UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Diseño de una red de sensores para detección de Rogue o Fake AP en la red wifi del área administrativa del Colegio fiscal mixto Patria Ecuatoriana.

AUTOR:

Barreiro León, Cristhian Iván

Trabajo de Titulación previo a la obtención del título de

INGENIERO EN TELECOMUNICACIONES

TUTOR:

ING. Suarez Murillo, Efraín Oswaldo

Guayaquil, Ecuador

13 de Septiembre del 2018

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr. **Barreiro León, Cristhian Iván** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES**.

TUTOR

_____

ING. Suarez Murillo, Efraín Oswaldo

DIRECTOR DE CARRERA

_____

M. Sc. Heras Sánchez, Miguel Armando

Guayaquil, a los 13 días del mes de Septiembre del año 2018

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Barreiro León, Cristhian Iván**

DECLARO QUE:

El trabajo de titulación **"Diseño de una red de sensores para detección de Rogué o Fake Ap en la red wifi del área administrativa del Colegio fiscal mixto Patria Ecuatoriana."** previo a la obtención del Título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 13 días del mes de septiembre del año 2018

EL AUTOR

_____

BARREIRO LEÓN, CRISTHIAN IVÁN

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Barreiro León, Cristhian Iván**

Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **"Diseño de una red de sensores para detección de Rogue o Fake Ap en la red wifi del área administrativa del Colegio fiscal mixto Patria Ecuatoriana."**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

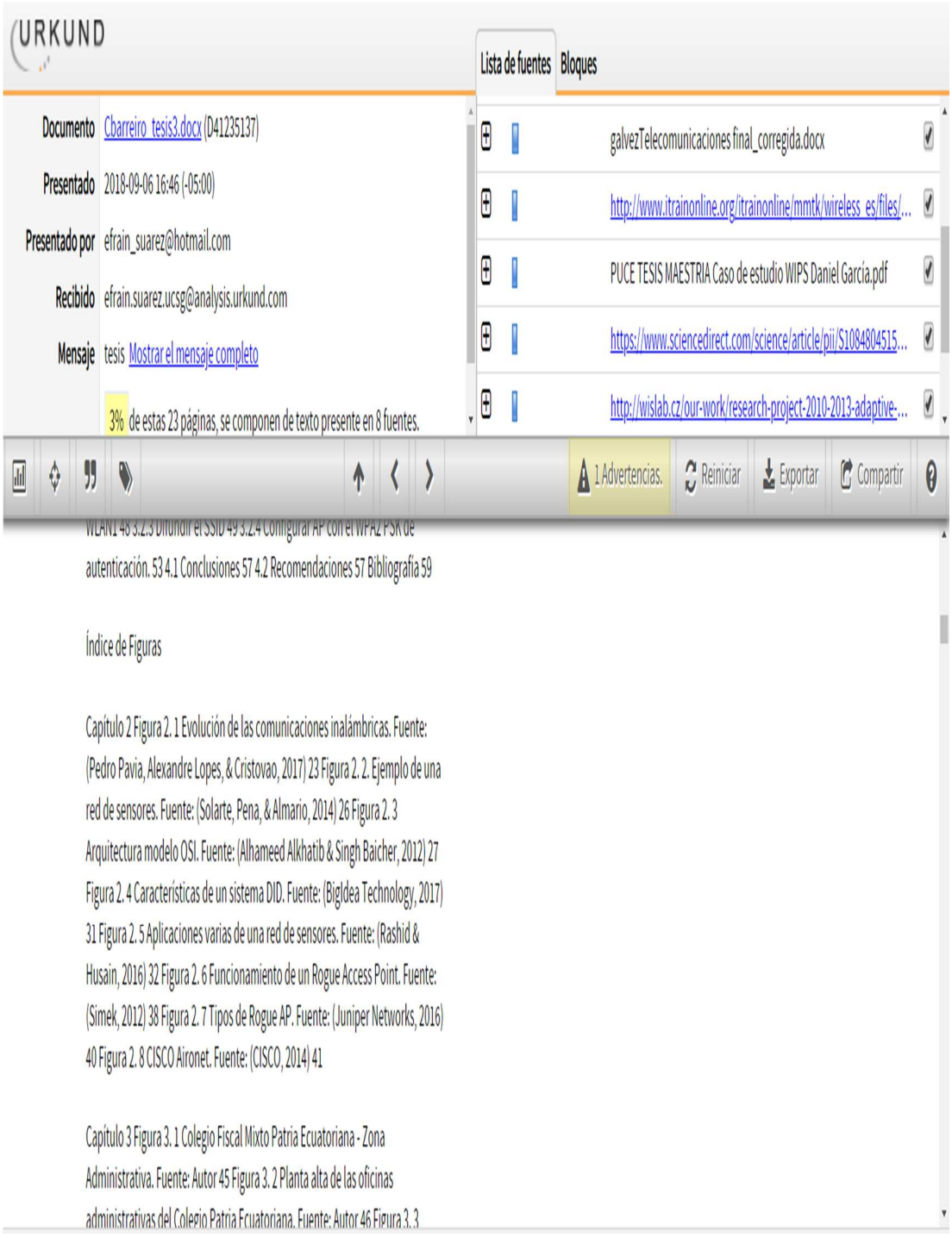
Guayaquil, a los 13 días del mes de Septiembre del año 2018

EL AUTOR

_____

BARREIRO LEÓN, CRISTHIAN IVÁN

REPORTE DE URKUND



DEDICATORIA

Este trabajo de titulación se lo dedico a Dios, a mis padres, familiares,
Amigos, docentes y a todos aquellos que me brindaron
Su comprensión, amor y ayuda en los momentos difíciles,
Pues a ellos les debo este logro.

EL AUTOR

_____

BARREIRO LEÓN, CRISTHIAN IVÁN

AGRADECIMIENTO

Este trabajo realizado con mucho cariño se lo agradezco primero que nada a Dios.

A mis padres Jorge Barreiro y Yolanda León que han sido mi apoyo fundamental durante estos años de estudio.

A mis hermanos por brindarme su apoyo y estar siempre conmigo.

A mis abuelos por ayudarme en todo momento, aun cuando se encontraban lejos.

EL AUTOR

_____

BARREIRO LEÓN, CRISTHIAN IVÁN

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. Sc. ROMERO PAZ, MANUEL DE JESÚS

DECANO

f. _____

M. Sc. ZAMORA CEDEÑO, NESTOR ARMANDO

COORDINADOR DE AREA

f. _____

M. Sc. PALACIOS MELENDEZ, EDWIN FERNANDO

OPONENTE

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

Capítulo 2

Capítulo 3

ÍNDICE DE TABLAS

Capítulo 2

RESUMEN

El trabajo de titulación consiste en el diseño de una red de sensores para el sistema de detección de Rogué o Fake Ap en la red WIFI del área administrativa del “Colegio fiscal mixto Patria Ecuatoriana”. Primero se hablará sobre la problemática actual y la importancia de la seguridad en las redes inalámbricas, luego definiremos los sistemas que nos van a permitir la localización de los Rogue o Fake Ap. En el siguiente capítulo se explica por qué el uso de CISCO Aironet para diseñar la red, luego modelos de optimización para la red de sensores, también expondremos la manera en que se manejara la información para desarrollar los algoritmos, a continuación, se mostrara la estructura de la programación con la cual se puede diseñar la red de sensores para evitar los Rogue o Fake Ap. Explicaremos la circunstancia y parámetros en el cual basamos los algoritmos generados, luego mostraremos el resultado final y el grado de cobertura obtenido. Por último, anunciaremos las conclusiones y recomendaciones a las que hemos llegado en el presente trabajo de titulación.

Palabras claves: SENSORES, ROGUE, DISEÑO, RED, SEGURIDAD, INALAMBRICA; WIFI.

ABSTRACT

This titling work is about the design of a wireless sensor network system that will provide help to detect Rogue or Fake AP's in the wireless network of the Patria Ecuatoriana Public School. First, this work will show the current problems at the school in terms of security networks and the importance of setting up one for all the sensitive data that is used in this educational facility, then we will define the systems that will allow users to detect Rogue or Fake AP's. After showing the proper terms that are used in this work, the importance of the CISCO Aironet design will be explained and all the possibilities of optimization models for the wireless sensor network. One topic that is showed is how the information can be managed and how this will also help to develop an algorithm, and its code structure to detect Rogue or Fake AP's. All the circumstances and parameters that helped the development of the algorithm will be presented along with the result and the degree of coverage. finally, all the conclusions and recommendations after the implementation of this work will be exposed.

Keywords: SENSORS, ROGUE, DESIGN, NETWORK, SECURITY, WIRELESS; WIFI.

CAPÍTULO 1: INTRODUCCIÓN

1.1. Introducción.

En los sistemas de comunicación inalámbrica, un Rogue o Fake APS es un punto de acceso que se conecta sin permiso o autorización a la red fija o realiza un cambio de identidad en un AP de una red privada, como la red del Colegio Fiscal Mixto Patria Ecuatoriana.

Un Rogue o Fake APS es una amenaza constante para la seguridad de la red, debido a que provee de un acceso alternativo logrando evitar las medidas de seguridad en las redes fijas como son los conocidos corta fuegos o firewalls y de igual modo, los Rogue o Fake up son utilizados para atrapar y hurtar información privada y valiosa, como son las credenciales de acceso a los usuarios desapercibido en su categoría de cobertura.

Para no permitir estos problemas o amenazas existen los sistemas de prevención de intrusos inalámbricos (WIPS), estos sistemas de prevención permiten un control de la red inalámbrica por medio del espectro radioeléctrico en su caza de Rogue o Fake APS o alguna otra advertencia. Los WIPS están aptos para detectar y sitiar, generar alertas e incluso ubicar la localización de un Rogue APS, por este motivo se requiere del uso de sensores inalámbricos Cisco 2700 series calificados para el monitoreo.

Los sensores compatibles con los puntos de acceso de la red “WLAN1” son los módulos WSSI de CISCO este módulo se colocara junto con el punto de acceso AIRONET 3700 de Cisco que van a formar parte de la red inalámbrica “WLAN1”.

1.2. Antecedentes

Actualmente en el “Colegio fiscal mixto Patria Ecuatoriana” no existe un sistema de detección de Rogue o Fake AP que de seguridad a las diferentes áreas del colegio y de brinde seguridad a los docentes como a todo el personal de área administrativa, lo cual ha llevado a buscar algunas soluciones para esta problemática.

Antiguamente no era tan viable debido a su costo y su mala cobertura, pero con el pasar de los años los costos fueron disminuyendo y ahora es mucho más factible tener un sistema de seguridad inalámbrica y necesario, la mayoría de las empresas e instituciones lo usan hoy en día por la cantidad de robos cibernéticos que se han presentado y lo ven más como una inversión.

1.3. Planteamiento del Problema.

La falta de una red de seguridad inalámbrica para que los docentes como personal administrativo y el colegio tengan mayor seguridad en todo lo que tiene que ver con seguridad informática.

1.4. Objetivos del Problema de Investigación.

1.4.1 Objetivo General.

El objetivo del trabajo de titulación es diseñar una red de sensores para detectar Rogue o Fake Ap en la red wifi del área administrativa del “Colegio Fiscal Mixto Patria Ecuatoriana”.

1.4.2 Objetivos Específicos.

- Analizar la infraestructura que posee el área administrativa del “Colegio fiscal mixto patria ecuatoriana”.
- Realizar el diseño de la red.
- Realizar pruebas del diseño y alcance del proyecto.

1.5. Hipótesis.

Con la implementación de la red diseñada se logrará la seguridad inalámbrica de toda el área administrativa que permita el trabajo efectivo de docentes y personal administrativo.

1.6. Metodología de Investigación.

Para este trabajo de investigación se utilizarán las metodologías científicas, descriptivas y analíticas. La metodología analítica ya que se

realizará un previo análisis de la arquitectura antes del realizar el debido diseño de dicha red y descriptiva porque se simulará la red para demostrar el desempeño de esta.

CAPÍTULO 2: MARCO TEÓRICO

2.1 Historia de la comunicación inalámbrica

La historia de las comunicaciones inalámbricas comenzó con el entendimiento con respecto al comportamiento de las propiedades magnéticas y eléctricas de los elementos inicialmente estudiados por científicos de la China, Grecia e Italia. El uso de la luz para las comunicaciones inalámbricas fueron una de las primeras etapas de experimentación para la comunicación inalámbrica. Inicialmente se utilizaban luces y banderas para simular un tipo de comunicación. De acuerdo con los avances tecnológicos respectivos al uso de este tipo de tecnología, y su desarrollo evolutivo como podemos ver en la figura 2.1. El estudio para la evolución de los equipos necesarios para la comunicación evoluciona favorablemente para las empresas como Bell. (Hindle, 2015)

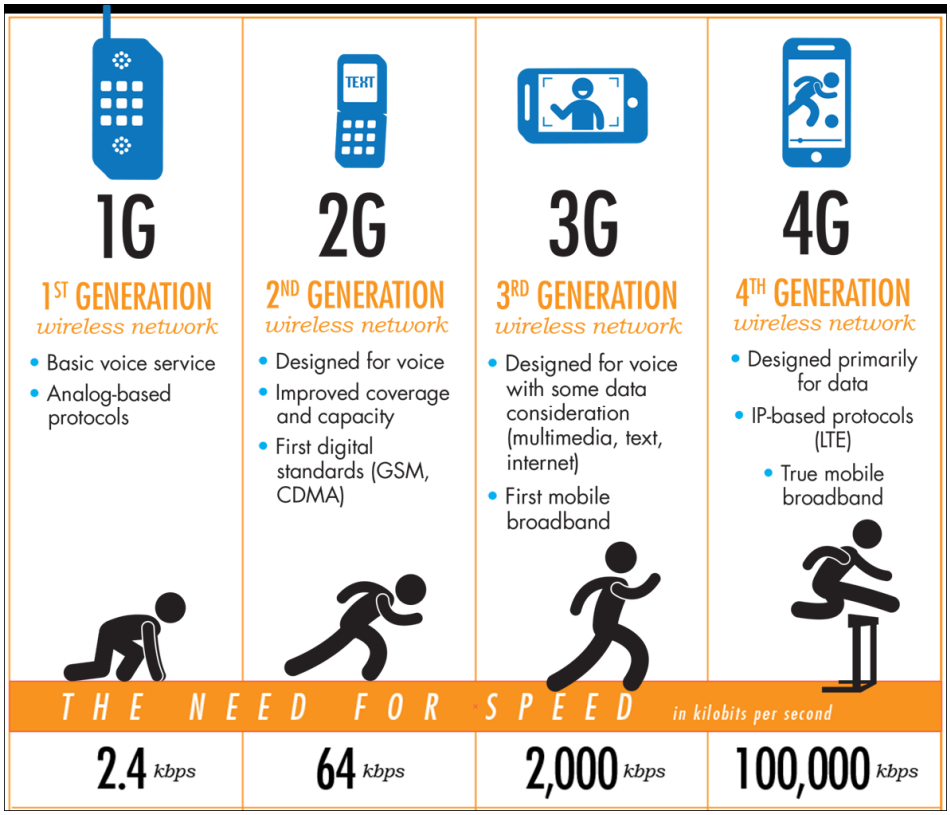


Figura 2. 1 Evolución de las comunicaciones inalámbricas por generación. Fuente: (Electronics for you, 2017)

Las comunicaciones alámbricas empezaron con la primera línea comercial de telégrafos entre Washington y Baltimore en 1843 y la invención del teléfono por Alexander Graham Bell. El estudio básicamente abarcó todos los sistemas de transmisión ópticos de alta frecuencia del transmisor de luz. Cada vez que se intentaba comunicarse cualquier tipo de perturbación opacaba el intento de comunicación. Durante estas pruebas no era posible enfocar la luz de manera eficiente como en la actualidad se lo puede hacer con un láser. Las comunicaciones inalámbricas no tuvieron un desarrollo marcado hasta que se estudió acerca de las ondas electromagnéticas y equipos con la capacidad de modularlos. (Hindle, 2015). Después de varios años los sistemas de comunicación inalámbrica se desarrollan de tal forma que aparte que nos permite comunicarnos de cualquier parte, el avance de los equipos emisores y receptores como de los amplificadores de señal móvil son muy importantes.

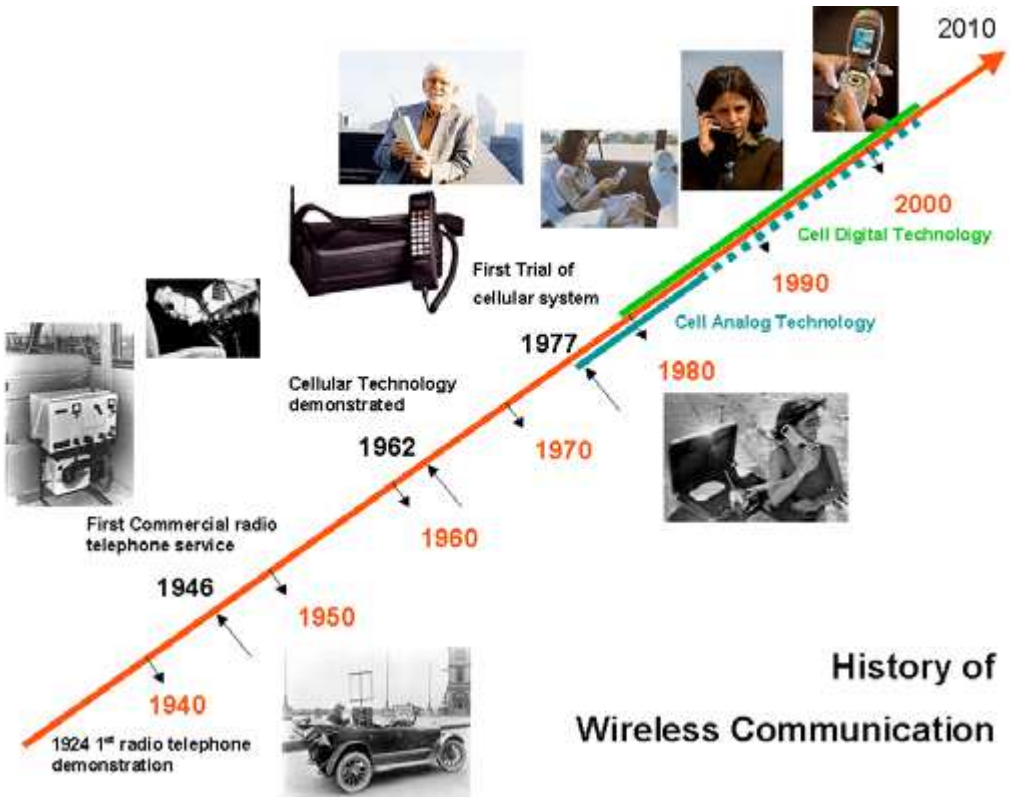


Figura 2. 2 Línea de tiempo de desarrollo tecnológico en comunicaciones inalámbricas.
Fuente: (Winters, Mielenz, & Hellestrand, 2014)

Como primera instancia podemos mencionar los estudios realizados por Heinrich Rudolf Hertz, quien logró un importante descubrimiento al poder transmitir electricidad en forma de ondas electromagnéticas. Como podemos ver en la figura 2.2, aunque no se poseía los equipos necesarios para poder tener mucho más alcance y poder comercializarlo, este descubrimiento no destaca, se lo conoce como una contribución importante para descubrimientos y aplicaciones posteriores. Otros de los personajes importantes que contribuyeron de gran forma fueron Calzecchi Onesti, Oliver Lodge o August Righi quienes hicieron importantes contribuciones en la recepción de las ondas electromagnéticas, aun así, las distancias seguían siendo un problema. El ruso Alexander Popov logró por medio de varios experimentos crear una antena que ayudaría a detectar señales electromagnéticas, teniendo como resultado una comunicación inalámbrica a 250 metros de distancia. En este experimento se utilizaron un oscilador, un detector y una antena. Teniendo en cuenta este tipo de experimento, Guillermo Marconi patenta en 1897 la primera conexión inalámbrica que originó lo que hoy se conoce como comunicaciones por radio. A partir de estos experimentos, el avance tecnológico siguió su curso dando como resultado comunicaciones entre Canadá y Gran Bretaña y este fue el inicio de las comunicaciones inalámbricas analógicas. (Seymour & Shaheen, 2011)

