Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

VULNERABILIDADES Y NIVELES DE SEGURIDAD DE REDES WI-FI

Tatiana Violeta Vallejo de León

Asesorado por el Ing. MsEE. PhD. Enrique Edmundo Ruiz Carballo

Guatemala, agosto de 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

VULNERABILIDADES Y NIVELES DE SEGURIDAD DE REDES WI-FI

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA POR

TATIANA VIOLETA VALLEJO DE LEÓN
ASESORADA POR EL ING. MsEE. PhD ENRIQUE EDMUNDO RUIZ CARBALLO

AL CONFERÍRSELE EL TÍTULO DE
INGENIERA EN ELECTRÓNICA

GUATEMALA, AGOSTO DE 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Guerrero de López
VOCAL III	Ing. Miguel Ángel Dávila
VOCAL IV	Br. Luis Pedro Ortiz de León
VOCAL V	Agr. José Alfredo Ortiz Herincx
SECRETARIO	Ing. Hugo Humberto Rivera García

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Otto Fernando Andrino
EXAMINADOR	Ing. Carlos Guzmán
EXAMINADOR	Ing. José de León
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi Trabajo de Graduación titulado:

VULNERABILIDADES Y NIVELES DE SEGURIDAD EN REDES WI-FI,

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica el 21 de Noviembre de 2008.

Tatiana Violeta Vallejo de León

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

Guatemala, 07 de mayo de 2010.

Ing. Julio César Solares Peñate
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica-Eléctrica
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Señor Coordinador:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación "**Vulnerabilidades y Niveles de Seguridad de Redes Wi-Fi**", desarrollado por la estudiante **Tatiana Violeta Vallejo de León**; con base a la revisión y corrección de dicho trabajo, considero que ha alcanzado los objetivos propuestos por el cual la estudiante y mi persona nos hacemos responsables del contenido del mismo.

Sin otro particular, me suscribo de usted.

Atentamente,

Ing. MsEE. PhD. (Cand) Enrique Edmundo Ruiz Carballo
Colegio 2225

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

Guatemala, 20 de mayo de 2010.

Señor Director
Ing. Guillermo Antonio Puente
Escuela de Ingeniería Mecánica-Eléctrica
Facultad de Ingeniería
Universidad de San Carlos

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: **Vulnerabilidades y Niveles de Seguridad de Redes Wi-Fi**, desarrollado por la estudiante **Tatiana Violeta Vallejo de León**, por considerar que cumple con los requisitos establecidos para tal fin.

Sin otro particular, me suscribo de usted.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Julio César Solares Peñate
Coordinador Area Electrónica

UNIVERSIDAD DE SAN CARLOS
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA
MECANICA ELECTRICA
GUATEMALA

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 28. 2010.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; Tatiana Violeta Vallejo de León titulado: VULNERABILIDADES Y NIVELES DE SEGURIDAD DE REDES WI-FI, procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

UNIVERSIDAD DE SAN CARLOS
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA
MECANICA ELECTRICA
GUATEMALA

GUATEMALA, 15 DE JULIO 2,010.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.280.2010

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **VULNERABILIDADES Y NIVELES DE SEGURIDAD E REDES WI-FI,** presentado por la estudiante universitaria **Tatiana Violeta Vallejo De León,** autoriza la impresión del mismo.

IMPRÍMASE

Ing. Murphy Olympo Paiz Recinos
Decano

Guatemala, agosto 2010

/cc

AGRADECIMIENTOS

- A Dios, por permitirme llegar a este día donde culmino una etapa tan importante de mi vida.
- A mis padres, por todos sus consejos, su apoyo, su comprensión y por supuesto todo su amor.
- A mi esposo, Josué Joel, por todo su amor, su ayuda y sus sacrificios, por trabajar tan duro para que yo no tuviera la necesidad de hacerlo.
- A mi hija, Jennifer Alejandra, por comprenderme y dejarme estudiar cuando se lo pedía y por todos los momentos de alegría que me ha brindado.
- A mi suegra, mis cuñados y sobrinos, por cuidar a mi hija mientras yo estudiaba o hacía tareas.
- A mis catedráticos, por sus consejos, sus enseñanzas y la amistad que me ofrecieron.
- A mi asesor, Ing. Enrique Ruiz, por asesorarme en este trabajo de graduación, por brindarme tantos consejos y por ser uno de los mejores catedráticos de esta Facultad.
- Al Liceo Guatemala, especialmente al Administrador de la Red, Pedro Arrivillaga, por brindarme la información que necesitaba para poder terminar este trabajo de graduación.

ACTO QUE DEDICO

A DIOS Fuente inagotable de sabiduría.

AL SANTISIMO SEÑOR DE ESQUIPULAS No sólo hizo el milagro de que naciera, sino también ha intercedido por mí y me ha ayudado cada vez que se lo he pedido.

A MIS PADRES José Nelton Vallejo y Violeta de León de Vallejo. Todos sus esfuerzos están aquí. Los amo profundamente.

A MIS ABUELITOS María Hermelinda (Q.E.P.D.), por sus enseñanzas y amor.

Elia Concepción (Q.E.P.D.), por cuidarme toda mi niñez.

Justo Rufino (Q.E.P.D.), nunca voy a olvidar los Q.0.10 que me daba antes de irme a estudiar, lo extraño.

A MI ESPOSO Josué Joel, su amor y comprensión me ayudaron a llegar a este día.

A MI HIJA Jennifer Alejandra, es mi principal motivación para seguir superándome, espero que este triunfo le sirva de ejemplo para lograr cada meta que se proponga.

A MI FAMILIA EN GENERAL

Especialmente a:

Aura Vallejo, por su amor y sus consejos.

Ileana, Pedro, Antonio, Mario, Nora y Berta, por recibirme todos los días en su casa y por quererme como una integrante más de su familia. Gracias por todo su cariño.

Carlo César, Paola, Karla y Linda, siempre tengo en mi mente los recuerdos de nuestra niñez.

Patricia Ramos, por el cariño que me ha demostrado.

Hortencia Rojas, por ser una gran suegra.

A MIS AMIGOS

Sonia Santis, por su cariño y por ser como una segunda madre para mí durante toda mi niñez. Sandra González, Lucy Morales, Karla Morataya, Cristian García, Jorge Monterroso, Javier Alay, Mario y Kelvin Silvestre, David Crocker, Freddy Álvarez, Soraya Martínez, Yesenia de León y Dinora Soto. Gracias por su amistad sincera.

A MIS CATEDRATICOS

Especialmente a: Ing. Enrique Ruíz, Ing. Guillermo Puente, Inga. Ingrid Rodríguez de Loukota e Ing. Gustavo Orozco, por los consejos brindados y la amistad que me ofrecieron.

A LA FACULTAD DE INGENIERIA

Por formarme como profesional

A LA USAC

Templo del saber.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

SÍMBOLO	SIGNIFICADO
Mbps	Megabits por segundo (10^6 bits por segundo)
Gbps	Gigabits por segundo (10^9 bits por segundo)
s	Segundos
ms	Milisegundos (10^{-3} segundos)
PPM	Pulsos por minuto
MHz	Mega hertzios (10^6 Hertz)
GHz	Giga hertzios (10^9 Hertz)
THz	Tera hertzios (10^{12} Hertz)
nm	Nanómetros (10^{-9} metros)
Km	Kilómetros (10^3 metros)

GLOSARIO

Algoritmo Conjunto pre-escrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien lo ejecute.

Ancho de banda Longitud del rango de frecuencias, medida en Hz, en el cual está la mayor parte de la potencia de la señal.

Área de cobertura Área en la cual un punto de acceso puede ofrecer el servicio de red inalámbrico.

Autenticación Proceso por el cual se autoriza a un cliente a accesar a la red.

Bit Acrónimo de ***B****inary digi****t***. (Dígito Binario). Es un dígito del sistema de numeración binario 0 ó 1.

Broadcast Transmisión de un paquete que será recibido por todos los dispositivos en una red.

Capa MAC Del inglés *Media Access Control*, (Capa de Control de Acceso al Medio). Se encarga de gestionar y mantener la comunicación entre estaciones.

CCK	Acrónimo de *Complementary Code Keying* (Modulación por código complementario). Es un tipo de modulación que recupera llaves de encriptación.
CDMA	Acrónimo de *Code Division Multiple Access* (Acceso múltiple por división de código). Término genérico para varios métodos de control de acceso al medio basado en la tecnología de espectro expandido.
Chipset	Conjunto de circuitos integrados.
Cifrado	Proceso usado para volver ininteligible información considerada importante. Se llama también encriptación.
Cifrado XOR	Cifrado que se basa en la tabla de verdad de una compuerta OR exclusiva.
CISCO	Empresa dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.
Cliente	Dispositivo o equipo que se conecta a una red.
Codec	Codificador-Decodificador.
Código convolucional	Es un tipo de código de detección de errores en paquetes transmitidos.

CSMA Acrónimo de *Carrier Sense Multiple Access* (Acceso múltiple sensible a la portadora). Medio de acceso a la red que opera bajo el principio de escuchar antes de hablar. Cuando envía datos, primero escucha el canal, si la línea esta desocupada, la estación transmite; si está ocupada, espera hasta que esté libre.

CSMA/CA Acrónimo de *Carrier Sense Multiple Access/Collision Avoidance* (Acceso múltiple sensible a la portadora con prevención de colisión), en este caso el emisor escucha para ver si la red está libre, si lo está transmite el dato y luego espera un reconocimiento por parte del receptor.

CSMA/CD Acrónimo de *Carrier Sense Multiple Access / Collision Detect* (Acceso múltiple sensible a la portadora con detección de colisión). Cuando detecta que dos estaciones trasmiten al mismo tiempo y se sobreponen sus trasmisiones, existe una colisión, entonces las estaciones deben retransmitir la señal.

DBPSK Acrónimo de *Differential Binary Phase Shift Keying* (Modulación por desplazamiento de fase diferencial binario). Es un tipo de modulación digital.

Dirección MAC Identificador de 48 bits que es único para cada dispositivo de red.

DMT Acrónimo de *Discrete Multi-Tone* (Modulación por multitono discreto). Es otra forma de llamar a OFDM.

DQPSK Acrónimo de *Differential Quadrature Phase Shift Keying* (Modulación por desplazamiento de fase diferencial en cuadratura).

DSSS Acrónimo de *Direct Sequence Spread Spectrum* (Espectro Ensanchado por Secuencia Directa). Técnica de modución que utiliza un código de pseudoruido para modular directamente una portadora, de tal forma que aumente el ancho de banda de la transmisión y reduzca la densidad de potencia espectral; la señal resultante tiene un espectro muy parecido al del ruido, por lo tanto a todos los radiorreceptores les parecerá ruido, menos al que va dirigida la señal.

EAP Acrónimo de *Extensible Authentication Protocol* (Protocolo de autenticación extensible). Es una autenticación usada habitualmente en redes inalámbricas punto a punto; puede también ser usado para autenticación en redes cableadas.

Encriptación Proceso usado para volver ininteligible información que se considera importante; se le llama también cifrado.

