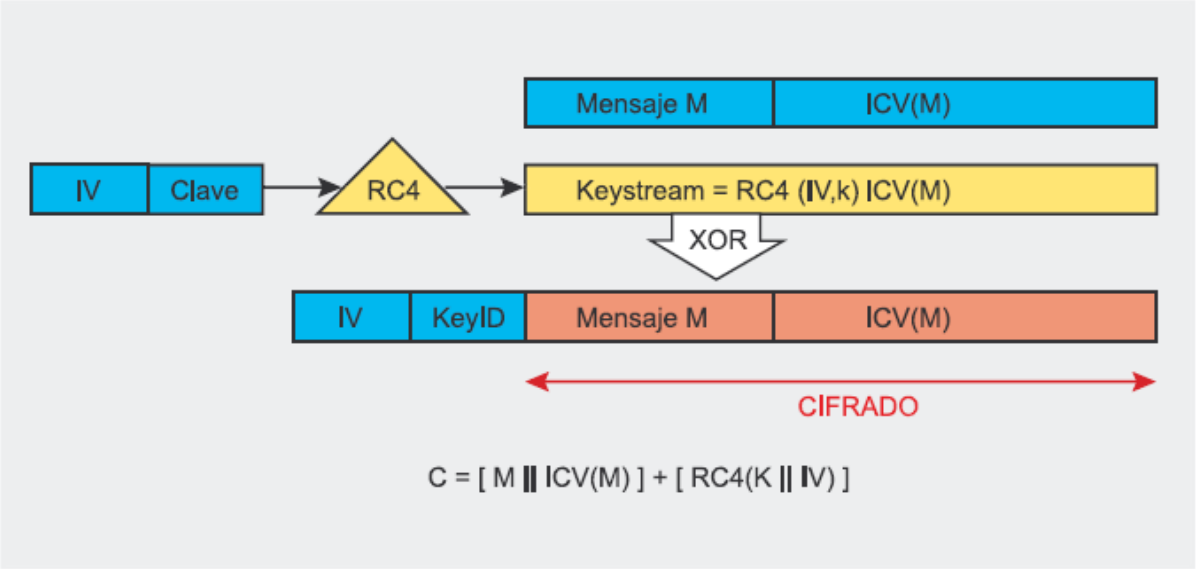

Figura: 1. 9 Protocolo de Encriptación WEB

Fuente: (Lehembre, 2006)

Uno de los propósitos de este tipo de encriptación es aumentar el nivel de seguridad para aquellos dispositivos que estén funcionando con WEB, con el objetivo de obtener la misma seguridad de las redes cableadas. WEB , fue diseñada con el propósito de implementarse sobre hardware no muy costoso, así como contar con una administración fácil y sencilla, donde cada dispositivo habilitado para la web usaría una clave, la cual funciona como clave de acceso a la red. Es por ello que la información protegida por WEB, es cifrada con la finalidad de que los datos o paquetes estén protegidos de los atacantes activos en las redes, así como poder constatar que solo los usuarios autentificados son los que reciben dicha información.

WEB fue diseñado para brindar seguridad en las redes inalámbricas utilizando un algoritmo de encriptación conocido como el RC4(Rivest Code 4), conocido como generador de claves de flujo.

- **Características y funcionamientos** *(Barajas, 2004)*

WEP (Wired Equivalent Privacy, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN. A continuación veremos las principales características de WEP.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca. El algoritmo de encriptación utilizado es RC4 con claves (seed), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante. (Barajas, 2004)

- **Fallos de seguridad WEB**

- Los IVs son cortos (24 bits – Para obtener el 50% de posibilidad de averiguar la clave se necesita menos de 5000 paquetes, además, se permite la reutilización del vector de inicialización, con esto quiero decir no hay seguridad contra la repetición de mensajes).

- La comprobación de la integridad de la información no es apropiada (se utiliza CRC32 para detectar errores y criptográficamente no es seguro por su linealidad).

- No existe un método integrado de actualización de las claves.

1.2.3.2 WPA (Wi-Fi Protected Access):

WPA es un protocolo de encriptación que se encarga de solucionar gran parte de las debilidades de la WEB debido a que este, tiene muchas vulnerabilidades. Este protocolo se lo considera suficientemente seguro, *Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.* (Barajas, 2004)

- **Tecnologías de la WPA**

Es uno de los estándares de la IEEE que facilita el control de acceso en redes basadas en puertos. El principio general de puertos, es enviar y recibir los diferentes tipos de datos a través de una interfaz, en un principio pensado para las ramas de un switch, pero también se puede aplicar a las diferentes formas de conectar a un Access Point con las estaciones. Las estaciones se conectarán a un puerto disponible del Access Point, el mismo que bloqueara el puerto hasta que se autentique el usuario para ello se utilizará el protocolo EAP y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service), si la autentificación del usuario es positiva entonces el punto de acceso abre el puerto que se encontraba bloqueado.

EAP (Extensible Authentication Protocol): establecido en el RFC 2284 como uno de los protocolos de autentificación extensible, la tarea principal es llevar acabo la autentificación,

autorización y contabilidad. EAP diseñado originalmente para el protocolo PPP (Point-to-Point Protocol), sin embargo WPA lo utiliza entre la estación y el servidor RADIUS. La forma EAP está definida en el estándar 802.1X bajo el calificativo de EAPOL.

TKIP (Temporal Key Integrity Protocol): Según revela Wi-Fi, es un protocolo encargado de la generación de claves para cada una de sus tramas.

MIC (Message Integrity Code): Comprueba la integridad de los datos de cada una de las tramas.

- **Modos de funcionamiento de WPA**

WPA puede funcionar en dos modos:

Con servidor AAA, RADIUS normalmente. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso.
Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

- **Mejoras de WPA respecto a WEP** (Barajas, 2004)

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes

deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (replay). Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un código nuevo nombrado MIC. Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP. Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

1.2.3.3 WPA2 o IEEE 802.11i

Este protocolo de encriptación posee un algoritmo de cifrado conocido como AES (Advanced Encryption Standard), que fue desarrollado por el NIS. Es un algoritmo de cifrado de bloque (RC4 es de flujo) maneja claves de 128, 192, 256 bits. Mientras mayor sea el tamaño de bits con el que se puede cifrar los datos, aumenta la complejidad del algoritmo de cifrado. El cual el requerimiento es un hardware potente para poder realizar sus algoritmos de encriptación. Es una técnica de cifrado de clave simétrica proporcionando una encriptación seguro para la protección de la información.

1.2.4 Configuraciones de seguridad

1.2.4.1. Configurar el firewall

Si el Router lo permite, es posible definir qué servicios y puertos pueden estar disponibles para el acceso externo a la red.

1.2.4.2. Acceso al Router por https:

Tomar medidas preventivas al momento de habilitar la configuración del punto de acceso a través del protocolo HTTPS, para evitar que personas no autorizadas puedan capturar paquetes y cifrar la contraseña de acceso a la configuración del dispositivo.

1.2.4.3. Modificar las credenciales de acceso

Cambiar la clave de acceso a la configuración del Router, ya que personas no autorizadas podrían acceder al dispositivo, mediante la clave por defecto. Es recomendable implementar para mayor seguridad una contraseña alfanumérica.

1.2.4.4. Configurar el tipo de cifrado de la red

Configurar la red para que utilice cifrado o encriptación. De esta forma, los datos que transiten por la red no serán comprensibles por terceros que estén monitoreando los mismos.

CAPITULO II

2. Tecnología de diseño y seguridad de redes inalámbricas

2.1Compatibilidad de estándares de la IEEE 802.11

"Todos los estándares de la IEEE 802.11 son compatibles con sus predecesores que operan en la misma banda de frecuencia. Sin embargo, cuando un dispositivo opera con una tecnología predecesora, toda la red se adapta a esa tecnología, lo que provoca que el rendimiento de la red disminuya considerablemente" (Castaño Ribes R. J., 2013)**.**

2.2 Redes inalámbricas según el Modo de operación

El estándar IEEE 802.11 define dos maneras de operar la primera se refiere ad Hoc y la segunda en infraestructura las mismas que se encargan de definir dos tipos de redes distintas las mismas que se explicaran a continuación

2.2.1 Redes Ad Hoc

La característica principal de este tipo de red, es que diferentes estaciones establecen conexiones inalámbricas directas entre sí, manteniendo una comunicación mutua. Estas redes suelen utilizarse de una manera puntual, cuando dos o más usuarios comparten algún recurso en un instante dado. *En el modo ad hoc el medio compartido es el aire (siendo más precisos, sería un canal dentro de una banda de frecuencia de radio) y no existe ningún intermediario. Todas las estaciones utilizan el medio para dirigirse a todas las estaciones que tienen en su radio de cobertura, todas estas estaciones deben estar provistas de una interfaz Wi-Fi. Sin embargo no se necesita ningún dispositivo adicional.* (Julio Barbancho Concejero, 2014)

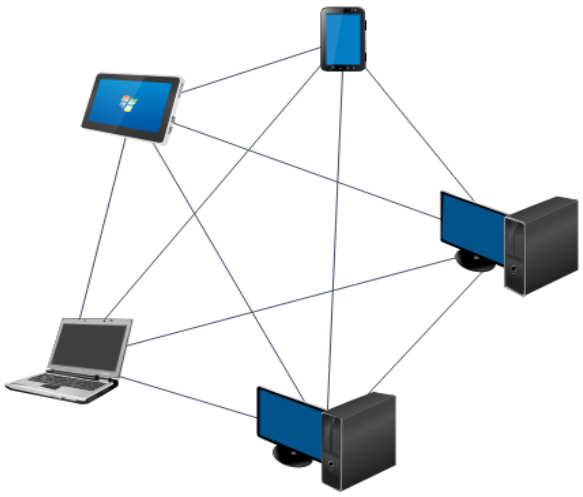

Figura: 2. 1 Configuración de una Red Ad-Hoc

Fuente: (Julio Barbancho Concejero, 2014)

2.2.2 Redes en infraestructura

El modo con infraestructura BSS (Basic Service Set). Está coordinado por una entidad denominada punto de acceso (AP). Todas las estaciones deberán asociarse para poder acceder al BSS (Basic Service Set). Si una estación quiere transmitir datos a otra deberá hacerlo pasando por el punto de acceso. Puede decirse que el punto de acceso actúa de concentrador. En este modo dos estaciones que no tengan cobertura entre sí, pueden transmitirse datos gracias al punto de acceso. (Julio Barbancho Concejero, 2014) . Se puede concluir que la red en infraestructura es de tipo cliente servidor, donde los clientes son los ordenadores que acceden a la red a través de un dispositivo inalámbrico denominado punto de acceso el mismo que trabaja como un nodo intermedio entre la red inalámbrica y la red cableada, este nodo intermedio se encarga de la comunicación entre las estaciones. Debo agregar que las estaciones se encargan de enviar y recibir información a través de un enlace o línea de transmisión por donde la información viaja.

Figura: 2. 2 Configuración de red Modo Infraestructura

Fuente: (Julio Barbancho Concejero, 2014)

2.3Redes inalámbricas según su relación funcional

2.3.1 Redes entre iguales (peer to peer)

La comunicación se realiza equipo a equipo, desde el equipo origen hasta el equipo destino. En otras palabras podemos decir que la tecnología de conexión peer to peer son dos dispositivos interconectados mediante un cable, o bien un servidor al cual están conectados. *No existe jerarquía y un equipo puede usar servicios o recursos de otro, del mismo modo que ofrecerlos.* (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015)

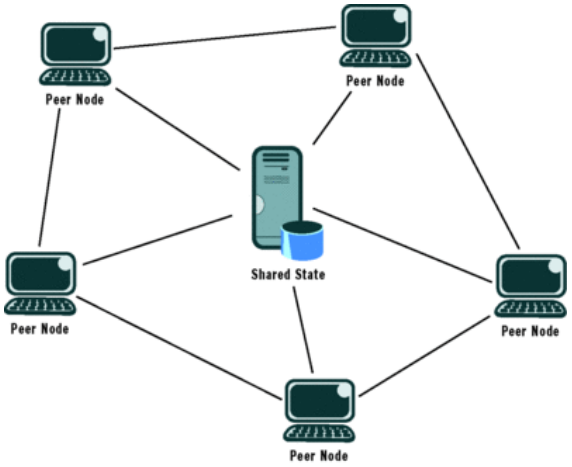

Figura: 2. 3 Configuración de una Red Peer to Peer

Fuente: https://www.unocero.com/noticias/ciencia/una-direccion-ip-no-es-una-persona/

2.3.2 Redes cliente servidor

Es la configuración más utilizada en redes medianas y grandes, está compuesta por dos partes: la primera corresponde a la cantidad de servidores considerando el tamaño y la complejidad de la red con la que se está trabajando y varias computadoras clientes. Una de las principales funciones de los servidores es centralizar y almacenar grandes volúmenes de datos, a los que se accede desde las computadoras clientes. Existe por lo menos un servidor que proporciona los servicios y los recursos, así como los clientes hacen uso de estos recursos

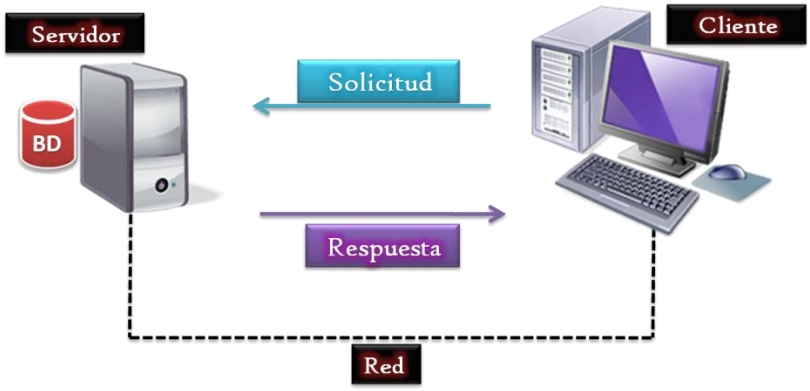

Figura: 2. 4 Configuración Cliente-Servidor

Fuente: http://tareaspswjessicavaldes.blogspot.com/2016/03/tarea-5-cliente-servidor.html

2.4Estándares de las redes inalámbricas

Existen varios protocolos y estándares para las redes locales inalámbricas, sin embargo las más aceptables y utilizadas son de la familia de la IEEE 802.11 definidos por el instituto de ingenieros eléctricos y electrónicos los mismos que se encargan de su mantenimiento y cumplimiento de este estándar, proporcionando la base para los productos con redes inalámbricas que hacen uso de la marca "Wi-fi". La aplicación de estos estándares ha permitido que las tecnologías inalámbricas alcancen tasas de transmisión necesarias para soportar datos, voz y video. Uno de los beneficios más importantes de estos estándares para las redes inalámbricas locales es que nos permite la interoperación de dispositivos de diferentes marcas. Esto permitirá la seguridad de que los productos ofrecerán y proporcionarán cierta funcionalidad independientemente de los fabricantes.

2.4.1 IEEE 802.11 (Redes Ethernet Inalámbricas)

Este estándar fue definido en el año de 1997, una de sus principales características es que opera en la banda de ISM a 2,4 GHz y trabaja con dos velocidades de transmisión teórica de 1 y 2 mega bits por segundo (Mbits/s), Cabe destacar que este estándar usa tres tecnologías diferentes

- Espectro de propagación de salto de frecuencia *(Frecuency Hopping Spread Spectrum (FHSS)).*
- Espectro de propagación de secuencia directa *(Direct Secuence Spread Spectrum (DSSS)).*
- Infrarrojo *(IR).*

Cada una de estas tecnologías utiliza un método diferente para transmitir señales inalámbricas a través del aire. El estándar original afirmaba la interoperabilidad entre dispositivos de comunicación que hacían uso de cada una de estas tecnologías inalámbricas ya mencionadas, pero no lo hacían entre las tres tecnologías. Estas debilidades encontradas fueron mejoradas en el estándar 802.11b, fue uno de los primeros estándares de la familia 802.11 en alcanzar una extensa aceptación entre los consumidores.

2.4.2 IEEE 802.11b (Ethernet Inalámbrico de alta velocidad)

El estándar fue introducido en el año 1999, es el estándar más utilizado, una de sus principales características que este estándar presente es el de ser robusto, maduro que al pasar del tiempo continua creciendo y evolucionando con relación a su antecesor. Además, presenta otras mejoras con respecto al estándar original 802.11, tiene velocidades de 5,5 y 11Mbps en el espectro de frecuencia de 2,4GHz. Esta ramificación es compatible con su antecesor original del estándar ya mencionado de 1 y 2 Mbps , la misma que presenta una nueva técnica de modulación de velocidad superior denominada Complementary Code Keying (CCK), Por tal razón, equipos de diferentes fabricantes tendrán la facilidad de conectarse con cualquier otro equipo, con la condición de que ambos cumplen con las especificaciones requeridas del estándar 802.11b.

2.4.3 IEEE 802.11a (Redes inalámbricas en la banda de los 5 GHz)

El estándar 802.11ª fue creado en el año de 1999 al mismo tiempo en el que el estándar 802.11b apareció, una de las características relevantes a este estándar, se encarga de operar en la banda de los 5Ghz y utiliza OFDM (*Orthogonal Frequency-Division Multiplexing*) que es una técnica de modulación de velocidad, la misma que permite una tasa de transmisión máxima de 54 Mbit/s. Uno de los mayores inconvenientes con este estándar es la no compatibilidad con los estándares que utilizan la banda de 2,4Ghz. Por lo demás y forma de trabajar es parecida al estándar 802.11g.

2.4.4 IEEE 802.11g (Velocidades de 54Mbps en la banda de 2,4GHz)

Este estándar fue introducido en junio del 2003, una de las características primordiales de su masiva aceptación en la interoperabilidad 802.11g con el 802.11b las mismas que utilizan la banda de 2,4 GHz al igual que su predecesor el estándar 802.11 b con la diferencia de que el mismo opera con una velocidad teórica de 54Mbps o cerca de 24.7 Mbit/s de velocidad real de trasmisión, similar a la del estándar 802.11ª. Además, es compatible con el estándar 802.11b y utiliza la misma técnica de modulación de velocidad que el estándar 802.11ª (ODFM), esto quiere decir que trabaja con una tasa máxima de transferencia de datos de 54bit/s.

2.5 Seguridad mediante controlador de punto de acceso

2.5.1 *Modificar las credenciales de acceso*

Las credenciales de acceso es una parte importante a la hora de ingresar a una red inalámbricamente, por lo que el administrador encargado de la red debe cambiar la clave de acceso a la configuración del Router, debido a que el dispositivo viene con claves por defecto lo que conlleva a que cualquier persona no autorizada podrían conocer los datos por defecto y

así tener acceso a la configuración de la red. Por tal motivo, se debe implementar para mayor seguridad una contraseña alfanumérica.

2.5.2 *Configurar el tipo de cifrado de la red*

Una vez que se ha establecido la red inalámbrica correspondiente, antes de navegar y conectar dispositivos inalámbricos a la red se debe tomar en cuenta la seguridad de la misma, para ello se debe configurar los parámetros de seguridad desde una computadora conectada por cable y acceder al Router o Access point a través de una dirección del tipo http://192.168.X.X que permitirá administrarlo de tal manera que se tome todas las medidas pertinentes de seguridad, configurando principalmente la técnica de encriptación. Todo esto ha fomentado que se quiera obtener una mayor seguridad en la transmisión de la información sobre todo a través de Internet especialmente en las redes inalámbricas ya que estas son mucho más vulnerables que las cableadas debidas que cualquier persona puede acceder a la red simplemente con tener un dispositivo con tecnología Wi-Fi.

2.5.3 *Configurar el firewall*

Si el Router lo permite, *el firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso*. (Alvarez, 2001). Además, es posible que los servicios y puertos pueden estar disponibles para acceder de forma externa a la red, evitando que terceros puedan acceder a información confidencial en la transmisión de datos o información. Por lo tanto, podemos asegurar que con un firewall bien configurado podemos evitar intromisiones no deseadas en nuestra red y computador.

2.5.4 *Acceso al Router por https:*

Configurar el Router mediante el protocolo HTTPS, para evitar que terceros puedan capturar la contraseña de acceso a la configuración del dispositivo. Con esto quiero decir, que toda

información que pasa a través de este protocolo se encripta, para que personas no autorizadas accedan a los datos y lean la información

2.5.5 *SSID de una red inalámbrica*

Todo tipo de red inalámbrica ya sea ad-hoc o infraestructura con único AP o con múltiples AP, tiene un nombre que la identifica: el identificador del conjunto de servicios (SSID). El SSID es un nombre compuesto por 32 dígitos alfanuméricos como máximo y es el que utilizan los usuarios para identificarse y conectarse a la red. Generalmente, los dispositivos que ofrecen conexión a una red inalámbrica publican su SSID para que las distintas estaciones los puedan reconocer con un simple escaneo de redes disponibles al alcance

2.6 Consideraciones para diseño de redes inalámbricas

En la actualidad las redes inalámbricas se consideran una solución de movilidad, flexibilidad y productividad. Por tal motivo, ha incrementado constantemente la implementación de este tipo de red debido a una fuerte tendencia entre los usuarios, debido a que existe mayor facilidad de acceso a la misma. Para el adecuado diseño de este tipo de red se debe tomar en cuenta la complejidad de la red, además, se debe considerar el uso de algunas herramientas de software que ayuden a previsualizar sobre los planos el funcionamiento de los puntos de acceso. De este modo, nos permitirá evaluar la cobertura y los niveles de señal. Para ello se debe considerar que en las redes inalámbricas existentes algunos factores que podrían influir en la cobertura de la señal, como pueden ser, las fuentes de atenuación de la señal (espejos, ventanas, paredes o muebles metálicos) y las posibles interferencias (teléfonos inalámbricos, hornos microondas, WLAN vecinas, etc.). *También se deberá tener en cuenta si es necesario instalar más de un punto de acceso inalámbrico en función de la densidad de usuarios o la necesidad de un ancho de banda mayor. En ocasiones, es necesario instalar más puntos de acceso con menor área de cobertura para satisfacer esta demanda y evitar a su vez la interferencia mutua.*

Una vez hecho el diseño y despliegue de infraestructura WLAN es imprescindible realizar un análisis de cobertura con el fin de asegurar el nivel de señal en cada punto y eliminar la interferencia entre los distintos puntos de acceso y canales. (Miranda, 2014)

2.7 Espectro de radio para las redes inalámbricas

Un espectro de radio no es nada más que un conjunto de ondas electromagnéticas cuyas propiedades permiten ser transportadoras de información. Además, tiene la capacidad de alterar los campos electromagnéticos a su alrededor, haciéndolos crecer y decrecer en intensidad de una manera periódica. Entre las principales propiedades de las ondas electromagnéticas encontramos las siguientes:

Frecuencia (v): número de ciclos o perturbaciones completas por unidad de tiempo. Se mide en hercios (Hz) o sus derivados (MHz, KHz, GHz). Un hercio corresponde a un ciclo por segundo.