Las comunicaciones se segunda generación o 2G, aparece a con la telefonía móvil en 1990 en la que se produce la sustitución de protocolos analógicos por digitales y de este modo mejorar la comunicación en su cobertura, como podemos ver en la figura 2.3. Un hecho importante a partir de estas nuevas implementaciones es la aparición de los SMS (Servicio de Mensaje de Texto). Las comunicaciones de tercera generación o 3G tiene como novedad el mejoramiento significativo de transmisión de voz y el flujo de datos de una manera más rápida. La segunda generación de comunicación inalámbricas que partió desde la implementación de dominios para la conservación de datos en cada uno de los dispositivos telefónicos, haciéndolos aptos para el intercambio de data mucho más efectivo. Esta

generación también se la conoce como 2.5G, el cual da cabida al desarrollo de sistemas de comunicaciones de tercera generación. (Seymour & Shaheen, 2011)

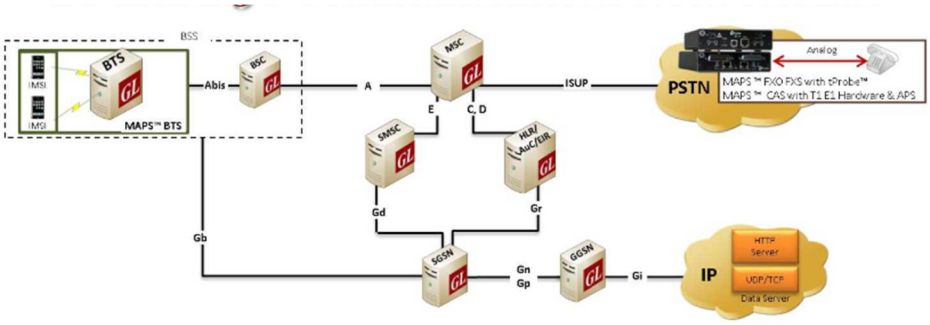


Figura 2. 3 Comunicaciones inalámbricas 2g.
Fuente: (GL Communications Inc., 2016)

La tercera generación de comunicaciones inalámbricas o también conocidas como el International Mobile Telecommunications-2000 (IMT-2000), es la que obedece a los estándares propuestos por la Unión Internacional de Telecomunicaciones como podemos ver en la figura 2.4. El uso de este tipo de tecnología permite transmitir paquetes de data eficientemente con un ancho de banda mucho más amplio. En el uso de este tipo de tecnología los celulares mejorar su capacidad de enviar paquetes de data entre dispositivos, llamadas son mucho más y las comunicaciones con respecto a internet, video y servicios de mensajería se desarrollan de manera rápida. (Seymour & Shaheen, 2011)

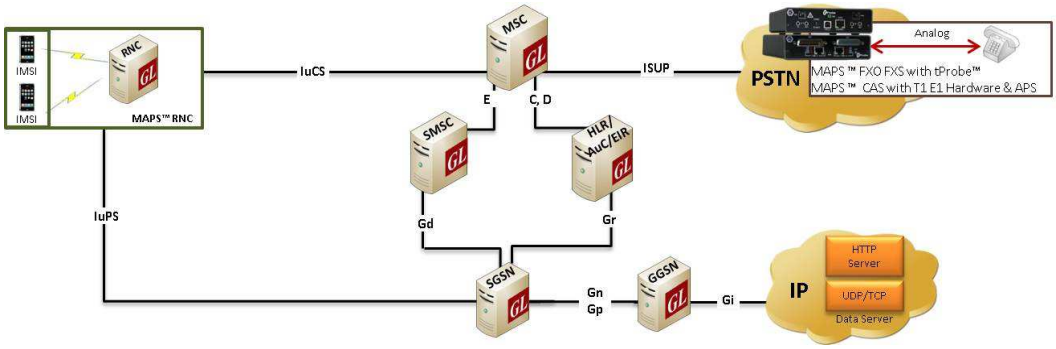


Figura 2. 4 Comunicaciones inalámbricas 3g.
Fuente: (GL Communications Inc., 2016)

La cuarta generación de comunicaciones inalámbricas se desarrolla mucho más en el ámbito de estándares. Ahora en este tipo de tecnología no solamente se amplifica el ancho de banda, pero también se agrega información con respecto a la posición del dispositivo móvil para que sea de uso para aplicaciones relevantes. Entre las aplicaciones que podemos nombrar tenemos Televisión Móvil, Video Conferencia, Telemedicina, entre otras aplicaciones más. (Seymour & Shaheen, 2011). Actualmente se encuentra en desarrollo la quinta generación de comunicaciones inalámbricas teniendo en cuenta que la nueva generación de dispositivos móviles está al alcance de la nueva fase de comunicación y de aplicaciones entre las que se destaca domótica, transportación inteligente, seguridad y e-books. (Seymour & Shaheen, 2011).

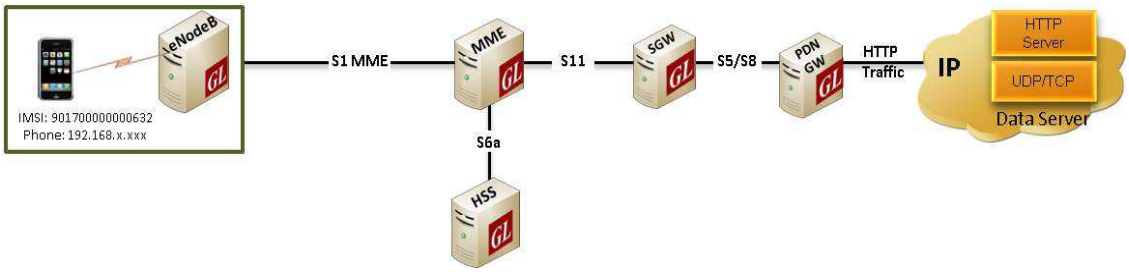


Figura 2. 5 Comunicaciones inalámbricas 4g.
Fuente: (GL Communications Inc., 2016)

En la figura 2.5, podemos ver la evolución de las comunicaciones inalámbricas dentro de los lapsos de tiempos pertinentes. Estos desarrollos se han mostrado con más frecuencia en la última década como podemos ver en la imagen. Entre las aplicaciones más importantes dentro de las comunicaciones inalámbricas, podemos destacar algunos usos dentro de la ingeniería, que, además están en constantes desarrollo para mejores y más eficientes métodos de comunicación. Primero se debe nombrar el satélite. La comunicación satelital es una de las tecnologías inalámbricas que es de mayor uso en casi todas las naciones del mundo, el cual ayuda a mantener conectado sin importar en que parte te encuentres. Los satélites usan este método de comunicación por medio de señales de radio. Con el desarrollo tecnológico ahora se puede portar dispositivos móviles satelitales y módems que tienen habilidades mucho más desarrolladas las cuales incrementan el

rango de uso de las señales sin importar el costo. Wireless Networking o redes inalámbricas es la capacidad de conectar computadores, sistemas y dispositivos móviles sin el requerimiento de cables. WIFI es una forma de conexión inalámbrica que requiere de baja capacidad y es utilizada por muchos dispositivos como teléfonos móviles, laptops, sistemas, etc. cuando se configura este tipo de sistema unos enrutadores sirven como medio de comunicación entre el servidor y el usuario. El bluetooth es un tipo de comunicación inalámbrica el cual su tecnología permite conectar cualquier aparato electrónico a un sistema para la transferencia data. Por último, también tenemos el ZigBee el cual es un tipo de comunicación inalámbrica standard diseñado para relacionar las necesidades de redes de control, sensores inalámbricos de baja gama, etc. Es importante mencionar que, aunque estas aplicaciones están formalmente asentadas en el mundo comercial e las telecomunicaciones, en la actualidad hay muchas más aplicaciones de las tecnologías aplicadas, y otras tecnologías innovadoras a punto de emerger. (Seymour & Shaheen, 2011)

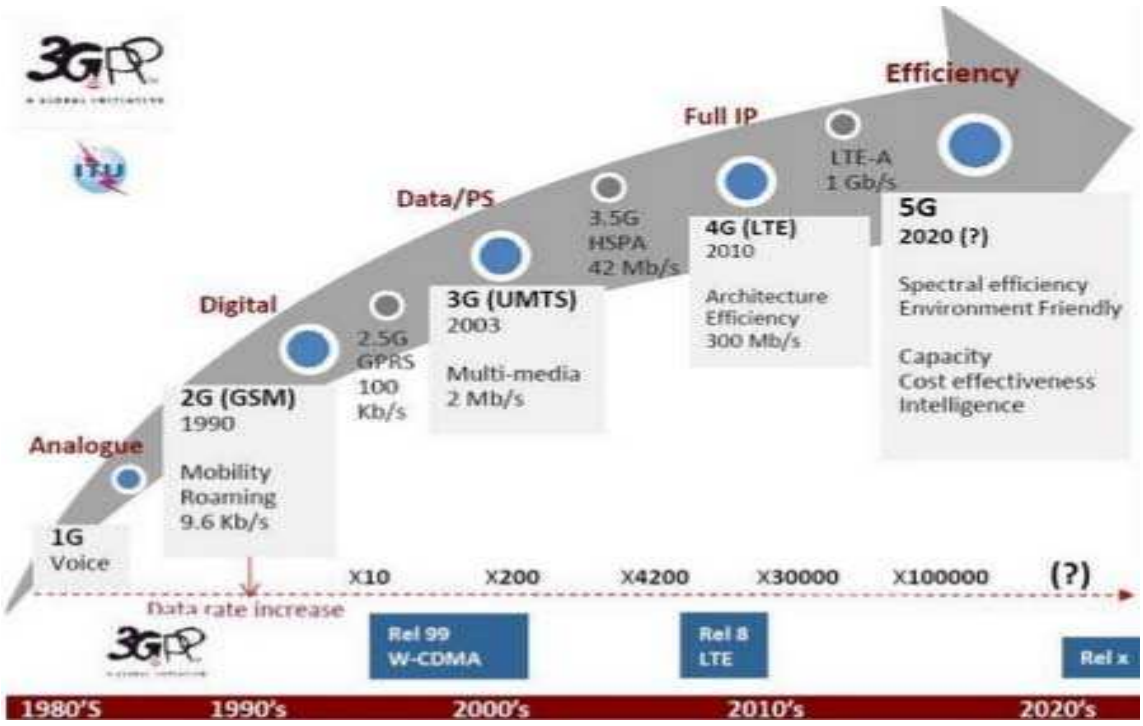


Figura 2. 6 Evolución de las comunicaciones inalámbricas.
Fuente: (Pedro Pavia, Alexandre Lopes, & Cristovao, 2017)

2.2 Estándares de las comunicaciones inalámbricas

Los estándares para las comunicaciones inalámbricas son el conjunto de reglas, condiciones o requerimientos que atañen a las definiciones de los términos. Existen dos tipos de estándares en la actualidad. Esta por un lado el estándar abierto, el cual está disponible al público, mientras el cerrado no lo está. Estos estándares obedecen a las exigencias emitidas por el fabricante o vendedor. El estándar abierto optimiza los recursos para poder mejorar comunicaciones entre hardware y software, aunque esto no necesariamente exime de cualquier tipo de pago de rubro. Entre las entidades de estandarización internacionales como son la UIT, ISO y la IEEE, tienen como propósito la regularización de estos estándares, así como las regalías del caso por posesión de patentes. Como podemos ver en la tabla 2.1, los diferentes estándares aparte que son de carácter internacional, estos también promueven de modo eficiente la competencia entre fabricantes para que los productos sean mucho más efectivos y baratos. (Escudero Pascual, 2016)

Tabla 2. 1 Normas para comunicaciones inalámbricas.

Norma	Bandas de frecuencia	Velocidad Máxima [Mbits/s]	Alcance [m]	Potencia [mW]
IEEE 802.15.4 Zigbee	868 – 870 MHz (Europa) 902 – 928 MHz (USA) 2,400 – 2,4835 GHz (Todos)	20 Kbit/s 40 Kbit/s 250 Kbit/s	10 a 75	1 min. 100 tip.
IEEE 802.11a WI-FI	5,15 – 5,35 GHz (Europa, USA) 5,47 – 5,725 GHz (Europa) 5,725 – 5,850 GHz (USA)	54	20	800
IEEE 802.11b WI-FI	2,4000 – 2,4835 GHz	11	30	100
IEEE 802.11g WI-FI	2,4000 – 2,485 GHz	54	30	200
IEEE 802.11n WI-FI	2,4000 – 2,485 GHz 5,15 – 5,35 GHz	108	50	100
IEEE 802.15.1 BLUETOOTH	2,4000 – 2,4835 Ghz	2,1	50	100
IEEE 802.16 WIMAX	5.x GHz	75	50 km	150
GPS	1575,43 MHz	50 bits/s		100

GSM/CDMA	900 MHz y 1800 MHz (Europa) 850 MHz y 1900 MHz (USA)	9,6 kbits/s		8W

Fuente: (Pallás Areny & Casas Piedrafita, 2014)

El estándar IEEE 802.11 fue creado específicamente para la regularización y control de sistemas inalámbricos. Estos estándares para redes LAN inalámbricas poseen varias enmiendas que necesitan ser respetadas. Entre los temas más importantes de las enmiendas que puede haber tenemos lo que respecta a la modulación, frecuencia, calidad. Es importante mencionar que este estándar del IEEE cubre las dos primeras capas del modelo regular OSI (Open System Interconnection). (Escudero Pascual, 2016)

2.2.1 IEEE 802.11a

Dentro de la normativa que embarca el estándar IEEE 802.11a podemos mencionar que se crees esta enmienda que contempla en funcionamiento en la banda de los 5GHz, es decir una técnica que permite transmisiones de 54 Mbits por segundo. Además, esto contempla 12 canales sin solapamiento, cuyas 8 conexiones son para uso interior y las otras cuatro para en laces en el exterior. (Escudero Pascual, 2016)

2.2.2 IEEE 802.11b

Dentro de la normativa IEEE 801.11 la enmienda b se concentra en las mejores continuas que el sistema deba. Las posibles tasas de transmisión pueden llevar de 5,5 a 11 Mbits por segundo, usando el método señalado anteriormente y la misma técnica. (Escudero Pascual, 2016)

2.3 Red de sensores

Las redes de sensores inalámbricos son un grupo de dispositivos o sensores especializados que se utilizan para monitorear diferentes condiciones ambientales y para recopilar y organizar esos datos en cierta

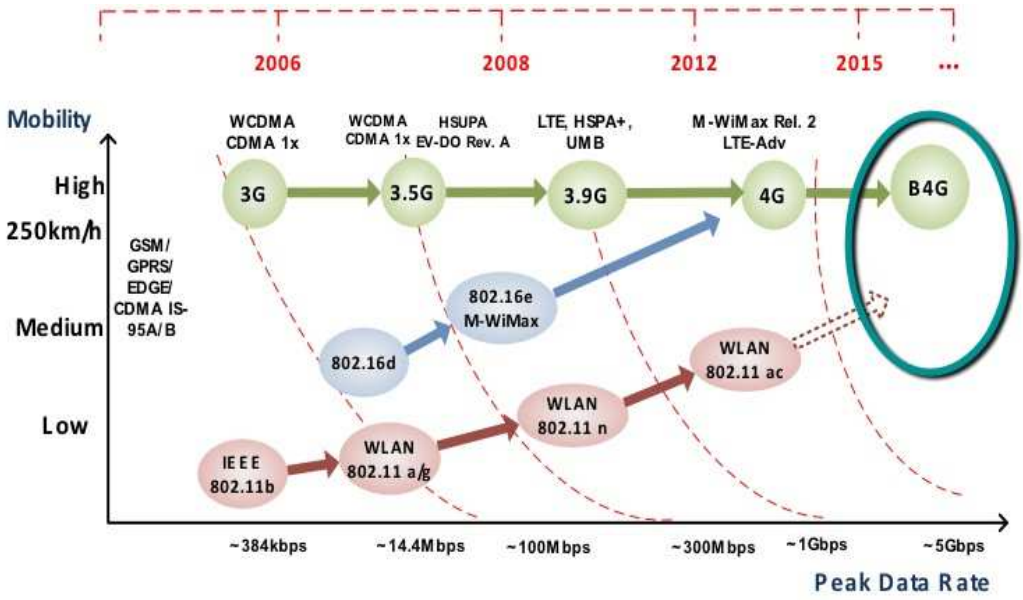


Figura 2. 7 Evolución de estándares de la IEEE junto con la evolución de las comunicaciones inalámbricas.
Fuente: (AisLab, 2016)

ubicación central. Detecta y mide una serie de condiciones físicas como humedad, temperatura, sonido, presión, velocidad y dirección, concentraciones químicas, vibraciones, niveles de contaminantes y muchas otras condiciones. La red de sensores establecida para este trabajo será un conjunto de dispositivos que sirve para poder adquirir datos necesarios para el sistema de control que se necesite desempeñar. Este tipo de dispositivos tienen la capacidad de no solamente estar conectados con un servidor que recopila los datos, pero también puede interactuar entre los dispositivos empleados para el sistema de control. Para esto debemos tener en cuenta la gran gama de dispositivos, marcas y disposiciones técnicas para poder armar el proyecto deseado. Como podemos ver en la figura 2.8, la arquitectura de una red de sensores es particularment sencilla, dependiendo de las aplicaciones y el alcance que se requiera tener en el proyecto, pero en su mayoría poseen características similares.

Como podemos ver en la figura 2.9, tenemos una red de wifi, que comprende desde interfaces de gestión de acceso con conexión entre los diferentes sensores que monitorean los diferentes puntos de acceso de la red.