FDMA Acrónimo de *Frequency Division Multiple Access* (Acceso múltiple por división de frecuencia); el acceso al medio se realiza dividiendo el espectro disponible en canales que corresponden a distintos rangos de frecuencia, asignando estos canales a los distintos usuarios y comunicaciones a realizar, sin interferirse entre sí.

FHSS Acrónimo de *Frequency Hopping Spread Spectrum* (Espectro ensanchado por salto de frecuencia). Consiste en transmitir cada tramo de información en una frecuencia distinta durante un intervalo muy corto de tiempo.

FSK Acrónimo de *Frequency Shift Keying* (Modulación por salto de frecuencia). En este tipo de modulación la señal moduladora hace variar la frecuencia de la portadora, de modo que la señal modulada resultante codifica la información asociándola a valores diferentes de frecuencia.

Hacker Especialista en entrar en sistemas informáticos ajenos sin permiso, generalmente para mostrar la baja seguridad de los mismos, para demostrar que es capaz de hacerlo o para robar información.

ICV Valor de comprobación de integridad.

IEEE	Instituto de Ingenieros Electricistas y Electrónicos.
Interfaz de red	Permiten a cualquier servidor que ejecute el servicio de enrutamiento y acceso remoto, o a comunicarse con otros equipos a través de redes privadas o públicas.
Itinerancia	Conocido también como *Roaming*, se aplica al concepto de que los dispositivo WI-FI cliente puede desplazarse e ir registrándose en diferentes puntos de acceso.
IV	Vector de inicialización.
Keystream	Torrente de caracteres aleatorios o pseudoaleatorios que se combinan con el texto plano para encriptarlo.
LAN	Acrónimo de *Local Area Network* (Redes de área local), es el término empleado para denominar redes cableadas.
Modelo OSI	Es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.
Modem	Dispositivo que sirve para enviar una señal portadora mediante otra señal llamada moduladora, el dispositivo puede modular y demodular al mismo tiempo.

Modulación Conjunto de técnicas para transportar información sobre una onda portadora.

Módulo Bluetooth Dispositivo inalámbrico diseñado especialmente por su bajo consumo y bajo costo, pero con un área de cobertura baja.

Nodo Puntos, dispositivos o equipos que conforman una red.

OFDM Acrónimo de *Orthogonal Frequency Division Multiplexing* (Multiplexación por división de frecuencias ortogonales), es una multiplexación que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información, la cual es modulada en cuadratura o en PSK.

PA Punto de acceso.

Paquete binario Es una parte del mensaje o información transmitida en forma binaria (1's y 0's).

Password Palabra clave de acceso.

PDA Del inglés *Personal Digital Assistant* (Asistente digital personal), computadora de mano diseñada como agenda electrónica con sistema de reconocimiento de escritura y algunas funciones de las computadoras de escritorio.

Programa *Sniffer* Programa que captura datos en la red para luego analizarlos.

Protocolo IAPP Protocolo de conexión entre puntos de acceso que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento; conocido también como Itinerancia.

Punto de acceso Dispositivo que interconecta equipos de comunicación inalámbrica para formar una red.

QoS Acrónimo de *Quality of Service* (Calidad del servicio), se refiere a las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado, es especialmente importante para ciertas aplicaciones tales como la transmisión de video o voz.

Red Ethernet Estándar más popular para las redes de área local, los equipos están conectados mediante cable coaxial o de par trenzado y accesan a la red utilizando el método CSMA/CD. Inicialmente podía manejar información a 10 Mb/s, aunque actualmente se han desarrollado estándares mucho más veloces.

Red inalámbrica Es una conexión de nodos o equipos por medio de ondas electromagnéticas en lugar de cables.

RF Radio frecuencia.

Roaming Término usado para describir la Itinerancia.

Router Dispositivo que se utiliza para interconectar redes informáticas, permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar. Se le llama también enrutador.

Secuencia PN Secuencia pseudoaleatoria o de ruido (*PseudoNoise*), se definida como un conjunto de señales binarias, periódicas y de cierta longitud de tal forma que, dentro de cada período, la señal puede aproximarse a una señal aleatoria.

Señal Portadora Forma de onda, generalmente sinusoidal, cuyas propiedades son cambiadas por una señal que se quiere transmitir.

Servidor DHCP Del inglés *Dynamic Host Configuration Protocol* (Protocolo Configuración Dinámica de Servidor). Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas están libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuanto tiempo la ha tenido y a quien se la ha asignado después.

Servidor Proxy Sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Software Programas o paquetes computacionales

SSID Nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.

Switch Dispositivo encargado de interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

TDMA Acrónimo de *Time Division Multiple Access* (Acceso múltiple por división de tiempo). Técnica de multiple-xación que distribuye las unidades de información en espacios alternos de tiempo, proveyendo acceso múltiple a un reducido número de frecuencias.

Tecnología MIMO Acrónimo en inglés de *Multiple Input – Multiple Output* (Múltiple entrada - múltiple salida). Se refiere a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos como enrutadores.

Topología	Cadena de comunicación usada por los dispositivos o nodos de una red para comunicarse
Vector de inicialización	Bloque de bits necesario para permitir un cifrado con un resultado independiente de otros cifrados producidos por la misma clave.
WECA	Acrónimo de *Wireless Ethernet Compatibility Alliance*, es una empresa creada con el fin de fomentar la compatibilidad entre tecnologías Ethernet e inalámbricas. Ahora llamada WI-FI Alliance.
Wireless	Inalámbrico
WLAN	Del inglés *Wireless Local Area Network* (Redes de área local inalámbrica), es el término empleado para denominar redes no cableadas.

RESUMEN

El presente trabajo de graduación fue realizado para analizar las vulnerabilidades a las que están expuestas las redes inalámbricas de alta velocidad conocidas comúnmente como Redes WI-FI, así como los métodos que brindan cierto grado de seguridad a estas redes.

En el primer capítulo se describe el protocolo en sí; es decir, sus características, componentes, bandas de transmisión, técnicas de transmisión, los mecanismos de acceso a la red, topologías y la familia completa de protocolos derivados de la norma inicial.

Los diferentes métodos de seguridad que pueden ser aplicados a redes inalámbricas se tratan en el segundo capítulo; estos medios son: autenticación de usuario, encriptación, lista de control de acceso o filtrado de direcciones MAC, WEP y WPA.

En el tercer capítulo se describen las vulnerabilidades de las redes WI-FI, se definen las características de los diferentes tipos de ataques a los que las redes están sujetos, además se enumeran los problemas concretos que pueden volver insegura una red inalámbrica.

Por último, en el cuarto capítulo se describen las medidas básicas de seguridad que usuarios y administradores de redes privadas deben tomar en cuenta para hacer menos insegura una red; inclusive se transcribe una porción de una entrevista realizada al administrador de una pequeña red inalámbrica privada.

OBJETIVOS

❖ GENERAL

Conocer las características de las redes inalámbricas de área local de alta velocidad (WI-FI), los procesos para brindar seguridad a este tipo de redes y las vulnerabilidades de las mismas.

❖ Específicos

1. Conocer las ventajas de las redes WI-FI.
2. Conocer las desventajas de estas redes inalámbricas.
3. Analizar los mecanismos que brindan seguridad a redes WI-FI.
4. Estudiar y analizar los tipos de ataques que pueden afectar a las redes inalámbricas para así poder evitarlos.
5. Determinar cuáles son concretamente los problemas a los que está expuesta una red inalámbrica.
6. Conocer y aplicar medidas básicas de seguridad en redes privadas.

INTRODUCCIÓN

Un área sumamente importante en el desarrollo y la evolución de la humanidad es la comunicación, ya que desde que el hombre prehistórico apareció sobre la faz de la tierra ésta se hizo necesaria para poder entenderse; por lo tanto, en conjunto con la evolución del hombre, la comunicación también evolucionó; desde las primitivas señales de humo, pasando por la escritura, el telégrafo, la radio y la telefonía fija hasta llegar a la tecnología que es ahora el "boom": la comunicación inalámbrica o móvil.

La telefonía inalámbrica y su evolución han capturado la atención de los profesionales de esta área, ya que el deseo de movilidad y la ruptura de conexiones físicas han forzado de alguna manera las mejoras en la misma. En la evolución de estos sistemas de comunicación inalámbricos se reconocen cuatro generaciones diferentes; la primera, caracterizada por la transmisión analógica de servicios, la segunda de ellas introdujo la transmisión digital de voz y una transmisión de datos con una velocidad de hasta 100 Kbps. El explosivo crecimiento del Internet y la demanda que este tenía dio origen a nuevos servicios de banda ancha, los cuales son los impulsores de los sistemas de tercera y cuarta generación. En la cuarta generación se puede alcanzar la convergencia entre las redes alambradas e inalámbricas, velocidades de acceso entre 100 Mbps en movimiento y 1 Gbps en reposo y el mantenimiento de la calidad del servicio en todos sus puntos.

La expansión de ondas de radio frecuencia no puede ser controlado por medio de barreras físicas, por lo tanto pueden ser recibidas desde casi cualquier punto en su zona de cobertura; en este trabajo de graduación se persigue analizar las vulnerabilidades de estas redes inalámbricas y describir los problemas concretos que afrontan en el tema de seguridad.

Con base en lo anterior se investigaron los ataques más comunes que sufren las redes inalámbricas y los métodos para hacerlas menos inseguras; esto debido a que no se puede decir que una red inalámbrica es totalmente segura, ya que día a día se intentan nuevos ataques o se crean nuevas formas de atentar contra la seguridad aplicada a estas redes. Entonces, si se aplican algunas o todas las medidas de seguridad descritas en el presente trabajo de graduación se puede tener una red inalámbrica sumamente difícil de accesar para usuarios no autorizados.