Longitud de onda (λ): distancia que es capaz de recorrer la onda en el vacío en un ciclo o perturbación completa. La velocidad de las ondas electromagnéticas en el vacío es la misma para todos los tipos de onda. Como por ejemplo la de la luz. Por consiguiente, a mayor frecuencia, menor longitud de onda y viceversa.

Energía (E): la energía asociada a una onda electromagnética depende de la frecuencia. A mayor frecuencia, mayor energía. (Castaño Ribes R. J., 2013)

Para impedir que diferentes ondas electromagnéticas puedan interferir con otras señales existen regulaciones por parte de la Unión Internacional de Telecomunicaciones (ITU) encargada de regular a nivel mundial mientras que el Instituto Europeo de Estándares de Telecomunicaciones (ETSI) encargado de la regulación a nivel de Europa. Estas organizaciones cuya responsabilidad es dividir el espectro electromagnético en rangos de frecuencia, a los que conocemos con otro nombre denominado bandas, cabe destacar que cada banda puede subdividirse en más bandas de acuerdo a las necesidades requeridas.

Las comunicaciones inalámbricas son aquellas que se encuentran dentro de un rango de frecuencia denominado espectro radioeléctrico o también conocido con el nombre de bandas de radiofrecuencias, el rango en que oscila el espectro radioeléctrico es entre los 300hz y los 300Ghz.

2.7.1 Las bandas ISM (Industrial, Scientific and medical)

Actualmente este tipo de bandas ha sido conocido y popularizado por su uso en las redes WLAN. Estas bandas son de uso frecuente y no requieren de licencia para utilizarlas. Cuando decimos "Uso común" implica que utilizan mecanismos de protección frente a interferencias. Un punto muy importante que hay que resaltar es que cada país puede reservar una parte para su uso sin licencia, siempre y cuando no supere los niveles de potencia transmitida.

Tabla: 2. 1 Frecuencia Máxima y Mínima de la Banda ISM

Banda ISM	Frecuencia mínima	Frecuencia máxima
0,9Ghz	902MHz	928MHz
2,4 GHZ	2,400MHz	2,4835GHz
5,7GHZ	5,150GHZ	5,825GHz

Fuente: (Julio Barbancho Concejero, 2014)

A continuación se expone uno de los principales estándares de las redes inalámbricas, los mismos que trabajan en una determinada Banda ISM.

- *IEEE 802.11b. Definida para operar a 11Mbps. Utiliza la banda de 2,4 GHz. Se ha organizado en 14 canales con un ancho de banda de 22MHz cada uno.* (Julio Barbancho Concejero, 2014)

- *IEEE 802.11a. Utiliza la banda de 5GHz aunque el alcance es inferior al IEEE 802.11b, su velocidad alcanza los 54Mbps.* (Julio Barbancho Concejero, 2014)
- *IEEE 802.11g. Esta especificación permite velocidades de 54Mbps en la banda de 2,4 GHz, con la consiguiente ventaja de mayor alcance que la norma IEEE 802.11a.* (Julio Barbancho Concejero, 2014)
- *IEEE 802.11n. Permite una velocidad real de transmisión de hasta 300Mbps (con un límite teórico de hasta 600Mbps) y mayor alcance de operación al utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas en los transmisores y receptores. Puede trabajar en dos bandas de frecuencias: 2,4GHz (como 802.11b y 802.11g) y 5GHz (como 802.11a). Gracias a ello 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Como la banda de 5GHz está menos congestionada permite un mayor rendimiento.* (Julio Barbancho Concejero, 2014).

2.8 Tipos de encriptación en una red Wi-Fi

2.8.1 Redes Abiertas

Una de las características fundamentales de este tipo de red es que no tiene implementado ningún tipo de sistema de autenticación o cifrado. Las comunicaciones entre las distintas terminales y los AP viajan en texto plano (sin cifrar) y no se requiere ningún tipo de dato para acceder a la red.

Para proporcionar algún tipo de seguridad a las redes abiertas se puede considerar los siguientes elementos:

- ✓ Dirección MAC.
- ✓ Dirección IP.
- ✓ El ESSID de la red.

Filtrar el acceso a la red solo a aquellos terminales que tengan una dirección MAC o IP determinada o bloqueando el envío de los BEACON FRAMES, de forma que sea necesario conocer de antemano el valor del EDDID para conectarse a la red, son los medios de los que se dispone para asegurar un poco este tipo de sistemas.

Nótese que estas medidas propuestas tienen en común que todas ellas intentan limitar el acceso no autorizado del sistema, pero no impiden que alguien espié las comunicaciones. A continuación vamos a ver como saltarse las medidas propuestas anteriormente y otro tipo de ataques a los que se pueden ver sometidos las redes abiertas.

2.8.2 Encriptación (WEB)

Este esquema de encriptación WEB (Wired Equivalent Privacy, Privacidad equivalente a la Cableada), fue introducido en el estándar internacional 802.11 que corresponde a una red de área local inalámbrica (WLAN), una de sus principales características es que se encuentra implementado en la capa MAC y apoyado por la mayoría de los fabricantes de dispositivos inalámbricos. El protocolo de encriptación WEB está encargado de comprimir y cifrar los datos que se envían a través de las ondas de radios correspondientes a una determinada frecuencia. La forma como este protocolo de encriptación trabaja es, *encriptando el cuerpo y el CRC de cada trama 802.11 antes de la transmisión, utilizando un algoritmo de encriptación simétrico RC4; la estación receptora, ya sea un punto de acceso o una estación cliente, es encargada de desencriptar la trama* (Chiu), *en* otras palabras podríamos decir que tanto el cliente como la estación base deben tener conocimiento de la clave que se encripto para que así terceros no puedan acceder a esta información.

Uno de los principales objetivos que podemos a destacar del diseño WEB son:

- Confidencialidad: la meta fundamental de la WEB es encargarse de prevenir el robo de información.

- *Control de acceso: Encargada de proteger el acceso a la infraestructura de la red inalámbrica, esto se puede lograr a través del descarte de paquetes que no están debidamente encriptados* (Chiu).
- Integridad de los Datos: para que terceras personas no puedan acceder a la información que transita a través de un canal se debe prevenir la manipulación por parte de terceros

2.8.2.1 Principios de Funcionamiento

WEB es un algoritmo de seguridad utilizado para ofrecer protección a las redes inalámbricas, mediante los proceso de identificación y cifrado, esto incluye a la primera versión del estándar IEEE 802.11 y manteniendo sin cambio alguno en los estándares 80211ª y 802.11b con el único fin de que estos estándares tengan compatibilidad entre los distintos fabricantes responsables de los dispositivos inalámbricos.

Una de las principales características que destaca la encriptación WEB es la utilización del algoritmo de encriptación conocido como el RC4 (Rivest Code 4) el mismo que fue desarrollado por RSA Laboratories por Ron Rivest, en el año de 1987. Este algoritmo funciona como generador aleatorio, también conocido como generador de claves de flujo, el mismo que se encarga de tomar una entrada relativamente corta, produciendo una salida mucho más grande conocida como Clave Pseudo Aleatoria de Flujo, encargada para el cifrado de la información. *"Este sistema de cifrado como ya mencionamos anteriormente está basado en el algoritmo de cifrado RC4, utilizando para ello claves de 64 o de 128 bits. Cada clave consta de dos partes, una de ellas la tiene que configurar el usuario en cada uno de los puntos de acceso de la red, mientras que la otra se genera automáticamente y se denomina vector de inicialización, cuyo objetivo es obtener claves distintas para cada trama que se mueve en la red."* (SEGURIDAD EN REDES INALÁMBRICAS: WEP, WAP Y WAP2).

WEB tiene como pilar fundamental una clave secreta para el manejo seguro de la información, la misma que será compartida para todos los comunicadores y que se utiliza para cifrar los datos o información enviada a través de un canal. En la actualidad todas las estaciones y puntos de acceso comparten una misma clave, provocando que se disminuya el nivel de seguridad que

ofrece este sistema de seguridad. Además, la encriptación WEB maneja un mecanismo de verificación de integridad mediante la utilización de un algoritmo de comprobación de integridad de los mensajes conocido como CRC-32 al texto plano, permitiendo obtener un ICV (Integrity Check Value) que es integrado al texto cifrado de tal manera que el receptor del mensaje pueda verificar si la integridad del mensaje no ha sido modificado, en otras palabras podemos decir “*garantiza que los mensajes se reciben tal y como son enviados, sin duplicación, inserción, modificación, reordenación ni repeticiones*” (STALLINGS, 2004).

2.8.2.2 Proceso a detalle del cifrado WEB

2.8.2.2.1 Llave

Las llaves que están formadas por 40 o 104 bits se crean a partir de una clave, la misma que puede ser creada de manera automática o manualmente; esta clave debe ser conocida por todos los participantes y este hecho conlleva a que normalmente se emplee claves sencillas y poco cambiantes. A partir de esta clave se generan cuatro llaves de 40 bits de las cuales se empleará una diferente cada vez que tengamos que realizar el cifrado WEB.

Para obtener las llaves a partir de la clave, consiste en la aplicación de la operación XOR con la cadena ASCII de la clave de la cual obtenemos una semilla de 32bits. Para la realización de la operación XOR dividimos la clave en grupos de 4bytes como se muestra en la siguiente imagen.

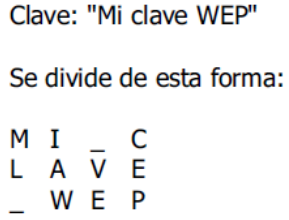

Figura: 2. 5 Inserción de la clave

Fuente: http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

Una vez que se tiene la clave dividida en grupos de 4 bytes se procederá hacer la operación XOR entre cada elemento de las columnas, permitiendo conseguir la semilla de 32 bits. Esta semilla utiliza un generador de números pseudoaleatorios, permitiendo así, formar 40 cadenas de 32 bits cada una. A partir del bit de cada una de las 40 cadenas se consigue 4 llaves de 40 bits, una de ellas se utilizará para realizar el cifrado WEB.

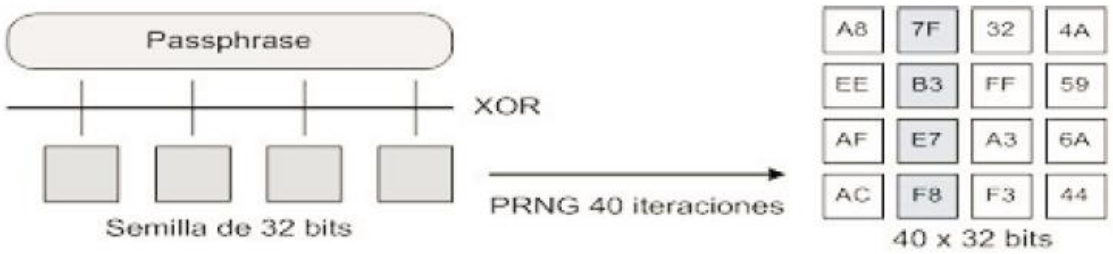

Figura: 2. 6 Operación XOR

Fuente: http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

2.8.2.2.2 Cifrado

Una vez obtenidas las llaves que se empleara para cifrar las tramas, se podrá visualizar el proceso de cifrado de las mismas.

Las tramas a cifrar están compuestas básicamente de una cabecera (header) y un contenido (payload), lo primero que se debe llevar a cabo es el cálculo del CRC del contenido a cifrar, de este cálculo se obtendrá el valor de chequeo de integridad, el mismo que será añadido al final de la trama cifrada para que el receptor pueda verificar que no ha sido alterada, en otras palabras podríamos decir que la integridad de la información ha quedado intacta.

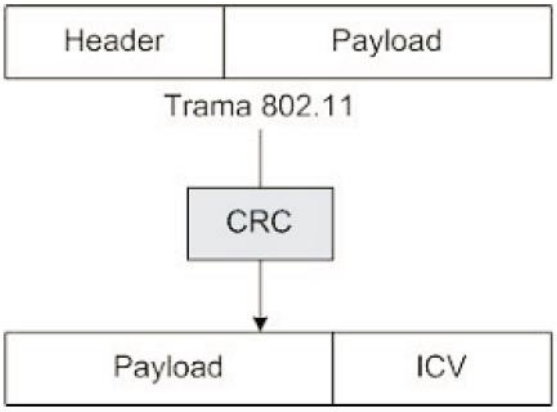

Figura: 2. 7 Creación del ICV

Fuente: http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

El siguiente paso a realizar es seleccionar una llave de 40bits de entre las posibles 4 y se añadirá el IV al inicio de la llave.

Podemos decir que el vector de inicialización es un contador que cambia de valor a medida que se van generando las tramas, de manera que, al agregar a la llave, se incremente el número de "llaves" posibles a utilizar.

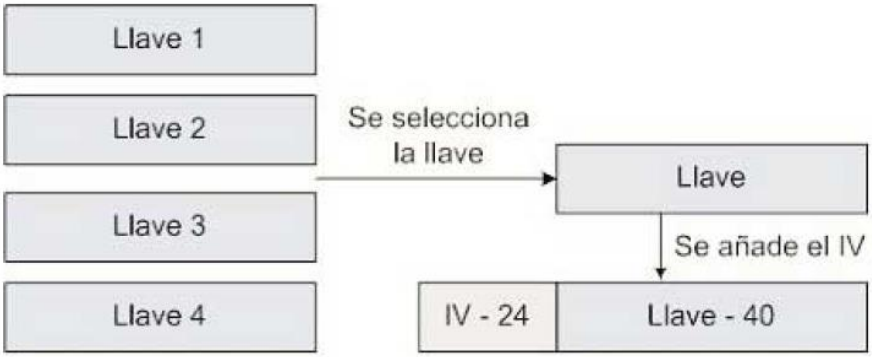

Figura: 2. 8 Se añade el IV a la llave seleccionada

Fuente: http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

El IV en palabras más sencillas, podemos decir que es un contador que cambia de valor a medida que se van generando las tramas, de manera que, al agregar a la llave, se incremente el número de "llaves" posibles a utilizar.

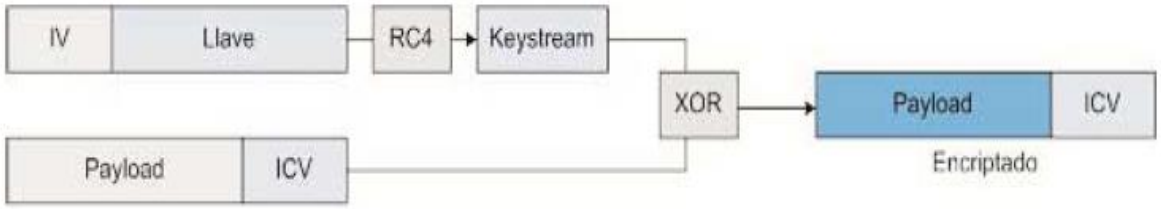

Figura: 2. 9 Obtención del contenido cifrado

Fuente: http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

Como parte final se efectuará un cifrado RC4 al conjunto IV + llave para conseguir el keystream o flujo de llave. El Keystream se utilizará para cifrar el conjunto Payload + ICV mediante la operación XOR, obteniendo así, el mensaje encriptado.

Figura: 2. 10 Paquete listo para ser enviado

Fuente: http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

2.8.2.3 Vulnerabilidades en el cifrado WEB

Originalmente se pensaba que el cifrado web era seguro, pero, se llegó a la conclusión de que no era así, manifestando que ofrece muchas vulnerabilidades tanto en el vector de inicialización como en el algoritmo de encriptación RC4.

2.8.2.3.1 Debilidad en el RC4

Una de las debilidades que destaca este algoritmo es que el primer byte de la clave de flujo revela información acerca de la clave secreta, por lo que esto puede ser explotado mediante un ataque planeado, mediante el cual terceros pueden tener suficiente número de paquetes cifrados buscando mensajes con el mismo IV, con lo que el atacante puede obtener información con respecto a la clave secreta byte por byte. Cabe notar que el atacante necesita entre 1,000.000 y 5,000.000 de paquetes para tener éxito en la obtención de la clave.

Uno de los objetivos principales de la encriptación web es proveer un mecanismo que permita garantizar la integridad de los mensajes. Con este fin, incluye un CRC-32 que viaja cifrado. Además, se ha demostrado que este método no es válido y es posible cambiar una parte del mensaje, así como el CRC, sin la necesidad de conocer el resto, debido a esta vulnerabilidad el atacante puede modificar algún número de la trama sin que el destino se diera cuenta de ello.

2.8.2.3.2 Debilidad del vector de inicialización

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. Recordemos que el IV es la parte que varía de la clave (seed) para impedir que un posible atacante recopile suficiente información cifrada con una misma clave (Saulo, 2010).

Aclarando que el estándar 802.11 no especifica cómo manejar el IV, por tal motivo el uso y manejo del mismo queda abierto a los fabricantes de los productos. El resultado de esto es que una gran parte de la implementación opta por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en uno para cada trama permitiendo que las primeras combinaciones de IVs y clave secreta se repitan frecuentemente. Además, hay que tomar en cuenta que cada estación utiliza la misma clave secreta, por lo que las tramas con igual clave se multiplican en el centro. Por añadidura el número de IVs no es lo suficientemente elevado (2^24 = 16 millones aproximadamente), por lo tanto terminará repitiéndose en cuestión de minutos u horas. Por consiguiente el tiempo será menor cuanto mayor sea la carga de la red.

En cuanto a lo que se refiere al IV lo ideal sería que este no se repitiese nunca, pero como podemos observar, esto es imposible en Web.

El número de veces que se repite un mismo IV dependerá de la implementación elegida para variar el IV por el fabricante (secuencia, aleatoria, etc.), además de la carga de la red. No se puede saber si dos tramas han sido cifradas con la misma clave, puesto que una de las características del IV es que se envía sin cifrar y por otro lado la clave secreta es estática.

¿Qué se podría hacer una vez que se ha capturado varias tramas con igual IV, es decir, con igual keystream? Se necesitara conocer el mensaje sin cifrar de una de ellas. Haciendo el XOR entre un mensaje sin cifrar y el mismo cifrado, nos dará el keystream para ese IV. Conociendo el keystream asociado a un IV, podremos descifrar todas las tramas que usen el mismo IV. El problema es entonces conocer un mensaje sin cifrar, aunque esto no es tan complicado, porque existen tráficos predecibles o bien, podemos provocarlos nosotros (mensajes ICMP de solicitud y respuesta de eco, confirmaciones de TCP, etc. (Saulo, 2010).

Con respecto a lo visto anteriormente no se pude deducir la clave secreta, por otro lado es posible generar una tabla con los IVs de los cuales se conoce los Keystream, por lo tanto nos permitirá descifrar cualquier mensaje que tenga un IV el mismo que se encuentra contenida en la tabla.

En lo que se refiere a la vulnerabilidad del protocolo de encriptación Web, es que este, permite deducir la clave total conociendo una parte de la clave (precisamente, el IV que es conocido). Por añadidura se necesita recopilar la cantidad suficiente de IVs y keystream asociados.

2.8.3 La encriptación WPA

Esta técnica de cifrado surgió para solucionar las deficiencias de seguridad que ofrecía el sistema WEB. En cuanto a este cifrado hace uso del TKIP, un protocolo que permite gestionar las claves de una forma dinámica, que resuelve mucho de las problemáticas que tenía el cifrado WEB entre las principales a destacar son la longitud de la clave, el cambio de la clave de forma estática a dinámica y la multidifusión.

Una de las principales características del cifrado WPA es la distribución dinámica de claves, así como también la utilización robusta del vector de inicialización (mejora de la confidencialidad de la información), así como también nuevas técnicas de integridad y autenticación. WPA protege la autenticación de los usuarios mediante la utilización de un servidor, donde se encuentran almacenadas las credenciales de acceso y contraseñas, que permiten el acceso a la red, Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante una clave precompartida, que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red. Además, *WPA nos permite utilizar un código de Integridad de Mensaje (Message Integrity Code - MIC) que es en realidad un algoritmo denominado “Michael”. El MIC de WPA incluye un mecanismo que contrarresta los intentos de ataque para vulnerar TKIP y bloques temporales. En resumen, WPA hace más difícil vulnerar las redes inalámbricas al incrementar los tamaños de las claves e IVs, reduciendo el número de paquetes enviados con claves relacionadas y añadiendo un sistema de verificación de mensajes* (Chacón, 2009).

Por otra parte WPA maneja diferentes sistemas de control de acceso como la validación de usuarios, contraseñas, certificado digital o simplemente utilizar una contraseña compartida cuyo objetivo es identificarse, podemos destacar algunos sistemas:

2.8.3.1 WPA-PSK (PRE_SHARED KEY)

Es un sistema de control de acceso mucho más simple tras WEB, una de las principales características es que trabaja con clave compartida, clave comprendida entre 8 y 63 caracteres. Es un sistema caracterizado por su fácil utilización y configuración. Por lo tanto, es uno de los más recomendables para ambientes familiares o pequeñas empresas. A propósito cualquier equipo que posea esta clave podrá conectarse a la red. Sin embargo, este sistema de acceso tiene el problema que al basarse en el uso de claves, está se puede identificar por medio de la utilización de la fuerza bruta, en otras palabras se va comprobando distintas claves hasta proporcionar la clave correcta.