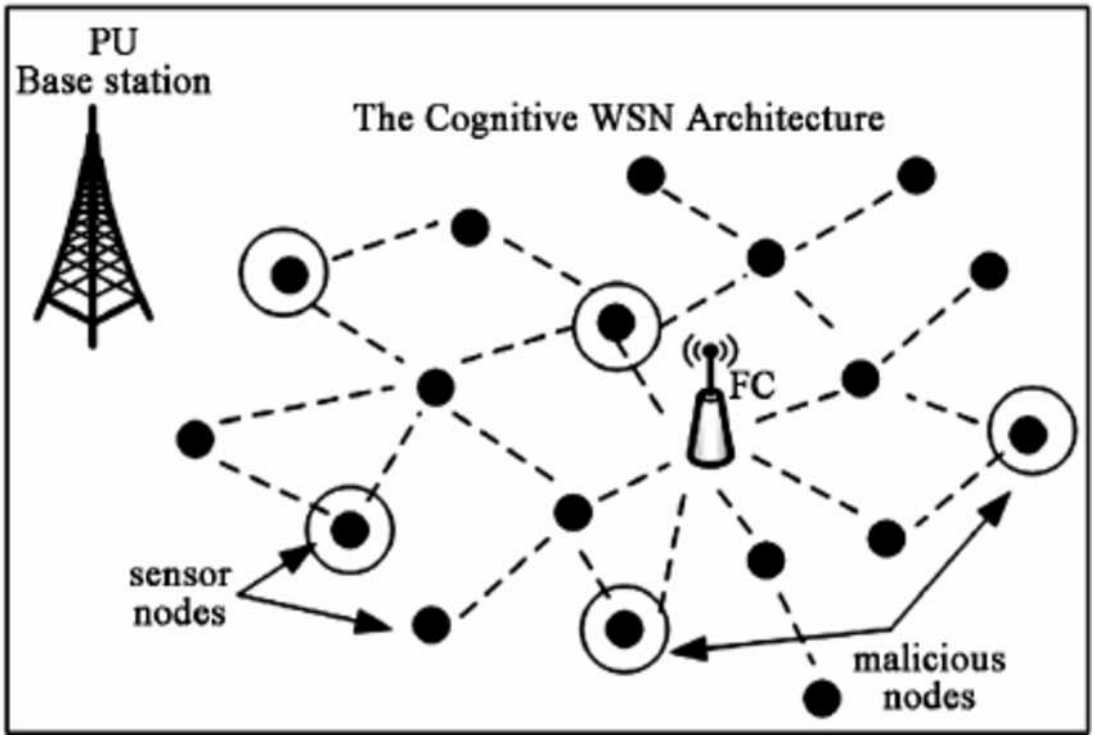


Figura 2. 8 Arquitectura cognitiva de una red de sensores.
Fuente: (Akbari & Falahati, 2011)

Tenemos también en el ejemplo dispositivos encargados de la gestión de variables fisiológicas las cuales se encarga de recibir cualquier tipo de actualización que corresponda a las variables del cliente que requiera una operación física. También se tiene como parte importante de este sistema un dispositivo de gestión de perfil de usuario encargado para administrar las jerarquías de gestión que se estipule para el control de datos adquiridos en el sistema. Además de estos dispositivos, también se tiene uno encargado de la gestión de comunicaciones que se trata de un controlador que permite el acceso del usuario desde cualquier plataforma configurada con el sistema. Por último, se tiene el gestor de información, el cual es el dispositivo encargado del acceso a la información recolectada, el cual será visible por el usuario. Todas estas disposiciones, son basadas en el alcance que se haya establecido dentro de los requerimientos de privasen de wifi. (Pedro Pavia, Alexandre Lopes, & Cristovao, 2017)

2.3.1 Red de sensores inalámbricos (WSN)

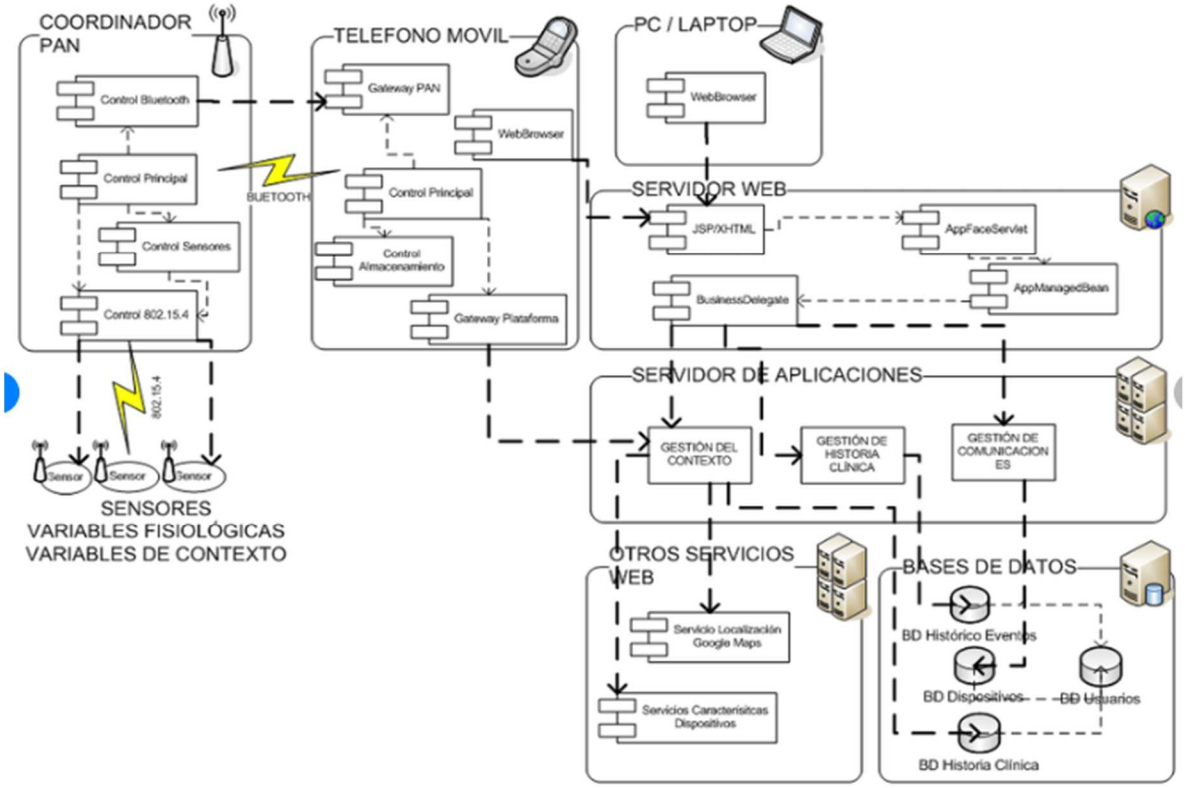


Figura 2. 9. Ejemplo de una red de sensores.
Fuente: (Solarte, Pena, & Almario, 2014)

Una red de sensores inalámbricos son un tipo de tecnología popular empleada en las telecomunicaciones de diferentes formas. Una de las arquitecturas más utilizadas es el modelo OSI. Este tipo de modelo básicamente responde a 7 capas las cuales son: aplicación, transporte, red, data, data enlace y físico. Es importante entender que las arquitecturas para este tipo de redes deben ser evaluadas dependiendo del tipo de aplicación que se requiera implementar. También es importante tener en cuenta que la red de sensores inalámbricos tiene como propósito no solamente la detección de intrusos, sino también crear una serie de procesos para poder contrarrestar el uso indebido de la red y proteger a usuarias y clientes de estos ataques. Para alcanzar una implementación de seguridad robusta es necesario también tener en cuenta los diferentes tipos de protocolos que existen dentro de una red de sensores. Como podemos ver en la figura 2.10,

el modelo OSI, es el conjunto de las 7 capas antes mencionadas con un diseño de manejo paralelo. Las capas que se pueden apreciar en esta figura corresponden al manejo de la red que se quiere administrar.

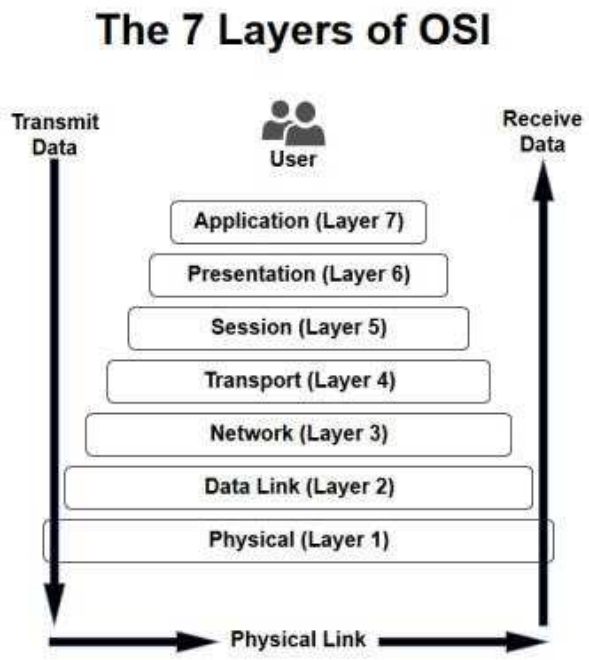


Figura 2. 10 Arquitectura modelo OSI.
Fuente: (Alhameed Alkhatib & Singh Baicher, 2012)

El manejo de las redes consta de tres capas, las cuales son: plano de gestión de energía, plano de gestión de movilidad y plano de gestión de tareas. Este tipo de capas son utilizadas para optimizar la eficiencia de la red en uso con respecto a los diferentes tipos de usuarios que este pueda administrar. (Alhameed Alkhatib & Singh Baicher, 2012)

Para poder entender un poco mejor las diferentes arquitecturas que existen con respecto a la ciberseguridad de servidores y clientes, primero debemos dar un breve concepto de cada una de las capas mencionadas en el modelo OSI, y el alcance de estos en diferentes sus diferentes fases. Como podemos ver en la tabla 2.2, los protocolos son los que van a direccionar de mejor manera la seguridad en la red consta de cinco capas que se menciona a continuación:

Tabla 2. 2 Diferencias en las arquitecturas de los modelos OSI, WLAN y WSN.

RED DE SENSORES INALÁMBRICOS (WSN)		**WLAN**	**MODELO OSI**
Aplicación WSN		Programa de aplicaciones	Capa de aplicación
WSN Middleware		Middleware	Capa de presentación
		Enchufe API	Capa de sesión
Protocolos de transporte WSN		TC{ / UDP	Capa de transporte
Protocolos de enrutamiento WSN		IP	Capa de red
Control de errores **Protocolos MAC WSN**		Adaptador WLAN y controlador de dispositivo	Capa de enlace de datos
Transceptor	Transceptor	Capa física	

Fuente: (Alhameed Alkhatib & Singh Baicher, 2012)

2.3.1.1 Capa de transporte (Transport Layer)

La función de esta capa es proporcionar confiabilidad y evitar la congestión donde muchos protocolos diseñados para proporcionar esta función se aplican tanto en sentido ascendente (de usuario a receptor, por ejemplo: ESRT, STCP y DSTN) como en sentido descendente (receptor a usuario, por ejemplo: PSFQ y GARUDA). Estos protocolos utilizan diferentes mecanismos para la detección de pérdidas ((ACK, NACK y número de secuencia)) y la recuperación de pérdidas ((End-to-End o Hop-by-Hop)). Esta capa es específicamente necesaria cuando un sistema está organizado para acceder a otras redes. Proporcionar un salto a salto confiable es más eficiente en términos de energía que extremo a extremo y esa es una de las razones por las que TCP no es adecuado para WSN. Por lo general, el enlace desde el receptor al nodo se considera como enlace descendente para la transmisión de multidifusión y el tráfico UDP debido a la memoria limitada y la evitación de gastos generales. Por otro lado, USER-TO-SINK se considera como enlace ascendente para la transmisión mono-cast y el tráfico TCP o UDP. Como podemos ver en la figura 2.11, se muestra un ejemplo de cómo actúa esta primera instancia de seguridad. Los datos que provienen de las capas superiores tienen direcciones de punto de servicio (puerto) j y k (j

es la dirección de la aplicación emisora, y es la dirección de la aplicación receptora). Dado que el tamaño de los datos es mayor que el que puede soportar la capa de red, los datos se dividen en dos paquetes, cada paquete conserva las direcciones del punto de servicio (j y k). Luego, en la capa de red, las direcciones de red (A y P) se agregan a cada paquete. Los paquetes pueden viajar por caminos diferentes y llegar al destino en orden o fuera de servicio. Los dos paquetes se entregan a la capa de transporte de destino, que se encarga de eliminar los encabezados de la capa de red y combinar los dos datos para enviarlos a las capas superiores. (Alhameed Alkhatib & Singh Baicher, 2012)

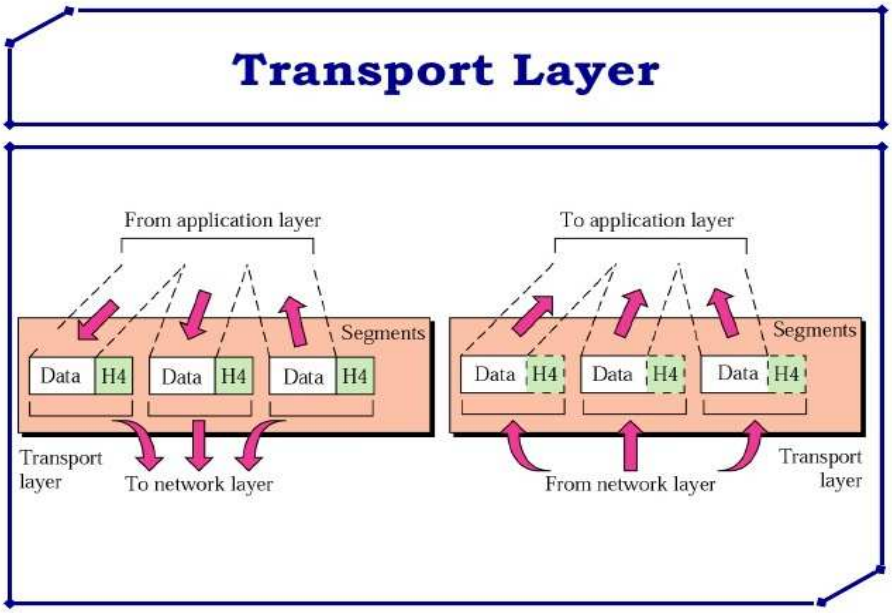


Figura 2. 11 Interacción de la capa de transporte con el resto de las capas o dominios de seguridad.
Fuente: (KULLABS, 2015)

2.3.1.2 Capa de red (Network Layer

La función principal de esta capa es el enrutamiento. Esta capa tiene muchos desafíos dependiendo de la aplicación, pero aparentemente, los principales desafíos radican en el ahorro de energía, la memoria limitada y los búferes, el sensor no tiene una ID global y debe organizarse por sí mismo. Esto es diferente a las redes de computadoras con dirección IP y dispositivo central para controlar.

La idea básica del protocolo de enrutamiento es definir una ruta confiable y rutas redundantes de acuerdo con una determinada escala llamada métrica, que difiere de un protocolo a otro. Hay muchos protocolos de enrutamiento disponibles para esta capa, se pueden dividir en; el enrutamiento plano (por ejemplo, difusión directa) y el enrutamiento jerárquico (por ejemplo, LEACH) o se puede dividir en tiempo impulsado, consulta impulsada y evento impulsado. En el protocolo de tiempo continuo, los datos se envían periódicamente y se controlan con el tiempo para aplicaciones que necesitan un monitoreo periódico. En los protocolos impulsados por consultas y por eventos, el sensor responde de acuerdo con la acción o la consulta del usuario. (Alhameed Alkhatib & Singh Baicher, 2012)

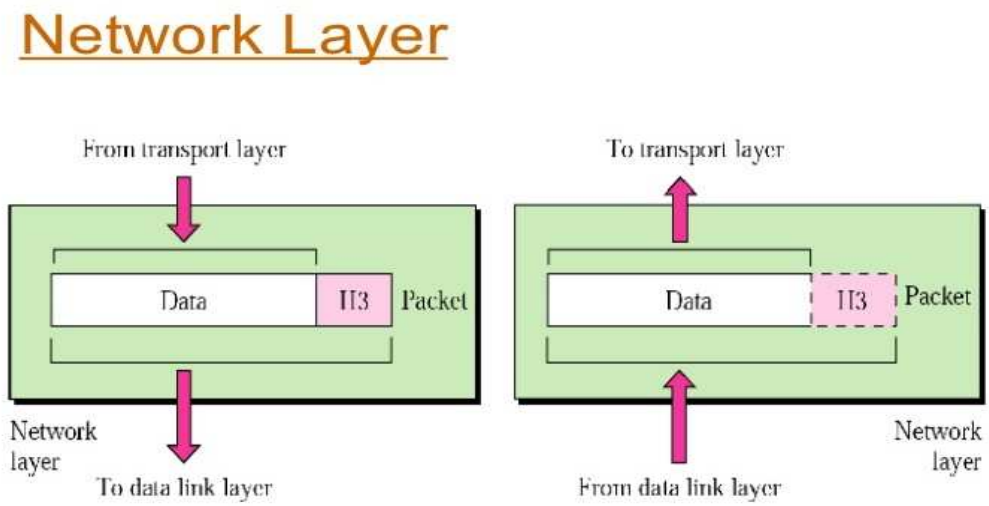


Figura 2. 12 Capa de red de acuerdo con el modelo OSI.
Fuente: (KULLABS, 2015)

Los controles de seguridad de la capa de red se han utilizado con frecuencia para proteger las comunicaciones, especialmente en redes compartidas como Internet, ya que pueden proporcionar protección para muchas aplicaciones a la vez sin modificarlas. Muchos protocolos de seguridad en tiempo real han evolucionado para la seguridad de la red asegurando principios básicos de seguridad tales como privacidad, autenticación de origen, integridad de mensajes y no repudio. La mayoría de

estos protocolos se mantuvo enfocado en las capas superiores de la pila de protocolos OSI, para compensar la inherente falta de seguridad en el protocolo de Internet estándar. Aunque valioso, estos métodos no se pueden generalizar fácilmente para su uso con cualquier aplicación. Por ejemplo, SSL está desarrollado específicamente para aplicaciones seguras como HTTP o FTP. Pero hay varias otras aplicaciones que también necesitan comunicaciones seguras. Esta necesidad dio lugar al desarrollo de una solución de seguridad en la capa IP para que todos los protocolos de capa superior pudieran aprovecharla. En 1992, el Grupo de Trabajo de Ingeniería de Internet (IETF) comenzó a definir un estándar conocido como IPSEC. (TutorialsPoint, 2017)

Tabla 2. 3 Protocolos de seguridad para la capa de red.

Layer	Communication Protocols	Security Protocols
Application Layer	HTTP FTP SMTP	PGP. S/MIME, HTTPS
Transport Layer	TCP /UDP	SSL, TLS, SSH
Network Layer	IP	IPsec

Fuente: (TutorialsPoint, 2017)

2.3.1.3 Capa de enlace de datos (Data Link Layer)

Responsable de la multiplexación de flujos de datos, detección de marcos de datos, MAC y control de errores, asegura la confiabilidad de punto-punto o punto-multipunto. Los errores o falta de fiabilidad provienen de Interferencia de canal en la capa MAC y este problema se resuelve mediante protocolos MAC.

El desvanecimiento y sombreado multi trayecto en la capa física y este problema se resuelve mediante la corrección de errores hacia adelante (FEC) y la solicitud de repetición automática (ARQ). ARQ no es popular en la red de sensores inalámbricas (WSN) debido a costos adicionales de retransmisión y gastos generales. ARQ no es eficiente para enmarcar la detección de errores, por lo que todo el cuadro debe retransmitirse si hay un solo error de bit. FEC disminuye el número de retransmisión al agregar datos

redundantes en cada mensaje para que el receptor pueda detectar y corregir los errores. Por eso podemos evitar la retransmisión y esperar el ACK. (Alhameed Alkhatib & Singh Baicher, 2012).

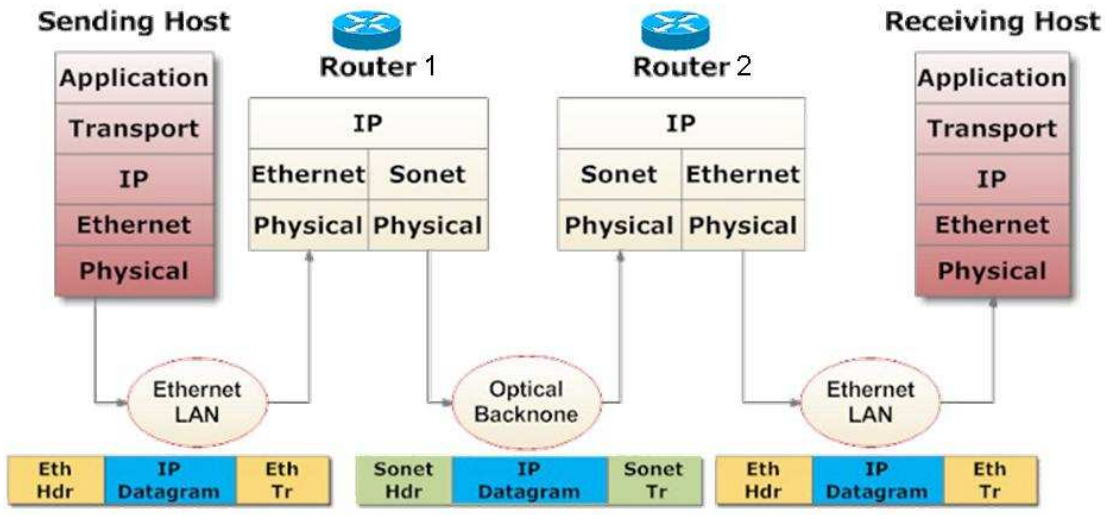


Figura 2. 13 Capa de enlace de datos y sus protocolos de seguridad.
Fuente: (Computer Networking Demystified, 2017)

La capa de enlace de datos se coloca justo encima de la capa física en todos los modelos de capas. Para que los datos viajen desde una computadora de origen a una computadora de destino remota, es posible que deba viajar a través de una variedad de enlaces de capa física cableada / inalámbrica en la ruta. Aunque la identificación de una ruta de extremo a extremo se realiza en la capa de red, los protocolos en la capa de red son independientes de los diferentes enlaces de telecomunicaciones subyacentes y, por lo tanto, no pueden interactuar directamente con los protocolos de capa física. Es aquí donde la capa de enlace de datos entra en escena. Como podemos ver en la figura 2.13, la capa de enlaces de datos actúa como una barrera protectora cuando entre en una interacción constante con diferentes enrutadores. (Computer Networking Demystified, 2017)

La ruta del datagrama IP desde la computadora de origen a la computadora de destino consiste en tres saltos, con el primer y tercer salto como enlaces de Ethernet y el salto intermedio como un enlace de SONET