1. PROTOCOLO IEEE 802.11

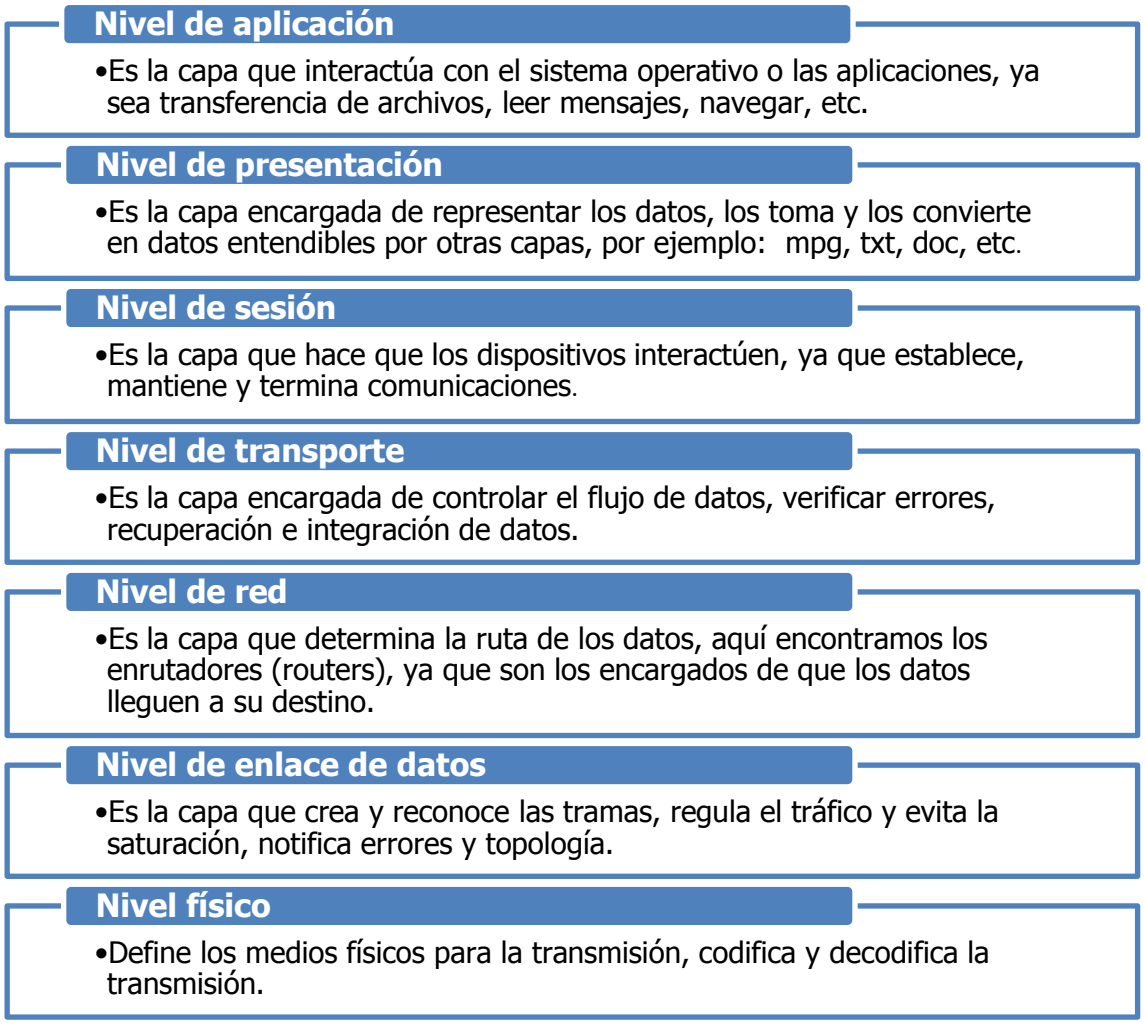
El protocolo IEEE 802.11 es el nombre genérico con el que se le conoce a una familia de estándares diseñado para redes inalámbricas. Este estándar 802.11 define las características de comunicación en redes de área local inalámbricas de alta velocidad comúnmente llamadas WI-FI, nombre que proviene de *Wireless Fidelity* análogo a *High Fidelity* en audio (HI-FI). *WI-FI* es el nombre comercial y marca registrada de la certificación con la que la WECA (*Wireless Ethernet Compatibility Alliance*) asegura la completa compatibilidad entre dispositivos que pueden ser usados para crear redes locales inalámbricas de alta velocidad.[1]

Una red de área local inalámbrica puede ser definida como una red de alcance local que utiliza ondas electromagnéticas como medio de transmisión, en lugar de cables o fibra óptica como en las redes cableadas. Se les llama redes WI-FI a las redes que cumplen con el estándar 802.11, las cuales pueden contener computadoras portátiles y de escritorio, asistentes digitales personales (PDA), consolas de video juegos o cualquier otro dispositivo de alta velocidad con propiedades de conexión de 11 Mbps o superior. El radio de cobertura va desde unos 20 a 50 metros en ambientes cerrados hasta cientos de metros en espacios abiertos. [2]

1.1 Modelo de referencia OSI

El modelo de referencia de interconexión de sistemas abiertos o modelo de referencia OSI está compuesto por siete diferentes capas o niveles, el nivel más cercano al usuario es el más alto ya que por medio de éste el usuario interactúa con otros equipos. En el esquema de abajo se muestra una estructura bastante general de este modelo.

Figura 1. **Modelo OSI**



Las capas que son importantes de describir de este protocolo son: La capa física y la capa de enlace de datos.

1.1.1 Capa física[3]

En esta capa se definen las características que deben tener la transmisión de los datos y el tipo de modulación a usar. El estándar IEEE 802.11 da a elegir entre tres opciones que son:

- FHSS o Espectro ensanchado por salto de frecuencia.
- DSSS o Espectro ensanchado por secuencia directa.
- Luz infrarroja en banda base.

La característica principal del espectro ensanchado es que utiliza todo el ancho de banda disponible en vez de concentrar la energía en una señal portadora, por lo que brinda posibilidades de encriptación y mayor inmunidad a interferencias. Este protocolo puede ser transmitido en la banda IMS (*Industrial, Scientific and Medical*) el cual contiene las frecuencias 902 - 928 MHz, 2.4 - 2.4835 GHz y 5.725 - 5.850 GHz.

1.1.1.1 Espectro ensanchado por salto de frecuencia

Esta técnica consiste en transmitir la información en una determinada frecuencia durante un intervalo de tiempo igual o inferior a los 400 ms y luego salta a otra frecuencia, y luego a otra, etc.

El orden de los saltos es pseudoaleatorio ya que tanto el transmisor como el receptor deben conocerlo; la cantidad de saltos por segundo es regulada en cada país.

La banda de aplicación de esta transmisión esta en la zona de los 2.4 GHz y se divide en 79 canales con 1 MHz de ancho de banda. La modulación aplicada es la FSK (*Frecuency Shift Keying*) con una velocidad de 1 a 2 Mbps, aunque en la revisión del estándar se aumentó a 11 Mbps.

Esta técnica reduce la interferencia ya que sólo podría ser afectada si otra señal está transmitiendo a la misma frecuencia al mismo tiempo.

1.1.1.2 Espectro ensanchado por secuencia directa

Esta técnica consiste en generar una secuencia de bits, la cual es redundante para cada bit que compone la señal; a mayor tamaño, mayor resistencia a interferencias. El estándar recomienda un tamaño de 11 bits, pero el óptimo es de 100. Esta secuencia de bits se conoce como Secuencia de Barrer o *PseudoNoise* y está diseñada para que aparezca la misma cantidad de 1s y 0s; solamente los receptores a los que el emisor haya enviado con anterioridad la secuencia podrán recomponer la señal original.

Los tipos de modulación aplicables en esta técnica son la DQPSK (*Differential Quadrature Phase Shift Keying*) y la DBPSK (*Differential Binary Phase Shift Keying*).

La tecnología DSSS utiliza el rango de frecuencias de los 2.4 a 2.4835 GHz, en el cual los 83.5 MHz de ancho de banda se subdividen en 14 canales de 5 MHz cada uno y cada país está autorizado a utilizar un subconjunto de estos canales. La división de canales se muestra en la siguiente tabla.

Tabla 1. **Canales y frecuencias utilizadas por la tecnología DSSS**

Canal	**Frecuencia inferior**	**Frecuencia superior**	**Frecuencia central**
1	2410 MHz	2414 MHz	2412 MHz
2	2415 MHz	2419 MHz	2417 MHz
3	2420 MHz	2424 MHz	2422 MHz
4	2425 MHz	2429 MHz	2427 MHz
5	2430 MHz	2434 MHz	2432 MHz
6	2435 MHz	2439 MHz	2437 MHz
7	2440 MHz	2444 MHz	2442 MHz
8	2445 MHz	2449 MHz	2447 MHz
9	2450 MHz	2454 MHz	2452 MHz
10	2455 MHz	2459 MHz	2457 MHz
11	2460 MHz	2464 MHz	2462 MHz
12	2465 MHz	2469 MHz	2467 MHz
13	2470 MHz	2474 MHz	2472 MHz
14	2475 MHz	2479 MHz	2477 MHz

1.1.1.3 Luz infrarroja

En esta tecnología se utiliza el rango infrarrojo del espectro electromagnético para transmitir a través del espacio; esto es justo por debajo de la luz visible, por lo que podría decirse que posee las mismas características que ésta. Las ventajas y desventajas son entonces las mismas que las de la luz visible.

Entre las ventajas podemos mencionar las siguientes:

- Posee un amplio ancho de banda,
- Es resistente a interferencias electromagnéticas radiadas,
- Es más seguro contra receptores no deseados ya que no puede atravesar paredes,
- Usa un protocolo simple,
- Consume poca potencia, y,
- No se necesita de una autorización especial para usarlo.

La otra cara de la moneda son las limitaciones que poseen estos sistemas, siendo las más sobresalientes:

- La restricción de cobertura a unas pocas decenas de metros.
- La sensibilidad a objetos que interfieren la comunicación entre transmisor y receptor.
- La interferencia que puede crear cualquier fuente de luz.

Los sistemas infrarrojos de acuerdo con el ángulo de apertura pueden clasificarse en:

- **Sistemas infrarrojos de corta apertura, de rayo dirigido o de línea vista**. Estos sistemas están formados por un cono de haz infrarrojo direccional por lo que el emisor debe orientarse hacia el receptor antes de empezar la transmisión. Este mecanismo es usado únicamente en enlaces punto a punto, por lo que se le considera inalámbrico, pero no móvil.
- **Sistemas de gran apertura, reflejados o difusos**. En este caso el receptor no debe estar necesariamente alineado con el emisor ya que la dispersión permite que la señal rebote en techos y paredes. Aquí entonces el problema no es la falta de movilidad sino que el rebote introduce interferencia y limita la velocidad de transmisión.

La IEEE especifica que las características principales que deben poseer las redes inalámbricas por medio de infrarrojos son:

- Entornos muy localizados, un aula o un laboratorio, inclusive podría ser un edificio.
- La modulación debe ser de 16-PPM y 4-PPM que permiten un 1 y 2 Mbps de transmisión.
- Longitudes de onda de 850 a 950 nm de rango.
- Frecuencias de emisión de 315 THz y 352 THz

1.1.2 Capa de enlace de datos

Esta capa es la que controla el acceso, flujo de datos entre componentes, exploración, autenticación y seguridad de las redes. La norma IEEE 802.11 define una única capa MAC para las redes físicas y hay que tener en mente que un protocolo de acceso a redes inalámbricas requiere una especial atención en los aspectos siguientes:

- La topología de la red.
- Las interferencias que puede sufrir.
- Roaming.
- Variaciones de potencia de la señal.
- Conexiones y desconexiones repentinas.

1.1.2.1 Mecanismos de acceso

El acceso múltiple por división de tiempo (TDMA) y por división de frecuencia (FDMA) constituyen los Protocolos de Acceso por Arbitraje. En el primer caso se le asigna todo el ancho de banda disponible a cada nodo durante un breve espacio de tiempo en forma cíclica, pero requiere que la sincronización sea muy precisa para evitar interferencias. En el caso del FDMA el ancho de banda se divide en distintos canales permitiendo así el acceso inmediato, pero, en sistemas informáticos es ineficiente por la forma en que los bits son transmitidos.

Otro tipo de protocolos de acceso son los llamados Protocolos de Acceso por Contienda, los cuales tienen similitudes con las redes cableadas definidas por el estándar 802.3. El acceso múltiple por división de código (CDMA) es uno de los protocolos de este tipo el cual se aplica únicamente a sistemas de radiofrecuencia de banda esparcida que son basados en una secuencia PN; en este caso el transmisor solamente necesita saber la secuencia PN del receptor, ya que cada equipo posee una en particular.