2.8.3.2 WPA Enterprise

Se trata de un sistema mucho más complejo el cual se recomendaría que adopten empresas que hacen uso de las redes inalámbricas. Una de sus principales características que destaca WPA Empresarial es que funciona mediante el uso de usuario y contraseña o sistemas de certificados. Por otra parte, se suele utilizar con equipos de grandes recursos como son los servidores, para una adecuada gestión de usuarios o certificados. *Para desempeñar las tareas de autenticación, autorización y contabilidad. Utiliza el estándar IEEE 802.1x, que proporciona un control de acceso a red basados en puertos para la autenticación y distribución de claves.* (Guillermo, 2011). El punto de acceso conservará el puerto bloqueado hasta que se autentifique el usuario, para este propósito se utiliza el protocolo EAP encargado de la autenticación y un servidor AAA (Authentication Authorization Accounting. Una vez que el usuario haya recibido la autorización positiva, entonces el punto de acceso automáticamente abre el puerto y permite el acceso a la red, en caso de que la respuesta sea negativa el usuario no tendrá acceso.

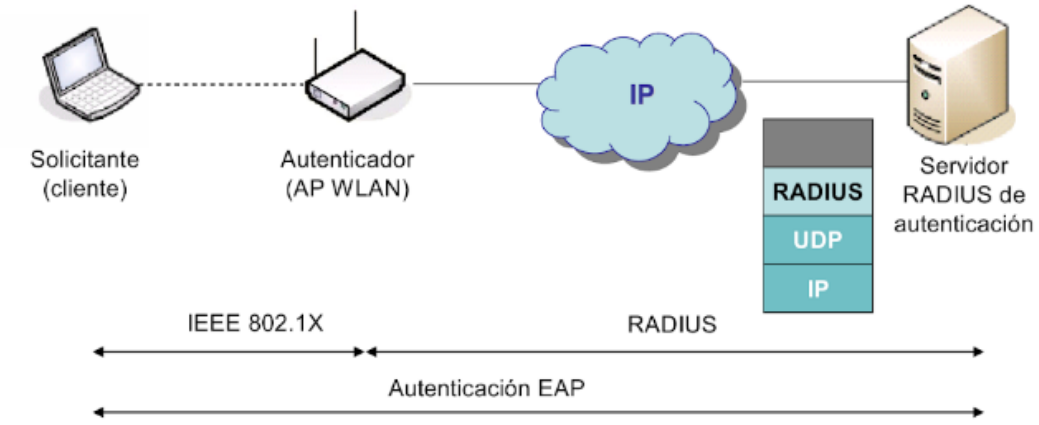

Figura: 2. 11 Arquitectura 802.1x/ EAP

Fuente: (Izaskun Pellejero F. A., 2006)

Los elementos que intervienen en un sistema 802.1x son:

- ✓ *Autenticador: generalmente un AP, cuya función es forzar el proceso de autenticación y enrutar en tráfico a los dispositivos adecuados de la red.*
- ✓ *Solicitante: es el usuario que solicita acceso a la red.*
- ✓ *Servidor de autentificación: lleva acabo la autenticación de las credenciales de usuario.*

Entre el cliente y el AP (Autenticador) Autenticador el protocolo utilizado es IEEE 802.1x. El protocolo entre el AP y el servidor de autenticación no está definido en el estándar IEEE 802.1x ni en el estándar 802.11 en este caso se usa RADIUS. Cuando el cliente se conecta a una AP que soporta 802.1x comienza el intercambio de mensajes de autenticación EAP entre ambos para llevar a cabo la autenticación de usuarios contra el servidor de autenticación. (Guillermo, 2011)

Dentro de este tipo de sistemas se puede complementar la seguridad haciendo uso de otros mecanismos como son: EAP-TLS, EAP-TLLs y LEAP, estos nos permiten contrarrestar las vulnerabilidades del 802.11, diversos fabricantes crearon varios de estos mecanismos EAP entre los cuales los detallaremos a continuación:

EAP-LEAP (Light EAP)

Este mecanismo fue desarrollado por Cisco cuya funcionalidad es proveer un mecanismo de autenticación mutua en base a una clave, por lo tanto se requiere que la estación del usuario se autentifique contra la red, así como también se necesita que la red se autentique con el usuario, asegurando de esta manera que terceros no accedan a la red, asegurando que los usuarios son los que dicen ser, por otra parte se introduce el uso de claves dinámicas por sesión.

EAP-TLS (Transport Layer Security EAP)

Fue desarrollado por Microsoft al igual que el anterior provee un mecanismo de autenticación mutua, además de credenciales seguras y claves de encriptación dinámicas; requiere de la distribución de certificado digitales por lo que puede llegar a generar overhead.

EAP-TTLS (Tunneled TLS)

Permite solo certificados del servidor, no de cliente; permite que los usuarios sean autenticados dentro de las WLANs con las credenciales existentes, utilizando criptografía de clave pública/privada, es más sencillo de gestionar y económico que EAP-TLS (Chiu).

2.8.3.3 TKIP (Temporal Key Integrity Protocol)

Fue un protocolo temporal introducido con WPA para sustituir el cifrado WEP también conocido como hashing de la clave WPA, incluye mecanismos del estándar emergente 802.11i para optimizar la seguridad de datos inalámbricos. WPA utiliza TKIP, el mismo algoritmo utilizado en WEB con la diferencia de que este construye claves de forma diferente para cada trama.

TKIP se considera una solución temporal encargada de resolver la problemática de la reutilización de claves WEB, de esta manera WEB utiliza periódicamente la misma clave para cifrar la información.

Para entender de una mejor manera el proceso de TKIP, este empieza con un clave temporal de 128 bits, cuya función principal es compartir entre los clientes y los puntos de acceso. La dirección MAC es combinada con la clave temporal, luego se encarga de agregar un vector de inicialización extenso, de 16 octetos, para generar la clave, encargada de cifrar los datos. Este procedimiento garantiza que cada una de las estaciones utilice Streams diferentes, claves para encriptar los datos. Además el hashing de la clave WEB está encargada de proteger los vectores de inicialización (IVs) débiles, para que de alguna u otra manera no sean expuestos haciendo el hashing del IV por cada paquete.

Para realizar el cifrado utiliza el algoritmo RC4, que es el mismo que utiliza WEB. Sin embargo una de las diferencias con la técnica de encriptación WEB, es que este, cambia las claves temporales cada mil paquetes, proporcionando así, un método de distribución dinámico de claves, mejorando notablemente la seguridad de la red inalámbrica

2.8.4 Mejoras de WPA con respecto a WEB

WPA soluciona la debilidad del vector de inicialización (IV) de WEB mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a la 48 combinaciones de claves diferentes, lo cual parece un número lo suficientemente elevado como para tener duplicados. (Guillermo, 2011).

El algoritmo RC4 es utilizado en el cifrado WEB, así como también en WPA. La secuencia de los IVs son conocidos por ambos extremos de la comunicación, en consecuencia se puede aprovechar para evitar ataques de repetición de tramas (replay).

WEB propone el método CRC-32 para garantizar la integridad de los mensajes (ICV), se ha demostrado que este método es inservible en este cifrado, por tal motivo se ha incluido un nuevo código denominado MIC (Message Integrity Code) o Michael, cuya principal característica es verificar la integridad de las tramas.

Actualmente las claves son generadas dinámicamente y distribuidas de manera automática, por lo tanto se evita tener que modificarlas de forma manual en cada uno de los elementos de la red en un determinado tiempo, como solía ocurrir en el cifrado WEB.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEB así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1x/EAP/RADIUS, su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad. (Saulo, 2010)

2.8.5 La encriptación WPA2

WPA2 (Wifi Protected Access 2) este cifrado es una de las versiones mejoradas de los protocolos de seguridad WEB y WPA. WPA2 es una certificación de producto que se encuentra disponible a través de Wi-Fi Alliance, por lo que se encarga de certificar que el equipo con

tecnología inalámbrica es compatible con el estándar IEEE 802.11i. La mejoría más importante de WPA2 con respecto a su antecesor fue el uso del estándar de cifrado avanzado (AES). Este cifrado es considerado, generalmente, seguro. Por otro lado, una de las principales vulnerabilidades de esta técnica de encriptación seria por ataques de fuerza bruta, las mismas que sería evitada por una fuerte contraseña.

En resumen, a lo expuesto anteriormente se puede decir que WPA2 soluciona las vulnerabilidades detectadas en la primera versión (WPA), incorporando todas las características del estándar IEEE 802.11i las mismas que su antecesor no tenía.

El cifrado WPA 2 presente dos cambios significativos con relación a la primera versión (WPA):

- ✓ *El reemplazo del algoritmo Michael por un código de autenticación conocido como el protocolo "Counter-Mode/CBC-Mac" que es considerado criptográficamente seguro.*
- ✓ *Reemplazo del algoritmo RC4 por el algoritmo AES, uno de los más seguros actualmente.*

2.8.5.1 Características de WPA2

WPA2 incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter- Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC. Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc). (Saulo, 2010)

2.8.5.2 AES (Advanced Encryption Standard)

Es un protocolo más seguro e introducido en WPA2, encargado de sustituir al cifrado WPA cuya versión fue su antecesor. Una de las ventajas de este mecanismo de seguridad es que puede implementarse tanto en hardware como en software. Además, este es un sistema criptográfico que se encarga de operar con bloques y claves de longitud variable entre los que se pueden destacar son los siguientes: AES de 128 bits, 192 bits y finalmente de 256 bits.

El resultado intermedio del cifrado constituye una matriz de bytes de cuatro filas por cuatro columnas. A esta matriz se le vuelve a aplicar una serie de bucles de cifrado basado en operaciones matemáticas (sustituciones no lineales de bytes, desplazamiento de filas de la matriz, combinaciones de las columnas mediante multiplicaciones lógicas y suma XOR en base a claves intermedias).

Con referencia a la seguridad, AES tiene 10 rondas para llaves de 128 bits, 12 rondas para llaves de 192 bits y 14 rondas para llaves de 256 bits (Guillermo, 2011). Además AES posee un algoritmo de cifrado de bloques encargado de separar el mensaje en trozos de tamaño fijo, por ejemplo de 64 o 128 bits. La forma como se manejan estos tipos de mensajes se denomina "modo de cifrado".

CAPITULO III

3. Diseño de la red inalámbrica y técnicas de encriptación

3.1Topologías de red

Es la manera física y lógica en que los computadores están conectados, cuyo objetivo es intercambiar datos entre sí mediante *un recurso de comunicación, es decir la estructura topológica de la red, es un parámetro primario que condiciona fuertemente las prestaciones que de la red pueden obtenerse."* (GARCÍA, 1989). *Sin embargo, …es conveniente aclarar que…Una cosa es como estén conectados y dispuestos los equipos desde un punto de vista físico y visual y otra cosa es como "entiendan" esos equipos que están conectados entre sí a un nivel lógico.* (Heredero, 2004). Entre las más destacadas topologías de red tenemos las siguientes:

3.1.1 Jerarquía

Es una extensión de la arquitectura en estrella por interconexiones de varias. Permite establecer una jerarquía clasificando a las estaciones en grupos y niveles según el nodo al que están conectadas y su distancia jerárquica al nodo central. De características similares a la red en estrella, reduce la longitud de los medios de comunicación incrementando el número de nodos. (GARCÍA, 1989)

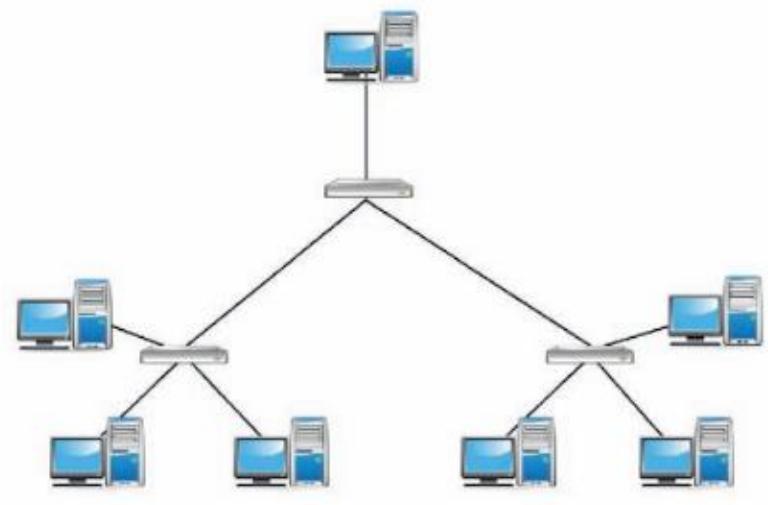

Figura: 3. 1 Topología jerárquica

Fuente: (Ma DEL CARMEN ROMERO TERNERO, 2010)

4.3.4.1 Ventajas e inconvenientes

Ventaja

- Facilita el crecimiento de la red, estableciendo jerarquía en grupos y niveles según el nodo al que se encuentran conectados, expandiéndose esta topología como ramas en un árbol.

Inconveniente

- *El fallo de un nodo implica la interrupción de las comunicaciones en toda la rama del árbol que cuelga de ese nodo* (Ma DEL CARMEN ROMERO TERNERO, 2010)

3.1.2 Bus

El flujo de información se fundamenta en un cable central; el cual se encarga de transmitir la información secuencialmente a todas las computadoras de la red que forman ramificaciones en cada nodo de red. "…*Este medio físico se encuentra interrumpido por los dos extremos y terminado por elementos eléctricos que aseguran sus características de transmisión."* (Heredero, 2004).

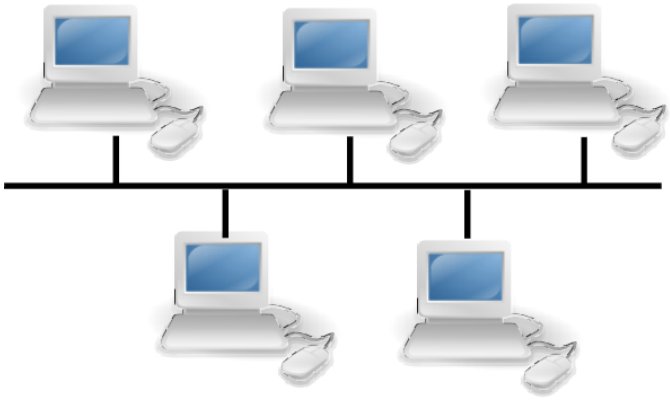

Figura: 3. 2 Topología Bus

Fuente: https://clasificaciondelasredesblog.wordpress.com/2017/05/09/topologia-bus-o-lineal/

4.3.4.2 Ventajas e inconvenientes

Ventajas

- Posee una arquitectura simple fácil de instalar y con potencial de crecimiento.

Inconvenientes

- El mayor problema de este tipo de topología es que cuando existe un problema en el canal, prácticamente degrada toda la red.

- A medida que la red crece el desempeño disminuye, producido por las limitaciones físicas del canal que afectan la calidad de la señal.

3.1.3 Anillo

Esta topología conecta las estaciones de trabajo en la red una tras otra en forma de anillo mediante un flujo de información en una sola dirección hasta llegar a su destino. Sin embargo, si fallará alguna estación de trabajo la red dejaría de funcionar, pero actualmente se ha provisto de soluciones para minimizar este riesgo mediante la aplicación de "…*un cableado redundante (anillo activo más anillo Stand-By), o colocar relés By Pass que permiten "saltarse" las estaciones que se encuentran fuera de servicio.."* (Rodríguez, 2006) Para poder sobrepasar el altercado hasta solucionar el incidente detectado.

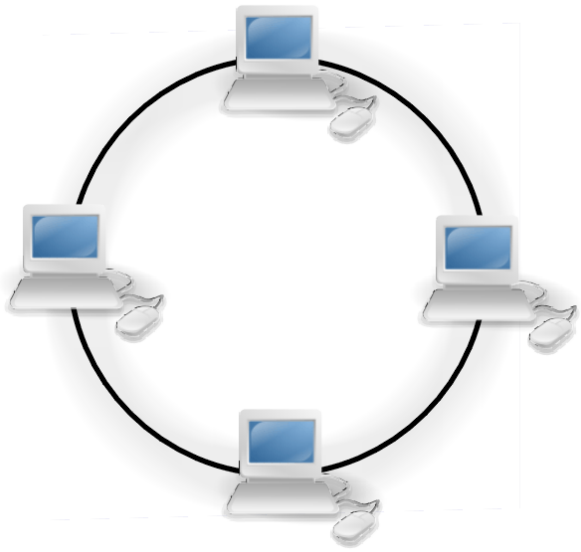

Figura: 3. 3 Topología de Anillo

Fuente: http://culturacion.com/topologia-de-red-malla-estrella-arbol-bus-y-anillo/

4.3.4.3 Ventajas e inconvenientes

Ventajas

- Mantiene el rendimiento del flujo de información a pesar del crecimiento de usuarios que utilizan la red.

Inconvenientes

- Para evitar que la red deje de funcionar al momento que una estación de trabajo no funcione se incurre en alternativas que aumentan el costo de su instalación y mantenimiento, lo que reduce en mucho su eficacia.

3.1.4 Estrella

En esta *topología en estrella todos los equipos están conectados a un nodo central, que realiza las tareas de distribución, conmutación y control de flujo de todas las comunicaciones que circulan por la red.* (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015) Notándose que estos dispositivos no están conectados directamente entre sí y que todos dependen de un punto central "activo" donde pasan todos los paquetes de usuarios.

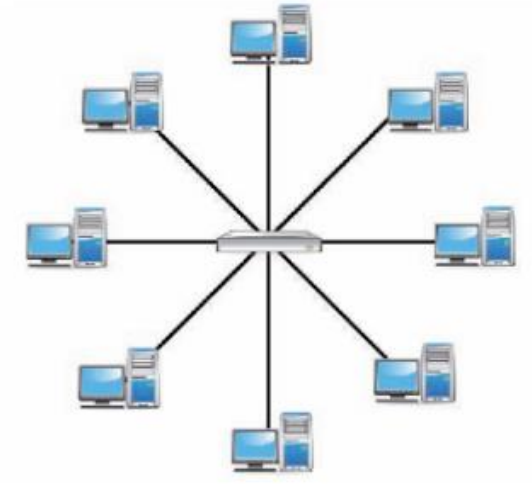

Figura: 3. 4 Topología Estrella

Fuente: (Ma DEL CARMEN ROMERO TERNERO, 2010)

4.3.4.4 Ventajas e inconvenientes

Ventajas

- Siempre y cuando el nodo central no falle, las estaciones de trabajo se mantendrán operativas, así otras se encuentren sin funcionar.
- Esta arquitectura permite agregar nuevas estaciones de trabajo fácilmente y su diseño, instalación y mantenimiento dependerá de la capacidad del nodo central.

Inconvenientes

- *Como toda la información que circula por la red debe pasar por el nodo central, este se convierte en el cuello de botella de la red, ya que todos los mensajes deben pasar por él. Si el nodo central falla, la red no funcionara.* (Ma DEL CARMEN ROMERO TERNERO, 2010)

3.1.5 Malla

"…En esta topología cada nodo se conecta a todos los demás, de forma que los datos pueden viajar del nodo origen al destino siguiendo distintas rutas." (Ma DEL CARMEN ROMERO TERNERO, 2010)

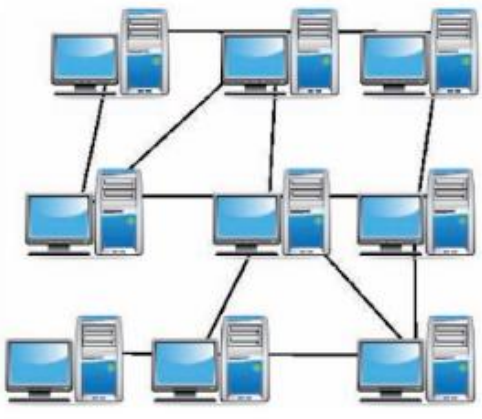

Figura: 3. 5 Topología en Malla

Fuente: (Ma DEL CARMEN ROMERO TERNERO, 2010)

4.3.4.5 Ventajas e inconvenientes

Ventajas

- *Como cada nodo está conectado físicamente a los demás, si algún enlace falla los datos siempre encontraran una ruta alternativa para llegar a su destino. Por este motivo, este tipo de red se instala para intentar garantizar que la comunicación nunca se interrumpa*. (Ma DEL CARMEN ROMERO TERNERO, 2010)

Inconvenientes

- La arquitectura de esta topología soporta un número limitados de nodos, pues en caso contrario el número de enlaces se dispararía.
- Este tipo de topología representa el uso de más recursos financieros para su diseño, implementación y mantenimiento.

3.2Tipos de AP y Ubicación de los Puntos de Acceso "PUCE" Facultad de Ingeniería

3.2.1 Especificaciones de la AP650 y AP7532

3.2.1.1. AP650 802.11n WLAN Access Point

Figura: 3. 6 AP650

Fuente:
https://www.simat.co.th/site/data/ckfinder/files/Motorola%20AP650,%20Access%20Point%20.pdf

El punto de acceso AP650 es un dispositivo de infraestructura WLAN, fácil de implementar y mantener, además, cabe mencionar que este dispositivo tiene la capacidad para proporcionar una LAN inalámbrica (WLAN) en oficinas o instalaciones de cualquier tipo de sede. Al respecto conviene decir que este dispositivo es un punto de acceso multipropósito, con esto quiero decir

que el AP650 permite expandir, el soporte inmediato del servicio de asistencia. Debo agregar que el servicio de asistencia es como si estuviera un técnico debajo del punto de acceso.

El dispositivo AP650 trabaja en una plataforma común, proporcionando un funcionamiento sin inconvenientes, un servicio seguro y un soporte técnico inmediato. Siendo, un dispositivos valioso para una adecuada administración de las redes inalámbricas en las múltiples sucursales o sedes. Por otro lado, conviene decir que la AP650 está equipado con la función Smart RF en la que el interruptor / controlador se encarga de optimizar automáticamente la potencia y selección de canales para que cada usuario que quiere acceder a la red inalámbrica tengan siempre movilidad y acceso.