Óptico. En consecuencia, puede ver que el encuadre varía en cada uno de estos saltos. Mientras que el datagrama IP se encapsula dentro de los encabezados y tráiler de trama específicos del protocolo de Ethernet en el primer y tercer salto, se encapsula dentro del encabezado de trama específico del protocolo SONET y el remolque en el segundo salto. Por lo tanto, a partir de este ejemplo, debe quedar claro que la estructura de trama y el protocolo de capa de enlace de datos varían en función del enlace físico subyacente. (Computer Networking Demystified, 2017)

En el contexto de la comunicación informática de extremo a extremo, la funcionalidad principal de la capa de enlace de datos es comprender los diferentes enlaces físicos en la ruta y trabajar de acuerdo con estos protocolos de enlace para transportar los datos en consecuencia. Más específicamente, la función de la capa de enlace de datos es facilitar la comunicación salto a salto a través de diferentes enlaces de capa física, llevando paquetes de datos (IP) dentro de unidades lógicas conocidas como marcos. (Computer Networking Demystified, 2017)

Cada cuadro contiene exactamente un datagrama de IP. El diagrama que se muestra a continuación ilustra el rol típico de una capa de enlace de datos, donde los paquetes se encapsulan dentro de los marcos de la capa de enlace de datos y se envían al siguiente salto a través de un enlace físico. (Computer Networking Demystified, 2017)

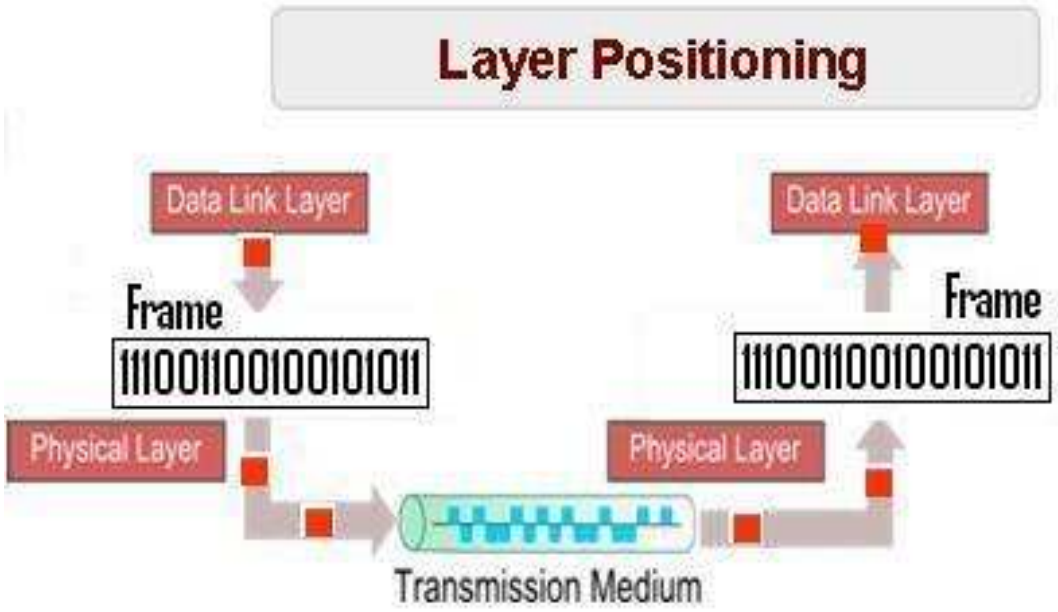


Figura 2. 14 Comportamiento de las capas de enlace de datos y la capa física.
Fuente: (Computer Networking Demystified, 2017)

2.3.1.4 Capa fisica (Physical Layer)

Puede proporcionar una interfaz para transmitir un flujo de bits en un medio físico. Responsable de la selección de frecuencia, generación de frecuencia portadora, detección de señal, modulación y encriptación de datos. IEEE 802.15.4 propone como estándar para área personal de baja velocidad y WSN con bajo costo, complejidad, consumo de energía, rango de comunicación para maximizar la duración de la batería. CSMA / CA usa topología de estrella de apoyo y peer-to-peer. Hay muchas versiones de IEEE 802.15.4 (Alhameed Alkhatib & Singh Baicher, 2012)

La capa física maneja reglas de bajo nivel para transmitir bits. Esta capa codifica o decodifica bits y envía o recibe la secuencia de datos. Este es el pavimento de la superautopista de la información. La capa física define:

- Propiedades electricas
- Medios de transmisión
- Dispositivos de transmisión

- Topología física
- Señalización de datos
- Sincronización de datos
- Ancho de banda de datos

Las propiedades eléctricas definen las reglas de cómo viaja el mensaje a través de los medios de transmisión, que luego crean rutas vinculadas o no vinculadas para la transmisión de bits. Una vez más, estos medios componen el hormigón de la superautopista de la información. Los dispositivos de transmisión proporcionan puntos medios y funcionalidad a los medios de transmisión. Son las herramientas de implementación en bruto.

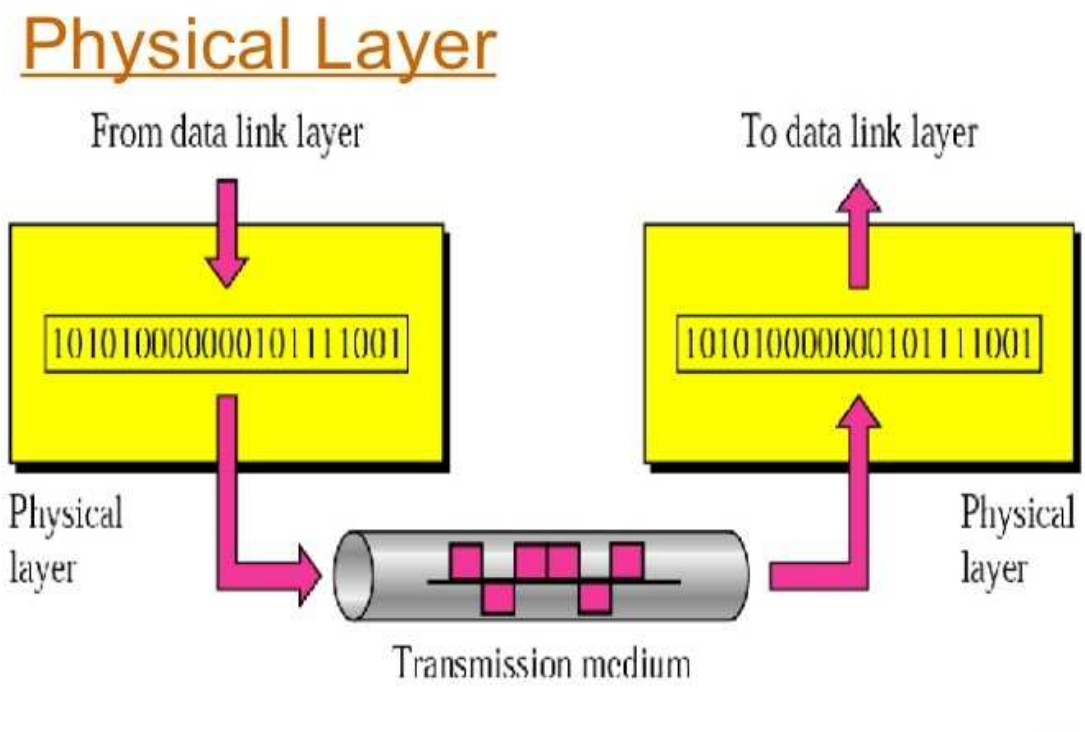


Figura 2. 15 Capa física de acuerdo con el Modelo OSI.
Fuente: (KULLABS, 2015)

2.3.1.5 Capa de aplicación (Application Layer)

Esta capa es responsable de la gestión del tráfico y proporcionar software para diferentes aplicaciones que traducen los datos de forma

comprensible o envían consultas para obtener cierta información. Las redes de sensores implementadas en diversas aplicaciones en diferentes campos, por ejemplo; campos militares, médicos, ambientales, agrícolas, etc. (Alhameed Alkhatib & Singh Baicher, 2012). La capa de aplicación se encuentra en la parte superior del modelo OSI. Es el objetivo final de la red, es decir, la prestación de servicios. La capa de aplicación hace la tarea de servicios como:

- Anuncio de servicio
- Servicio disponible

La capa de aplicación utiliza protocolos de red especiales para proporcionar servicios de archivos, impresión, mensajes, aplicaciones y bases de datos. La publicidad de servicio permite a otros sistemas y usuarios saber qué servicios están disponibles. Los proveedores usan técnicas activas o pasivas para definir el alcance de sus servicios de red. (KULLABS, 2015)

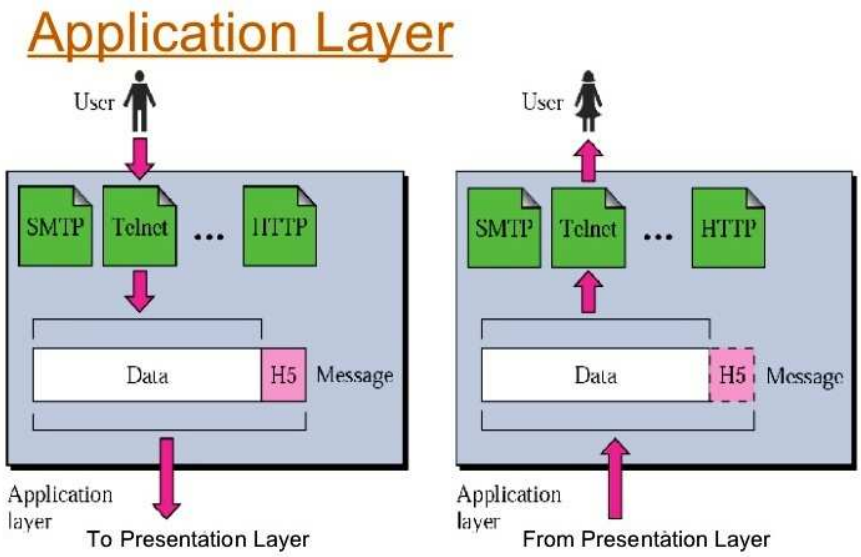


Figura 2. 16 Capa de aplicación según el modelo OSI.
Fuente: (KULLABS, 2015)

2.3.1.6 Capa de presentación

La meta principal de esta capa es de cuidar la sintaxis y la semántica de la información que se está intercambiando entre los dos sistemas de comunicación. La capa de presentación también tiene como propósito cuidar

la información que es enviada de tal manera que el receptor puede entender la información que va a estar disponible. Los lenguajes de programación implementados en los sistemas de configuración de seguridad en redes inalámbricas pueden ser diferente si la comunicación está establecida en más de dos sistemas. Si los sistemas provienen de dos fabricantes diferentes, y por consecuencia, posee dos lenguajes de programación diferentes, este tipo de capa se encargaría de poder establecer el puente necesario para la comunicación de estos sistemas. Bajo esta condición esta capa cumple el rol de traductor o interprete. Para que esta función sea posible los computadores con diferentes tipos de representación de información, las estructuras que van a formar parte del intercambio pueden ser definidos como abstractos. La capa de presentación maneja estas estructuras de información abstractas y permite la definición y el intercambio de estructuras mucho más complejas. Las funciones principales de esta capa, definidas bajo la estructura OSI son básicamente tres. La primera función es la de traducción. La traducción consiste en el cambio de información que existe justo antes de que la información sea transmitida entre equipos. La información que está presentada en forma de caracteres y números deben ser cambiadas a cadenas de bits. En esta operación la capa es responsable de la interoperabilidad entre codificar los métodos como diferentes tupos de métodos de codificación son empleados en computadoras. Traduce datos entre los formatos requeridos entre los equipos encargados de esta operación. La segunda función de esta capa es la de encriptación. En esta operación solamente se establece la fase de cifrado que sale de un equipo a la parte de descifrado cuando llega al equipo receptor. La tercera fase se la conoce como compresión. En esta fase y última función de la capa de presentación, los datos son comprimidos de tal forma que el ancho de banda no sufra un desgaste importante al transmitir estos datos entre los equipos. El rol principal de la compresión de datos es reducir el número de bits que van a ser transmitidos, y es importante por los diferentes tipos de datos que existen en el contexto multimedia. (Shekhar, 2016)

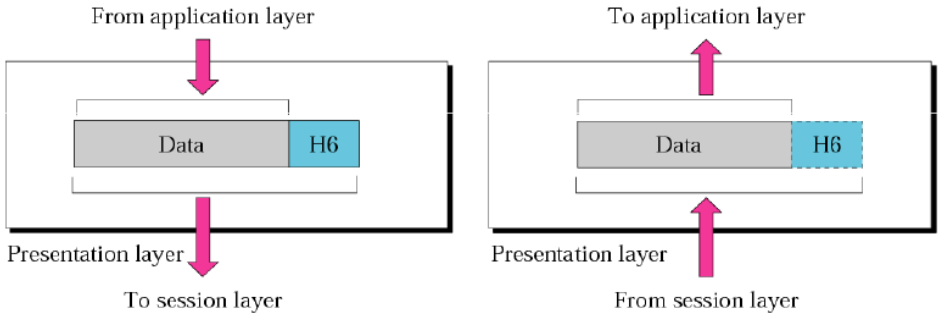


Figura 2. 17 Modelo OSI de la capa de presentación.
Fuente: (Shekhar, 2016)

2.3.1.7 Capa de sesión

La capa de sesión del modelo osi controla los diálogos (conexiones) entre computadoras. Establece, administra y termina las conexiones entre la aplicación local y remota. Proporciona operación dúplex completo, semidúplex o símplex, y establece procedimientos de punto de control, interrupción, terminación y reinicio. El modelo OSI hizo que esta capa fuera responsable del cierre de las sesiones, que es una propiedad del protocolo de control de transmisión, y también para el punto de control y la recuperación de la sesión, que generalmente no se usa en Internet Protocol Suite. La capa de sesión se implementa comúnmente de forma explícita en entornos de aplicaciones que usan llamadas a procedimientos remotos. (Shekhar, 2016)

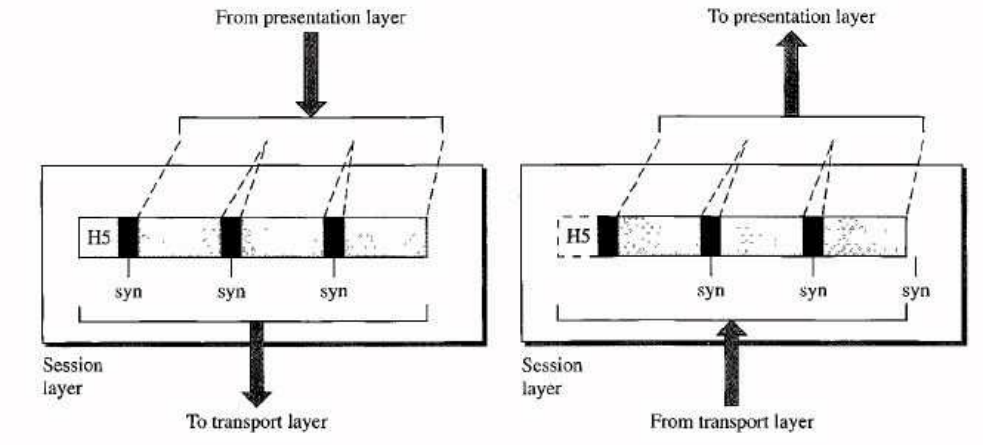


Figura 2. 18 Capa de sesión según el modelo OSI.
Fuente: (Shekhar, 2016)

2.3.2 Aplicaciones de red de sensores inalámbricos

Para poder establecer las diferentes aplicaciones dentro de la red de sensores inalámbricos, primero debemos saber cuáles son nuestras posibles amenazas y cómo podemos protegernos de una mejor manera. Como primera característica de la red de sensores inalámbricas o WSN y su aplicación, Defense in Depth es una de las estrategias que se utiliza bastante en el área de la tecnología de la información o IT. Uno de los principios básicos de esta estrategia es que los componentes que integran una red de sensores no deben confiar el uno al otro, queriendo decir que cada componente supone que otros componentes de una organización o grupo tecnológico se han visto comprometidos. No es práctico tener todos los componentes en un sistema grande que no confíe en nada. Como tal, se establecen capas que no confían entre sí. (Spacey, 2016)

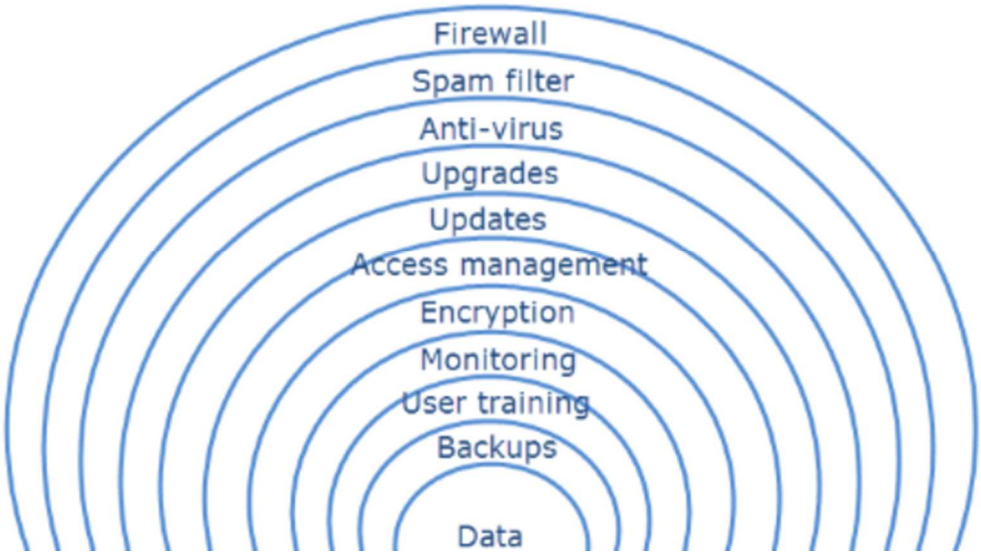


Figura 2. 19 Características de un sistema DID.
Fuente: (BigIdea Technology, 2017)

Como podemos ver en la figura 2.19, el uso de varias capas de controles de seguridad aumenta la seguridad general de su empresa, ya que, si un mecanismo falla, otros mecanismos pueden ofrecer protección contra el ataque. En el caso de que un programa o aplicación intrusa logre

superar sus capas de defensa y encripte sus archivos, tener una copia de seguridad recuperable es esencial para la recuperación del ataque. Si bien una copia de seguridad de datos por sí sola puede ser satisfactoria para su hogar, una copia de seguridad de los sistemas operativos, configuraciones y datos es esencial para empresa o domicilio que lo necesite. Una copia de seguridad basada en imágenes toma una instantánea de su sistema en puntos específicos en el tiempo. Esto le permite a su proveedor de internet o compañía que provee seguridad cibernética retroceder a una imagen de respaldo antes del incidente del intruso, lo que permite que sus sistemas se respalden en horas, en lugar de días. Su proveedor de internet o seguridad cibernética debe probar su copia de seguridad antes de un incidente para asegurarse de que la copia de seguridad sea recuperable. (BigIdea Technology, 2017)

En general, las aplicaciones de red de sensores pueden ser de gran ayuda con respecto a la seguridad y otras aplicaciones más. Como podemos ver en la figura 2.5, las diferentes aplicaciones dentro de la seguridad de redes pueden variar dependiendo de la industria donde se la aplica, y a partir de eso se crea diferentes tipos de aplicaciones extras tratan de ser versátil en su uso. A partir de esta noción, podemos decir que para la detección de intrusos dentro del área donde se piensa implementar una red de sensores, pueden variar de diferentes formas. Si se informa que un área ha sido afectada por algún tipo de calamidad, como un incendio forestal, y se sueltan los nodos de los sensores en el fuego desde un avión el control de los datos de cada nodo y la construcción de un mapa de temperatura para idear formas y técnicas adecuadas para superar el incendio es una forma de aplicación de red de sensores. (Microcontrollers Lab, 2015)