En la familia de los Accesos por contienda encontramos también el acceso múltiple sensible a la portadora con detección de colisión (CSMA/CD) y, el acceso múltiple sensible a la portadora con prevención de colisión (CSMA/CA). El más usado es este último, ya que en una red inalámbrica es más fácil prevenir una colisión que detectarla.

El funcionamiento del CSMA/CA es básicamente el siguiente:

- El transmisor escucha a la red, si la red se encuentra ocupada la transmisión se queda en espera por unos instantes; al momento de estar libre la red, el transmisor envía un mensaje que contiene la cantidad de datos a enviar y su velocidad de transmisión.
- El receptor avisa que está listo para recibir los datos y se inicia la transmisión.
- Cuando ya se han recibido todos los datos, el receptor envía un mensaje al transmisor indicándole que recibió correctamente los datos.

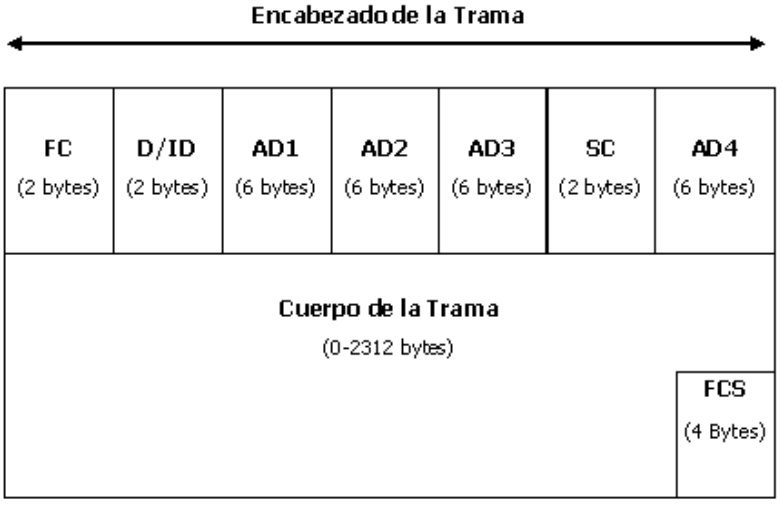
1.1.2.2 Control de errores, fragmentación y trama[4]

A diferencia de las redes *Ethernet*, la capa MAC del protocolo 802.11 tiene un mecanismo de detección de errores que le permite verificar la integridad de los datos enviados. Debemos recordar que en una red inalámbrica el índice de errores es mayor y es por esto que la detección de errores se ha incluido en el nivel de enlace de datos. El mecanismo de detección de errores se basa en el siguiente polinomio de 32 bits:

$$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

El índice de errores de transmisiones en redes inalámbricas se ve incrementado cuando se envían paquetes de gran tamaño, por lo que existe un mecanismo de fragmentación, el formato de trama de estos fragmentos es el siguiente:

Figura 2. **Formato de trama de los fragmentos**



Fuente: **http://es.kioskea.net/contents/WI-FI/WI-FImac.php3**

- **FC (Control de trama):** Contiene información sobre versión, tipo, encriptación y otros que serán analizados abajo.
- **D / ID (Duración / identificador):** Indica la duración del canal de transmisión que se utiliza.
- **AD1-AD4 (Campos de dirección):** Aquí se incluyen las direcciones de la estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino.
- **CS (Control de secuencia):** Contiene el número de secuencia y el número de fragmento de la trama que se esta enviando, permitiendo así rearmar el paquete fragmentado.
- **FCS (Secuencia de verificación de trama incorrecta):** Es el encargado de chequear si la transmisión fue correcta.

El control de trama (FC) contiene la siguiente información:

Figura 3. **Formato del control de trama**

Versión	Tipo	Sub tipo	Hacia DS	De DS	Más frag	Reintentar	Adm. De energía	Más datos	WEP	Orden
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 Bit	1 bit	1 bit	1 bit	1 bit

Fuente: **http://es.kioskea.net/contents/WI-FI/WI-FImac.php3**

- **Versión del protocolo:** Hace un seguimiento de los cambios entre las distintas versiones del estándar 802.11. Para la primera versión se establece un 0.
- **Tipo:** Identifica si la trama es del tipo de datos, control o gestión.

- **Subtipo**: Identifica cada subtipo que puede ser generado por cada uno de los tipos.
- **Hacia DS:** Se ajusta en 1 cuando la trama se envía a un sistema de distribución (DS); es decir cualquier información que se envía al punto de acceso.
- **De DS:** Se ajusta en 1 cuando la trama viene de un sistema de distribución. Si los campos Hacia DS y De DS están en 0 significa que la comunicación es entre dos estaciones de la red.
- **Más fragmentos:** Se activa o se ajusta en 1 si todavía falta transmitir más fragmentos del mensaje.
- **Reintentar:** Este bit indica si el fragmento es una retransmisión de otro enviado con anterioridad que probablemente fue perdido.
- **Administración de energía:** Se activa si la estación utiliza el modo de economía de potencia.
- **Más datos:** Este es usado en conjunto con el bit de administración de energía para especificar que en la estación hay tramas adicionales en espera de ser enviadas.
- **WEP:** Indica si el fragmento fue encriptado.
- **Orden:** Indica si la trama fue enviada a través de una clase de servicio de orden estricto.

1.2 Familia de estándares 802.11[5]

Como fue mencionado anteriormente, el estándar IEEE 802.11 especifica las normas de funcionamiento de una red inalámbrica de alta velocidad. El estándar original de esta familia fue creado en 1997 y tenia velocidades de 1 hasta 2 Mbps en la banda de los 2.4 Ghz. Este estándar fue modificado para dar paso a velocidades superiores que iban de 5 a 11 Mbps siempre en la misma banda de frecuencias; posteriormente se realizaron mas modificaciones que incluían características de los puntos de acceso, características de seguridad, calidad de servicio, armonización entre redes, y tipos de modulación entre otras. Actualmente esta familia cuenta con 16 estándares diferentes, los cuales van a ser explicados brevemente en forma individual.

1.2.1 Protocolo 802.11 *Legacy*

Es la versión original que fue publicada en 1997, que es el que especifica las velocidades de transmisión de 1 y 2 Mbps a través de infrarrojos. Define también el método de acceso por medio de la técnica CSMA/CA. Este tuvo problemas de interoperabilidad entre equipos de diferentes marcas por lo que fue descartado y corregido en el estándar 802.11b.

1.2.2 Protocolo 802.11a

Creado en el año 2001, usa la banda de los 5 GHz y opera a una velocidad máxima de 54 Mbps, aunque ésta puede ser reducida a 48, 36, 34, 18, 12, 9 o 6 Mbps si se requiere. Este protocolo está dividido en doce canales no sobrepuestos, ocho de ellos son dedicados a transmisiones en espacios cerrados y cuatro a conexiones punto a punto.

El método de acceso es por medio de Multiplexación por división de frecuencias ortogonales (OFDM), también llamado modulación por multitono discreto (DMT).

Operar a 5 GHz es una ventaja para este protocolo ya que presenta menos interferencia, pero restringe la red a puntos en línea vista por lo que es necesario instalar más puntos de acceso.

1.2.3 Protocolo 802.11b

Este estándar fue ratificado en 1999; tiene un alcance de aproximadamente 50 metros con una antena omnidireccional de baja ganancia. Con antenas externas de alta ganancia se puede llegar hasta 8 km de alcance y algunos reportes sugieren que en línea vista se puede llegar a tener un alcance de 80 a 120 km.

La velocidad máxima de transmisión es de 11 Mbps aunque en realidad ésta va de 5.9 a 7.1 Mbps; La banda de operación se encuentra en el espectro de los 2.4 GHz; y, al igual que el estándar original, se puede acceder por medio de CSMA/CA, aunque también se puede utilizar la técnica DSSS.

1.2.4 Protocolo 802.11c

Es una combinación del estándar 802.11 *Legacy* y el 802.11d en lo que se refiere a la capa de enlace de datos. Define las características de los puntos de acceso para que puedan operar como puentes.

1.2.5 Protocolo 802.11d

Esta pensado para permitir el uso global de redes WLAN. Provee puntos de acceso con la habilidad de comunicar información en canales de radio disponibles de acuerdo con las regulaciones de los distintos países; es decir que cubre las especificaciones donde los estándares de la familia 802.11 no están permitidos para operar.

Las reglas están sujetas a variaciones que incluyen frecuencias, niveles de potencia y ancho de banda permitidos. La especificación elimina la necesidad de diseñar y fabricar grandes cantidades de hardware que permita la interoperabilidad.

1.2.6 Protocolo 802.11e

Contiene estándares físicos de los protocolos a, b y g que proveen soporte complementario a servicios que requieren garantías QoS (Calidad de Servicio) a la capa MAC de las aplicaciones LAN en tiempo real.

Es usado por servicios con manejo de niveles QoS para aplicaciones de datos, voz y video. La introducción de un nuevo elemento llamado Función de Coordinación Híbrida (HCF por sus siglas en inglés) fue un factor clave para cumplir con el objetivo propuesto por este estándar.

1.2.7 Protocolo 802.11f

El objetivo principal de este protocolo es lograr una interoperabilidad entre proveedores y fabricantes de redes WLAN.

Determina el registro de los puntos de acceso en una red y cubre el intercambio de información de un punto de acceso a otro cuando un usuario migra entre ellos, tal como sucede en las redes de telefonía celular. A esta propiedad se le llama Itinerancia y el protocolo IAPP es el encargado de permitir esta migración.

1.2.8 Protocolo 802.11g

Este protocolo aplica el método de acceso Multiplexación por División de Frecuencia Ortogonal (OFDM) y puede ser usado conjuntamente con los dispositivos que aplican el estándar 802.11b por medio de Manipulación de Código Complementario (CCK) y paquetes binarios de códigos convolucionales. Su velocidad máxima es de 54 Mbps, lo cual le da una ventaja sobre el estándar 802.11b cuya velocidad máxima es de 11 Mbps.

1.2.9 Protocolo 802.11h

Este estándar fue creado debido a que en Europa existen ciertas regulaciones de potencia para transmisiones en la banda de los 5 GHz. Los dispositivos creados para cumplir esta norma deben contar con un Control de Potencia Transmitida (TCP) y una Selección de Frecuencia Dinámica (DFS). El primero restringe la potencia transmitida a la menor cantidad necesaria para alcanzar al usuario más lejano, luego el DFS selecciona el canal de radio en el cual el punto de acceso puede reducir la interferencia creada por otras redes.

La mayoría de las funciones del TPC y del DFS son útiles para otros propósitos y no solo para satisfacer las regulaciones europeas; ya que mejoran el desempeño general de la red y simplifican su mantenimiento.

1.2.10 Protocolo 802.11i

Este estándar fue ratificado el 24 de junio de 2004 y se refiere particularmente a la seguridad en redes inalámbricas. El estándar se basa en un algoritmo de cifrado como el WEP, pero también admite el Estándar de Cifrado Avanzado (AES) que es mucho más seguro.