Tabla: 3. 1 Especificaciones Generales del AP650

Physical Characteristics	AP650 (internal antenna)	AP650 (external antenna)
Dimensions:	9.5 In. L x 7.5 in. W x 1.7 in. 241.3 cm L x 189.61 cm W x 43.6 cm H	8.5 In. L x 5.6 in. W x 1.5 in. H216.4 cm L x 141.0 cm W x 37.71 cm H
Weight:	2.0 lbs./.91 kg	2.5 lbs./1.14 kg
Part number:*	AP-0650-60010-WW; AP-0650-60010-US; AP-0650-66030-WW ; AP-0650-66030-US	AP-0650-60020-WW; AP-0650-60020-US AP-0650-66040-WW; AP-0650-66040-US
Available mounting configurations:	Ceiling-mount (to suspended ceiling T-bars, below tile); wall mount	Ceiling-mount (above tile); wall-mount
Plenum rated:	No	Yes, certified to UL 2043
LED indicators:	2 LED indicators with multiple modes indicating 2.4GHz/5 GHz Activity, Power, Adoption and Errors	
Wireless Data Communications and Networking		
Data rates supported:	802.11b/g: 1,2,5.5,11,6,9,12,18,24,36,48, and 54Mbps802.11a: 6,9,12,18,24,36,48, and 54Mbps 802.11n: MCS 0-15 up to 300Mbps	
Network standard:	802.11a, 802.11b, 802.11g, 802.11n	
Wireless medium:	Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM), and Spatial Multiplexing (MIMO)	
VLANs/WLANs supported:	RFS6000 — 32 VLANs/32 WLANs; RFS7000 — 256 VLANs/256 WLANs	

Uplink:	Auto-sensing 10/100/1000Base-T Ethernet	
Radio Characteristics		
Operating channels:	5GHz: All channels from 4920 MHz to 5825 MHz 2.4GHz: Chan 1-13 (2412-2472 MHz), Chan 14 (2484 MHz) Japan only Actual operating frequencies depend on national regulatory limits	
Maximum available transmit power:	24dBm	
Transmit power Adjustment:	1dB increments	
Antenna configuration:	2x3 MIMO (transmit on two and receive on all three antennas)	
Operating bands:	FCC EU 2.412 to 2.462 GHz 2.412 to 2.472 GHz 5.150 to 5.250 (UNII -1) 5.150 to 5.250 GHz 5.725 to 5.825 (UNII -3) 5.150 to 5.350 GHz 5.725 to 5.850 (ISM) 5.470 to 5.725 GHz (Country Specific) Japan 2.412 to 2.484GHz 4.900 to 5.000 GHz 5.150 to 5.250 GHz	
Maximum radio transmit power:		
BAND	**SINGLE ANTENNA COMPOSITE TRANSMIT POWER**	**DUAL ANTENNA COMPOSITE TRANSMIT POWER**
2400MHZ 5200MHZ	+21 dBm +19dBm	+24 dBm +22 dBm

Fuente: http://www.tpi1.com/documents/motorola_ap650.pdf

3.2.1.2. AP7532 802.11n WLAN Access Point

Figura: 3. 7 AP7532

Fuente: https://cdn.barcodesinc.com/themes/barcodesinc/pdf/Motorola/ap7532.pdf

El punto de acceso AP7535 es un dispositivo de infraestructura WLAN que trabaja conjuntamente con otros puntos de acceso en armonía. Al respecto conviene decir que este tipo de dispositivo tiene la capacidad de definir la ruta más rápida para cada uno de los datos que se transmiten y pueden ser adoptados por controladores que permitirán una adecuada administración de la red. Destacando que; no importa la cantidad de puntos de acceso que tenga la sede, este puede desplegar, monitorear, resolver y administrarse desde cualquier punto geográfico.

Una de las características principales de este punto de acceso es que soporta el tráfico de alta densidad, un mejor rendimiento en la red y finalmente añade un ancho de banda 802.11ac en los dispositivos portátiles, tablets, Smartphone y otros dispositivos que se encuentran conectados de manera inalámbrica proporcionando una mayor velocidad en aplicaciones de voz y video HD sin excluir que este tiene seguridad avanzada dentro de su configuración.

Tabla: 3. 2 Especificaciones Generales del AP7532

General	
Factor de forma	external
Alimentación por Ethernet (PoE)	PoE
Método de autentificación	RADIUS
Marca	Extreme Networks, Inc.
Redes	
Tipo	Wireless Access Point
Tecnología de conectividad	Wireless
Protocolo de interconexión de datos	IEEE 802.11a, IEEE 802.11ac, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
Red / Protocolo de transporte	BOOTP, PPPoE
Características	3T3R MIMO technology, BOOTP support, Stateful Packet Inspection (SPI), Type of Service (ToS), VPN support, Wi-Fi Multimedia (WMM) support, auto-sensing per device, ceiling mountable, dynamic DNS server, firewall protection, load balancing, power over Ethernet (PoE), DHCP server, roaming function, routing, wall mountable, DHCP support, DiffServ support, IP address filtering, LLDP support, Low Density Parity Check (LDPC), Quality of Service (QoS), Space Time Blocking Code (STBC)
Cumplimiento de normas	IEEE 801.1p, IEEE 802.11a, IEEE 802.3af, Wi-Fi CERTIFIED, IEEE 802.11ac, IEEE 802.11b, IEEE 802.11d, IEEE 802.11g, IEEE 802.11i, IEEE 802.11n, IEEE 802.1Q, IEEE 802.1x
Protocolo inalámbrico	802.11a/b/g/n/ac
Velocidad de transferencia de datos	1.9 Gbps
Bandas Wi-Fi	2.4 GHz, 5 GHz
Método de espectro expandido	DSSS, OFDM
Algoritmo de cifrado	WPA, WPA2
Indicadores de estado	Link/activity
Formato código de línea	256 QAM
Método de autentificación	RADIUS
Alimentación por Ethernet (PoE)	PoE

Formato código de línea	256 QAM

Fuente: https://www.cnet.com/es/analisis/extreme-networks-ap-7532-wireless-access-point/

3.2.2 Estándar 802.11n

Este estándar es una propuesta de mejora del estándar IEEE 802.11b que se encuentra aun sin estandarizar. Uno de sus principales objetivos es ofrecer una mayor velocidad de transmisión en redes WLAN permitiendo *"…trabajar en dos bandas, en la banda de 2,4 Ghz y en la de 5Ghz. Gracias a esto es compatible con todos los dispositivos de las versiones anteriores. Su velocidad de transferencia llega a los 300Mb/s…".* (MIRANDA, 2005)

3.2.3 Estándar 802.11ac

Este estándar 802.11 ac también conocido con el nombre de 5G Wi-fi es la mejora del estándar 802.11n cuyo objetivo principal es garantizar una mayor velocidad de transmisión en las redes inalámbricas. Al respecto conviene decir que *"…mejora la tasa de transferencia hasta 1Gb/s dentro de la banda de 5Ghz…"* (MIRANDA, 2005). Con un incremento significativo en los canales, en relación a su predecesor que tenía un ancho de canal de 40Mhz y que actualmente este estándar lo incremento a 80Mhz o incluso hasta 160Mhz. Aclarando que existe una mejora en la modulación y transmisiones simultaneas a varios clientes, maximizando el manejo de la banda RF.

3.2.4 Comparación entre estándares 802.11n y 802.11ac

Tabla: 3. 3 Estándar IEEE802.11n y IEEE 802.11ac

	IEEE 802.11n	**IEEE 802.11ac**
Frecuencia (F) de operación	2.4GHz y 5GHz	5GHz
Canales de operación	20, 40MHz	20, 40, 80 y hasta 160 MHz
Máxima tasa de transferencia por radio (1x1)	150 Mbps	450 Mbps
Máxima tasa de transferencia por radio (3x3)	450 Mbps	1.3 Gbps

Fuente: https://www.wni.mx/index.php?option=com_content&view=article&id=75:80211ac&catid=31:general&Itemid=79

3.3Diseño básico de la red "PUCE" Facultad de Ingeniería

3.3.1 Red en Infraestructura

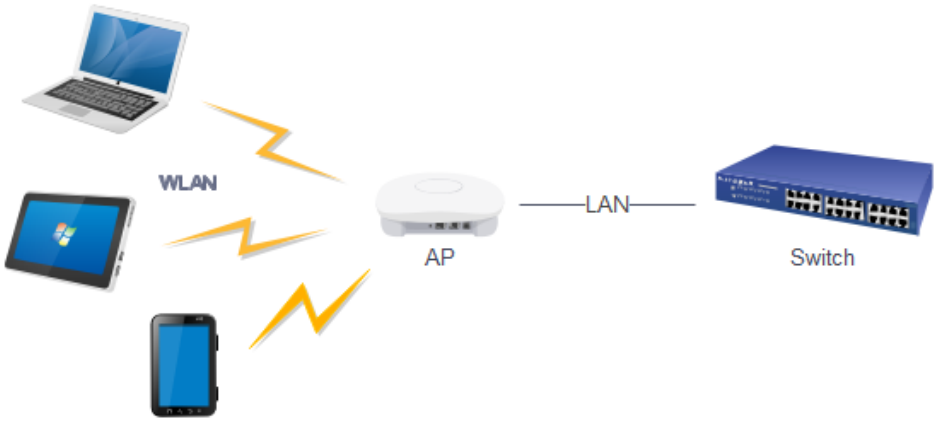

Figura: 3. 8 Red en Infraestructura "PUCE"

Fuente: Dirección informática PUCE

En la red inalámbrica de la PUCE corresponde al tipo cliente-servidor; siendo los clientes los ordenadores o dispositivos que solicitan el acceso a la red por medio del servidor, en este en

este caso el punto de acceso, cuya función es forzar el proceso de autenticación de cada uno de los usuarios que quieren acceder a la red.

Sin embargo, para llevar acabo la autenticación del usuario contra el servidor de autenticación Domain Controller (DC) con autentificación de seguridad dentro de un dominio deberán existir las credenciales del usuario para permitir su acceso a la red.

3.3.2 Topología Estrella

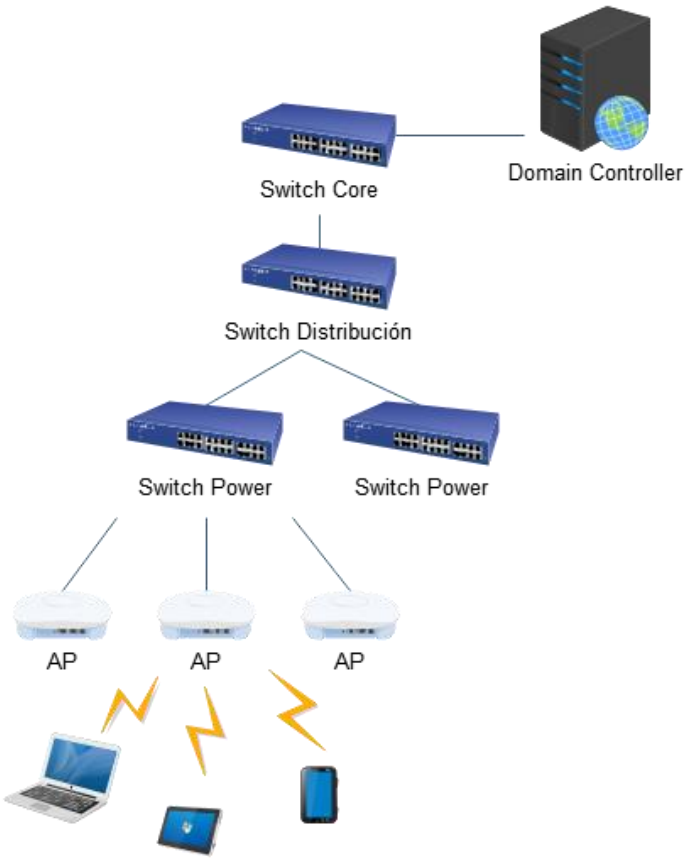

Figura: 3. 9 Topología estrella "PUCE"

Fuente: Dirección Informática PUCE

La arquitectura de la red “PUCE” se basa en una extensión de la topología en estrella permitiendo establecer una jerarquía; clasificando a las estaciones en grupos y niveles según al nodo al que se encuentran conectados en relación a la distancia con respecto al nodo central. Facilitando que este grupo de dispositivos estén interconectados entre sí, sea mediante enlaces físicos o inalámbricos con el propósito de generar el intercambio de información entre las estaciones a través de los nodos de red conectados.

3.4Conmutación de la red

Una red de comunicaciones está formado por múltiples nodos conectados, los mismos que se encargan de la comunicación entre sí a través de enlaces o líneas de transmisión por donde viaja la información. Para que dos dispositivos situados a una cierta distancia puedan comunicarse entre sí, se establecen conexiones temporales entre los dispositivos intermedios. A esta práctica se la conoce como conmutación.

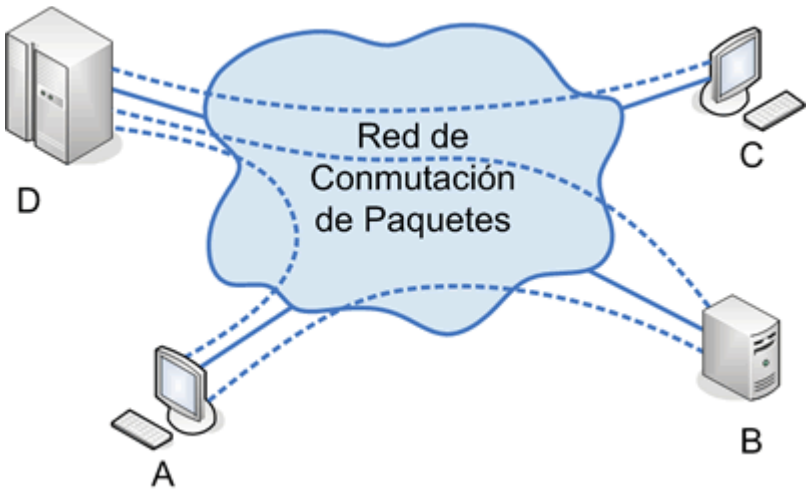

Figura: 3. 10 Red de Conmutación de Paquetes

Fuente: http://conmutacionenrutamientoicep.blogspot.com/

3.4.1 Elementos de conmutación

En una red de comunicación tenemos un conjunto de elementos que comunican a través de una serie de enlaces o líneas de transmisión. En una red se produce un intercambio de información entre dos puntos, la información se envía desde un origen a un destino por un enlace. Toda red de comunicación está compuesta por una serie de elementos. (Toro, 2015)

- Estaciones: las estaciones son dispositivos encargados de enviar y recibir la información tanto del origen como destino.
- Nodos: son los encargados de transmitir la información de un nodo a otro
- Enlaces: son conocidos también como líneas de transmisión por donde viaja la información

3.4.2 Enlaces de comunicación

Los enlaces son líneas de transmisión por donde se transporta la información, estos enlaces pueden ser físicos o inalámbricos. Para enviar y recibir información es necesario tener un componente denominado tarjeta de red. Esto depende de la estructura y tecnología que se esté ocupando en la red.

4.3.4.6 Enlaces físicos

Los enlaces físicos también son conocidos como medios de comunicación guiados, los mismos que se encargan de transportar la información por medio de cable. La velocidad y capacidad de transmisión depende de la distancia, tipo y tecnología de la red con la cual se está trabajando.

4.3.4.7 Enlaces inalámbricos

Los enlaces inalámbricos son conocidos como medios de comunicación no guiados, se los denomina así, porque no utilizan cable. Para transportar la información utilizan ondas de radio frecuencia

4.3.4.8 Tipos de enlace de comunicación

Tabla: 3. 4 Tipos de Enlaces

Físicos	La información se transporta a través de un cable, se denomina medios de comunicación guiados	• Par trenzado • Cable coaxial • Fibra óptica
Inalámbricos	La información no está unida a un enlace físico, si no que el medio de propagación que utiliza es el aire	• Radio • Microondas • Infrarrojo

Fuente: (Toro, 2015)

3.5Protocolos de comunicación

Los protocolos son un conjunto de normas que, aplicadas a un proceso de comunicación, permiten que dos entidades intercambien información. Existe una gama bastante amplia de protocolos de comunicación. De todos ellos destacamos los siguientes, tomando como referencia el modelo OSI, donde la distribución de protocolos por capa es mucho más clara que en el modelo TCP/IP. (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015)

3.5.1 Protocolo de Capa 1

Es el medio que se utilizara para hacer la conexión, estos pueden ser medios guiados y no guiados, en otras palabras cableadas e inalámbricas, así como las características más representativas de esta capa:

- Cable coaxial: en la actualidad este tipo de cable se suele utilizar en algunos tramos de distribuciones de redes extensas.
- Cable UTP: este es el más utilizado en redes de área local (LAN). Existen diferentes categorías de cables con sus respectivas características.
- Fibra Óptica: es la media que transmite a mayor velocidad. Se emplea en redes de gran longitud.

3.5.2 Protocolo de Capa 2

Aquí destacamos los protocolos específicos de la interfaz que se utiliza para conectar la entidad a la red de comunicaciones. Entre los más característicos están:

- Ethernet: una las principales características es que opera a 10Mbps. Es orientado a redes de área local (LAN)

- Fast Ethernet: este opera a una velocidad superior a la de Ethernet hasta llegar a los 100Mbps
- Gigabit Ethernet: es la mejora del Fast Ethernet hasta 1000Mbps
- 10 Gigabit Ethernet: existe una mejora de velocidad hasta 10Gbps

Un protocolo típico en esta capa es ARP. Este protocolo se encarga de localizar la dirección MAC de una entidad a partir de su dirección IP. (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015).

3.5.3 Protocolo Capa 3

El protocolo más característico de esta capa es el protocolo IP. Una de sus principales funcionalidades de este protocolo es asegurarse que la información viaje del origen al destino por la mejor ruta posible. Para ello, a cada entidad se le asigna una dirección IP. El trazado de la mejor ruta desde el origen hasta su destino se lo realiza a través de un mecanismo denominado encaminamiento o enrutamiento

3.5.4 Protocolo de Capa 4

- *UDP: se basa en el envió de paquetes al destino sin necesidad de una conexión previa con este. Cada paquete contiene información suficiente como para llegar al destino por su cuenta. Es un protocolo donde no existe sincronización ni confirmación de llegada, por lo que algunos paquetes pueden adelantarse a otros o incluso no llegar nunca. Se utiliza cuando es más importante la velocidad de la transmisión que la integridad de lo que se transmite (por ejemplo audio y video)* (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015)
- *TCP: junto con IP, es uno de los principales protocolos de internet. Al contrario que UDP, TCP establece una conexión entre emisor y receptor, garantizando que los datos*

que se transmiten llegan en el mismo orden en que se transmiten y sin errores. Este protocolo es la base de gran parte de las aplicaciones que trabajan sobre internet, así como muchos de los protocolos de capas superiores. (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015)

3.5.5 Protocolo Capa 5

- RPC: es uno de los protocolos utilizados para las conexiones remotas, de tal manera un equipo puede trabajar sobre otro sin la necesidad de preocuparse por sus comunicaciones. Este protocolo en la actualidad es la base para la asistencia remota, así como también la ejecución remota de aplicaciones y de los denominados servicios Web.
- SSL y TLS: tanto SSL como su sucesor, TLS, son protocolos cuya función principal es encriptar la información que se transmite la misma que solo puede ser descifrada por el receptor. Este protocolo se utiliza en capas superiores para brindar seguridad a otros protocolos, estos pueden ser correos electrónicos o los de interpretación de páginas web.

3.5.6 Protocolo Capa 6

No hay protocolos a destacar en esta capa

3.5.7 Protocolo Capa 7

Esta capa es la que más protocolos representativos tiene ya que, al fin y al cabo, es con la que interactúa el usuario. Los más representativos son:

- HTTP: Una de sus principales características de este tipo de protocolo es encargarse de publicar e interpretar páginas Web. Debo agregar que, la versión de HTTP con SSL/TSL se llama HTTPS.

- SMTP: es un protocolo para remitir correo electrónico.
- POP3 e IMAP: protocolo para recibir correo electrónico. Habría que decir también, que el protocolo IMAP es una mejora de POP3.

3.6Modelo OSI

El modelo OSI (Interconexión de Sistemas Abiertos, Open Systems Interconnection), de la organización internacional de estándares (ISO), es un estándar internacional que describe como crear protocolos de comunicaciones en red estructurados, en capas o niveles. (Moro Vallina, 2013). Una de las principales características de este modelo es encargarse de dividir las funciones de la comunicación en siete capas, de manera que, cada una de las capas se comunica con la anterior y la siguiente.

Figura: 3. 11 Capas del Modelo OSI

Fuente: (Moro Vallina, 2013)

3.6.1 Capas del modelo OSI

- *Capa 1. Capa Física: Define las especificaciones eléctricas, mecánicas, y funcionales de todos los equipos que intervienen en el proceso de comunicación.* (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015).
- *Capa 2. Enlace a datos: se ocupa de la transferencia de las cadenas de datos (en este nivel llamadas tramas) de una entidad a otra, así como de detectar y corregir errores en este proceso. Aquí tiene importancia el código que identifica a la interfaz de comunicación del equipo (Dirección MAC).* (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015).

- *Capa3. Red: su misión es enrutar las cadenas de datos (en este nivel llamadas paquetes) entre entidades de la misma red o incluso de distintas redes, estén o no estas conectadas directamente. En este nivel a cada entidad se le asigna un código lógico llamado dirección IP*. (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015).
- *Capa 4. Transporte: se encarga de segmentar las cadenas de datos a transmitir (en este nivel llamadas segmentos) y transportarlas de una entidad a otra, con independencia del tipo de red que se utilice.* (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015).
- *Capa 5. Sesión: tiene como misión controlar el enlace que se ha establecido en la capa anterior entre las dos entidades que se comunican, así como mantenerlo o reestablecerlo en caso de que la transmisión de datos se interrumpa.* (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015).
- *Capa 6. Presentación: esta capa garantiza que dos dispositivos diferentes puedan comunicarse entre sí. Los dispositivos que intercambian datos en una red puede emplear representaciones de datos diferentes. La capa de presentación deberá implementar los mecanismos de traducción necesarios para asegurar la compatibilidad entre sistemas. Además de ello, esta capa incluye mecanismos para la encriptación del mensaje, si la seguridad lo requiere, y para la compresión del mismo, con objeto de consumir menos ancho de banda del canal y hacer la comunicación más eficiente.* (Moro Vallina, 2013)
- *Capa 7. Aplicación: la capa de aplicación es la que permite al usuario acceder a la red. Proporciona las interfaces necesarias para servicios como el correo electrónico, las transferencias de archivos, o el control remoto de otros ordenadores.* (Moro Vallina, 2013).

3.6.2 Funcionamiento del modelo OSI

La base del sistema de capas del modelo OSI es el encapsulamiento. Mediante este proceso, todo lo que concierne a una capa se encapsula, ofreciendo a las capas colindantes solo la

información que necesitan para comunicarse. (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015).