En una red de área local inalámbrica (WLAN), un punto de acceso inalámbrico (802.11 g) es un dispositivo que permite que dispositivos inalámbricos como una computadora portátil, tableta, móvil, etc. se conecten a una red cableada usando Wi-Fi, Bluetooth o estándar relacionado. El punto de acceso es una columna vertebral de una red inalámbrica para proporcionar diferentes servicios en el entorno inalámbrico. El punto de

acceso es muy popular debido a características como proporciona movilidad; es escalable, rentable y fácil de instalar. La falta de conocimiento sobre la red inalámbrica segura causa una serie de amenazas a la seguridad. Rogue o Malicious AP es una de las amenazas de seguridad en una red inalámbrica. También muestra que, del total de puntos de acceso disponibles en la red, casi el 20% de los puntos de acceso son maliciosos. Las aplicaciones para poder contrarrestar este tipo de eventos, es una de las aplicaciones más importantes de un sistema de redes inalámbricas, aunque también se considera otros tipos de aplicaciones. (Microcontrollers Lab, 2015)

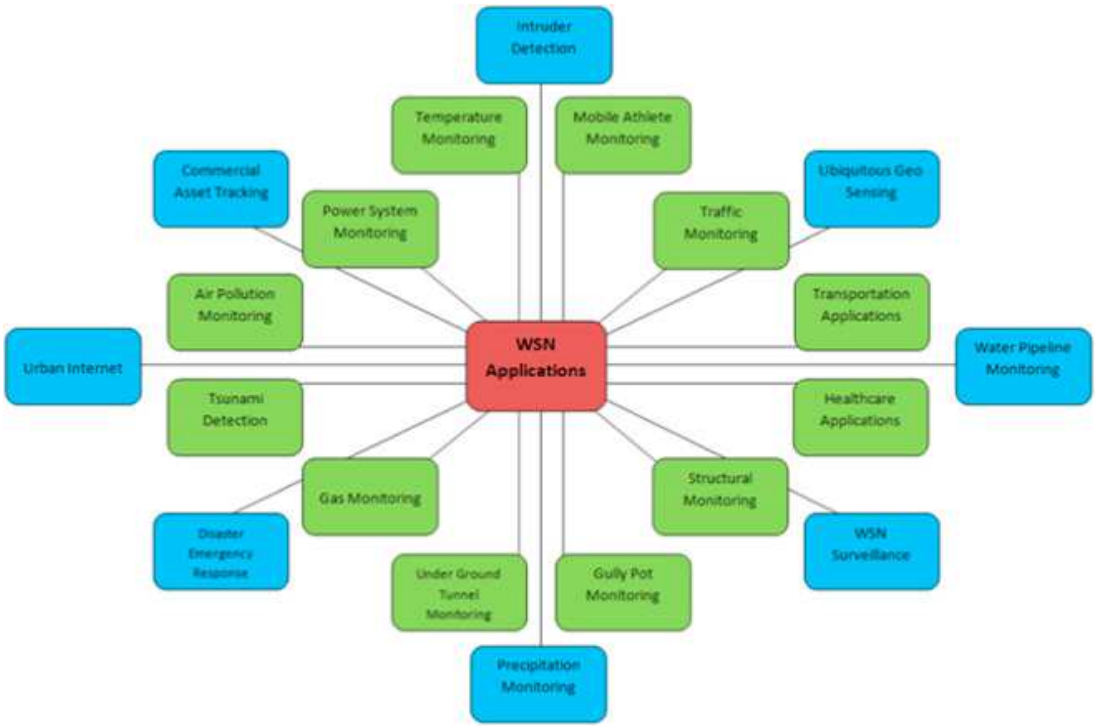


Figura 2. 20 Aplicaciones varias de una red de sensores.
Fuente: (Rashid & Husain, 2016)

Otro ejemplo de los WSN y su aplicación puede ser el uso de estos dispositivos y su capacidad de desplegarse rápidamente y auto organizarse, por lo tanto, son muy útiles en operaciones militares para detectar y monitorear movimientos amistosos y hostiles. La vigilancia en el campo de batalla se puede hacer a través de los nodos de los sensores para controlar todo en caso de que se necesiten más equipos, fuerzas o municiones en el campo de batalla. Los ataques químicos, nucleares y biológicos también se

pueden detectar a través de los nodos del sensor. Estas redes de sensores tienen una gran cantidad de aplicaciones en el medio ambiente. Se pueden usar para rastrear el movimiento de animales y aves y registrarlos. El monitoreo de la tierra, el suelo, el contexto atmosférico, el riego y la agricultura de precisión se puede hacer a través de estos sensores. También se pueden usar para la detección de incendios, inundaciones, terremotos y brotes químicos / biológicos, etc. En aplicaciones de salud, la monitorización integrada de un paciente se puede realizar utilizando WSN. Los procesos y movimientos internos de los animales pueden ser monitoreados. El diagnóstico se puede hacer. También ayudan a controlar la administración de medicamentos en los hospitales y a controlar tanto a los pacientes como a los médicos. (Microcontrollers Lab, 2015)

En lo que respecta a la seguridad cibernética, una red de sensores puede ser aplicada para que pueda asistir de forma correcta a los puntos de acceso de internet inalámbrico. Esto debe estar acompañado no solamente de un tipo de software que pueda estar establecido en manera de capas en la red local de un establecimiento, pero también puede ser de gran ayuda los usos de equipos para que la detección sea mucho más rápida Como se va en la tabla 2.4 existen varios tipos de ataques que perjudican a la red y equipos que estén conectados a esta red. Existen equipos ayudan a detectar a aplicaciones fraudulentas cuyos propósitos pueden variar desde obtener información relevante y personal de los usuarios, hasta suplantación de identidades para poder tener acceso a bienes, y con este trabajo se pretender tener un conocimiento mucho más generalizado para que haya una adecuada identificación de los ataques. (Kaschel, Mardones, & Quezada, 2013)

Tabla 2. 4 Ataques cibernéticos y sus características.

Ataques	**Características**
DoS (Denial of Service)	Producido por la acción no intencional de los nodos o la acción de un atacante
Ataques a la información en tránsito	Alteran, falsifican y repiten la información en tránsito a la fuente. Toman el control de un nodo y son capaces de fabricar nuevos paquetes falsificados. Su alcance

	puede estar sobre varios nodos de sensor al mismo tiempo
Ataque de Sybil	Un atacante toma las mismas características de otro nodo para involucrarse en la red. Este ataque intenta degradar la integridad de los datos, la seguridad y el uso de los recursos a los que se puede acceder mediante el sensor robado. Ataca el almacenamiento distribuido, los mecanismos de enrutamiento y la agregación de datos. Cuando se ataca, la red puede luchar con protocolos fuertes.
Agujero de fondo / hundimiento	Un nodo actúa como un agujero negro para atraer a todo el grupo de nodos de sensor. Cuando el nodo malicioso intercepta los nodos de comunicación, puede hacer cualquier cosa con ellos
Ataques de inundación con Hello	El atacante usa paquetes de saludos para atraer y convencer a los nodos. Los nodos están convencidos de que el atacante es su vecino. Una vez que los nodos envían el paquete al receptor, deben pasar por el atacante, interceptando los paquetes y haciendo lo que quieren que haga.
Ataque de agujero de gusano	En este ataque crítico, el atacante guarda los paquetes en una dirección de red y los túneles en otro. Es una amenaza importante, porque puede ocurrir al principio, cuando los nodos del sensor solo están averiguando sobre los sensores vecinos

Fuente: (Kaschel, Mardones, & Quezada, 2013)

Ante los posibles ataques que pueden existir en una red de wifi, también existen varios tipos de tácticas y métodos para poder combatir estos ataques. Como podemos ver en la tabla 2.5, existe ya componentes y protocolos que ayudan a combatir cualquier tipo de amenaza contra una red o equipo.

Tabla 2. 5 Lista de diferentes ataques y métodos de seguridad para WSN.

Método de seguridad	**Ataque**	**Arquitectura de red**	**Característica**
JAM	Ataque DoS	Redes de sensores inalámbricos tradicionales.	Utiliza nodos vecinos vinculados para evitar que se evite la región atascada.
Agujero de gusano	Ataque DoS	Red de sensores híbridos	Utiliza agujero de gusanos para evitar atascos.
Pre-distribución	Ataque Sybil	Gran cantidad de	Utiliza recursos de

de clave aleatoria prueba de recursos de radio, etc.		sensores Red de sensores inalámbricos altamente densos	radio, pre-distribución de clave aleatoria, procedimiento de registro, verificación de posición y pruebas de código para detectar la entidad Sybil.
Verificación bidireccional, enrutamiento de estaciones de múltiples bases, multirrutas	Ataque inundación HELLO	Redes de sensores inalámbricos tradicionales.	Adopta un compartimiento secreto, probabilístico y compartido. También utiliza la verificación bidireccional y el enrutamiento y multirrutamiento de estaciones base múltiples.
Basado en comunicaciones de seguridad	Información o spoofing de datos.	Redes de sensores inalámbricos tradicionales.	Uso eficiente de los recursos. Protege la red incluso si parte de la red está en peligro.
TIK	Ataque de agujero de gusano, información o falsificación de datos.	Redes de sensores inalámbricos tradicionales.	Basado en criptografía simétrica, requiere sincronización entre todas las partes que se comunican, implementa correas temporales.
Pre-distribución de llave	Datos e información suplantando. Ataque a la información en tránsito	Redes de sensores inalámbricos tradicionales.	Proporciona resistencia en la red, protege la red, incluso si parte de la red está comprometida, proporciona medidas de autenticación para los nodos del sensor.
ESCHENAUER &	Información o	Red de sensores	Permitido para una

GLIGOR	spoofing de datos.	distribuidos, gran escala de red de sensores inalámbricos con una naturaleza dinámica.	gran cantidad de sensores inalámbricos que hacen posible agregar y elimina
REWARD	Ataques agujero negro	Redes de sensores inalámbricos tradicionales.	Utiliza enrutamiento geográfico, aprovecha el hecho de ser el remitente para ver la transmisión del vecino y detectar ataques de agujero negro.
TINYSEC	Información o spoofing de datos.	Redes de sensores inalámbricos tradicionales.	Centrado en proporcionar mensajes autenticidad, integridad y mensajes de confidencialidad: funciona en la capa de enlace.
SNEP y TESLA	Datos e información falsos, los mensajes repiten los ataques	Redes de sensores inalámbricos tradicionales.	Protección de repetición, seguridad semántica, autenticación de datos, baja sobrecarga de comunicación

Fuente: (Kaschel, Mardones, & Quezada, 2013)

2.4 Métodos de seguridad para redes wifi

Los algoritmos de seguridad Wifi han pasado por muchos cambios y mejoras desde la década de 1990 para volverse más seguros y efectivos. Se desarrollaron diferentes tipos de protocolos de seguridad inalámbricos para la protección de redes inalámbricas domésticas. Los protocolos de seguridad inalámbricos son WEP, WPA y WPA2, que cumplen el mismo propósito, pero son diferentes al mismo tiempo. Los protocolos no solo impiden que las partes no deseadas se conecten a su red inalámbrica, sino que también los protocolos de seguridad inalámbricos cifran sus datos privados enviados a

través de las ondas. No importa cuán protegidas y encriptadas, las redes inalámbricas no puedan mantenerse al día con seguridad en las redes cableadas. Estos últimos, en su nivel más básico, transmiten datos entre dos puntos, A y B, conectados por un cable de red. Para enviar datos de A hacia B, las redes inalámbricas lo transmiten dentro de su rango en todas las direcciones a cada dispositivo conectado que esté escuchando. Entre los métodos más utilizados se mencionará algunos de los cuales se los considera comercial y otros que son más adecuados para usos gubernamentales y empresarial. Para muchas de estos protocoles, su creación ha pasado por bastantes fases de aprobación por entidades competentes como lo es la IEEE, pero estos también han desarrollado un mayor rango de desarrollo en las telecomunicaciones como parte organizadora y fiscalizadora de mejora continua de estos procesos. (Pastor, 2017)

2.4.1 WEP (WIRED EQUIVALENT PRIVACY)

WEP fue desarrollado para redes inalámbricas y aprobado como un estándar de seguridad Wi-Fi en septiembre de 1999. WEP tenía como objetivo ofrecer el mismo nivel de seguridad que las redes cableadas, sin embargo, hay un montón de problemas de seguridad conocidos en WEP, que también es fácil de comprender y configurar. A pesar de todo el trabajo que se ha hecho para mejorar el sistema WEP, sigue siendo una solución altamente vulnerable. Los sistemas que dependen de este protocolo deberían actualizarse o reemplazarse en caso de que no sea posible la actualización de seguridad. WEP fue oficialmente abandonado por la Wi-Fi Alliance en 2004. (Pastor, 2017)

2.4.2 WPA (WI-FI PROTECTED ACCESS)

En el momento en que el estándar de seguridad inalámbrica 802.11i estaba en desarrollo, se utilizó WPA como una mejora de seguridad temporal para WEP. Un año antes de que WEP fuera oficialmente abandonado, WPA fue formalmente adoptado. La mayoría de las

aplicaciones WPA modernas utilizan una clave previamente compartida (PSK), más comúnmente conocida como WPA Personal, y el Protocolo de integridad de clave temporal o TKIP para el cifrado. WPA Enterprise utiliza un servidor de autenticación para la generación de claves y certificados. WPA fue una mejora significativa con respecto a WEP, pero como los componentes principales se crearon para que pudieran implementarse a través de actualizaciones de firmware en dispositivos habilitados para WEP, aún confiaban en elementos explotados. WPA, al igual que WEP, después de someterse a una prueba de concepto y las demostraciones públicas aplicadas resultaron ser bastante vulnerables a la intrusión. Sin embargo, los ataques que representaron la mayor amenaza para el protocolo no fueron los directos, sino los que se realizaron en Wi-Fi Protected Setup (WPS): sistema auxiliar desarrollado para simplificar la conexión de dispositivos a puntos de acceso modernos. (Pastor, 2017)

2.4.3 WPA2 (WI-FI PROTECTED ACCESS VERSION 2)

El protocolo basado en el estándar de seguridad inalámbrica 802.11i se introdujo en 2004. La mejora más importante de WPA2 sobre WPA fue el uso del Estándar de cifrado avanzado (AES) para el cifrado. AES está aprobado por el gobierno de EE. UU. Para cifrar la información clasificada como de alto secreto, por lo que debe ser lo suficientemente buena como para proteger las redes domésticas. En este momento, la principal vulnerabilidad para un sistema WPA2 es cuando el atacante ya tiene acceso a una red Wifi segura y puede obtener acceso a ciertas claves para realizar un ataque a otros dispositivos en la red. Dicho esto, las sugerencias de seguridad para las vulnerabilidades conocidas de WPA2 son en su mayoría significativas para las redes de niveles empresariales, y no son realmente relevantes para redes domésticas pequeñas. Desafortunadamente, la posibilidad de ataques a través de Wi-Fi Protected Setup (WPS) sigue siendo alta en los puntos de acceso actuales compatibles con WPA2, que también es el problema con WPA. Y aunque entrar en una red segura WPA / WPA2 a través de este agujero tardará entre 2 y 14 horas, sigue siendo un problema de seguridad real y WPS debería deshabilitarse y sería bueno si el

firmware del punto de acceso se pudiera restablecer a una distribución no es compatible con WPS para excluir por completo este vector de ataque. (Pastor, 2017)

2.4.4 TKIP (TEMPORAL KEY INTEGRITY PROTOCOL)

Es un protocolo de cifrado incluido como parte del estándar IEEE 802.11i para LAN inalámbricas (WLAN). Fue diseñado para proporcionar un cifrado más seguro que el conocido Wired Equivalent Privacy (WEP), el protocolo de seguridad WLAN original. TKIP es el método de encriptación utilizado en Wi-Fi Protected Access (WPA), que reemplazó a WEP en productos WLAN. TKIP es un "envoltorio" que gira alrededor del cifrado WEP existente. TKIP comprende el mismo motor de cifrado y el algoritmo RC4 definido para WEP. Sin embargo, la clave utilizada para el cifrado en TKIP es de 128 bits de longitud. Esto resuelve el primer problema de WEP: una longitud de clave demasiado corta. (Navas, 2016)

2.4.5 AES

Es un cifrado de bloques simétrico elegido por el gobierno de EE. UU. para proteger la información clasificada y se implementa en software y hardware en todo el mundo para cifrar datos confidenciales. (Kak, 2018)

2.4.6 CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) es un protocolo de cifrado que forma parte del estándar 802.11i para redes inalámbricas de área local (WLAN), especialmente las que utilizan la tecnología WiMax. El algoritmo CCMP se basa en el Estándar de Encriptación Avanzada (AES) del gobierno federal de EE. UU. (Kak, 2018)

2.5 Rogue AP

Un Rogue Access Point (AP deshonesto) es cualquier punto de acceso inalámbrico que se haya instalado en la infraestructura cableada de una red sin el consentimiento del administrador o propietario de la red, proporcionando acceso inalámbrico no autorizado a la infraestructura cableada de la red. La mayoría de las veces, los Rogue AP son configurados por empleados que desean acceso inalámbrico cuando ninguno está disponible. Otro ejemplo, quizás más común, de un punto de acceso deshonesto o Rogue AP es lo que a veces se conoce como un "gemelo malvado". Esto, en ningún momento, implica conexiones Ethernet no autorizadas como en el ejemplo anterior. Más bien, esto implica un dispositivo inalámbrico que se encuentra justo afuera de una organización que recibe balizas transmitidas por puntos de acceso legítimos dentro de la organización. El gemelo malvado luego comienza a transmitir balizas idénticas con la intención de que los usuarios finales de la organización se conecten con él. Una vez conectado, el gemelo malvado puede ser utilizado por personas nefastas como una avenida en la red de la organización. Un requisito fundamental del sistema de prevención de intrusiones inalámbricas (WIPS) es que debe ofrecer una protección sólida contra los puntos de acceso inalámbrico deshonestos. La protección debe incluir detección instantánea seguida de bloqueo automático (prevención). La detección Rogue AP debe estar libre de falsas alarmas, tanto en los lados positivos como negativos. (Juniper Networks, 2016)

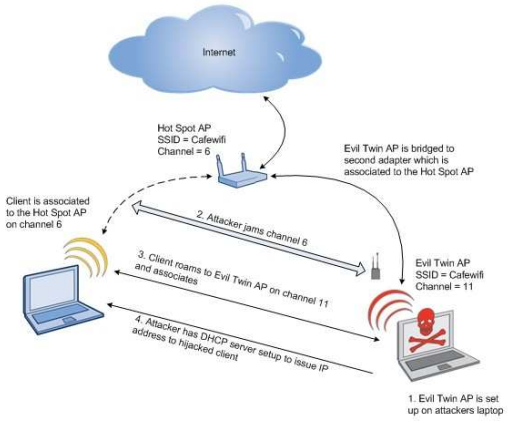


Figura 2. 21 Funcionamiento de un Rogue Access Point.
Fuente: (Simek, 2012)

Los puntos de acceso deshonestos o Rogue AP, y sus clientes socavan la seguridad de una red empresarial al permitir potencialmente el acceso no cuestionado a la red por parte de cualquier usuario o cliente inalámbrico en las cercanías físicas. Los puntos de acceso no autorizados también pueden interferir con el funcionamiento de su red empresarial. Los puntos de acceso no autorizados pueden hacer el siguiente daño:

- Permita que un pirata informático realice un ataque de hombre en el medio. El atacante establece conexiones independientes con las víctimas y transmite mensajes entre ellas, haciéndoles creer que están hablando directamente entre sí a través de una conexión privada, cuando en realidad toda la conversación está controlada por el atacante.
- Inunde la red con datos inútiles, creando una denegación de servicio.
- Envíe SSID falsos que anuncien características atractivas, como conectividad gratuita a Internet. Una vez que un usuario se conecta, el SSID falso se agrega a la configuración inalámbrica del cliente y el cliente comienza a transmitir el falso SSID, infectando así a otros clientes.
- Proporcione un conducto para el robo de información de la compañía.

2.5.1 Tipos de Rogue AP

Los tipos de Rogue AP, pueden clasificarse de muchas maneras. Como podemos ver en la tabla 2.6, el Rogue AP, puede tener diferentes acciones dentro de una red wifi, pero se los clasifica de acuerdo con lo que se llegue a ejecutar dentro del sistema.

Tabla 2. 6 Clasificación de los ROGUE AP.

Rogue AP	Descripción
Miembro	El punto de acceso está en este dominio de movilidad. La huella digital del punto de acceso (también conocida como firma) se usa para identificar de manera segura los puntos de acceso de los miembros.
Vecino	El dispositivo de confianza (buen vecino) figura en la lista de

	SSID de terceros permitidos. Generalmente, este punto de acceso es parte de una red inalámbrica vecina o dominio de movilidad.
Sospechoso	No hay suficiente información para clasificar este punto de acceso como vecino o pícaro. Puede decidir agregarlo a la lista deshonesta, la lista SSID o la lista de vecinos.
Rogue	Dispositivo ROGUE en el aire. Por ejemplo, punto de acceso no autorizado en una red empresarial.