Para lograr obtener una certificación WI-FI los productos WLAN deben implementar algunas características de seguridad adicionales a las de este estándar. Las redes corporativas constantemente deben desarrollar e integrar técnicas de modulación encriptadas que provean un mayor nivel de seguridad durante sus transmisiones.

1.2.11 Protocolo 802.11j

Básicamente es el estándar que permite que la IEEE 802.11 pueda coexistir y armonizar con las regulaciones europeas y japonesas (HiperLAN y ARIB respectivamente).

1.2.12 Protocolo 802.11k

Es el encargado de permitir el cálculo y la valoración de recursos de radiofrecuencia a los conmutadores y puntos de acceso de una red WLAN; lo cual mejora su desempeño.

Este estándar está diseñado para ser implementado en software y, tanto los clientes como la infraestructura deben ser compatibles.

1.2.13 Protocolo 802.11m

Es el estándar encargado del mantenimiento de las redes inalámbricas, además es el encargado de supervisar y mantener todos los otros estándares de la familia y sus publicaciones.

1.2.14 Protocolo 802.11n

Es un sistema en desarrollo que se basa en la tecnología MIMO (Múltiple Entrada, Múltiple Salida). La velocidad real de transmisión podría llegar hasta los 600 Mbps, la que es aproximadamente 40 veces más que el estándar 802.11b. Este estándar permitiría, por medio de varias antenas, utilizar varios canales al mismo tiempo para enviar y recibir datos, por lo que aprovecharía mejor las ondas secundarias de radiofrecuencia que hasta el momento se han visto como interferencias.

Adicionalmente, se espera que este estándar pueda trabajar en dos bandas de frecuencia, la de 2.4 GHz y la de 5 GHz, por lo que sería compatible con las ediciones previas a este estándar.

1.2.15 Protocolo 802.11p

Este estándar también conocido por el acrónimo WAVE (Acceso Vehicular para Ambiente Vehicular, por sus siglas en ingles) tiene la misión de definir mejoras para que pueda se usado en Sistemas de Transporte Inteligentes (ITS).

1.2.16 Protocolo 802.11r

Este estándar conocido también como *Fast BSS Transition* está enfocado a permitir una transición entre nodos menor a 50 ms, lo cual da una gran ventaja a aplicaciones de VoIP ya que permitiría a los clientes establecer la seguridad y la QoS en forma casi automática y sin cortes perceptibles.

1.2.17 Protocolo 802.11w

Este es un protocolo no concluido, busca mejorar la seguridad de los protocolos de autenticación y codificación sin necesidad de realizar cambios en el hardware; lo que extendería la protección brindada por el estándar 802.11i más allá de las tramas de gestión.

Al ser ratificado, proporcionará tres diferentes tipos de protección; el primero de ellos brindará seguridad a las tramas entre un punto de acceso y un cliente. El segundo método es la protección de tramas de gestión en modo *broadcast* que son utilizadas para ajustar las propiedades de la frecuencia de radio o para iniciar la medición, a este nivel ese estándar solamente protegería contra falsificaciones sin proporcionar confidencialidad. Por último, el tercer método de protección consistirá en la protección de tramas de disociación y desautenticación.

1.3 Modos de funcionamiento

Los componentes básicos de una red inalámbrica WI-FI son:

- **Puntos de acceso (PA),** también llamadas zonas locales de cobertura; éstos actúan como enlace entre la parte cableada y la inalámbrica y permiten el acceso a la red de las estaciones cercanas a ellos.
- **Los adaptadores de WLAN** o controladores de interfaz de red, que proporcionan la conexión inalámbrica a equipos terminales o estaciones, son básicamente tarjetas de red que cumplen con lo especificado en los estándares 802.11. Se encuentran en diferentes formatos, tales como tarjetas PCI, PCIMA, adaptadores USB y tarjetas Compact Flash.
- **Estaciones o equipo terminal**, son dispositivos que contienen un adaptador WLAN.

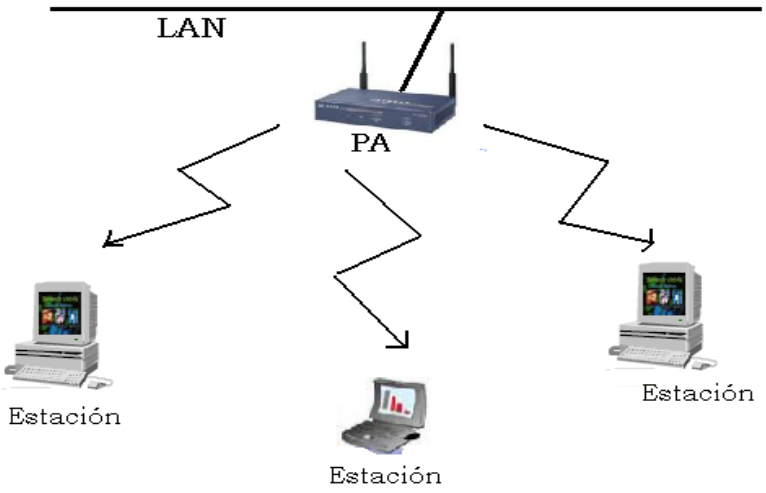
En lo referente a las topologías mismas, el estándar 802.11 define dos métodos distintos de funcionamiento que son:

- Modo Infraestructura
- Modo Ad-Hoc

1.3.1 Modo infraestructura

En esta topología es necesario contar con un punto de acceso conectado a la parte cableada de la red que lo convierte prácticamente en un puente entre la red cableada y la inalámbrica. Este es el elemento centralizado que se encarga de controlar los accesos de las diferentes estaciones en el área de cobertura y dirigir los datos hacia y desde la red cableada.[6]

Figura 4. **Red inalámbrica modo infraestructura**



La desventaja principal de un punto de acceso es que, el hecho de ser un medio compartido reduce la capacidad del canal en forma proporcional al número de clientes. Su alcance va desde 20 a 100m en interiores, y en exteriores varia entre 200 m y algunos kilómetros dependiendo de la antena utilizada.

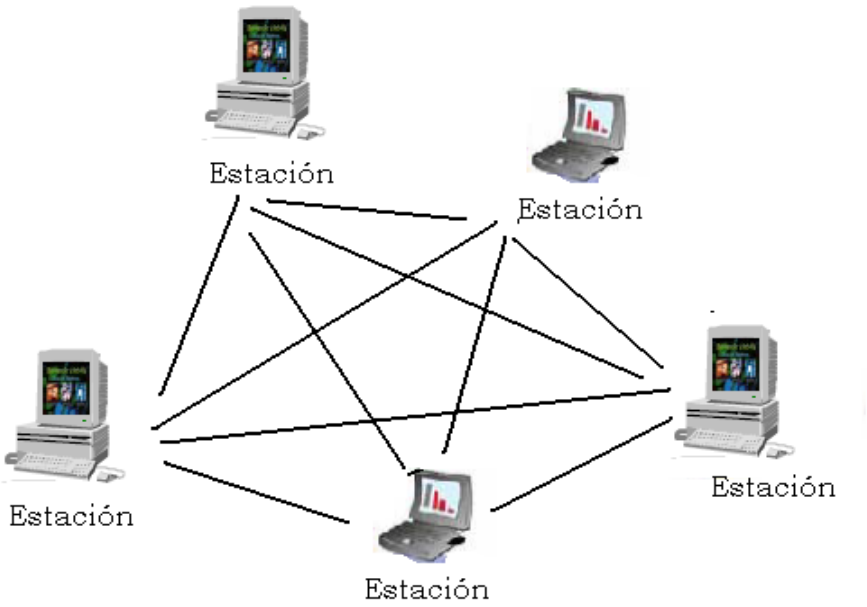
Es posible reunir varios puntos de acceso por medio de una conexión llamada Sistema de Distribución o DS y de esa manera los puntos de acceso conectados entre sí proporcionan una célula de cobertura, la cual amplía la cobertura a través del solapamiento; así, cuando un usuario se mueve, el adaptador de su equipo puede cambiarse a otro PA sin perder la conexión consiguiendo así el efecto de una cobertura celular como la dada en la telefonía móvil. Los puntos de acceso de un DS se comunican entre si para intercambiar información acerca de sus estaciones y para verificar su volumen de tráfico; si una estación está dentro del rango de varios puntos de acceso ésta elegirá a cual le conviene conectarse.

1.3.2 Modo ad-hoc

En esta topología no se requiere de puntos de acceso, ya que los dispositivos interactúan unos con otros permitiendo la comunicación directa entre dispositivos. Esta característica brinda una ventaja económica a las redes y puede ir creciendo a medida que se incorporen nuevos elementos siempre y cuando estén en el mismo espacio de cobertura y tengan la misma identificación de red. A esta topología también se le conoce como red "punto a punto".[7]

En esta red debe haber al menos dos estaciones para poder funcionar. Además todas las estaciones que deseen conectarse a la red deben operar en el mismo rango de frecuencias; de lo contrario, aunque se puedan ver, no van a poder interactuar entre ellas.

Figura 5. **Red inalámbrica modo ad-hoc**



1.3.3 Otras topologías

La mezcla de las dos topologías anteriores es conocida como Red Mesh o Red de Acoplada. Básicamente son redes con topología de infraestructura que permite a dispositivos que están fuera del rango de cobertura del PA a unirse a alguna tarjeta de red que se encuentre en su mismo rango de cobertura, siempre y cuando esta se encuentre directa o indirectamente ligada al rango de cobertura del PA. [8]

Este tipo de red es tolerante a fallos, ya que la caída de un solo nodo no implica que toda la red caiga.

1.4 Ventajas y desventajas de las redes WI-FI

Como cualquier tipo de red, las redes WI-FI poseen una serie de ventajas que pueden ser mencionadas, siendo las más importantes las siguientes:

- La comodidad provista por una red inalámbrica es superior a las redes cableadas debido a la movilidad que poseen.
- Debido a que la WI-FI Alliance asegura la compatibilidad de dispositivos, cualquier estación WI-FI puede trabajar en los diferentes países alrededor del mundo, contrariamente a los teléfonos celulares.
- Una vez configuradas, las redes WI-FI permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, no así en la tecnología por cable.[9]

- WI-FI usa el espectro de radio no licenciado y no requiere aprobaciones reguladoras porque usa la banda 2.4 GHz que es libre en casi todos los países del mundo.

Entre las desventajas que estas redes WI-FI presentan, las más importantes son:

- La pérdida de velocidad debido a interferencias.
- La banda de 2.4 GHz no requiere licencia, pero está por debajo de los 100mW, lo que la hace más susceptible a interferencias; además muchos otros dispositivos operan en el mismo rango de frecuencias, tales como los hornos de microondas, los módulos *bluetooth* y los teléfonos inalámbricos.
- El consumo de electricidad es bastante alto comparado con otros estándares, haciendo la vida de la batería corta y calentándola también.
- La mayor desventaja consiste en que la seguridad disminuye notablemente debido a la falta de medios físicos que detengan la intromisión de *hackers.*

2. SEGURIDAD EN REDES INALAMBRICAS

Las redes inalámbricas han proporcionado conectividad, flexibilidad y movilidad en el ámbito de la transmisión de datos y voz, sin la necesidad de onerosos y dificultosos cableados. El aire es el medio de trasmisión que estas redes utilizan para la propagación de las ondas de radio; y, es este mismo medio de transmisión la principal desventaja de estas redes ya que no existen barreras que detengan el paso de ondas en el aire, por lo que cualquier persona con conocimientos básicos de redes y un equipo adecuado puede "entrometerse" a la red.