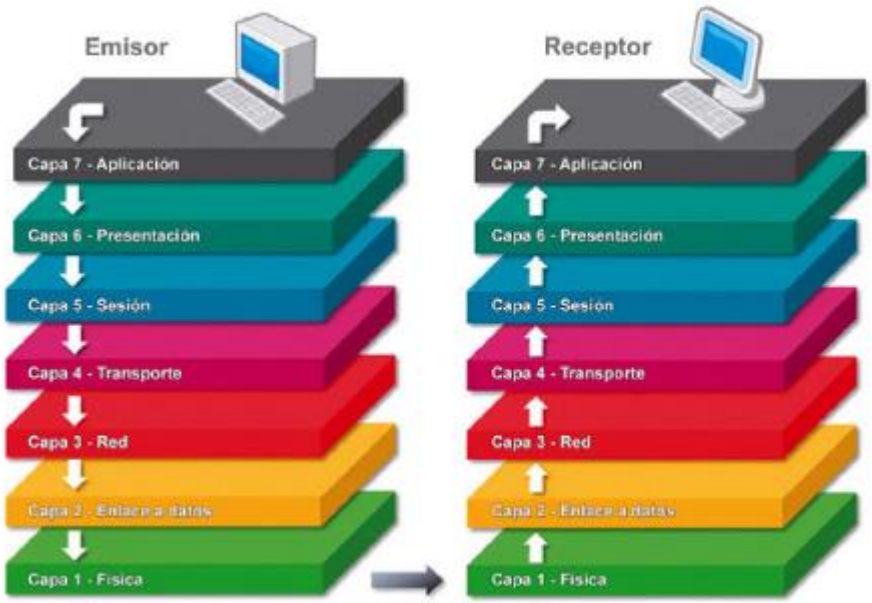

Figura: 3. 12 Funcionamiento del modelo OSI

Fuente: (Gallego, FPB - Instalación y mantenimiento de redes para transmisión de datos, 2015).

Cuando la información se transmite de una entidad A denominada Emisor a una entidad B denominada Receptor, el emisor parte de la capa más alta en este caso la capa de aplicación. Va descendiendo por las capas colindantes, añadiendo en cada una de ellas unas trazas de información que son propias de la capa, en otras palabras podeos decir que pasa información relevante de unas capas a otras. Cuando finalmente llega a la capa 1 denominada capa física se produce el enlace físico con el receptor y, en ese instante se recibe la información en la capa 1 de la entidad receptora, siguiendo el proceso inverso: va ascendiendo por las capas colindantes, liberando las trazas correspondientes en cada una. Finalmente llegara a la capa más alta del receptor, donde el receptor recibirá la información que se trasmitió. Debo agregar que el flujo descendente en el emisor y ascendente en el receptor siempre se produce.

3.6.3 Seguridad en el modelo OSI

Existen diversos mecanismos de seguridad, los mismos que se pueden aplicar en las redes WLAN y estos actúan en diferentes capas del modelo OSI. A nivel de la capa de enlace los más utilizados son los siguientes WEB, WPA, WPA2, IEEE 802.11i. A nivel de red se emplea la solución VPN basado en IPsec encargada de una comunicación segura de extremo a extremo. En la capa de transporte trabaja el protocolo SSL y en cuanto a nivel de aplicación, trabaja los protocolos más utilizados SSH y HTTPS.

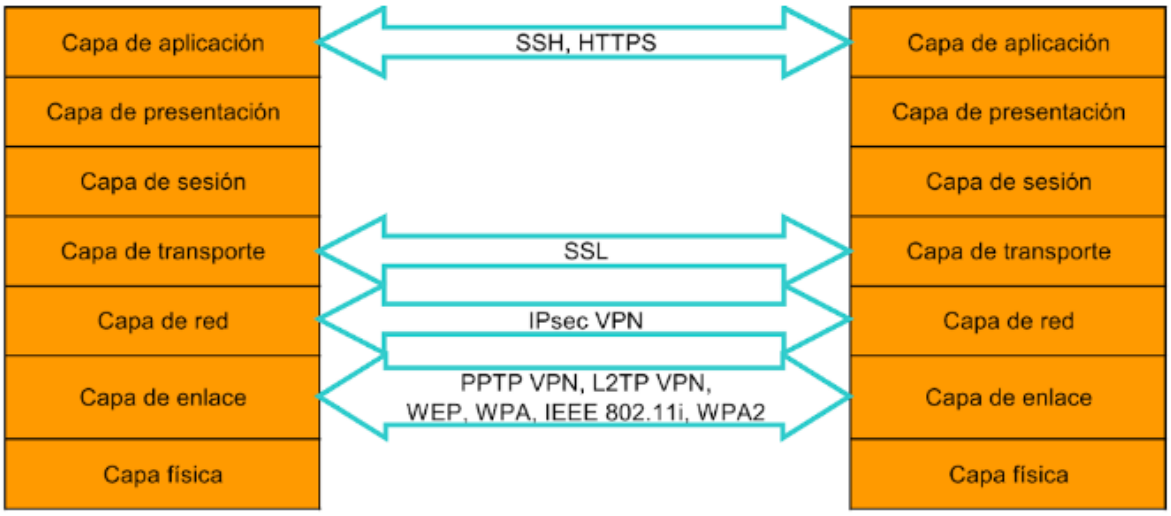

Figura: 3. 13 Mecanismo de Seguridad Existentes en las Distintas Capas del Modelo OSI

Fuente: (Izaskun Pellejero F. A., 2006).

Dentro de los mecanismos de seguridad mencionados anteriormente, son propios de redes IEEE 802.11 correspondiente al estándar de redes inalámbricas.

El funcionamiento básico de estos protocolos se basa en el cifrado de la información de usuario en el interfaz aire (entre el terminal de usuario y el punto de acceso WLAN). Además, todos excepto WEB, implican autenticación de usuario. En el caso del protocolo WEB la única

autenticación que se realiza es la autenticación de terminal, pero no contempla ningún otro modo de autenticación de usuarios ni de punto de acceso. (Izaskun Pellejero F. A., 2006).

El resto de protocolos (SSH, HTTPS, SSL, IPsec VPN, PPTP VPN, L2TP VPN) son aplicables no solo a redes inalámbricas sino también a otros tipos de redes. Además los protocolos SSL, HTTPS y SSH, solo permiten asegurar el tráfico generado por cierto tipo de aplicaciones.

3.7Estándares

Los estándares definen las características físicas, eléctricas y mecánicas, asi como los procedimientos de comunicación de los dispositivos. Por ejemplo, un estándar de comunicaciones puede definir el tipo de conector, las tensiones y las intensidades eléctricas que se deben emplear, el formato de codificación de los datos, etc. El empleo de estándar presenta ventajas como la compatibilidad entre productos, la reducción de costes y la flexibilidad del mercado para la tecnología estandarizada, proporcionando además un marco para la investigación y el desarrollo en dicha tecnología. (Moro Vallina, 2013).

Alguna de las organizaciones de estándares con más relevancia en telecomunicaciones son las siguientes

- Organización internacional de estándares, International Standard Organization (ISO).
- Instituto Americano Nacional de Estándares, American National Standard institute (ANSI).
- Union Internacional de Telecomunicaciones, International Telecommunications Union (ITU).
- Instituto de Ingenieros Eléctricos y Electrónicos, institute of Electrical and Electronic Engineers (IEEE).
- Asociación de las Industrias Electrónicas, Electronic Industries Association (EIA).
- Instituto Europeo de Estándares de Telecomunicaciones, European Telecommunications Standard institute (ETSI).

- Asociación Española de Normalización y Certificación (AENOR).

3.8Estándares, Técnica de Encriptación y protocolos de trabajo "PUCE"

3.8.1 Técnica de encriptación WPA2 empresarial

"…Se utiliza en el ámbito de las empresas y organizaciones, ya que tiene mayor seguridad al tener que identificarse los usuarios mediante un nombre, contraseña y, además un certificado digital…". (MARIA DEL PILAR ALEGRE RAMOS, 2011)

En la Dirección Informática de la Pontificia Universidad Católica del Ecuador (PUCE), la técnica de encriptación utilizada para la integridad y autenticidad de la información es el WPA2, que trabaja conjuntamente con el estándar 802.1x y el Protocolo de Autenticación Extensible (EAP) con requerimientos estrictos de cifrado y autenticación hace que sea más apropiada la utilización de estos elementos de conexión y seguridad.

Resaltando que Protocolo de Autenticación Extensible (EAP) utiliza una estructura de transporte de extremo a extremo para los métodos de autenticación entre los dispositivos de usuario y los puntos de acceso. Mientras que el IEEE 802.1x se emplea como marco para encapsular los mensajes EAP en el enlace radio formando una fuerte estructura de autenticación que utiliza un servidor de autenticación centralizado con un estándar más extendido para llevar a cabo la autenticación de usuarios, permitiendo a los usuarios acceder a la red inalámbrica "PUCE" con nombre y contraseña.

3.8.2 Estándar 802.1x

Es un estándar para el control de acceso a la red de nivel 2 basado en puertos que ofrece un marco para una autenticación superior (basada, por ejemplo, en una pareja identificador de usuario y contraseña o certificados) y distribución de claves de cifrado. No obstante, IEEE 802.1x no es una alternativa al cifrado (RC4, 3DES, AES,…). IEEE 802.1x solo contempla un

marco para la autenticación y la distribución de claves, por lo que puede y debe ser usado junto a una técnica de cifrado mediante el correspondiente algoritmo de cifrado… es un estándar que establece una capa o nivel entre la capa de acceso y los diferentes algoritmos de autenticación que existe hoy en día. IEEE 802.1x traduce las tramas enviadas por un algoritmo de autenticación en el formato necesario para que estas sean entendidas por el sistema de autenticación que utilice la red. Por lo tanto ,IEEE 802.1x no es por sí mismo un método de autenticación y bebe emplearse de forma conjunta con protocolos de autenticación para llevar a cabo la verificación de las credenciales de usuario, como por ejemplo cualquier tipo de EAP , así como la generación de las claves de cifrado. (Izaskun Pellejero F. A., 2006).

3.8.3 Protocolo EAP

El Protocolo de Autenticación Extensible (EAP) se usa en medios guiados y no guiados, es decir; cableados e inalámbricos. Agregando que EAP es el encargado de la autenticación y gestión de claves de WPA, WPA2 e IEEE 802.11i.

3.8.3.1. Requerimientos técnicos

Una vez delimitado los tipos de autenticación, es importante validar y seleccionar el más apropiado en relación a los requerimientos técnicos exigidos para su funcionamiento. Pero, para serlo posible es necesario verificar que estos servicios de autenticación sean compatibles con el estándar IEEE 802.11 y de ser así; se determinaría los tipos de autenticación EAP que puedan soportar. Por lo tanto, los requerimientos necesarios para cada uno de los requerimientos de la red inalámbrica son:

- Cliente: Considerar sí; las plataformas utilizadas por los usuarios soportan el tipo de autenticación elegido, es decir; el tipo de sistema operativo usado por el cliente para elegir el adecuado método de autenticación.

Sistema operativo	EAP-TLS	EAP-TTLS	PEAP	LEAP
Windows XP, 2000, Vista, 7 y 8	Cliente nativo	Cliente de tercero	Cliente nativo	Cliente de tercero
Windows 9x	Cliente de tercero	Cliente de tercero	Cliente de tercero	Cliente de tercero
Linux	Cliente de tercero	Cliente de tercero	No soportado	No soportado
MacOS	Cliente de tercero	Cliente de tercero	No soportado	No soportado

Figura: 3. 14 Sistemas Operativos Compatibles

Fuente: (MIRANDA, 2005)

Puntos de acceso: "…*los principales requerimientos de estos dispositivos (para poder implementar un mecanismo de seguridad para el control del acceso inalámbrico) son la compatibilidad con 802.11 y un soporte de cifrado..."* (MIRANDA, 2005)

Servidor de autenticación: "…*estos equipos necesitan compatibilidad con 802.1, soporte de diversos tipos de autenticación EAP, capacidad de registro, soporte para el control de acceso en redes inalámbricas y flexibilidad para validar a los clientes mediante varios métodos (base de datos de usuarios locales, directorio de usuarios LDAP, certificados, etc.)..."* (MIRANDA, 2005)

Los requerimientos ya mencionados tanto de seguridad como de funcionalidad podremos determinar el método de autenticación EAP más adecuado.

CAPITULO IV

4. Autenticación, configuración y técnicas de encriptación

4.1 Configuración del servicio Wireless "PUCE"

Para poder acceder al servicio de internet en la PUCE se debe efectuar la configuración correspondiente para ciertos equipos que no pertenecen al dominio y quieren acceder al Internet "LA CATO Wireless".

Pasos:

Se inicia con Clic derecho sobre el ícono de Wi-Fi en la parte inferior derecha de la pantalla y seleccionar Abrir el Centro de redes y recursos compartidos.

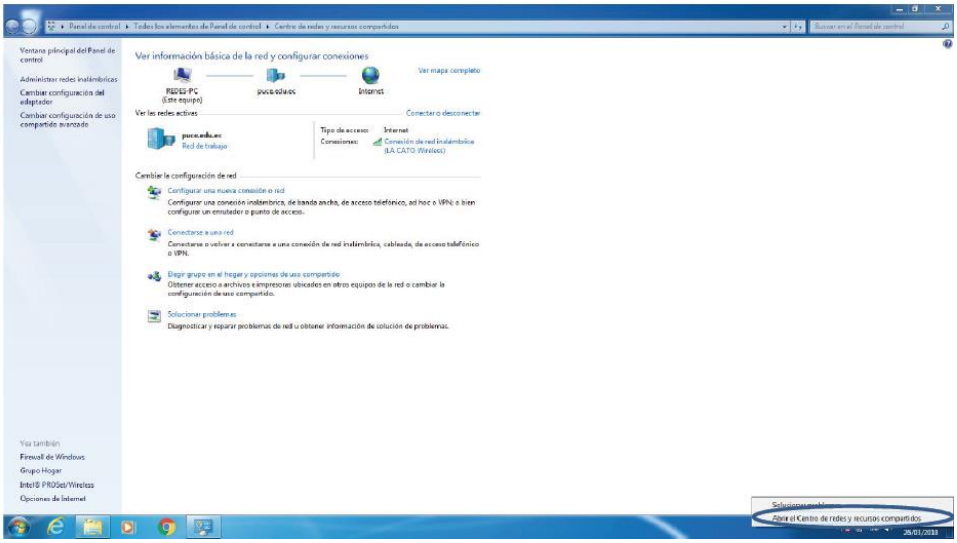

Figura: 4. 1 Centro de Redes y Recursos Compartidos

Fuente: Dirección Informática PUCE

Clic en Administrar redes inalámbricas y finalmente agregar

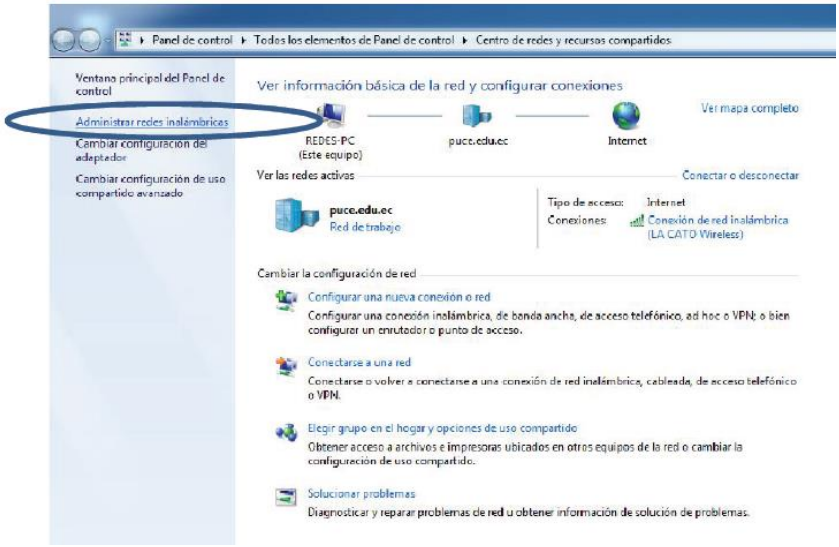

Figura: 4. 2 Administrador de redes inalámbricas

Fuente: Dirección Informática PUCE

Crear perfil de red manual

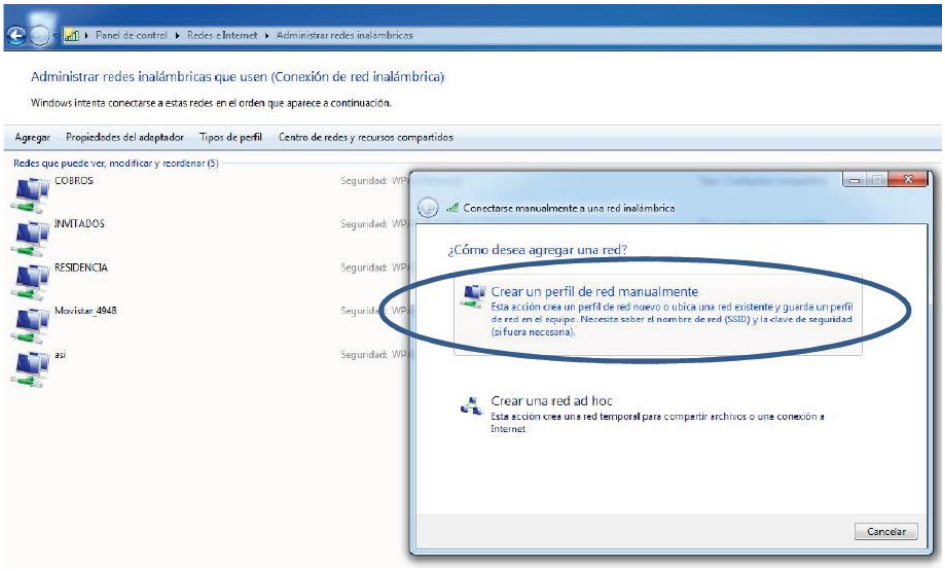

Figura: 4. 3 Red Manual

Fuente: Dirección Informática PUCE

Se ingresará la información como se detalla en la imagen con sus respectivo nombre de red, tipo de seguridad y cifrado.

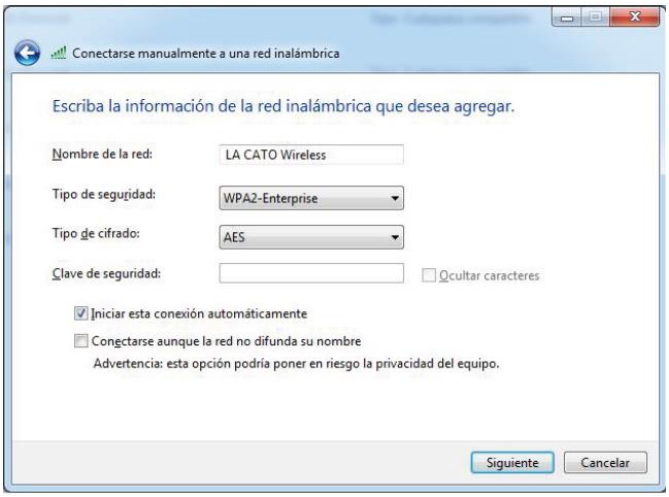

Figura: 4. 4 Nombre de Red, Tipo de Seguridad y Cifrado.