Fuente: (Juniper Networks, 2016)

Cualquier AP que no sea AP autorizado es de tipo Rogue AP. La conectividad de red de AP a la red empresarial no es un criterio para la detección fraudulenta. El administrador tendrá que separar minuciosamente manualmente los AP vecino. La inspección manual debe realizarse de forma continua a medida que aparecen nuevos AP dentro del rango donde se pretenda realizar el control y se reconfiguran los antiguos. Si la inspección manual no se realiza de manera rápida y regular, este crea un agujero de seguridad. La prevención automática de AP maliciosos no se puede activar ya que el administrador tendrá que decidir primero si un AP recientemente detectado está en la red o solo un AP de donde se está realizando el control.

Las reglas de clasificación son incorporadas o seleccionadas a partir de un conjunto de reglas predefinidas. Las reglas incorporadas son constantes y no se pueden cambiar. Las reglas de usuario son las reglas que le permiten configurar ciertos comportamientos de clasificación. Se tiene en cuenta que la primera regla de clasificación elimina los puntos de acceso en la lista de Rogue AP y no se puede modificar. Dos reglas configurables predeterminadas para la clasificación deshonesta y puede establecer un tercero para clasificar la condición predeterminada como deshonesto, como podemos ver en la figura 2.7. (Juniper Networks, 2016)

La conectividad de AP a la red empresarial monitoreada todavía no es un criterio para la detección de un Rogue AP, pero es posible filtrar los AP vecinos gracias a las propiedades inalámbricas reconfiguradas de AP como red, SSID, OUI del proveedor MAC y RSSI. Esta lógica solo parece mejor que la primera.

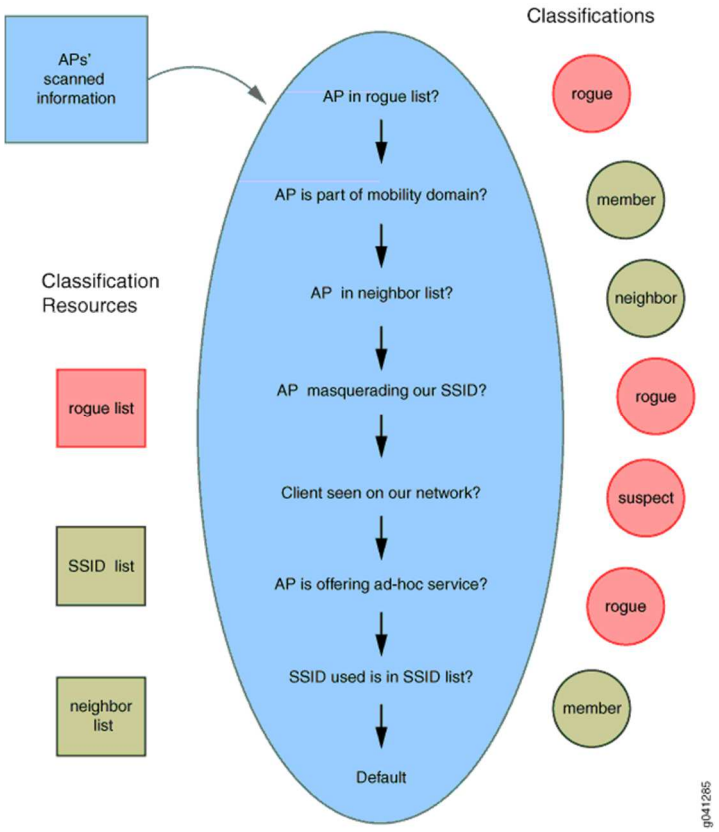


Figura 2. 22 Tipos de Rogue AP.
Fuente: (Juniper Networks, 2016)

De hecho, sin embargo, solo da una falsa sensación de sofisticación por diferentes razones. No hay nada que requiera que las propiedades solo inalámbricas sean diferentes entre el AP pícaro alámbrico y el AP vecino amistoso. Uno podría traer fácilmente AP cuyo SSID y proveedor coinciden con uno de sus AP vecinos, ponerlo en baja potencia de transmisión para que parezca distante y conectarlo a la red de su empresa. Esta situación puede ocurrir incluso en casos no maliciosos, si el empleado ingresa un AP básico de baja potencia con SSID predeterminado. El sistema lo clasificará incorrectamente como un vecino amigable, ya que su SSID y proveedor coinciden con su plantilla pre configurada para el vecino amigable y su RSSI es lo suficientemente bajo. Si los AP vecino legítimos cambian su configuración de lado inalámbrico o si se implementan nuevos AP vecinos amigos, no se ajustarán a la plantilla pre configurada para vecinos amigables. Por lo tanto, activar la prevención automática es un riesgo y se requerirá una inspección manual frecuente. (Juniper Networks, 2016)

La conectividad de AP a la red empresarial monitoreada es un criterio esencial en la clasificación de AP como los mandatos de definición de amenaza Rogue AP; por supuesto, además de eso, el AP no está en la lista AP autorizada. La conectividad de red por cable de todos los puntos de acceso visibles en el aire es determinada de forma instantánea, automática y precisa por el sistema. Si no está en la lista de AP autorizados y está conectado a la red supervisada, es un punto de acceso no autorizado. Si no está en la lista AP autorizada y no está conectado a la red empresarial supervisada, es AP externo o vecino. La prevención automática se puede activar de forma segura y no hay una interrupción de seguridad. No se requiere ningún esfuerzo manual al principio para configurar las plantillas de propiedades de AP del vecindario o en forma permanente a medida que surgen nuevos AP y los antiguos cambian sus propiedades. (Juniper Networks, 2016)

2.5.2 CISCO AIRONET 3600

Como podemos ver en la figura 3.4, CISCO AIRONET 3600 es un dispositivo que puede proveer internet a todos los dispositivos en el rango de los 802.11n y 802.11ª/g, incluyendo hasta 3 clientes espaciales. Estos puntos de acceso también pueden escanear los 26 canales en el espectro de Wi-Fi a través del CleanAir de Cisco. La serie 3600 está diseñada para permitir a los usuarios conectarse a la red sin problemas desde cualquier dispositivo inalámbrico, incluso aquellos con una señal inalámbrica débil, como tabletas, con un rendimiento más rápido que cualquier otro punto de acceso. (CISCO, 2014)

Figura 2. 23 CISCO Aironet.
Fuente: (CISCO, 2014)

2.5.3 Módulo WSSI

El módulo actualizable en campo de WSSI es una radio dedicada que descarga todos los servicios de monitoreo y seguridad de las radios de servicio del cliente / datos al módulo del monitor de seguridad. Esto permite un mejor rendimiento y además reduce los costos al eliminar la necesidad de puntos de acceso del modo de monitor dedicado y la infraestructura Ethernet requerida para conectar esos dispositivos a su red. Juntos, los puntos de acceso de la serie 3600 y el módulo WSSI permiten funciones avanzadas de análisis de espectro y seguridad para clientes Wi-Fi en todos los canales, tanto en la banda de 2,4 como en la de 5 GHz. (CISCO, 2014)

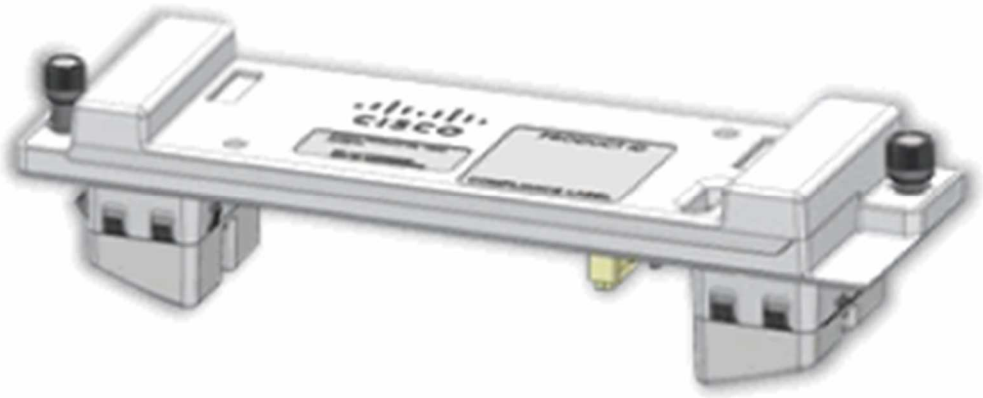


Figura 2. 24 Módulo WSSI.
Fuente: (CISCO, 2014)

CAPÍTULO 3: DISEÑO DE LA RED DE SENSORES

3.1 Colegio Mixto Fiscal Patria Ecuatoriana

El Colegio Fiscal Patria Ecuatoriana se encuentra ubicada en el cantón de Guayaquil, en la provincia del Guayas, en la intersección de las calles 40 y avenida Portete. Entre algunos datos interesantes del establecimiento donde se está haciendo el estudio para la construcción de una red de sensores para detección de ROGUE AP, podemos decir que esta institución fue creada por un grupo de estudiantes de la Universidad Católica de Santiago de la carrera de psicología, de Guayaquil el 22 de noviembre de1971, por sus reconocidos fundadores Lcda. Mérida López Vera y Lcdo. César Noboa Bohórquez. (Wikimapia, 2013)

Figura 3. 1 Colegio Fiscal Mixto Patria Ecuatoriana - Zona Administrativa.
Fuente: Autor

La zona administrativa consta de dos plantas en las cuales se va a distribuir el servidor de internet, los puntos de acceso fijo y los puntos de acceso inalámbrico. De esta manera podemos tener una mejor perspectiva de como colocar los equipos y como calcular la zona de distribución de

internet. La parte de oficinas administrativas de la planta alta consta de la parte de rectorado y sala de reuniones. La planta baja consta de oficinas cuyo rol es netamente administrativo. Como dato extra la distribución de la parte administrativa donde se quiere contemplar CISCO Aironet 3600, será en la parte superior del establecimiento, el cual se encuentra distribuido como se puede ver en la figura 3.2.

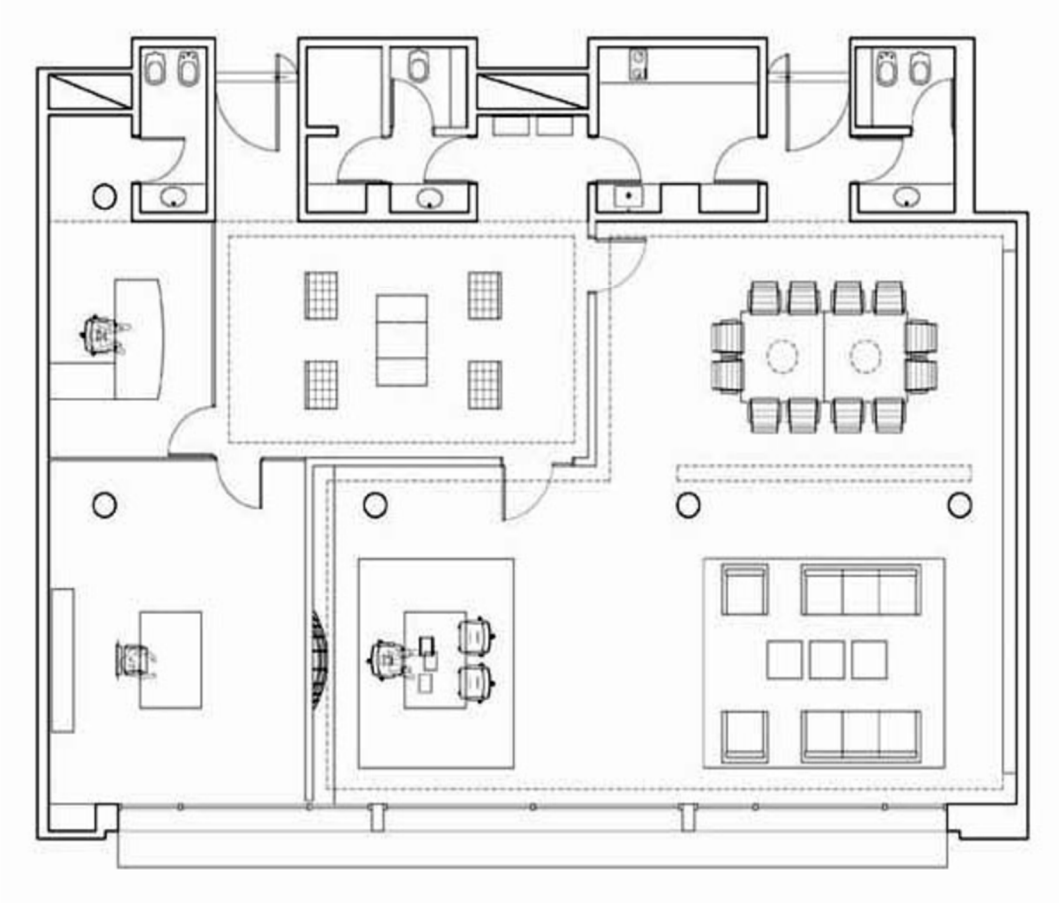


Figura 3. 2 Planta alta de las oficinas administrativas del Colegio Patria Ecuatoriana.
Fuente: Autor

3.2 Instalación del equipo

El equipo estará colocado en la entrada principal de la planta alta del establecimiento, donde se requiere más la implementación de esta tecnología. Debemos recordar que el equipo que se utilizará en este trabajo tiene especificaciones técnicas específicas para poder configurarlos junto con los módulos WSSI. La detección no autorizada le permite al

administrador de red monitorear y eliminar este problema de seguridad. Cisco Unified Network Architecture proporciona métodos de detección fraudulenta que permiten una solución completa de identificación y contención sin la necesidad de herramientas y redes superpuestas costosas y difíciles de justificar. A continuación, se presenta los procesos respectivos para la detección y ejecución de una secuencia para evitar Rogue AP.

3.2.1 Asignación de un IP estático

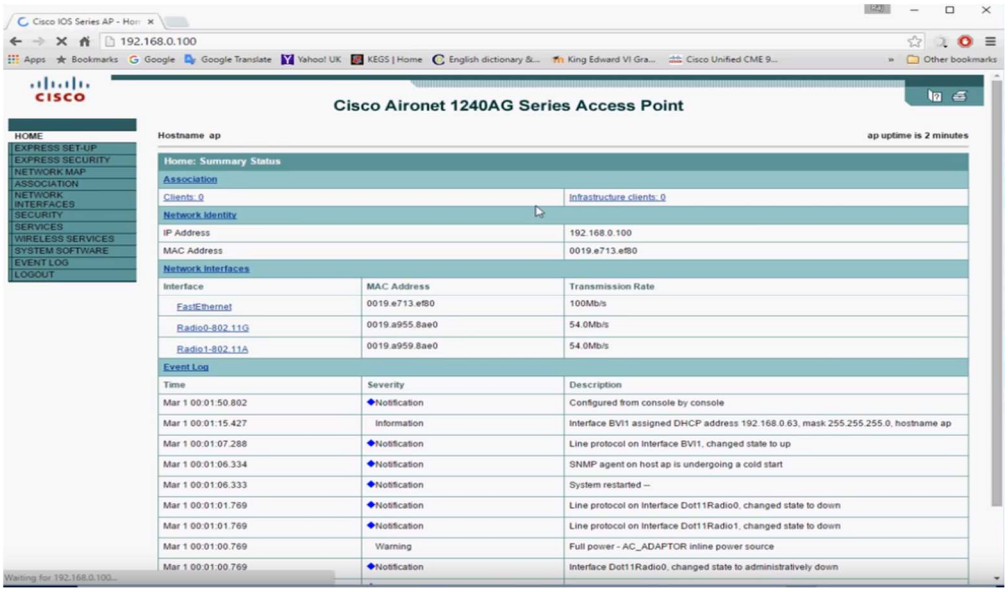


Figura 3. 3 Asignación de un IP estático.

Fuente: Autor

Uno de los primeros pasos para comenzar con la configuración de la red, es asignar un IP estático donde se va a encontrar nuestra red y nuestro sistema de control contra Rogue AP. Esto lo conseguimos entrando a la interface de los dispositivos CISCO. Podemos ingresar a esta interfaz ingresando el IP local de nuestro servidor en un navegador de internet. Una vez ingresado nuestro IP en el navegador una ventana como la que vemos en la figura 3.3, y en la cual procedemos a ingresar los datos correspondientes en la pestaña de EXPRESS SETUP. Dentro de esta pestaña tenemos que configurar el HOST NAME, el cual es la opción que tenemos para definir nuestro punto de acceso, el cual para este proyecto lo llamaremos AP1 (Access Point 1).

Una vez ingresado el HOST NAME procedemos a dar clic en STATIC IP dentro de la opción de CONFIGURATION SERVER PROTOCOL, o protocolo de configuración dinámica de HOST. En la opción de puerta de enlace predeterminada o DEFAULT GATEWAY procedemos a escribir nuestro IP para poder lograr el enlace correspondiente de nuestra computadora con el acceso fijo a internet y que controlará de manera directa el tráfico de datos en la red. Como podemos ver en la figura 3.4, además de la configuración mencionada nosotros también debemos dar nombre a nuestro anillo de seguridad que va con el nombre de SNMP Community.

Esta opción es como una identificación de usuario o contraseña que permite el acceso a las estadísticas de un enrutador u otro dispositivo. De este modo, estableceremos una mejor manera la localización de Rogue AP en nuestra red. IPCheck Server Monitor envía la cadena de la comunidad junto con todas las solicitudes de SNMP. Si la cadena de la comunidad es correcta, el dispositivo responde con la información solicitada. Si la cadena de la comunidad es incorrecta, el dispositivo simplemente descarta la solicitud y no responde.

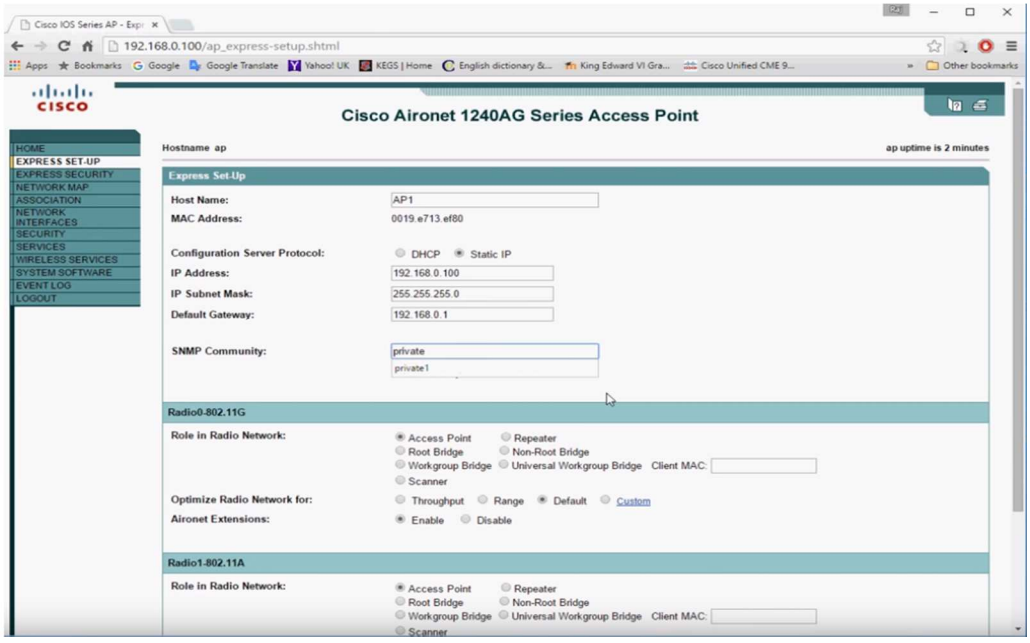


Figura 3. 4 Configuración de la puerta de enlace.