Para los riesgos que corren las redes inalámbricas existen soluciones y mecanismos de seguridad, podría decirse que algunos son bastante seguros y otros se rompen fácilmente. A continuación se describen los mecanismos más conocidos.

2.1 Autenticación

La autenticación se usa para verificar que la información es autentica, es decir que viene de una fuente confiable y que no ha sido alterada.[10] En el caso de una red inalámbrica ésta corrobora si el cliente tiene permiso para accesar al sistema o no.

Para prevenir que un usuario no autorizado ingrese a la red, se puede ajustar el *router* para permitir únicamente conexiones de tarjetas de red inalámbricas autorizadas.

Cada equipo tiene una dirección MAC (Control de acceso al medio, por sus siglas en inglés) propia que la identifica; entonces el *router* autenticará solamente aquellas redes con una tarjeta de red preautenticada, lo que protegerá la red contra usuarios que tratan de accesar al sistema estando dentro del perímetro de cobertura.[11]

El proceso de autenticación puede ser llevado a cabo por dos métodos: la autenticación de sistema abierto (OSA) y la autenticación de clave compartida. Para ambos casos el cliente debe conocer cual es el identificador de conjuntos de servicios (SSID).

En el primer caso, autenticación de sistema abierto, en realidad no se autentica sino que solamente se validan las identidades de los usuarios por medio del intercambio de mensajes entre clientes y puntos de acceso.

En el caso de la autenticación de clave compartida, se comprueba si el cliente conoce un secreto compartido, el proceso básicamente es que el cliente solicita la autenticación y el punto de acceso responde enviando un cifrado WEP; el cliente puede descifrar y responder si y solo si conoce la contraseña WEP correcta. Cualesquiera de los dos procesos de autenticación puede ser aplicado, pero la autenticación de clave compartida es más eficaz[12].

2.1.1 Servidor Radius[13]

Radius es un acrónimo de *Remote Authenticacion Dial-In User Server* (Servicio de Usuario de Acceso Telefónico de Autenticación Remota). Este es un servidor que permite administrar de manera central cuentas de usuarios y permisos de acceso relacionados.

Al realizarse una conexión a Internet con un proveedor de servicios, ya sea por Modem, Ethernet o WI-FI se envía un nombre de usuario y una contraseña que es transferido a un servidor de acceso de red, éste lo redirige al servidor RADIUS que comprueba si la información es correcta para así autorizar el acceso.

2.2 Encriptación

La acción de codificar la información para que no pueda ser entendida por cualquier persona es llamada encriptación, aunque algunas personas prefieren llamarlo cifrado.

Los sistemas de encriptación en redes pertenecen a dos categorías[14]:

- Encriptación de clave simétrica, y
- Encriptación de clave pública.

En la encriptación de clave simétrica cada estación tiene una clave secreta con la que encripta cada paquete de información antes de ser enviada a otra estación o al punto de acceso, cabe mencionar que tanto las otras estaciones de la red como el punto de acceso deben conocer esta clave secreta.

La encriptación de clave pública es en realidad una combinación de clave privada y una clave pública; la clave privada solamente es conocida por la estación que envía el mensaje; mientras que la clave pública es enviada por la propia estación a las estaciones o el punto de acceso con las que desea comunicarse.

Para poder descifrar estas encriptaciones, cada estación debe usar la clave pública que le enviaron y su propia clave privada.

Los *routers* inalámbricos brindan niveles medianos de encriptación que altera el orden de los datos y los hace imposibles de leer para cualquiera que trate de acceder a la red sin autorización, solamente los usuarios autorizados pueden entonces ver y usar la información; lastimosamente la mayoría de usuarios no activan esta encriptación en sus *routers* debido a que no saben que éstos tienen un sitio WEB interno que permite configurar la encriptación fácilmente.

La mayoría de estos *routers* inalámbricos ofrecen una encriptación de 64 y 128 bits con una clave de encriptación especificada por el usuario que hace ininteligible los datos para usuarios no autorizados, pero, es necesario que los usuarios que van a decodificar estos mensajes tengan esta clave; por lo que la mayoría de usuarios prefiere deshabilitar esta opción.[15]

2.3 Lista de control de acceso

El control de acceso se da por medio de una lista de permisos de acceso llamada ACL (Lista de Control de Acceso) basada en las direcciones MAC de los dispositivos autorizados para conectarse a la red inalámbrica, estas listas controlan y filtran el flujo del trafico, ya sea permitiéndolo o denegándolo de acuerdo a alguna condición en su configuración. Las interfaces de configuración de los puntos de acceso son las que permiten mantener esta lista de permisos de acceso.[16]

Este método también es conocido como Filtrado de Direcciones MAC, ya que las direcciones que no se encuentren en la lista no podrán acceder a la red. A simple vista parecería que este mecanismo es bastante bueno, pero tiene sus desventajas, entre ellas[17]:

a) Si hay muchos puntos de acceso en la organización se podrían cometer errores al teclear las direcciones MAC en todos los puntos, por lo que los usuarios "legales" podrían ser rechazados.

b) Con muchos puntos de acceso en un sistema, teclear Direcciones MAC en cada uno de ellos resulta ser muy trabajoso, ya que por cada adición de equipo a la red habría que añadir su Dirección MAC en cada punto de acceso.

c) La transmisión en Wi-Fi se hace por medio de paquetes, y en muchos de estos paquetes la Dirección MAC es enviada para permitir el ingreso del paquete de datos a la red. Esta dirección no va encriptada por lo que un *hacker* puede capturarla e inclusive imitarla.

d) Si un equipo se pierde, la persona que lo encuentre podrá tener libre acceso a la red ya que la Dirección Mac es una característica del dispositivo o hardware y no del usuario.

2.4 WEP

Es un acrónimo de *Wired Equivalent Privacy* (Privacidad Equivalente a Cableado); su objetivo es garantizar que los sistemas WLAN dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio.

Este cifrado de trama de datos se lleva a cabo conjuntamente con un algoritmo llamado RC4[1] para crear claves de cifrado 64 bits. Estas claves están compuestas por un vector de inicialización (IV) y una clave secreta.

WEP también proporciona dos tipos de autenticación; de sistema abierto y de clave compartida. En el primer caso, todos los usuarios tienen permiso para acceder a la WLAN; en el segundo, se utiliza una clave secreta compartida entre todas las estaciones y los puntos de acceso del sistema.

El método de autenticación por medio de clave compartida está dividida en cuatro etapas:

1. El cliente envía el pedido de autenticación al Punto de Acceso.
2. El Punto de Acceso envía de vuelta un texto modelo

[1] Sistema de cifrado de flujo que genera un flujo pseudoaleatorio de bits que se combina con el dato a cifrar por medio de la función XOR.

3. El cliente tiene que cifrar el texto modelo usando la clave WEP ya configurada y reenviarlo al Punto de Acceso pidiendo nuevamente la autenticación.

4. El Punto de Acceso deberá descifrar el texto codificado y compararlo con el texto modelo que había enviado.

5. Si la comparación resulta exitosa (ambos datos iguales) el Punto de Acceso envía una autorización, en caso contrario deniega el acceso.

Después de realizar está autenticación, WEP puede ser usado para cifrar los datos.

Para cifrar los datos, WEP utiliza una clave secreta entre una estación inalámbrica y un punto de acceso; todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida.

Para proteger el cifrado contra modificaciones no autorizadas mientras esta en tránsito, se aplica un algoritmo de comprobación de integridad llamado CRC-32[2] lo que genera un dato llamado Valor de Comprobación de Integridad (ICV).

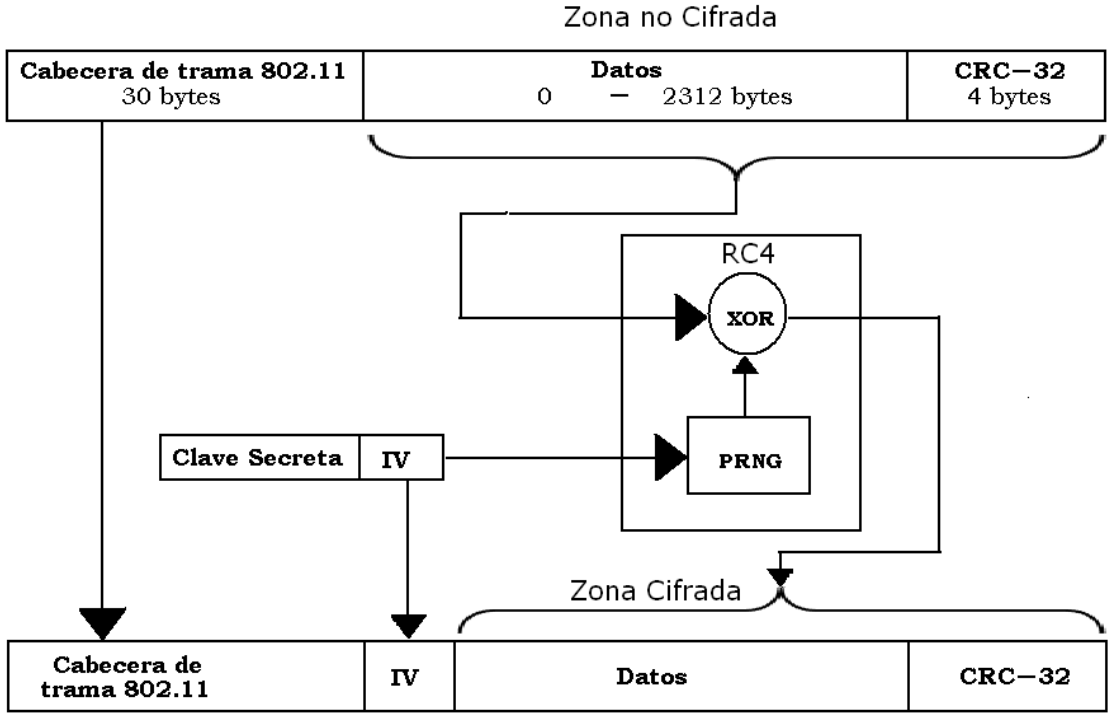
El valor del ICV se añade en el texto cifrado y se envía junto con el vector de inicialización, el receptor combina el texto cifrado con la clave para recuperar el dato.

[2] Comprobación de Redundancia Cíclica de 32 bits.

El proceso de encriptación de WEP es el siguiente:

- Se calcula el CRC-32
- Se concatena la clave secreta y el vector de inicialización (Clave + IV)
- El PRNG (*Pseudo-Random Number generator*, Generador de números pseudoaleatorios) del RC4 genera una secuencia de caracteres de la misma longitud del CRC-32.
- Se calcula la XOR de todos los bits de datos y CRC-32 con el dato creado por el PRNG lo que da como resultado el mensaje cifrado.