Fuente: Dirección Informática PUCE

Cambiar la configuración de conexión

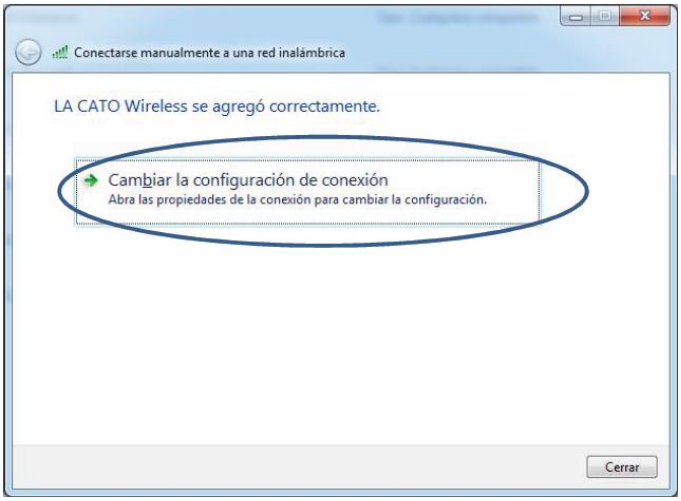

Figura: 4. 5 Configuración de Conexión

Fuente: Dirección Informática PUCE

Click en configuración para elegir el método de autenticación de la red

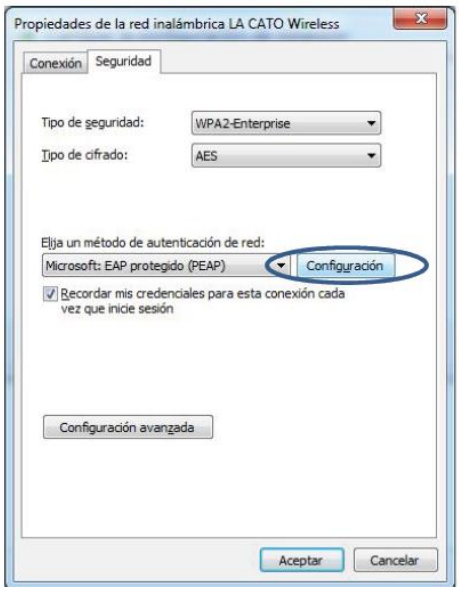

Figura: 4. 6 Método de Autenticación

Fuente: Dirección Informática PUCE

Se procederá a realizar las configuraciones correspondientes para hacer uso de los recursos de la red a través del proceso de autenticación de usuario, configurando el método de autenticación MSCHAPv2

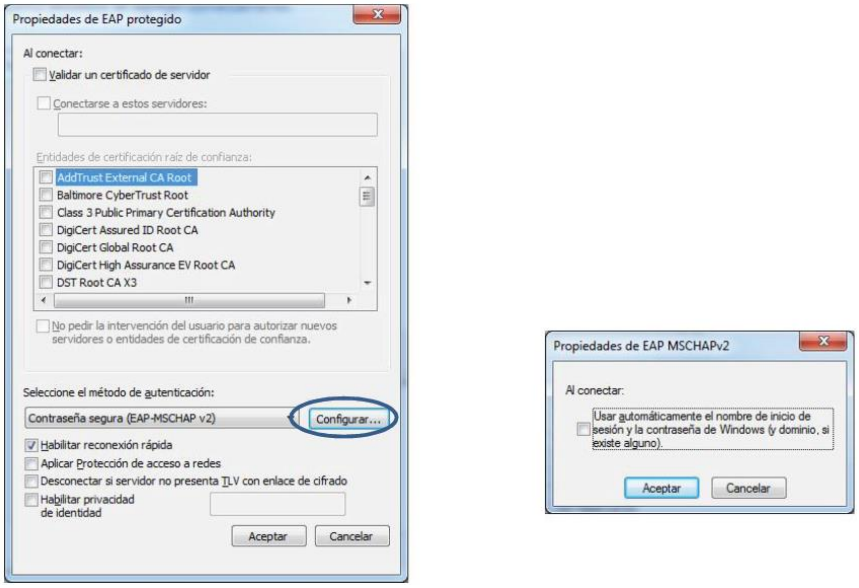

Figura: 4. 7 EAP MSCHAPv2

Fuente: Dirección Informática PUCE

Click en configuración avanzada

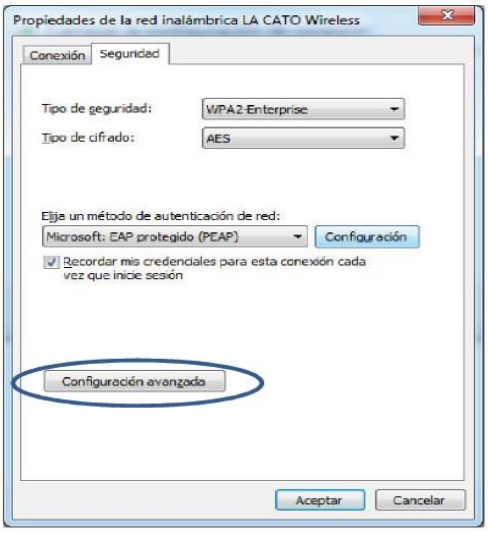

Figura: 4. 8 Propiedades de Redes Inalámbricas

Fuente: Dirección Informática PUCE

Ubicar y seleccionar autenticación de usuarios, luego click en guardar credenciales. Ingresar las credenciales respectivas de cada usuario para hacer uso de la red inalámbrica “LA CATO Wireless”

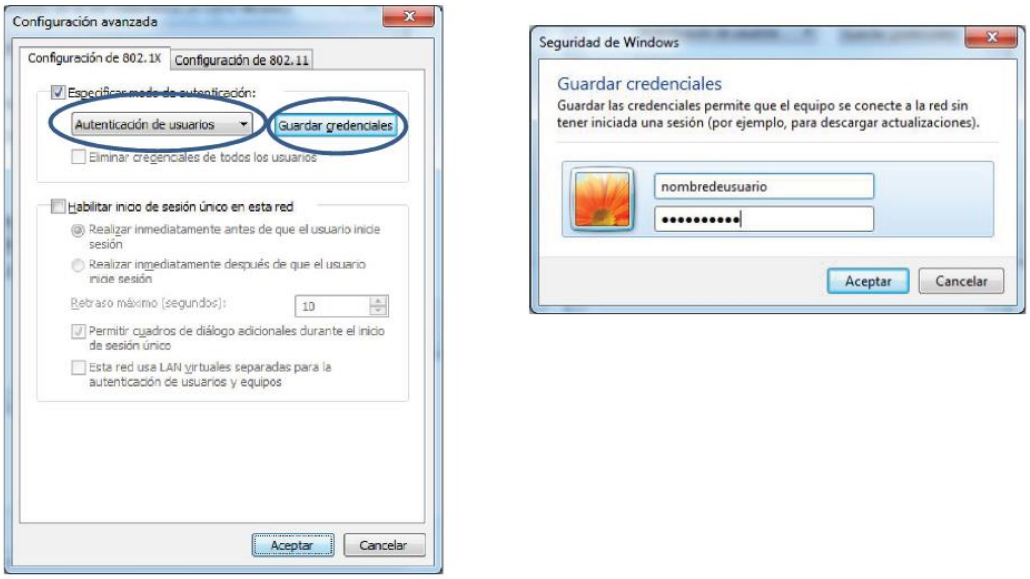

Figura: 4. 9 Credenciales de Acceso

Fuente: Dirección Informática PUCE

4.2Conexión a la red inalámbrica “LA CATO Wireless”

A través de un dispositivo móvil con tecnología Wi-Fi se conectara a la red inalámbrica de la PUCE cuyo nombre de la red o SSID es “LA CATO Wireless”, la misma que podemos constatar en la lista de redes que el dispositivo capta en un radio de cobertura con su respectiva intensidad de señal, como se puede observar en la figura.

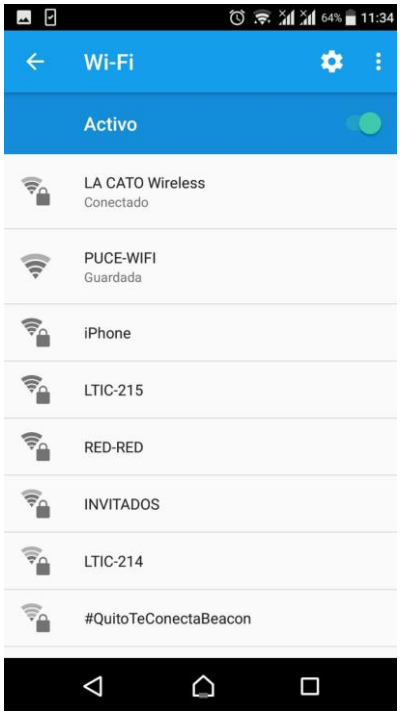

Figura: 4. 10 Red inalámbrica

Fuente: Pontificia Universidad Católica del Ecuador

A continuación se pulsará el nombre de la red a la que se quiere conectar, en este caso es “LA CATO Wireless”, necesariamente el usuario que quiere acceder a la red debe tener sus credenciales de acceso como son su usuario y su contraseña.

Figura: 4. 11 Credenciales de Acceso

Fuente: Pontificia Universidad Católica del Ecuador

Una vez ingresado correctamente el usuario y la contraseña, automáticamente cambiara el estado de la red de “desconectado” a “conectado”, además desplegará la información de la red: su estado, su intensidad de la señal, velocidad de vínculo, frecuencia y seguridad.

Figura: 4. 12 Estado de Conexión de la Red

Fuente: Pontificia Universidad Católica del Ecuador

Una vez que se ha conectado exitosamente a la red, permitirá acceder a la información y a los recursos de la misma, como se muestra en la figura.

Figura: 4. 13 Métodos de Autenticación

Fuente: Pontificia Universidad Católica del Ecuador

Proporcionando métodos de autenticación como son: el protocolo de Autenticación Extensible (EAP) y el método de autenticación de fase 2 MSCHAPV2 encargados de la autenticación y gestión de claves de WPA2 Enterprise. Se debe agregar que el estándar 802.1x al ser un método de autenticación trabaja conjuntamente con los protocolos ya mencionados (EAP y MSCHAPV2) como se puede observar en el despliegue de la información de la red.

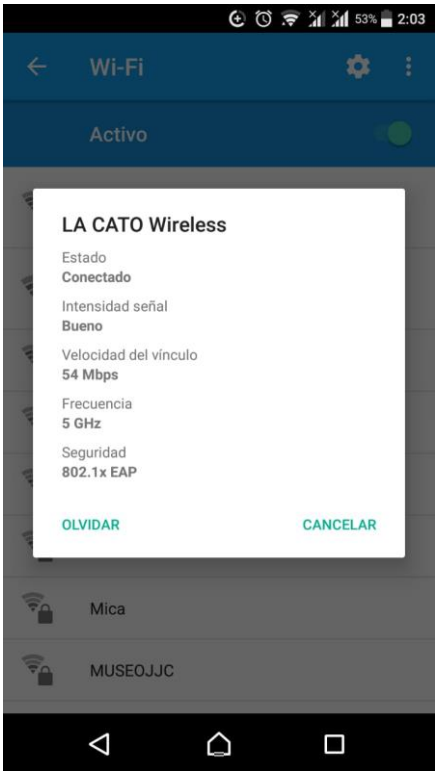

Figura: 4. 14 Estándar 802.1x + EAP

Fuente: Pontificia Universidad Católica del Ecuador

Proporcionando un acceso inalámbrico seguro a internet a estudiantes, docentes y personal administrativo.

4.3Funcionamiento EAP “PUCE”

Este protocolo de Autenticación Extensible (EAP) es usado en medios guiados y no guiados, cuando se refiere a “medios guiados” es un medio físico o cableado por el cual se trasmite la información, y el “medio no guiado” es aquel que conduce su información de forma inalámbrica a través de ondas electromagnéticas, siendo que; los dispositivos de tecnología Wi-Fi pueden acceder a este medio.

En la facultad de ingeniería se puede encontrar dos tipos de medios, debido a que la red de la universidad es de tipo infraestructura (cliente- servidor), diciendo así, que los clientes son los ordenadores personales que se conectan al servidor en este caso es el punto de acceso que permitirá la comunicación de manera inalámbrica entre los dispositivos. Cuando referimos a los “medios guiados” de la universidad, se aclara que a partir del punto de acceso se distribuye los enlaces físicos a través de los switch de distribución hasta llegar al servidor de la universidad cual es encargado de autenticar al usuario. Para entender de una mejor manera de cómo funciona la autenticación de usuario en la universidad se explicará a continuación.

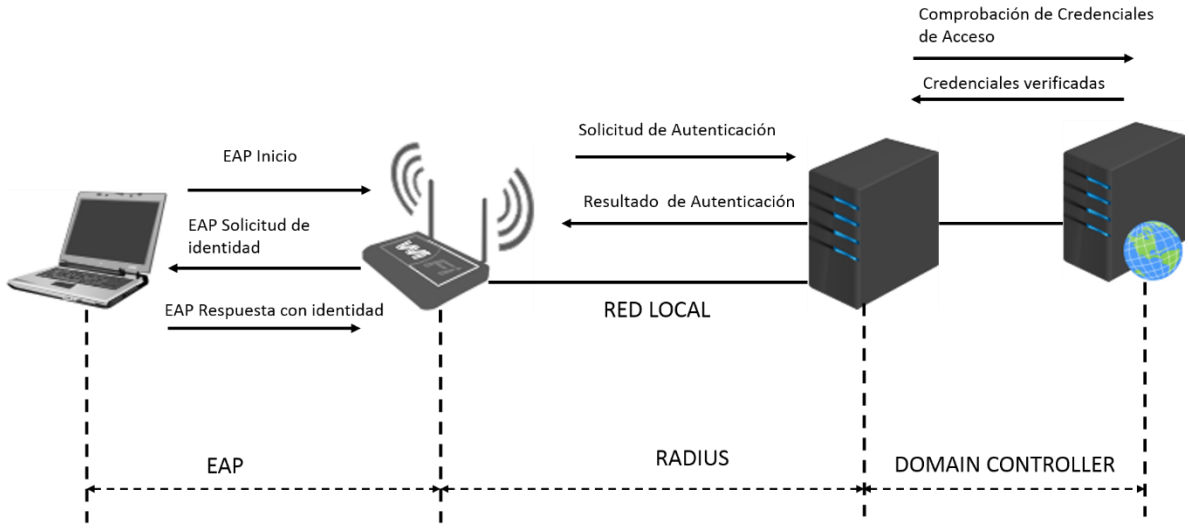

Figura: 4. 15 EAP PUCE

Fuente: Dirección informática PUCE

Se deberá considerar los requerimientos técnicos para delimitar el tipo de autenticación, es importante seleccionar el más adecuado, que sea compatible con el estándar IEEE 802.11 y soporte cifrado, permitiéndonos determinar el tipo de autenticación. En el caso de la Universidad utiliza el protocolo de autenticación extensible EAP debido a que la plataforma utilizada por la mayoría de usuarios es de sistema operativo Windows con sus respectivos predecesores con compatibilidad con todas las versiones del protocolo EAP.

Para verificar la identidad de los usuarios que se conectan de manera inalámbrica a la red "LA CATO Wireless" a través de un punto de acceso, cuya función principal es utilizar una de las múltiples versiones del protocolo EAP, encargado de la autenticación y gestión de claves de WPA2 Enterprise. Esto permitirá el proceso de autenticación del usuario que quiere acceder a los recursos de la red mediante las credenciales de acceso que se encuentran en el Domain Controller. Notándose que el sistema de autenticación de usuario, no solamente es necesario en disponer de un servidor con su software RADIUS (Remote Authentication Dial In User Service, 'Servicio de autenticación de clientes de acceso telefónico') correspondiente. Sino también, de un punto de acceso compatible con el estándar 802.1x y finalmente el equipo del cliente debe ser compatible con EAP. Por lo que, el cliente debe disponer de un software que entienda los mensajes de autenticación que el punto de acceso envía. Una vez que estos requerimientos técnicos se hayan cumplido, automáticamente el domain controller verifica las credenciales del usuario e inmediatamente envía un mensaje para autorizar el acceso.

4.3.1 Autenticación IEEE 802.1x + EAP

El estándar 802.1x al no ser un método de autenticación deberá trabajar de manera conjunta con protocolos de autenticación que facilite la verificación de credenciales de usuario. Adicionalmente IEEE 802.1x se podría emplear con distintos tipos de identificaciones EAP, así como; numerosas tecnologías de acceso inalámbricas o cableadas.

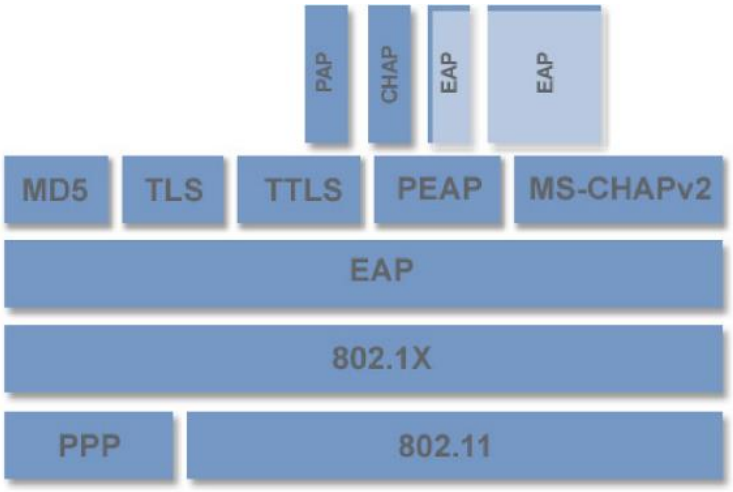

Figura: 3. 15 IEEE 802.1x + EAP

Fuente: (Izaskun Pellejero F. A., 2006)

4.3.2 EAP - MS-CHAPv2

Es un protocolo de enlace que requiere que cada parte, cliente y servidor de autenticación, se autentiquen entre sí. MS-CHAPv2 se desarrolló originalmente como un protocolo de autenticación PPP para proporcionar una mejor protección para las conexiones de acceso telefónico y redes privadas virtuales (VPN). Esta versión de CHAP proporciona una mejor protección que los protocolos previos de respuesta al desafío. Sin embargo, aún es susceptible a ataques de diccionario sin conexión… EAP-MS-CHAPv2 utiliza el siguiente proceso para realizar la autenticación. El servidor desafía al cliente y el cliente al servidor de autentificación. Si alguno de los desafíos no se responde correctamente, la conexión se rechaza. La autenticación dentro de este método se inicia cuando se establece el estándar IEEE 802.1x entre el autenticador y el cliente. El cliente emitirá una respuesta. Como se esperaba, el autenticador reenvía esto al servidor de autenticación. El servidor emite un desafío cifrado. El cliente envía una respuesta cifrada derivada de las credenciales del usuario. En este punto, la autenticación es exitosa o fallida. (Brown, 2006)

4.3.3 Autenticación IEEE 802.1x +EAP + MSCHAPV2 "PUCE"

El estándar 802.1x es utilizado para una autenticación y distribución de claves de cifrado , pero, para ello necesariamente debe complementarse con el protocolo de autenticación EAP + MSCHAPV2, estos dos protocolos deben trabajar de manera conjunta para que facilite la verificación de las credenciales de acceso en el domain controller, para disponer de los recursos de la red, además, este trabaja conjuntamente con su correspondiente algoritmo de cifrado WPA2 Enterprise, una de sus principales características que destaca esta técnica de encriptación es que funciona mediante un usuario y contraseña. Debo agregar que esta técnica de encriptación se utiliza en equipos de grandes recursos como son los servidores, para una adecuada gestión de las credenciales de acceso.

4.3.4 Domain controller (DC)

El controlador de dominio no es nada más que un servidor encargado de responder a las solicitudes de autenticación de seguridad de los usuarios que quieren acceder a la red. Esto lo realiza mediante la corroboración de la información que se encuentra almacenada en el LDAP (***L****ightweight* ***D****irectory* ***A****ccess* ***P****rotocol, protocolo simplificado de acceso a directorios*) donde se encuentra almacenada la información de cuenta de usuario y políticas de seguridad, permitiendo el acceso a los recursos informáticos de la red “LA CATO Wireless”, cuya corroboración se realiza simplemente con la combinación de usuario y contraseña.

4.3.4.1 LDAP

Es un sistema de almacenamiento de información, para enormes cantidades de datos que se manipulan a diario. Debo agregar que, *es un modelo que describe cómo organizar y consultar los datos del directorio* (Tim Howes, 2003) , permitiendo una autenticación de usuario de acuerdo a las credenciales acceso existente. *Además, las organizaciones que eligen directorios LDAP encuentran que son relativamente económicos de implementar y mantener.* (Tim Howes, 2003)

4.4Autenticación de Usuarios al Sistema

El funcionamiento de intercambio de mensajes entre el usuario y el servidor de autenticación es el siguiente, como se muestra en la figura

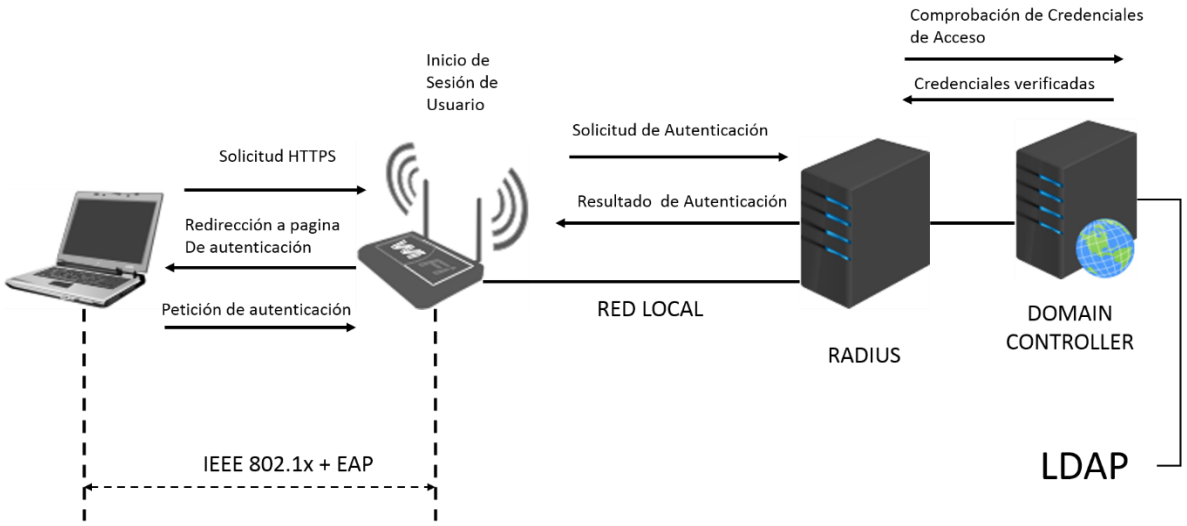

Figura: 4. 16 Sistema de Autenticación de usuario

Fuente: Fuente: Dirección informática PUCE

Una vez que el usuario intenta acceder a la red “LA CATOLICA WIRELESS” el navegador arranca, independientemente de la página web que tenga configurada como página inicio, el usuario será redireccionado a un portal web conocido como portal cautivo, que es una página web cuya función principal es pedir al usuario sus credenciales de autenticación. Esta sitio Web esta albergada en un servidor local ubicado en un Gateway de control de acceso.

El usuario que quiere acceder a los recursos de la red introduce las credenciales de acceso, generalmente un nombre de usuario y una contraseña. La validación de las credenciales de usuario suele llevarse a cabo con un servidor de autenticación, generalmente es un servidor RADIUS. *El servidor RADIUS lo contrastara contra una base de datos para comprobar si el usuario es un usuario autorizado o no. Una vez corroborada la veracidad de la identidad de*

usuario, a este se le permite el acceso y puede hacer uso de la red y sus servicios. (Izaskun Pellejero . A., 2006).

A continuación aclararemos de una mejor manera el proceso de autenticación del usuario entre el cliente y el servidor de autenticación el mismo que contrastara la información que se encuentra en el Domain Controller.

El proceso inicia cuando el usuario se conecta a la red “LA CATO Wireless” e introduce sus credenciales de acceso

A continuación el punto de acceso envía un mensaje de petición de acceso, RADIUS envía las credenciales de acceso del usuario solicitante, las mismas que son corroboradas con el servidor Domain Controller donde se almacena el nombre de usuario y contraseña.

El servidor se apoyara en la dirección origen del paquete, el autenticador en este caso el punto de acceso determinara si el solicitante está autorizado para llevar a cabo la petición.

En caso de que la petición sea positiva, el servidor contrastara la información de las credenciales de acceso del solicitante que coincida con el enviado en la petición, si lo encuentra automáticamente comprobara el tipo de acceso asociado al perfil del solicitante.

Si el usuario es autenticado y autorizado a utilizar los recursos de la red, el servidor le envía un mensaje de acceso aceptado. En caso de que no coincida con el perfil de usuario el servidor enviara un mensaje de rechazo, a continuación el punto de acceso desconectara al usuario o solicitante.

Por lo tanto el método de autenticación utilizada en la PUCE actúa a nivel de aplicación por lo cual el proceso de autenticación es invocado por el dispositivo inalámbrico del solicitante a través de una petición HTTPS. El solicitante no tiene acceso a la red WLAN hasta que no se verifique las credenciales de acceso del usuario a través del proceso de autenticación.