Fuente: Autor

3.2.2 Crear un nombre para el SSID del WLAN1

Una vez realizado estos cambios, damos clic en el botón APPLY para que se guarden los cambios, y pasamos al siguiente paso el cual es el de definir el SSID (Service Set Identifier), el cual es un identificador de paquetes de servicios e identifica a cualquier red dentro del rango de los equipos. Este tipo de identificador consta de 32 caracteres ASCII (American Standard Code for Information Interchange), y la cual lo más común es de realizar una combinación de estos caracteres entre números y letras. En la opción de EXPRESS SECURITY, como podemos ver en la figura 3.5, nos muestra una interfaz en la que nos permita configurar nuestra red que estará a disposición de todos los que se encuentran conectados. Para este proyecto se llamará a la red WLAN1, y será la única opción que vayamos a usar en este paso dentro de la opción de esta interfaz. Bajo la segunda opción dentro de este esquema tenemos la configuración del VLAN o Red de Área Local Virtual, el cual nos permite crear un grupo de equipos para mejorar la seguridad de ellos. En este caso, nosotros daríamos clic en NO VLAN para que de este modo podamos trabajar con la capa de seguridad que nos proporciona CISCO Aironet.

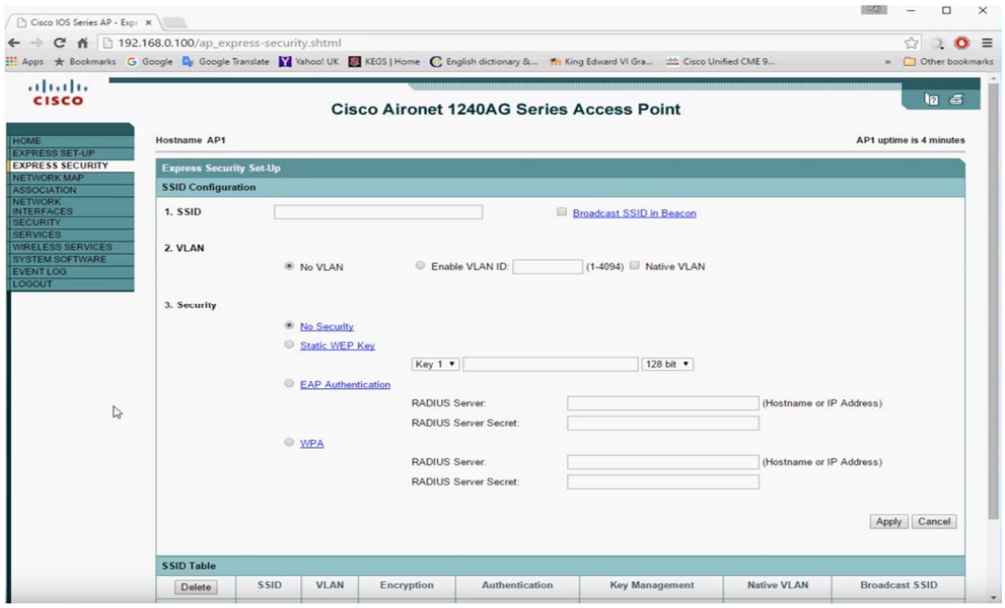


Figura 3. 5 Configuración del SSID.

Fuente: Autor

3.2.3 Difundir el SSID

Una vez aplicado los cambios en la opción de EXPRESS SECURITY, procedemos a dar clic en APPLY para poder configurar el siguiente paso de nuestra red de seguridad. Este siguiente paso como lo podemos ver en la figura 3.6, nosotros debemos ir a la pestaña de NETWORK INTERFACES y una vez establecido en esta opción, se nos abrirá una interfaz donde se nos dará la opción de configurar de RADIO 802.11g. Esta opción nos sirve no solamente para configurar la velocidad de banda de nuestra red. Como este está configurado para trabajar en un rango de frecuencia de 2.4 GHz, este es compatible con cualquier dispositivo de la familia de los 802.11b codificados en OFDM (Orthogonal Frequency-Division Multiple Access), o acceso múltiple por división d frecuencia octogonales.

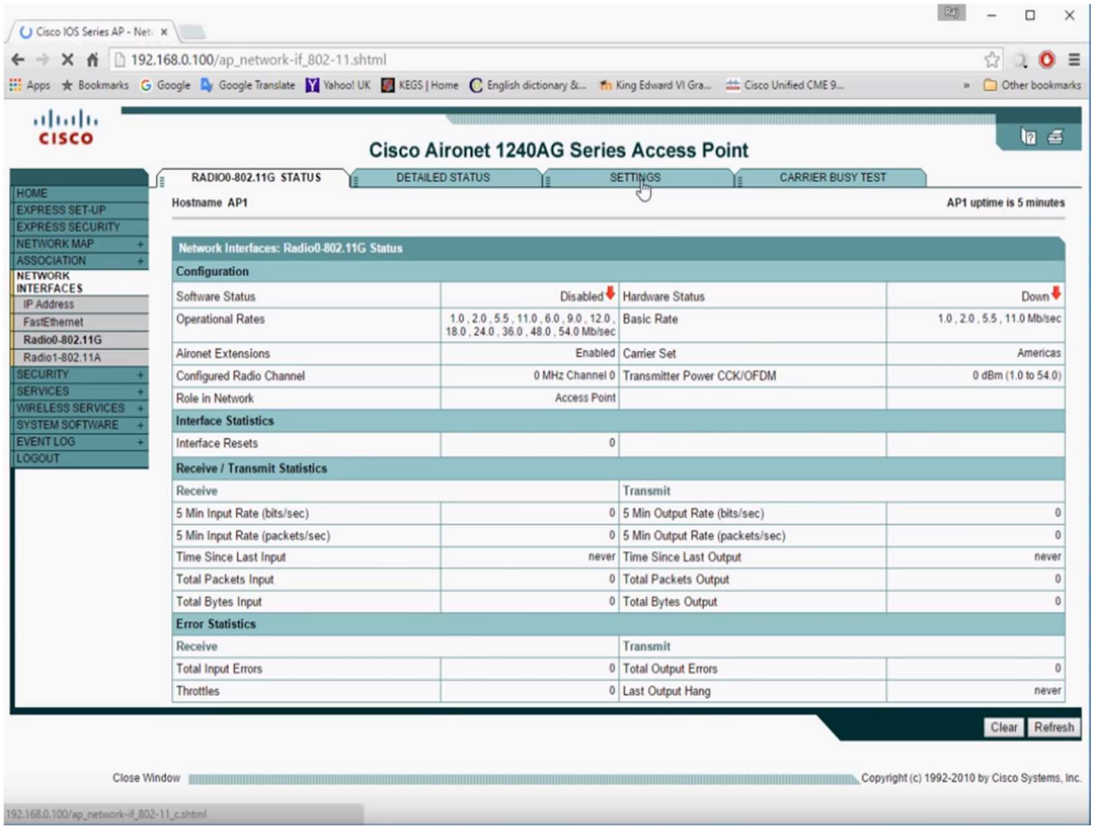


Figura 3. 6 Configuración del interfaz de red.

Fuente: Autor

Dentro de la opción de SETTINGS, nosotros verificamos que la opción de ENABLE RADIO esté activa, dando clic en la opción de ENABLE y una vez que damos click en APPLY, nosotros inmediatamente podemos verificar

que nuestra red pueda ser verificada dentro del rango de los equipos que estén en la zona administrativa del colegio. Como podemos ver en la figura 3.7, esta interfaz nos permite ver la habilitación de nuestra RADIO 802.11g, además de tener otras opciones para poder mejorar nuestra seguridad en la red. Una vez que terminamos con este paso, podemos verificar en nuestra red que nuestro punto de acceso WLAN1 se encuentre disponible. Esta es una de las ideas principales de seguridad que se puede ofrecer en el área administrativa, aunque aún así se puede tener ROGUE AP, y para este necesitaríamos otro tipo de seguridad mucho más complejo.

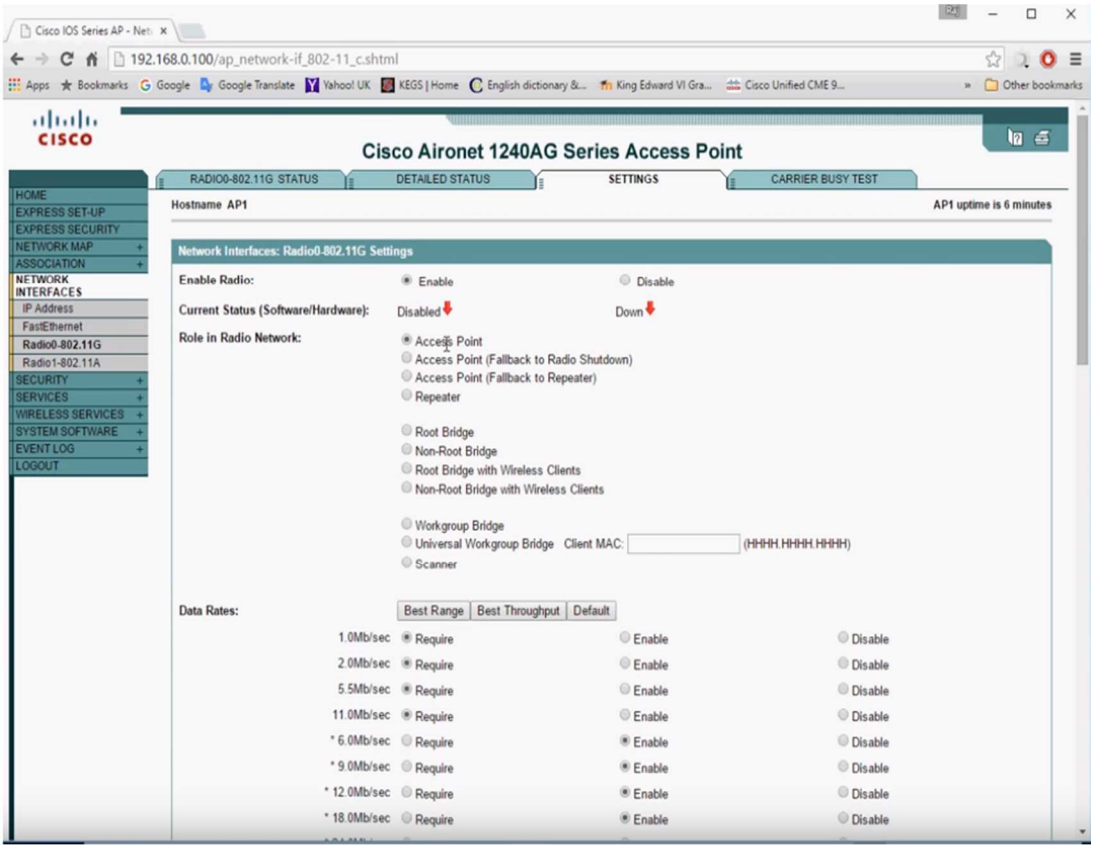


Figura 3. 7 Configuración del 802.11g.

Fuente: Autor

Como método de comprobación de que nuestra red está segura podemos dirigirnos a nuestra red en el explorador de redes wifi de nuestra computadora, dar clic derecho y verificar si efectivamente nuestra red está configurada apropiadamente como lo pudimos hacer en la interfaz de CISCO. Como podemos ver en la figura 3.8, nuestra red WLAN1 está activa y disponible para la conexión de cualquiera de los equipos y dispositivos móviles que se encuentren dentro del rango. Las autenticaciones

proporcionan una unidifusión de manera dinámica para cualquier dispositivo, pero es importante mencionar que las claves estáticas juego un rol importante. Si se da una rotación de claves WEP o multidifusión se puede configurar la red con la activación de un MIC. Esta opción permite que el cliente se proteja de ataques a paquetes cifrados o ataques de volcado de bits. Ese ataque lo que hace es interceptar un mensaje cifrado, y una vez obtenida la información este es retransmitido como legítimo. Si se activa un MIC lo que se obtendrá es un aumento de bytes a cada paquete para que este no se pueda modificar y entrar en peligro el cliente.

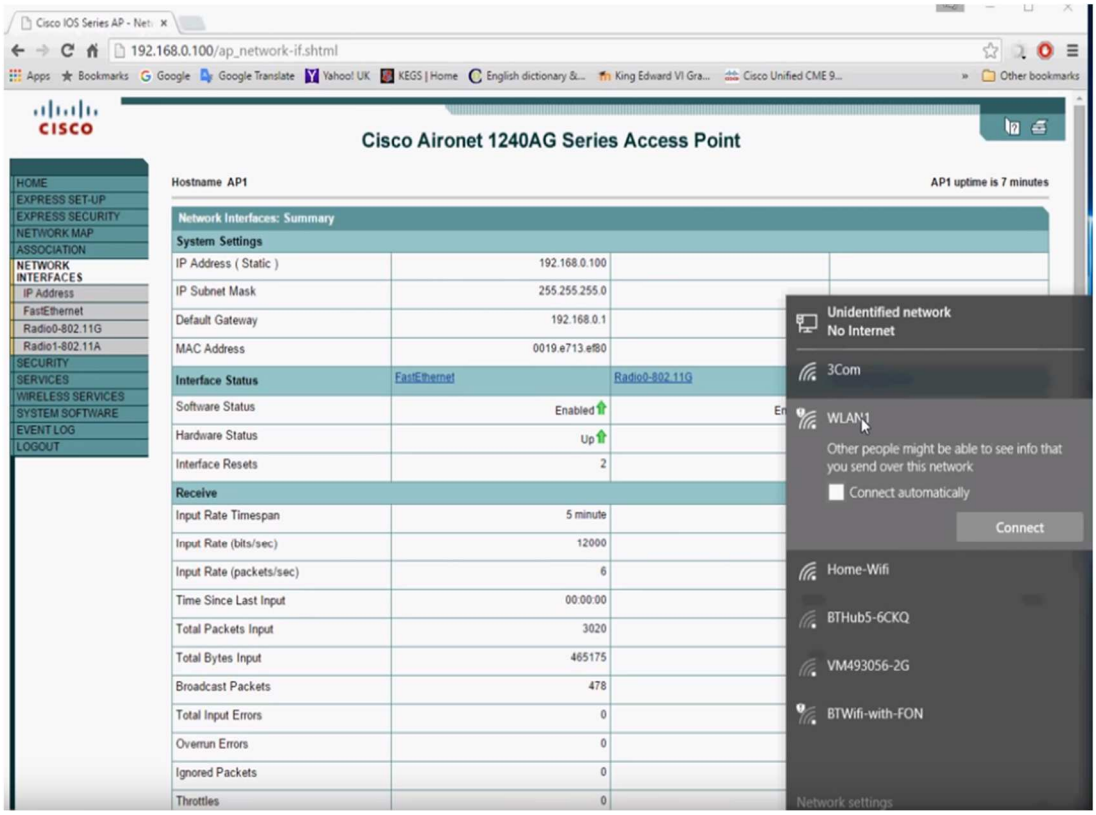


Figura 3. 8 Comprobación de seguridad de red.

Fuente: Autor

Una vez que configuramos la red, comprobamos que nuestro protocolo y nuestro SSID sean los que se habían definidos desde un principio, como podemos ver en la figura 3.9, y además este tipo de información de ser vulnerada ante la falsificación de identidad, se debe considerar un último paso dentro de nuestra configuración para proteger nuestra red de Rogue AP. Dentro de este paso se contempla el uso de una herramienta encriptadora cipher. Este tipo de herramienta usa un algoritmo

de cifrado utilizado en el protocolo de seguridad 802.11i. Utiliza el cifrado de bloques AES, pero restringe la longitud de la clave a 128 bits. AES-CCMP incorpora dos técnicas criptográficas sofisticadas (modo contador y CBC-MAC) y las adapta a tramas Ethernet para proporcionar un protocolo de seguridad robusto entre el cliente móvil y el punto de acceso. AES en sí es un cifrado muy fuerte, pero el modo contador hace que sea difícil para un espía detectar patrones, y el método de integridad del mensaje CBC-MAC asegura que los mensajes no se hayan manipulado.

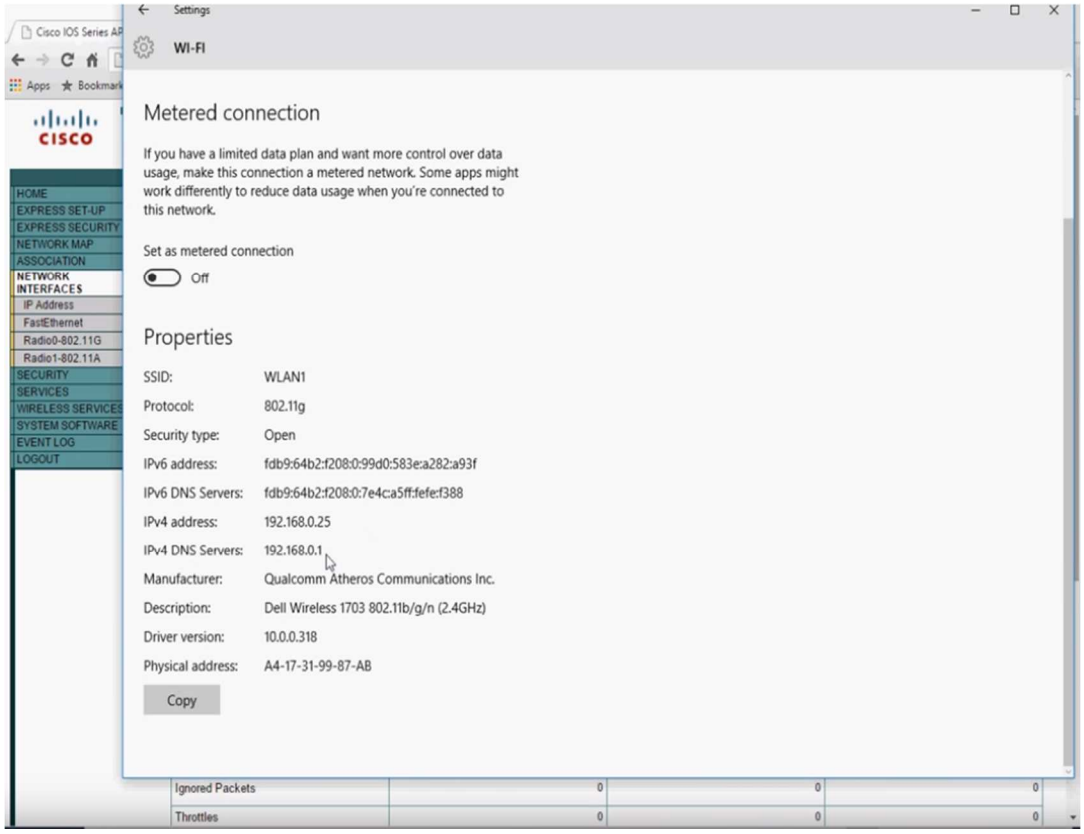


Figura 3. 9 Verificación de red con nueva configuración.

Fuente: Autor

El siguiente paso tiene como objetivo reconocer las maquinas tienen acceso a otro punto de internet que no sea el definido para este proyecto como WLAN1. Para esto podemos verificar dentro de la configuración de redes wifi para nuestra maquina si está habilitada e incluso correr pruebas para chequear si nuestra red en realidad está protegida.

3.2.4 Configurar AP con el WPA2 PSK de autenticación.

Para el último paso de nuestra configuración, se procede con la configuración de un punto de accesos o AP (Access Point) para que se corra el WPA2 PSK de autenticación. Como podemos ver en la figura 3.10, esta opción la encontramos en la sección de SECURITY, dando clic en ENCRIPTION MANAGER y este nos dirige a una interfaz para poder configurar aspectos de la conexión como lo es el cipher y el SSID. El cipher nos ayuda a la conectividad de nuestra red y además los cifrados no implican significado. En cambio, son operaciones mecánicas, conocidas como algoritmos, que se realizan en trozos individuales o pequeños de letras.