Figura 6. **Algoritmo de encriptación WEP**



Fuente**: http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml**

La desencriptación se realiza calculando nuevamente la XOR de los datos recibidos y la clave secreta unida con el vector de inicialización.

Los principales problemas o defectos que encontramos al implementar WEP son los siguientes:

- Es necesario ingresar manualmente la clave secreta en todos los elementos del sistema.
- En algún momento del envío y recepción de datos entre elementos del sistema, el vector de inicialización podría repetirse, lo cual no solamente crearía un conflicto, sino que también los *hackers* podrían analizar los paquetes enviados y descifrar la codificación; inclusive hay programas en Internet que pueden realizar está función, son llamados WEP *Crackers*.

A pesar de estos inconvenientes, WEP es uno de los protocolos de cifrado más populares debido a que es fácil de configurar y cualquier sistema o equipo con el estándar 802.11 es compatible con éste. De cualquier manera WEP también ha evolucionado y ahora existen otras alternativas, tales como: WEP2 que usa un cifrado y un vector de iniciación de 128 bits en lugar de 64, WEP Plus (Wep +) que simplemente mejora la generación pseudoaleatoria de los vectores de iniciación y por último encontramos el WEP Dinámico, el cual utiliza dos claves: la primera llamada de Asignación, que es compartida entre una estación y el punto de acceso y, la segunda, llamada Predeterminada que es compartida por todas las estaciones.

2.5 Estándar IEEE 802.1x

Es una norma de la IEEE ratificada en Junio de 2001 que fue diseñada para mejorar la seguridad en redes inalámbricas. Este estándar está basado en el control de acceso a puertos, el cual autentica al usuario y no al dispositivo que desea establecer conexión; por lo tanto el puerto no se abrirá ni permitirá la conexión si el cliente no está autenticado y autorizado por una base de datos existente en el servidor de autenticación.

En este estándar se definen tres elementos básicos del sistema que son:

1. **Servidor de autenticación**. Llamado también NAS (*Network Autenticación Service*, Servidor de autenticación de red). Es el encargado de verificar la identidad del usuario y otorgar el acceso según sus credenciales.

   También puede almacenar información y hacer un seguimiento de ésta; por ejemplo, tiempo de conexión, datos transferidos, intentos de conexión, etc. Este servidor generalmente es un Servidor RADIUS que puede generar claves dinámicas y cambiarlas cada cierto tiempo dependiendo de la programación definida por el administrador.

2. **Autenticador**. Es el dispositivo que recibe la información y la traslada al servidor, normalmente esta función es llevada a cabo por el punto de acceso.

3. **Suplicante**. Como su nombre lo indica es el que "suplica" o solicita la autenticación. Esta tarea es llevada a cabo por un software "cliente" que está instalado en el dispositivo.

Hay diversos tipos de suplicantes; los más simples pueden ser descargados de Internet en forma gratuita, como *SecureW2*, o vienen en el CD del software del punto de acceso; pero, si el usuario lo prefiere, existen suplicantes bastante complejos y multifuncionales que pueden ser adquiridos comercialmente y es necesario pagar una licencia para ser instalados en el equipo.

Una red segura que aplica el estándar 802.1x funciona de la siguiente manera:

1. El usuario envía una solicitud de conexión.
2. El controlador de acceso recibe la solicitud y envía una solicitud de autenticación.
3. El usuario envía la respuesta al controlador de acceso.
4. El control de acceso envía la respuesta del usuario al servidor de autenticación.
5. El servidor de autenticación envía un "*challenge*" o "desafío" al controlador de acceso que a su vez lo envía al usuario.
6. Si el cliente no puede evaluar el "desafío" se envían otros "desafíos" hasta que el cliente pueda evaluarlo.
7. El usuario responde el "desafío". Si la identidad es correcta, se aprueba el ingreso a la red, de lo contrario se envía un mensaje de denegación de servicio.

La autenticación en sí es llevada a cabo con base en el protocolo EAP (*Extensible Authentication Protocol*-RFC 2284, Protocolo de autenticación extensible) que cuenta con cinco versiones diferentes:

- **EAP-LEAP**. Desarrollado y patentado por CISCO, emplea autenticación mutua fuerte, credenciales de seguridad y claves dinámicas de encriptación. Su principal desventaja es que requiere infraestructura CISCO y un servidor RADIUS LEAP *Aware* exclusivamente; además es vulnerable a "ataques diccionario"[3].
- **EAP-TLS**. Desarrollado por Microsoft y, al igual que al anterior, emplea autenticación mutua fuerte, credenciales de seguridad y claves dinámicas de encriptación. Entre sus limitaciones principales está que necesita un Certificado Digital en cada dispositivo cliente y solo soporta bases de datos de Microsoft.
- **EAP-TTLS**. Desarrollado por *Funk Software* y Certicom (Programadores independientes); emplea también autenticación mutua fuerte, credenciales de seguridad y claves dinámicas; además funciona en todas las plataformas y es compatible con los otros EAP. Solo requiere Certificados Digitales con servidores RADIUS.
- **EAP-PEAP**. Es un proyecto desarrollado en conjunto por Microsoft, CISCO y RCA; no requiere certificados digitales y es más flexible que el LEAP y el TLS pero similar al TTLS. Existen dos versiones, una de Microsoft y una de CISCO pero ambas son compatibles. La versión de Microsoft viene incluida en Windows XP y Windows 2003.

[3]Método de cracking que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario. Estos tienen pocas probabilidades cuando las contraseñas combinan mayúsculas, minúsculas y números.

- **EAP-FAST**. Es el más reciente de los protocolos EAP, desarrollado por CISCO. Al igual que el PEAP, no requiere certificados digitales en los clientes y es compatible con LEAP.

Una vulnerabilidad detectada de este estándar es que el 802.1x autentica únicamente al inicio de la sesión; por lo que después de iniciada la sesión la red es susceptible a ataques lo que hace necesario aplicar otro método de seguridad en conjunto con éste.

2.6 WPA / WPA2[18]

Es el acrónimo de *WI-FI Protected Access*, Acceso protegido WI-FI que fue diseñado para proteger las redes inalámbricas corrigiendo las deficiencias de WEP, ya que presenta unas bastante serias; principalmente en el vector de inicialización. Fue diseñado para utilizar un servidor de autenticación que distribuye claves diferentes a cada usuario. La información es cifrada utilizando el algoritmo RC4 con una clave de 128 bits y un vector de inicialización de 48 bits.

Entre las ventajas más importante de WPA podemos mencionar las siguientes:

- Se implementa el protocolo de integridad de clave temporal (TKIP) que cambia las claves dinámicamente a medida que el sistema es utilizado.
- Mejora la integridad de la información cifrada ya que implementa un código de integridad del mensaje (MIC) llamado también Michael.

- Incluye un cortador de tramas para proteger el sistema contra ataques de repetición. Las redes WPA se desconectan durante 60 segundos al detectar dos intentos de ataque durante 1 minuto.

WPA2 implementa elementos obligatorios del estándar 802.11i. En particular introduce el protocolo de encriptación llamado CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*, Protocolo de autenticación de código en modo contador y mensaje encadenado al cifrado por bloques) que es basado en el algoritmo AES[4].

Este algoritmo es considerado completamente seguro ya que integra llaves de 128, 192 o 256 bits con un bloque fijo de 128 bits; hasta el año 2005 no se había logrado ningún ataque exitoso en contra de él.

[4] AES es el acrónimo de Advanced Encryption Standard (Estandar de Encriptación Avanzado); es un esquema de cifrado por bloques

3. VULNERABILIDADES DE REDES WI-FI

Absolutamente todos los equipos conectados a una red pueden ser vulnerables a ataques; más aun si está en una red no cableada, debido a que la transmisión de datos se hace a través del aire.

A las personas que realizan estos ataques se les conoce como piratas informáticos o "*hackers*", los cuales utilizan software especial creado por "crackers" para desproteger una red y analizar o robar información.

Los ataques informáticos pueden dividirse en dos grupos: el primer grupo es conocido como "ataques pasivos", ya que no modifican datos, solamente espían y obtienen información. Al segundo grupo se le conoce como "Ataques Activos" debido a que en este caso la información es alterada, modificada o interrumpida.

3.1 Ataques pasivos[19]

Este tipo de ataque ocurre cuando un usuario no autorizado accede a la red para espiar información y, aunque no la modifica, la guarda para analizarla y poder realizar un ataque activo más tarde, o también por simple curiosidad sobre aspectos confidenciales.

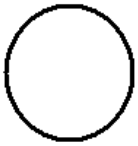
Este tipo de ataque es muy difícil de detectar por la no alteración de datos, pero, como administradores de la red, podemos darnos cuenta de alguna intrusión analizando el consumo de recursos; por ejemplo una reducción del ancho de banda, un incremento del tiempo de respuesta de los equipos, tiempos de carga y descarga, etc.

Los ataques pasivos más comunes son los siguientes:

3.1.1. *Warchalking / Wardriving*

El detectar redes inalámbricas se ha convertido en un pasatiempo muy popular, el *warchalking* consiste en recorrer lugares con una computadora portátil o un PDA compatible con WI-FI con el fin de buscar puntos de acceso inseguros o con fácil ruptura de seguridad; al encontrar estos puntos se dibuja (normalmente con yesos) uno de los tres símbolos siguientes:

(Dos semicírculos opuestos) Identifica a una red abierta con total acceso.



(Círculo) Indica que existe una red abierta, pero tiene unas pocas barreras de seguridad que, en general, no representan gran desafío.

(Círculo con una W dentro) Este símbolo indica que hay una red completamente segura, y si se quiere acceder a ella es necesario ser un *hacker* muy experimentado.

El *wardriving* es básicamente lo mismo, pero se realiza desde un automóvil y se utiliza un GPS para obtener las coordenadas de los puntos de acceso de la red.

Existe un software muy popular para realizar *warchalking* y *wardriving*, llamado NETSTUMBLER; éste es un software de descarga libre, su función es buscar datos de acceso en los adaptadores de redes inalámbricas que utilizan un *chipset*[5] Hermes para detectar puntos de acceso dentro de su rango de operación

3.1.2. *Sniffing* o intercepcion de datos

Consiste en "escuchar" las transmisiones de los usuarios de una red; de hecho, cualquier persona con el hardware y software adecuado dentro del área de cobertura de un punto de acceso puede potencialmente escuchar las comunicaciones de la red.

Los programas *sniffers* capturan, interpretan y almacenan los paquetes de datos para analizarlos posteriormente; por supuesto que nosotros mismos podemos tener un programa *sniffer* en nuestra red para monitorearla, ya que nos permite analizar la red, detectar intentos de intrusión, filtrar contenido sospechoso, etc. El problema se da cuando alguien externo a nuestra red la esta monitoreando, seguramente con la intención de obtener *passwords*, usuarios, direcciones electrónicas, información monetaria, etc.

[5] Conjunto de circuitos integrados que controlan funciones en computadoras o dispositivos electrónicos.