4.5WPA2-Enterprise con arquitectura de certificados digitales

Esta técnica de encriptación es la mejor solución para aquellos entornos que demanden de la máxima seguridad en sus comunicaciones inalámbricas, se caracteriza por la utilización de certificados digitales para autenticar a los usuarios y cifrar las comunicaciones.

Una de las grandes ventajas de utilizar certificados digitales es que se obtiene los siguientes beneficios:

- Proporcionan un sistema de autenticación más robusta para evitar que terceros puedan acceder a los recursos e información de la red.
- Los certificados digitales son difíciles de comprometer y robar, por tal motivo la información se mantiene integra y segura.
- El sistema y la máquina del usuario pueden realizar el proceso de autenticación sin la necesidad de que intervenga el usuario.

Además, el uso de certificados digitales va a permitir que se produzca una autenticación mutua. El cliente se autenticara a la red inalámbrica y la red inalámbrica autenticara al cliente. (CASTRO GIL Manuel Alonso, 2014)

4.6Cuadro comparativo de las técnicas de Encriptación

Los parámetros seleccionados para llevar a cabo la comparativa de las diferentes técnicas de encriptación con sus respectivos mecanismos de seguridad, son por un lado parámetros relacionados con la autenticación y cifrado, los mismos que se detallan a continuación.

Tabla 4. 1 Mecanismo de Seguridad

		WEB	WPA	WPA2
Autenticación	Autenticación	WEB	802.1x + EAP	802.1x + EAP
	Pre autenticación	No	No	802.1x +(EAPOL)
Cifrado	Negociación del cifrado	No	Si	Si
	Cifrado	RC4 (40bits 0 104bit)	TKIP: RC4 128 bits	CCMP: AES 128 bits
	Vector de inicialización	24 bits	48 bits	48 bits
	Integridad de la cabecera	No	CCM	CCM
	Integridad de los datos	CRC-32	CCM	CCM
	Protección de respuesta	No	Fuerza secuencia IV	Fuerza secuencia IV
	Gestión de claves	No	Basada en EAP	Basada en EAP
	Distribución de claves	Manual	802.1x (EAP)	802.1x (EAP)
	Clave asignada a	Red	Paquete, sesión y usuario	Paquete, sesión y usuario
	Clave por paquete	Concatenación de IV	Mezclado TKIP	No necesario
Otros	Seguridad Ad-Hoc	No	Si (IBSS)	Si (IBSS)

Fuente: (Izaskun Pellejero F. A., 2006).

4.7Ejemplo práctico de seguridad e integridad de la información Repositorio Digital PUCE

4.7.1 Protocolo no seguro

Para entender de una mejor manera las técnica de encriptación se procederá a dar un ejemplo práctico donde se puede constatar la seguridad e integridad de la información, mediante el uso de la herramienta Wireshark encargada del análisis del tráfico de la red en tiempo real,

permitiendo capturar los paquetes y determinar el nombre de usuario y contraseña de una página web donde el usuario necesita loguearse.

Para probar la seguridad de los datos en una red inalámbrica que no utiliza protocolos de seguridad ni técnicas de encriptación, se procederá al registro del usuario en una página Web no segura “http://pucedspace.puce.edu.ec/ un Repositorio Digital PUCE Quito.

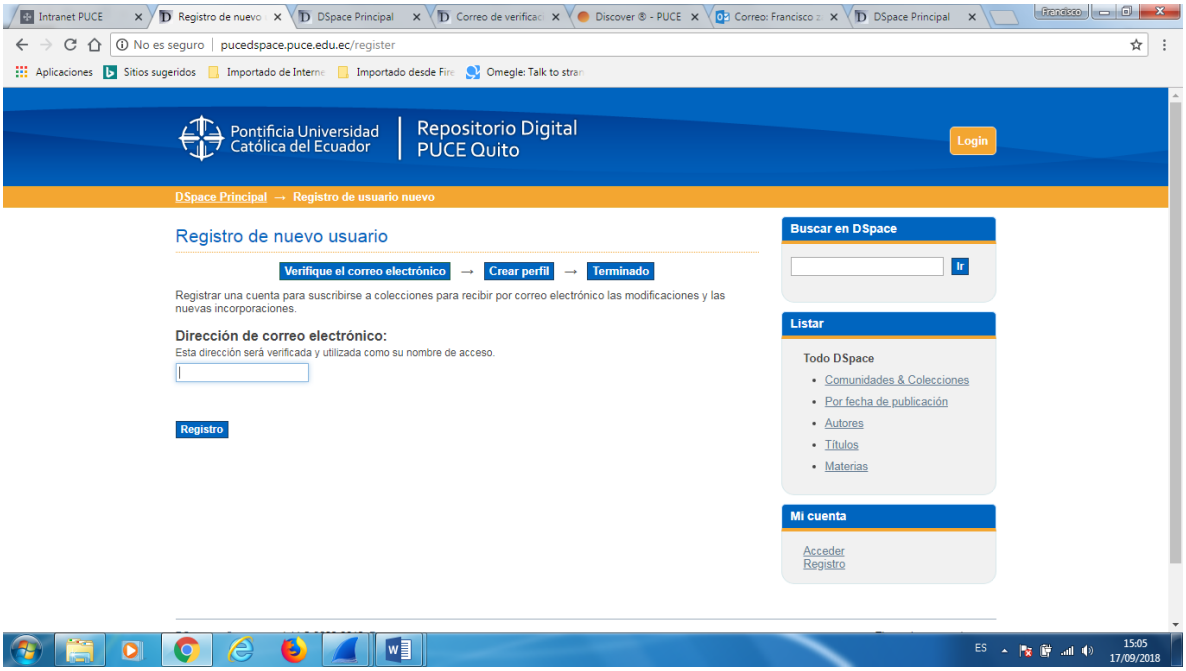

Figura: 4. 17 Formulario de Registro

Fuente: http://pucedspace.puce.edu.ec/

Una vez registrado en el portal tenemos nuestro usuario y contraseña de logueo , las mismas que permitirán acceder al portal de la página web ya mencionada, como podemos observar en la figura.

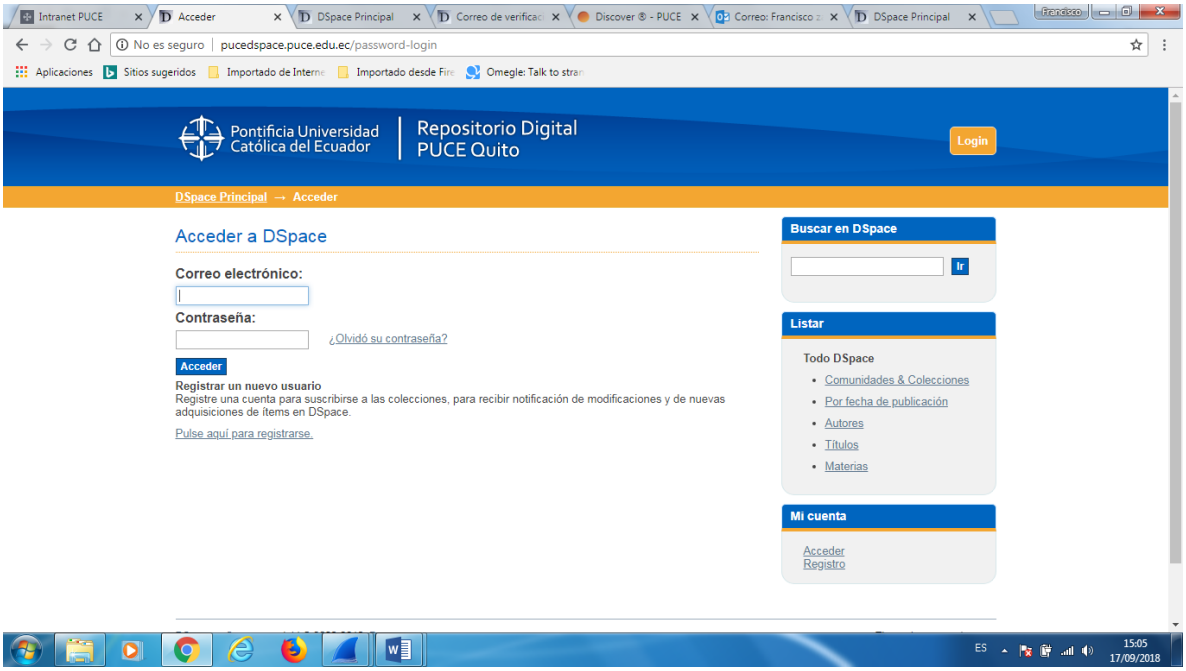

Figura: 4. 18 Usuario y Contraseña

Fuente: http://pucedspace.puce.edu.ec/

Se iniciará sesión con nuestro usuario y contraseña

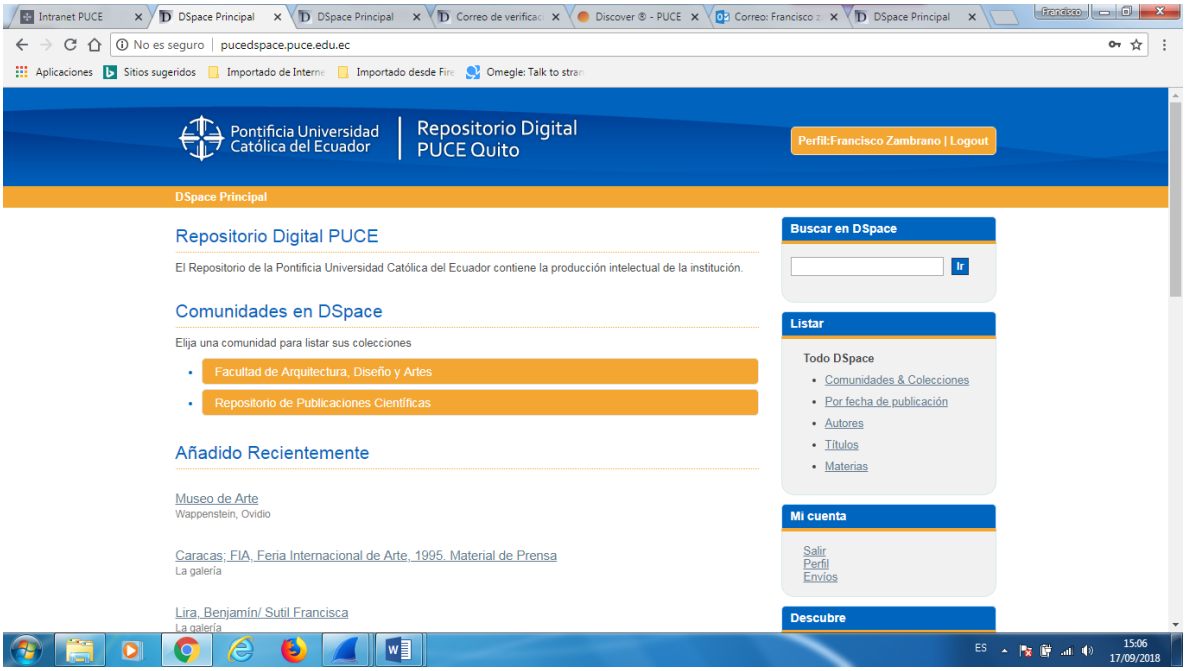

Figura: 4. 19 Inicio de Sesión

Fuente: http://pucedspace.puce.edu.ec/

Mediante el uso de la herramienta WIRESHARK permitirá analizar y capturar el tráfico de la red en tiempo real, los mismos que serán mostrados a detalle.

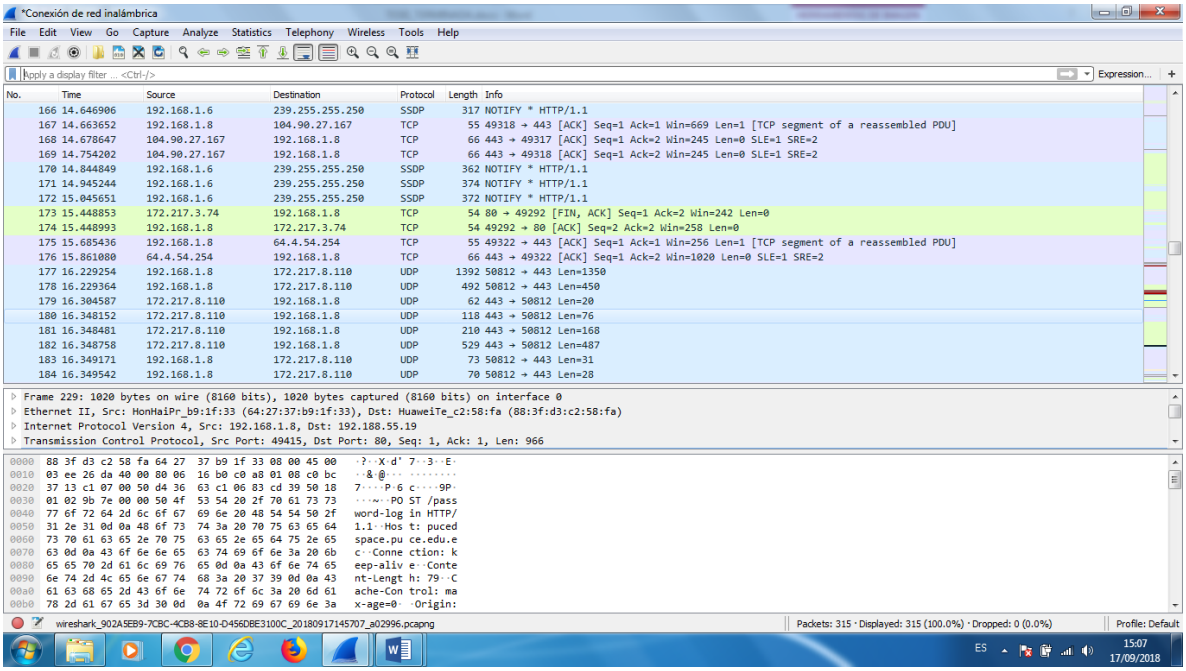

Figura: 4. 20 Trafico de Red en Tiempo Real

Fuente: WIRESHARK

Se utilizará filtros para segregar la información, que permitirá el análisis de determinados paquetes. En este caso se filtrará mediante protocolo no seguro HTTP, permitiendo visualizar solo el trafico HTTP como se muestra en la figura.

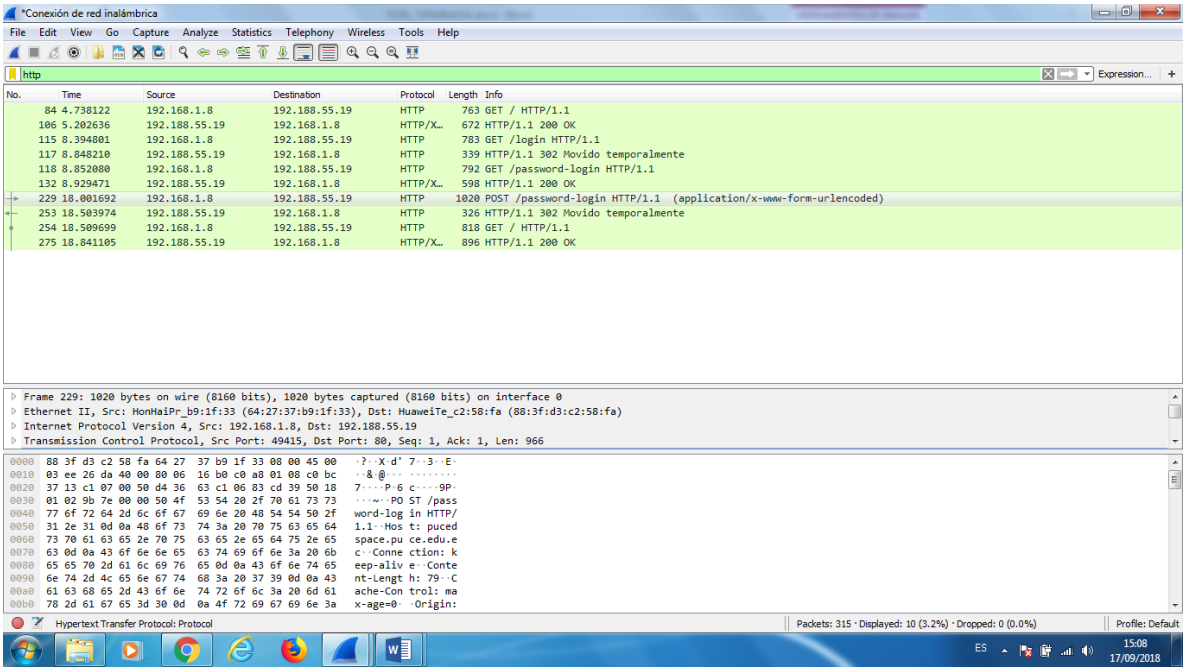

Figura: 4. 21 Filtro de Protocolo HTTP

Fuente: WIRESHARK

Aplicado el filtro nos mostrara todo el tráfico de la red que sea HTTP y a su vez, este enviando información a través del método POST, ya que la mayoría de sitios Web que manejan credenciales de acceso utilizan protocolos HTTP.

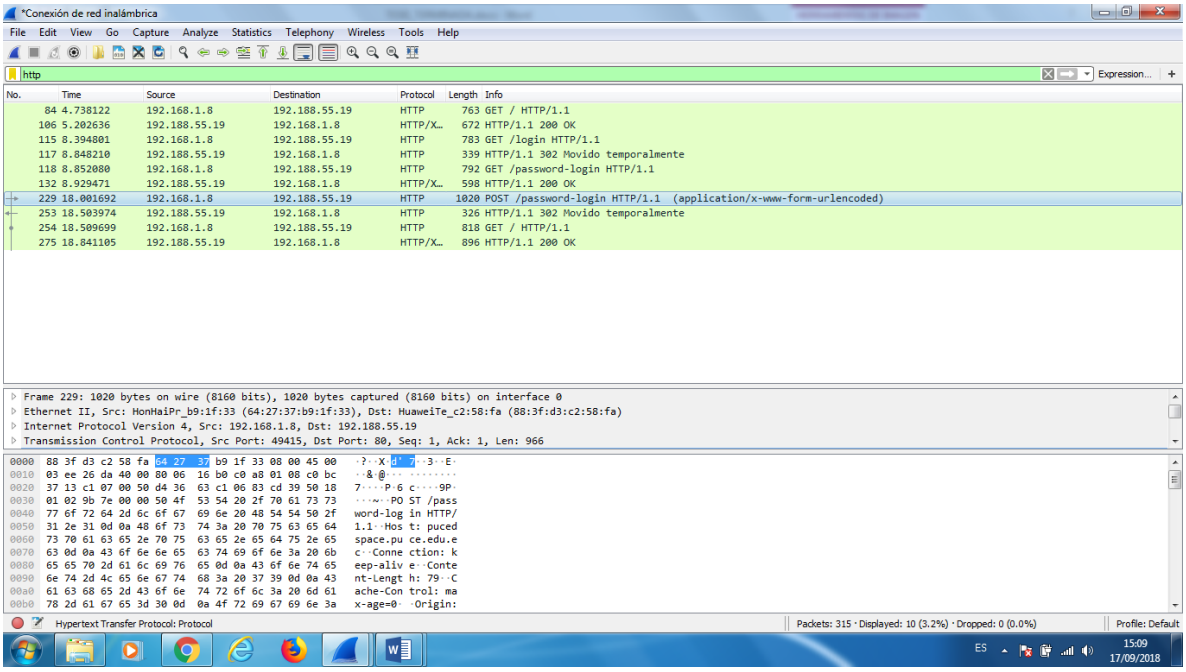

Figura: 4. 22 Paquete Capturado

Fuente: WIRESHARK

Damos doble click sobre la línea POST, se abrirá una ventana con varias entradas desplegables, donde situaremos el URL o HTML que almacena la información de logueo de la determinada página WEB, se puede observar que se capturo la trama del método POST dentro del Sniffer.

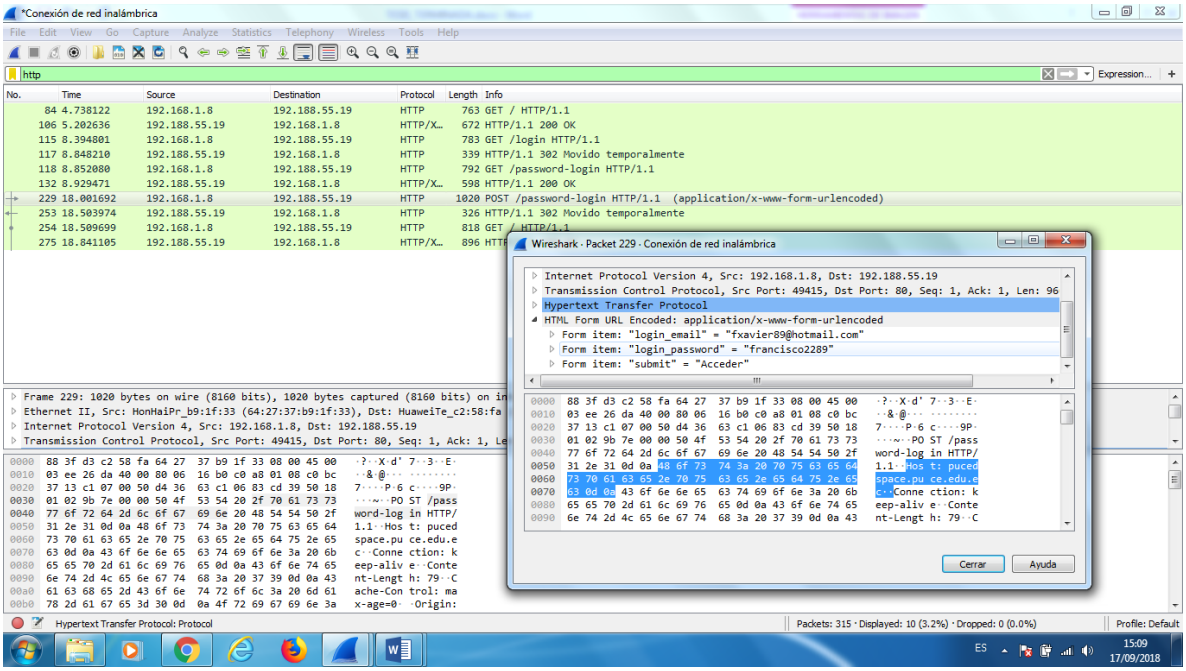

Figura: 4. 23 Análisis del Paquete

Fuente: WIRESHARK

Se analiza el paquete y se obtiene el usuario y contraseña que se capturo en el filtro

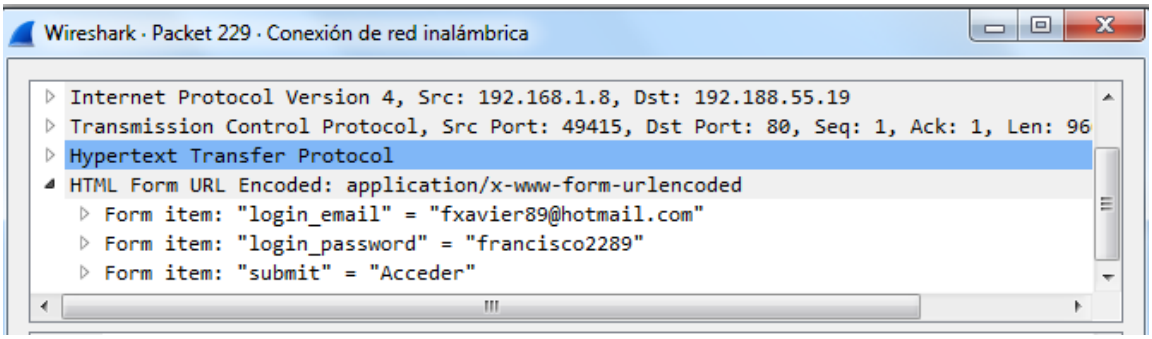

Figura: 4. 24 Obtención de Usuario y Contraseña

Fuente: WIRESHARK

Cuando se utiliza protocolo no seguro, la información esta vulnerable, debido a que esta, no se encuentra encriptada, por tal motivo está expuesta para que personas no autorizadas intercepten los paquetes y los analicen, obteniendo así, su usuario y contraseña de acceso.