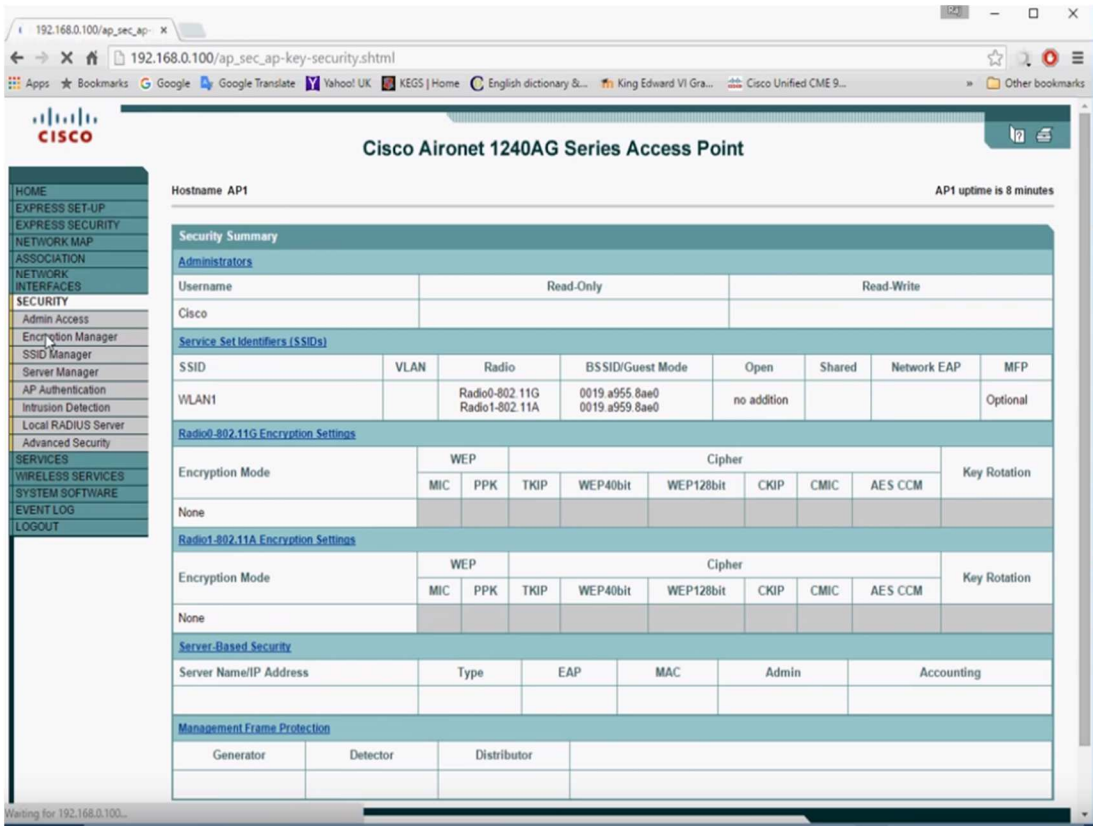


Figura 3. 10 Uso de cipher para protección de la red inalámbrica.

Fuente: Autor

Una vez dentro del programa podemos configurar las diferentes opciones que nos permite asegurar la fluidez de nuestro punto de acceso. Como podemos ver en la figura 3.11 nuestro siguiente paso consiste en la

configuración de RADIO 802.11G, la cual debemos configurarla con la opción de Cipher, y dentro del menú de opciones procedemos a definirlo con el AES CCMP. Esta opción fue creada para reemplazar el TKIP el cual es obligatorio para protocolos como el WPA y el WEP. La integridad que se requiere para esta red se tiene en cuenta que la clave de la administración y mensaje será mejorada unos 128 bits en bloque y con 10 rondas de codificación bajo el estándar FIPS 197.

En el sistema, habiendo configurado la primera opción del cipher, procedemos a ir a la pestaña de SSID manager y verificamos la opción de CURRENT SSID LIST, en la cual debemos seleccionar nuestra red de seguridad que lleva por nombre para este proyecto WLAN1. Cuando hemos terminado con esta parte, también procedemos a definir cuál será nuestra clave de red. Dentro de esta opción, tendremos que verificar nuestro manejo de llaves.

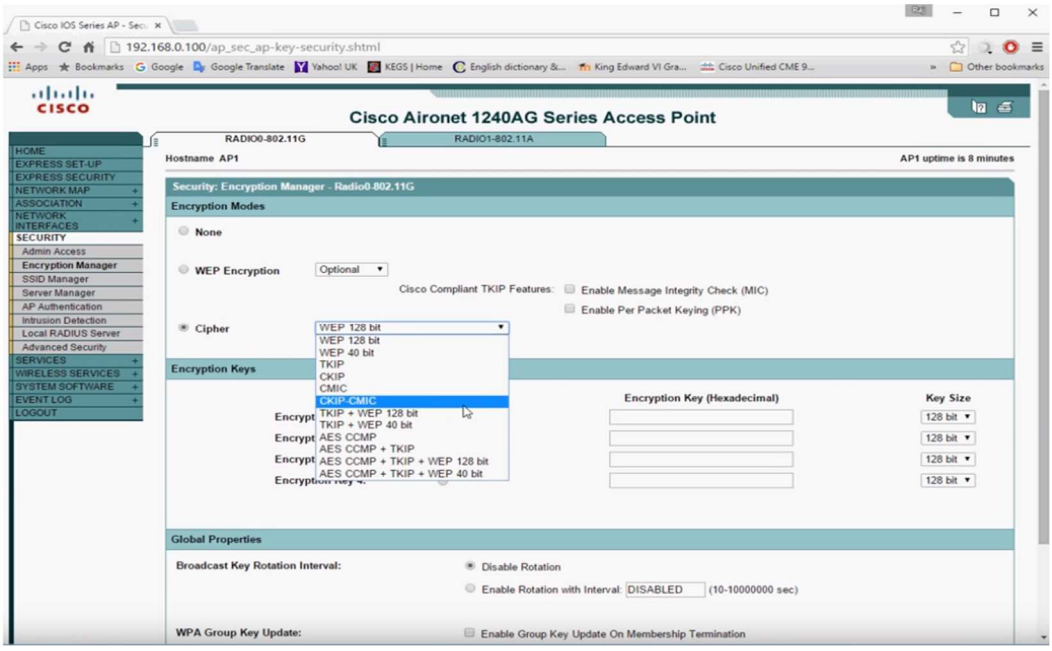


Figura 3. 11 Configurando cipher a AES CCMP.

Fuente: Autor

Cuando se haya terminado con las opciones mencionadas anteriormente, también deberíamos definir nuestro Client Authorized Key Management. Dentro de esta opción como lo vemos en la figura 3.12, este se debe cambiar la opción a MANDATORY. Una vez establecida esa opción,

procedemos a configurar la contraseña en la opción de WPE – Pre Shared. Establecemos la clave en la cual todos los equipos deberán acceder. También debemos definir el acceso a este punto de seguridad. Tenemos que también habilitar la opción de WPA2. Una vez hecho esta opción, procedemos a aplicar todos los cambios. Con esto se terminar el proceso de configuración del equipo. Una vez que todos los cambios se hayan realizado, debemos comprobar si la red no presenta dificultades de conexión con otros equipos. Una vez confirmada el punto de acceso y la conectividad entre el router y demás clientes, se puede conectar de manera libre. Para poder comprobar si la red no está bloqueada por un Rogue podemos ir al cuadro de comando y revisar si las claves de acceso sean gratis. Como podemos ver en la figura 3.12, se comprueba todo el proyecto mediante el cuadro de dialogo de C+.

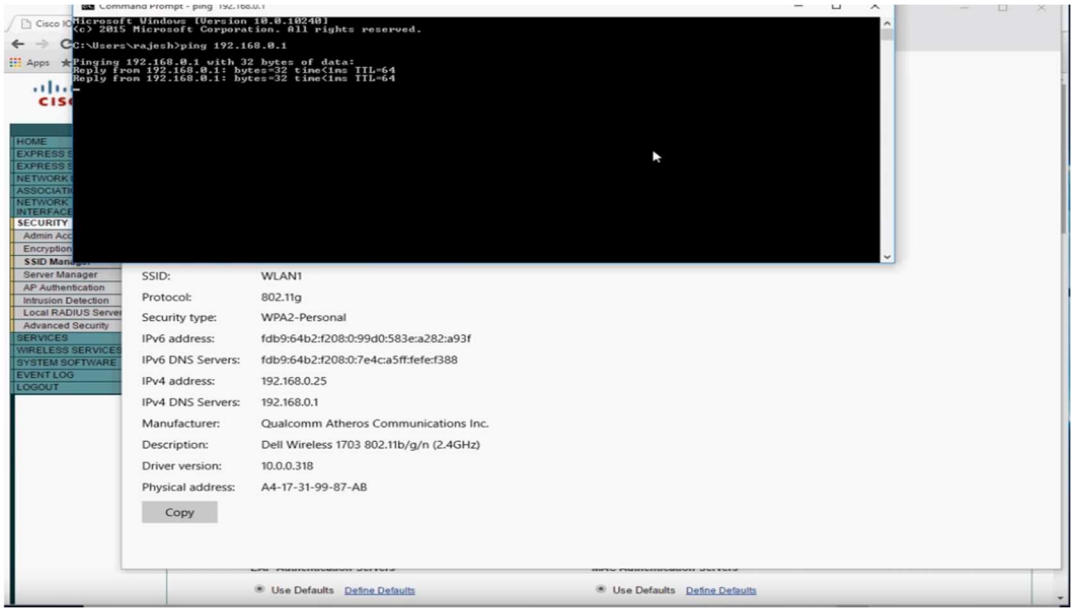


Figura 3. 12 Comprobación del sistema wifi en la computadora.
Fuente: Autor

Como última parte de este proyecto se procede a hacer la instalación del punto de acceso protegido con la consola CISCO Aironet 2600 para poder finalizar con la instalación el puesto en marcha del proyecto.

Figura 3. 13 Instalación de dispositivo CISCO Aironet 3600.
Fuente: Autor

Capítulo 4: Conclusiones y recomendaciones

4.1 Conclusiones

El propósito de este trabajo es el de establecer una medida de seguridad contra Rogue Access Point eficaz para el Colegio Fiscal Mixto Patria Ecuatoriana. Como parte del trabajo se considera la instalación de equipos CISCO Aironet 3600 con su respectivo modulo para un mejor control del tráfico de usuarios en una red que se encuentra ubicada en el área administrativa del colegio. En particular, en lugar de enviar paquetes de prueba desde el lado inalámbrico, nuestra solución tiene un verificador en la red cableada que envía la prueba paquetes hacia el lado inalámbrico. Los paquetes especiales mandados por el programa garantizan efectivamente que el AP sospechoso que retransmite estos paquetes es de hecho en la red interna y por lo tanto es un Rogue AP. El enfoque debe abordar dos cuestiones para la robustez usando el equipo necesario y creando una tercera capa de acción para la protección contra Rogue AP y esto logra que la seguridad de la información que corre entre las redes del plantel no sea vulnerada de forma inteligente. El bloqueo automático se logró de forma exitosa y las máquinas que se encuentran dentro de la zona administrativa fueron protegidos sin ningún tipo de problema de conectividad. En la actualidad, el detector implementado trabaja de forma exitosa en la oficina administrativa. Ya que este tipo de método usa paquetes de verificación en la red de modo secuencial, este mismo paquete se encarga de verificar si todas las máquinas y dispositivos conectados pasan la prueba de verificación que se implementa.

4.2 Recomendaciones

La configuración de los equipos tiende a ser complejas, por lo que se recomienda tener cuidado con la configuración del WLAN y los Access Point para los dispositivos móviles. También debemos tener precaución en el momento de hacer las pruebas, para que cuando se lance el programa y la configuración determinada para que suelten los paquetes de prueba a las

diferentes maquinas conectadas, estos puedan desempeñar una función más idónea, cuando se encuentren Rogue AP verificables. Si se va a llevar este proyecto a una escala más grande, se debe tener en cuenta que las conexiones no deben ser redundantes para que el tiempo de respuesta del programa sea mucho más corto y acertada.

BIBLIOGRAFÍA

AisLab. (2016). *AISLab.* Obtenido de Beyond 4G and 5G Wireless Mobile Communications : http://ais.unist.ac.kr/?page_id=211

Akbari, M., & Falahati, A. (2011). *Research Gate.* Obtenido de A Fault-Tolerant Cooperative Spectrum Sensing Algorithm over Cognitive Radio Network Based on Wireless Sensor Network: https://www.researchgate.net/figure/A-typical-distributed-cognitive-wireless-sensor-network-that-senses-the-spectrum-in-a_fig1_220279275

Alhameed Alkhatib, A. A., & Singh Baicher, G. (2012). *Research Gate.* Obtenido de Wireless Sensor Network Architecture: https://www.researchgate.net/publication/227352986_Wireless_Sensor_Network_Architecture

BigIdea Technology. (2017). *The WannaCrypt Scare – Part 2.* Obtenido de How a Defense-in-Depth Strategy Protects Businesses from Ransomware and other Cyberattacks?: https://bigideatech.com/how-a-defense-in-depth-strategy-protects-businesses-from-ransomware-and-other-cyberattacks/

CISCO. (2014). *Technical References.* Obtenido de Cisco Aironet 1600/2600/3600 Series Access Point Deployment Guide: https://www.cisco.com/c/en/us/td/docs/wireless/technology/apdeploy/Cisco_Aironet.html

Computer Networking Demystified. (2017). *Computer Networking Demystified.* Obtenido de Core functionality of Data Link Layer: http://computernetworkingsimplified.in/data-link-layer/core-functionality-data-link-layer/

Electronics for you. (2017). *Electronics for you.* Obtenido de Mobile Communication: From 1G to 4G: https://electronicsforu.com/technology-trends/mobile-communication-1g-4g

Escudero Pascual, A. (2016). *Itrainonnline.* Obtenido de Estándares en Técmolgías Inalábricas: http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/02_es_estandares-inalambricos_guia_v02.pdf

Fisher Telecommunication Services . (2016). *Fisher Telecommunication Services .* Obtenido de Transport Layer: http://www.fishercom.xyz/division-multiplexing/transport-layer.html

GL Communications Inc. (2016). *GL Communications Inc.* Obtenido de Communications Network Lab: https://www.gl.com/telecom-test-solutions/communications-networking-2G-3G-4G-lab.html

Hindle, P. (2015). *Microwave Journal.* Obtenido de History of Wireless Communications: http://www.microwavejournal.com/articles/24759-history-of-wireless-communications

Juniper Networks. (2016). *Juniper Networks.* Obtenido de Understanding Rogue Access Points: https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.1/topics/concept/wireless-rogue-ap.html

Kak, A. (2018). *Purdue University.* Obtenido de Computer and Network Security: https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf

Kaschel, H., Mardones, J., & Quezada, G. (2013). *Research Gate.* Obtenido de Safety in Wireless Sensor Networks: Types of Attacks and Solutions: https://www.researchgate.net/publication/269398801_Safety_in_Wireless_Sensor_Network_Types_of_Attacks_and_Solutions

KULLABS. (2015). *KULLABS.* Obtenido de Note on Open System Interconnection (OSI) Model: https://www.kullabs.com/classes/subjects/units/lessons/notes/note-detail/7055

Microcontrollers Lab. (2015). *Microcontrollers Lab.* Obtenido de WIRELESS SENSOR NETWORKS (WSN) & APPLICATIONS: http://microcontrollerslab.com/wireless-sensor-networks-wsn-applications/#DISASTER_RELIEF_OPERATION

Navas, M. A. (2016). *Professional Review.* Obtenido de Seguridad Wi-Fi: ¿AES o TKIP?: https://www.profesionalreview.com/2016/10/16/seguridad-wi-fi-aes-o-tkip/

Ortiz Tapia, F. (2018). *Universidad Técnica Federia Santa maría.* Obtenido de Red de sensores inalámbricos: http://profesores.elo.utfsm.cl/~tarredondo/info/networks/Presentacion_sensores.pdf

Pallás Areny, R., & Casas Piedrafita, O. (2014). *Interempresas.* Obtenido de Redes inalámbricas de sensores en aplicaciones agroambientales: http://www.interempresas.net/Robotica/Articulos/120885-Redes-inalambricas-de-sensores-en-aplicaciones-agroambientales.html

Pastor, J. (2017). *XATAKA.* Obtenido de Caos en la seguridad WiFi: un repaso a las vulnerabilidades de WEP, WPA, y WPA2: https://www.xataka.com/seguridad/caos-en-la-seguridad-wifi-un-repaso-a-las-vulnerabilidades-de-wep-wap-y-wap2

Pedro Pavia, J., Alexandre Lopes, D., & Cristovao, P. (2017). *Research Gate.* Obtenido de Evolution of mobile communications: https://www.researchgate.net/figure/Evolution-of-mobile-communications-16_fig1_320601176

Rashid, B., & Husain, M. (2016). *Science Direct.* Obtenido de Applications of wireless sensor networks for urban areas: A survey: https://www.sciencedirect.com/science/article/pii/S1084804515002702

Seymour, T., & Shaheen, A. (2011). *Review of Business Information Systems.* Obtenido de History of Wireless Communication: https://s3.amazonaws.com/academia.edu.documents/5321519/wireless-seymour.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1534807111&Signature=1jsZ0oif6tn2PPyp8G60651VgVE%3D&response-content-disposition=inline%3B%20filename%3DHistory_of_Wireless_Communicat

Shekhar, A. (2016). *Fossbytes.* Obtenido de Presentation Layer - OSI Model: https://fossbytes.com/presentation-layer-of-osi-model/

Simek, M. (2012). *WISLAB.* Obtenido de RESEARCH PROJECT (2010-2013) - ADAPTIVE WIRELESS SENSOR NETWORKS (AWSN): http://wislab.cz/our-work/research-project-2010-2013-adaptive-wireless-sensor-networks-awsn

Solarte, Z., Pena, L., & Almario, D. (2014). *Research Gate.* Obtenido de Red de sensores: https://www.researchgate.net/figure/Figura-2-Arquitectura-del-Sistema-UbiHealth-Red-de-Sensores-Conformada-por-los-sensores_fig2_254042967

Spacey, J. (2016). *Simplicable.* Obtenido de What is Defense In Depth?: https://simplicable.com/new/defense-in-depth

TutorialsPoint. (2017). *TutorialsPoint.* Obtenido de Network Security – Network Layer: https://www.tutorialspoint.com/network_security/network_security_layer.htm

Wikimapia. (2013). *Wikimapia.* Obtenido de Colegio Fiscal Mixto Patria Ecuatoriana : http://wikimapia.org/13068339/es/Colegio-Fiscal-Mixto-Patria-Ecuatoriana

Winters, F. J., Mielenz, C., & Hellestrand, G. (2014). *Research Gate.* Obtenido de Design process changes enabling rapid development: https://www.researchgate.net/publication/228782214_Design_process_changes_enabling_rapid_development

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Barreiro León, Cristhian Iván** con C.C: # 092595160-0 autor del Trabajo de Titulación: **Diseño de una red de sensores para la detección de Rogue o Fake AP en la red wifi del área administrativa del Colegio Fiscal Mixto Patria Ecuatoriana** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 13 de Septiembre de 2018

f. _____

Nombre: Barreiro León, Cristhian Iván

C.C: 0925951600

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	Diseño de una red de sensores para la detección de Rogue o Fake AP en la red wifi del área administrativa del Colegio Fiscal Mixto Patria Ecuatoriana		
AUTOR(ES)	BARREIRO LEON, CRISTHIAN IVAN		
REVISOR(ES)/TUTOR(ES)	M. Sc. Suarez Murillo, Efraín Oswaldo		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	13 de Septiembre de 2018	**No. DE PÁGINAS:**	78
ÁREAS TEMÁTICAS:	Sistemas Telemáticos y Seguridad informática		
PALABRAS CLAVES/ KEYWORDS:	Sensores, Rogue, Diseño, Red, Seguridad, Inalámbrica; Wifi.		

RESUMEN/ABSTRACT (150-250 palabras):

El trabajo de titulación consiste en el diseño de una red de sensores para el sistema de detección de Rogué o Fake Ap en la red WIFI del área administrativa del "Colegio fiscal mixto Patria Ecuatoriana". Primero se hablará sobre la problemática actual y la importancia de la seguridad en las redes inalámbricas, luego definiremos los sistemas que nos van a permitir la localización de los Rogue o Fake Ap. En el siguiente capítulo se explica por qué el uso de CISCO Aironet para diseñar la red, luego modelos de optimización para la red de sensores, también expondremos la manera en que se manejara la información para desarrollar los algoritmos, a continuación, se mostrara la estructura de la programación con la cual se puede diseñar la red de sensores para evitar los Rogue o Fake Ap. Explicaremos la circunstancia y parámetros en el cual basamos los algoritmos generados, luego mostraremos el resultado final y el grado de cobertura obtenido. Por último, anunciaremos las conclusiones y recomendaciones a las que hemos llegado en el presente trabajo de titulación.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593990244478	E-mail: cristhian.barreiro4@gmail.com
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Palacios Meléndez Edwin Fernando	
	Teléfono: +593-9-68366762	
	E-mail: edwin.palacios@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	