4.7.2 Protocolo seguro

Cuando la página WEB utiliza seguridades y encripta la información es difícil capturar los paquetes y las credenciales de acceso del usuario a la página, el proceso es un poco diferente al anterior utilizaremos el símbolo del sistema de Windows o CMD para saber la dirección IP origen correspondiente al computador del usuario, permitirá ubicarnos dentro de las capturas realizadas por el programa WIRESHARK encargado de capturar el tráfico generado dentro de la red “PUCE” en tiempo real , para ello utilizaremos el comando ipconfig como se puede observar en la imagen.

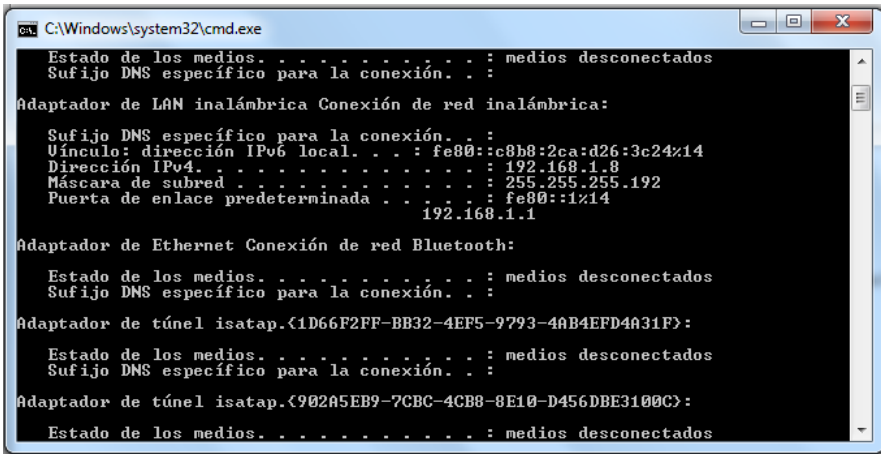

Figura: 4. 25 Dirección IP Origen con el comando ipconfig

Fuente: CMD

A continuación se utilizará el comando *nslookup* que permitirá conocer la dirección IP de un dominio o página WEB, en este caso es la página de Facebook, que vendría hacer la dirección

IP destino a la que el usuario accede desde su computador a través de la red “LA CATO Wireless” como se muestra en la imagen.

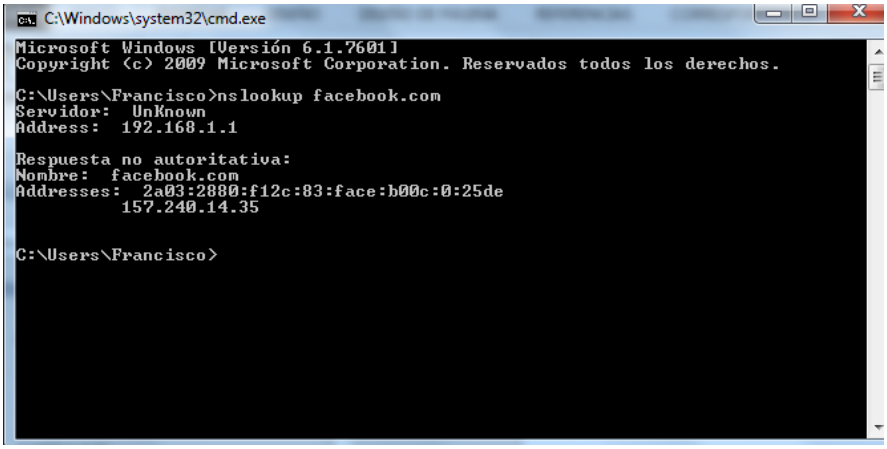

Figura: 4. 26 Dirección IP Destino con el comando nslookup

Fuente: CMD

Una vez que se tiene las direcciones IP tanto origen como destino, se procede a utilizar el filtro ip.src == 192.168.1.8 correspondiente a la dirección origen y el ip.src == 192.168.1.1 correspondiente a la dirección destino para filtrar el tráfico generado dentro de la red como se puede visualizar el la imagen.

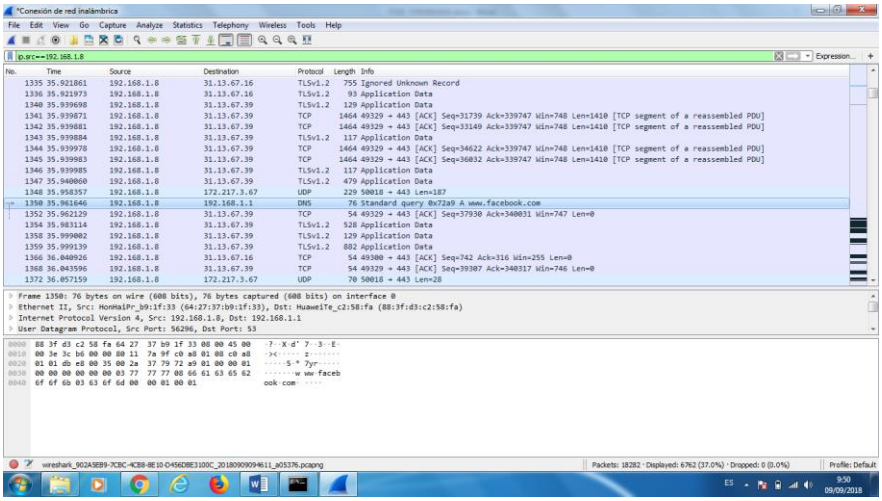

Figura: 4. 27 Filtro ip.src

Fuente: WIRESHARK

Como la página WEB encripta la información es imposible analizar los paquetes para identificar las credenciales de acceso, además no es posible visualizar el método POST encargado de enviar información del paquete capturado para su análisis.

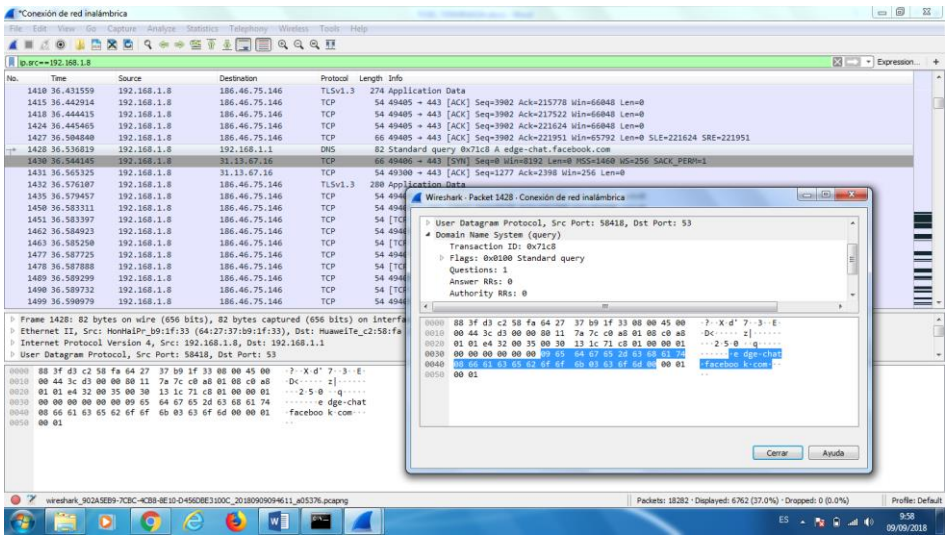

Figura: 4. 28 Captura del paquete a través de la dirección IP Origen-Destino

Fuente: WIRESHARK

Cuando se utiliza protocolo seguro HTTPS se crea un canal seguro sobre una red insegura, encriptando la información a enviarse, en otras palabras se mantiene la integridad de los datos. En caso de que una persona no autorizada intercepte la transferencia de datos de la conexión, lo único que capturara será un flujo de datos cifrados, que al momento de analizarlos, resultará imposible de descifrar.

El caso práctico expuesto sobre la encriptación de redes inalámbricas a nivel de aplicación, permitirá saber con más exactitud de cuán importante es utilizar las técnicas de encriptación en las redes Wi-Fi para mantener la confidencialidad, autenticación e integridad de la información, brindándonos mayor seguridad a la hora de enviar datos a través del internet y saber que estos llegan tal y como fueron enviados.

4.8 Diagrama de Flujo para Encriptar/Desencripar Información

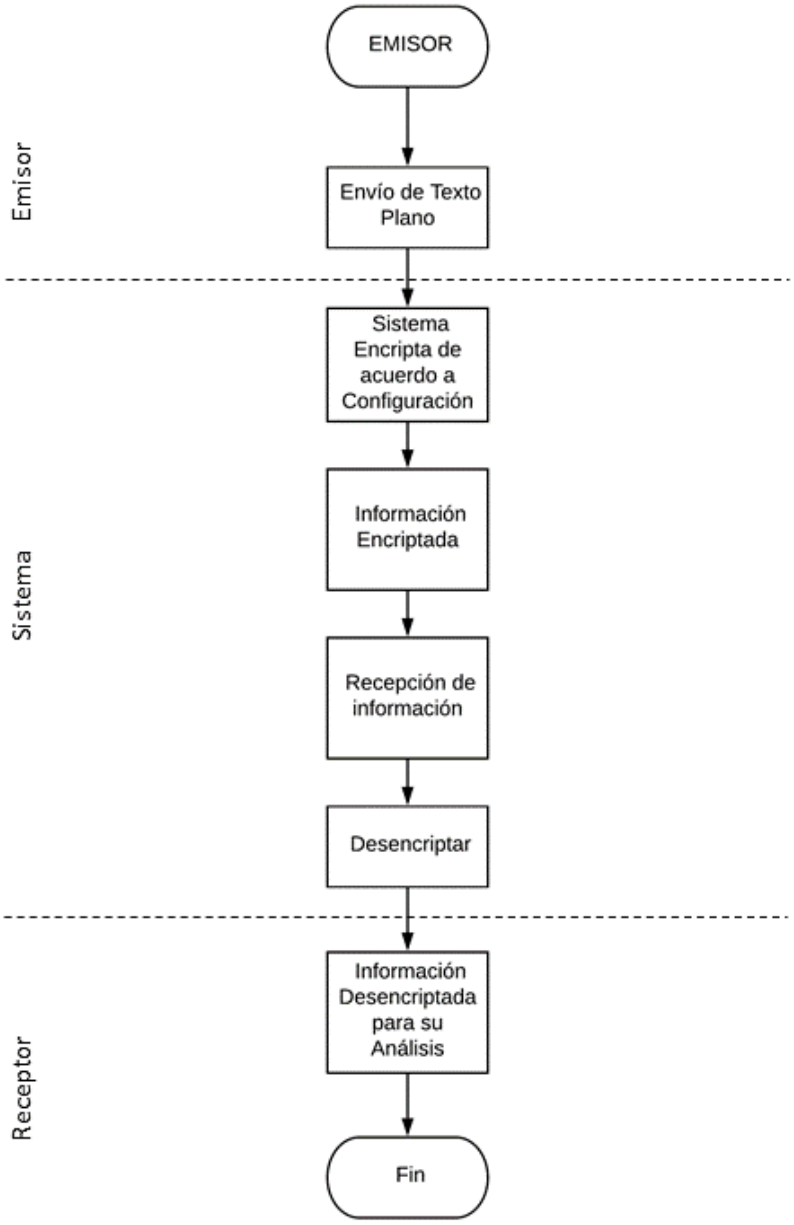

Figura: 4. 29 Encriptar/Desencriptar la Información

Fuente: Francisco Zambrano

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusión:

1. Las redes inalámbricas se han vuelto muy populares en la sociedad, debido a que estas nos permiten acceder a lugares donde el cableado sea inaccesible, además de la facilidad de movilidad y los costos reducidos de mantenimiento.

2. Las redes inalámbricas son más vulnerables de ataques que las redes cableadas debido a que la señal se expande por aire en un cierto radio de cobertura, pero, gracias a los avances tecnológicos se ha mejorado la seguridad de este tipo de red con la utilización de protocolos de seguridad, restricción de dirección MAC, autenticación y métodos de encriptación.

3. De acuerdo al análisis realizado de las diferentes técnicas de encriptación se concluye que la PUCE (Pontificia Universidad Católica Del Ecuador) utiliza una técnica de encriptación WPA2-enterprise, para entornos empresariales ya que este cifrado tiene mayor seguridad que sus predecesores debido a que trabaja conjuntamente con el estándar 802.1x encargado del control de acceso a la red para una autenticación superior y distribución de claves, por lo que debe ser usado con una técnica de cifrado, el mismo que posee un algoritmo de cifrado que garantiza la integridad de la información. Además de trabajar conjuntamente con el Domain Controller donde encontramos las credenciales de acceso de cada usuario, permitiendo autenticar al usuario que quiere acceder a los recursos de la red, garantizando la privacidad e integridad de las comunicaciones que pasan a través de una red inalámbrica en este caso "LA CATO Wireless". Por lo tanto la técnica de encriptación mencionada es mucho más segura que sus predecesores WEB, WPA debido a que trabaja conjuntamente con estándares, protocolos de autenticación y distribución de claves dinámicas.

4. WPA2- Enterprise Mejora notablemente el nivel de protección de datos y el control de acceso a las redes inalámbricas. Debido a que trabaja conjuntamente con protocolos de autenticación de usuario y algoritmos de encriptación.

5. El conjunto de estos dos mecanismos (estándar 802.1x y protocolo EAP) junto con el esquema de cifrado forman una fuerte estructura de autenticación.

6. Mediante el caso práctico expuesto y relacionado con la seguridad e integridad de la información, se puede concluir que personas no autorizadas pueden acceder a la información cuando no se tiene las medidas de seguridad, sólo basta el uso de herramientas para analizar el tráfico de la red a la que se quiere acceder y capturar los paquetes. En el ejemplo se capturó el usuario y contraseña del Repositorio Digital PUCE Quito, esto pudo ser posible ya que la página web no manejaba ningún tipo de seguridad.

5.2 Recomendaciones:

1. Considerar la seguridad física de los puntos de acceso y de otros equipos de la infraestructura de la red local (como puntos de acceso y switch) para impedir que estos puedan ser manipulados por usuarios no autorizados.

2. Actualizar de forma periódica el firewall de los puntos de acceso y los controladores (driver) de la tarjeta de red para subsanar posibles agujeros de seguridad.

3. El servidor RADIUS debería bloquear al usuario que intenta acceder a los recursos de la red tras una serie de intentos de logueo fallido, cuando la cuenta de usuario está bloqueada el usuario no puede ser autenticado y por lo tanto, no puede utilizar la red WLAN, necesariamente tendrá que acudir al administrador de la red.

4. Para poder acceder a los recursos de la red inalámbrica de la PUCE, cuando no pertenece al dominio es recomendable realizar las configuraciones correspondientes dependiendo del sistema operativo, caso contrario no podrá acceder con las credenciales de acceso que se encuentran almacenadas en el active directory.

5. Por razones de seguridad se recomienda emplear HTTPS en el portal cautivo de autenticación de usuario de la "LA CATO Wireless" para llevar a cabo un adecuado control de acceso. De esta manera se protege al usuario de terceros que podrían usurpar la identidad y acceder a los recursos de la red.

6. Es importante tomar conciencia, que para mantener la seguridad e integridad de la información sólo basta tomar alguna de las muchas alternativas de seguridad existentes, para un tratamiento de la información en forma segura y así establecer una barrera en el adecuado manejo de datos.

BIBLIOGRAFÍA

Alvarez, M. A. (22 de Agosto de 2001). *DesarrolloWeb.com* . Obtenido de DesarrolloWeb.com : https://desarrolloweb.com/articulos/513.php

Barajas, S. (2004). Protocolos de seguridad en redes inalámbricas. *saulo*, 5.

Bautista, H. (25 de Septiembre de 2013). *Rootear.* Obtenido de Rootear: http://rootear.com/seguridad/vulnerabilidades-una-red-wi-fi

Brown, E. L. (2006). *802.1X Port-Based Authentication.* CRC Press.

Castaño Ribes, R. J. (2013). *Redes Locales.* Macmillan Iberia,S.A.

Castaño Ribes, R. J. (2013). *Redes Locales .* Macmillan Iberia, S.A.

CASTRO GIL Manuel Alonso, D. O. (2014). *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES.* UNED.

Chacón, C. H. (2009). *Criptoanálisis práctico de WEP y WPA sobre WLAN 802.11.*

Chiu, H. (s.f.). *Seguridad de Redes Inalámbricas 802.11.*

Dahua Tenazoa, A. (2011). *Academia.* Obtenido de Academia: http://www.academia.edu/13192576/MONOGRAFIA_DE_INVESTIGACION-Redes_Inalambricas

Dominguez, C. V. (2002). *blyx.* Obtenido de blyx: http://www.blyx.com/public/wireless/redesInalambricas.pdf

Dordoigne, P. A. (2006). *Redes Informáticas conceptos fundamentales.* Barcelona: ENI.

EcuRed. (s.f.). Obtenido de Estándares Inálambricos: https://www.ecured.cu/Est%C3%A1ndares_Inal%C3%A1mbricos

Gallego, J. C. (2015). *FPB - Instalación y mantenimiento de redes para transmisión de datos.* Editex.

Gallego, J. C. (2015). *FPB - Instalación y mantenimiento de redes para transmisión de datos.* Editex.

GARCÍA, A. A. (1989). *TELEINFORMÁTICA Y REDES DE COMPUTADORES.* MADRID: MARCOMBO S.A.

Gómez, J. A. (2010). *Servicios en Red.* Editex.

Guillermo, S. F. (2011). *Análisis de Vulnerabilidades de seguridades en redes inalámbricas dentro de un entorno empresarial que utilizan cifrado AES y TKIP, WPA personal y WPA2 personal del DMQ.* Quito.

Heredero, C. d. (2004). *Informática y comunicaciones en la empresa.* Madrid: ESIC Editorial.

Internacional, P. S. (2005). *Seguridad en redes inalámbricas .* Obtenido de http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

Izaskun Pellejero, . A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN:.* Marcombo.

Izaskun Pellejero, F. A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN.* Barcelona-España: MARCOMBO S.A.

Izaskun Pellejero, F. A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN:.* Marcombo.

Julio Barbancho Concejero, J. B. (2014). *Redes locales.* Paraninfo, S.A.

Lehembre, G. (2006). Seguridad Wi-Fi - WEP, WPA y WPA2. *Hacking9-Wifi*, 15.

Ma DEL CARMEN ROMERO TERNERO, J. B. (2010). *REDES LOCALES.* Paraninfo.

Marañón, G. Á. (2009). *Cómo protegernos de los peligros de Internet.* CSIC - CSIC Press.

MARIA DEL PILAR ALEGRE RAMOS, A. G.-C. (2011). *SEGURIDAD INFORMÁTICA .* Paraninfo.

MIRANDA, C. V. (2005). *Sistemas informáticos y redes locales.* Paraninfo, S.A.

Miranda, C. V. (2014). *Sistemas Informáticos y Redes Locales.* Madrid, España: Paraninfo.

Moro Vallina, M. (2013). *Infraestructuras de redes de datos y sistemas de telefonía.* Editorial Paraninfo.

Picón, J. m. (2014). *Tecnología de la comunicacion y la informacion.* Málaga-España: Planeta Alvi.

Rodríguez, L. D. (2006). *Ampliar, configurar y reparar su PC.* Marcombo.

Saulo, B. (2010). Protocolos de seguridad en redes inalámbricas.

SEGURIDAD EN REDES INALÁMBRICAS: WEP, WAP Y WAP2. (s.f.). *Acens the Cloud Hosting Company*, 6. Obtenido de www.acens.com

STALLINGS, W. (2004). *Fundamentos de Seguridad en redes Aplicaciones y estandares.* Madrid (España): PEARSON EDUCACIÓN S.A.

Tävrâ, C. A. (s.f.). *Scribd.* Obtenido de Guía de Seguridad en Redes Inaambricas: https://es.scribd.com/document/111386282/Documento-Guia-de-Wifi

Tim Howes, M. S. (2003). *Understanding and Deploying LDAP Directory Services.* Addison-Wesley Professional.

Toro, J. A. (2015). *Mantenimiento de la infraestructura de la red de comunicaciones.* Editorial Elearning, S.L.