Entre los programas *sniffer* mas populares esta el SpyNet, que contiene un analizador de tráfico y un analizador de datos, éste puede reproducir contraseñas de e-mails, además encuentra la dirección MAC de cada equipo, el protocolo de transferencia y los programas utilizados en el equipo. Otro programa *sniffer* es el Ethereal , el cual es gratuito y de código abierto. El WinSniffer es otro de estos programas pero tiene una versión demo y una versión paga, en la versión demo podemos descubrir usuarios, y en su versión pagada, nos muestra la lista de usuarios y sus contraseñas. El AirCrack es también uno de los programas *sniffers* mas utilizados porque captura paquetes para romper el cifrado WEP y además permite la inyección de tráfico en la red.

El *sniffing* puede ser detectado en un ambiente Windows utilizando el programa AntiSniff, y, en ambiente Linux podemos chequear la red con el comando ifconfig. Estos programas detectan interfaces de red que estén trabajando en modo promiscuo[6] y nos envía una advertencia de ello.

3.2. Ataques activos

Se dan cuando alguien no autorizado modifica o altera el contenido de la información y/o impide la utilización de la misma. Los más comunes son:

3.2.1. Enmascaramiento o suplantación

Se le llama también robo de identidad, imitación o falsificación. En este caso el *Hacker* se hace pasar como un usuario autorizado o suplanta a un cliente que se encuentra desconectado en ese momento.

[6] Se le llama Modo Promiscuo o Modo Monitor cuando un equipo conectado a la red captura todo el tráfico que circula en la red y no solamente el que va dirigido al equipo en si.

Este ataque también se puede dar reemplazando un Punto de Acceso y haciendo creer que este punto de acceso pirata es legítimo. Los ataques tipo suplantación más usados son los siguientes:

3.2.1.1 Secuestro de sesión

En este ataque el *hack*er monitorea la red para recopilar usuarios, claves, direcciones MAC, SSID y elige un usuario X para enviarle un ataque de denegación de servicio y así desconectarlo; luego, el *hacker* se conecta a la red utilizando la información detectada del usuario eliminado. Comúnmente el secuestro de sesión no dura mucho tiempo, pero sí puede ser hecho a varios usuarios en la misma red. Los *switches* WLAN nos ayudan a descubrir este tipo de ataque.

3.2.1.2 Suplantación de dirección MAC

Este ataque se da más que todo cuando la red está protegida únicamente por la técnica de filtrado de direcciones MAC[7] ya que es más fácil para el usuario detectar las direcciones MAC autorizadas y así utilizarlas en su equipo para suplantar una verdadera. Esta suplantación puede hacerse a través de software adecuado tal como Ethereal, NetStumbler o con un programa llamado Air Jack que puede ser descargado de forma gratuita en la página http://sourceforge.net/projects/airjack/.

[7] Ver el tema 2.3 Lista de Control de Acceso.

3.2.2. Denegación de servicio (DoS)

Estos ataques se hacen con el objetivo de volver inútil la red o para sacar clientes autorizados y así suplantarlos; es difícil detectarlos y erradicarlos, ya que duran poco tiempo y solamente es posible identificarlos en tiempo real, a diferencia del ataque de enmascaramiento, ya que éste se puede detectar analizando el comportamiento del punto de acceso. Las formas más comunes de denegar servicio son las siguientes:

3.2.2.1 Saturar el ambiente con ruido de RF

La relación señal/ruido en todos los puntos de una red inalámbrica debe ser mayor o igual a 0.3 (30%) pues de lo contrario el ruido prácticamente anulará la señal y la red será inutilizable. Este ataque básicamente se da inyectando ruido RF en nuestro aire por medio de un generador de ruido RF o por medio de microondas.

3.2.2.2 Torrente de autenticaciones

Este ataque se da cuando el *hacker* le envía al servidor Radius muchas peticiones de autenticación falsas de manera repetitiva y simultánea; entonces la red se mantiene ocupada tratando de autenticar estas peticiones a este usuario falso, por lo tanto lo usuarios reales no tienen la oportunidad de autenticarse y no podrán acceder a la red.

3.2.2.3 Modificación de paquetes WPA

El chequeo de integridad de paquetes del WPA permite sin querer los ataques de Denegación de Servicio, ya que si el *hacker* altera un par de paquetes, el TKIP-WPA detecta que 2 o mas paquetes han sido modificados, entonces asume que lo están atacando y desconecta automáticamente a todos sus usuarios por un momento; al volver a conectarlos la red, el *hacker* puede alterar otra vez un nuevo par de paquetes y así lograr otra desconexión. El Air-Jack es el programa más usado para este tipo de ataque.

3.2.2.4 *Signaling* DOS

Este ataque finaliza sesiones móviles activas en la red. Comprende el envío de pequeñas cantidades de datos para reiniciar una sesión después de que ésta haya sido liberada. El ataque de bajo volumen puede crear congestión en el controlador de radio de la red (RNC). Sobrecargar el RNC resulta en una denegación de servicio para el usuario.

3.2.2.5 Drenado de batería

Este ataque envía paquetes a un cliente para evitar que éste entre en modo suspensión y así consume recursos de radio y agota las baterías de los dispositivos.

3.2.3. Retransmisión

A este ataque también se le conoce como Hombre-en-el-medio o MITM por sus siglas en inglés (*Man-In-The-Middle*). Se da cuando el *hacker* se ubica en el medio de la comunicación entre el punto de acceso y el usuario. Para esto el *hacker* debe haber analizado el tráfico previamente para conocer todos los datos del punto de acceso que quiere simular ser (el SSID, la dirección MAC, DHCP, etc.) y también los de los clientes de la red. Al emular el punto de acceso, el *hacker* puede bloquear la información que el cliente transmite o modificarla para engañar al receptor.

3.3. Problemas concretos de seguridad[20]

Los problemas a los que se enfrenta día a día las redes inalámbricas son los siguientes:

3.3.1. Puntos ocultos

Estos puntos ocultos existen porque los usuarios de una red privada empresarial muchas veces instalan sus propios puntos de acceso y si esta situación no es controlada por un administrador de red, le estaríamos dando un acceso ilimitado a cualquier *hack*er. El peor de estos casos es la situación en la cual un intruso (y no un usuario autorizado) lo deja oculto y luego ingresa a la red desde cualquier ubicación cercana a la misma. La gran ventaja que queda de este problema es que es muy fácil su identificación siempre y cuando se propongan medidas de revisión y control periódicas específicas para toda la infraestructura WI-FI de la empresa como política de seguridad.

3.3.2. Falsificación de AP

Existen varios productos ya diseñados para falsificar AP, en la terminología WI-FI se les llama "Rogue AP" o Fake AP", el más común es uno llamado "FakeAP", que envía tramas con diferentes ESSID y diferentes direcciones MAC con o sin empleo de WEP. Se puede descargar de Http://www.blackalchemy.to/project/fakeap/ . Este es usado también para el ataque MITM.

3.3.3. Deficiencias en WEP

Actualmente es fácil encontrar programas que rompan el cifrado WEP debido a que el CRC32 tiene unas características especiales que le permiten detectar errores, pero deja abierta la posibilidad de manipular la información ya que matemáticamente es posible encontrar el CRC; por lo tanto el mensaje puede ser modificado, se hace el calculo del CRC y se le agrega al final del mensaje modificado y así el mensaje es tomado como real y no podrá detectarse esa alteración.

3.3.4. ICV independiente de la llave

El ICV se calcula antes de comenzar el proceso criptográfico, por lo tanto no depende de la clave ni del IV. El problema es que al reconocer el texto plano de un solo paquete encriptado con WEP, se posibilita la inyección de paquetes en la red.

3.3.5. Tamaño de IV demasiado corto

El IV tiene 24 bits de longitud (224 = 16.777.216) y viaja como texto plano. Un punto de acceso que opere con grandes volúmenes de tráfico comenzará a repetir este IV a partir de aproximadamente 5 horas. Esta repetición hace que matemáticamente se pueda operar para poder obtener el texto plano de mensajes con IV repetido (sin gran nivel de dificultad). El estándar especifica que el cambio de IV es opcional, siendo un valor que empieza con cero y se va incrementando en uno.

3.3.6. Deficiencias en el método de autenticación

Cuando el atacante captura el segundo y tercer mensaje de administración en un proceso de autenticación mutua entonces posee todos los elementos para autenticarse con éxito en una red, aún sin conocer el secreto compartido entre los puntos de acceso y el usuario. El segundo mensaje posee el desafío en texto plano y el tercero contiene el mensaje criptografiado con la clave compartida. Debe quedar claro que con esto solamente logra la autenticación en la red, más no el total acceso a ella.

3.3.7. Debilidades en el algoritmo *key scheduling* de RC4

Se ha demostrado que con sólo analizar la primera palabra de un *keystream* se puede obtener información de la clave secreta compartida.

El número de paquetes que se necesitan recolectar antes de descubrir un byte de la llave varía en función de en que valor se encuentre el contador de IV's de las tarjetas que se estén monitoreando. Hay 9.000 IV's débiles en los 16 millones de IV's posibles.

Anteriormente era posible adivinar la llave después de analizar unos 2000 o 4000 paquetes, pero ahora existen los programas Wepcrack y Airsnot que hacen el trabajo en unos pocos minutos y sin mayor esfuerzo, estos programas pueden ser descargados de http://wepcrack.sourceforge.net, www.uptodown.com/buscar/wep-crack, http://www.programas-gratis.net/b/wep-crack y http://airsnort.shmoo.com

3.3.8. Debilidad en WPA

Un estudio realizado por Robert Moskowitz, director de ICSA Labs, indica que el sistema utilizado por WPA para el intercambio de la información utilizada para la generación de las claves de cifrado es muy débil. Según este estudio, WPA en determinadas circunstancias es incluso más inseguro que WPE. Cuando las claves preestablecidas utilizadas en WPA utilizan palabras presentes en el diccionario y la longitud es inferior a los 20 caracteres, el atacante sólo necesitará interceptar el tráfico inicial de intercambio de claves. Sobre este tráfico, realizando un ataque tipo diccionario, el atacante puede obtener la clave preestablecida, que es la información necesaria para obtener acceso a la red. Es decir, a diferencia de WEP en que es necesario capturar un volumen significativo de tráfico para poder identificar las claves, en WPA únicamente se debe capturar el tráfico de intercambio de claves para poder realizar este ataque tipo diccionario.

No es un problema nuevo, pues fue apuntado durante la verificación inicial del protocolo. Es conveniente entonces utilizar claves largas y que incluyan caracteres especiales o que no sean palabras solamente; puede ser una mezcla de letras y caracteres que signifique algo para nosotros, pero nada especifico o entendible por otros.

4. PROTECCIÓN DE REDES WI-FI

La tecnología inalámbrica brinda muchos beneficios, ya que da más libertad para navegar en internet, permite compartir dispositivos, no ata a un escritorio en el trabajo, inclusive permite comer en un restaurante o tomarse un café mientras se revisa el correo electrónico o se navega por la red. Esta tecnología hace la vida más fácil, pero deja vulnerables a ataques de *hackers* que por una u otra razón desean investigar datos confidenciales.

4.1. Medidas de seguridad básicas en equipos[21]

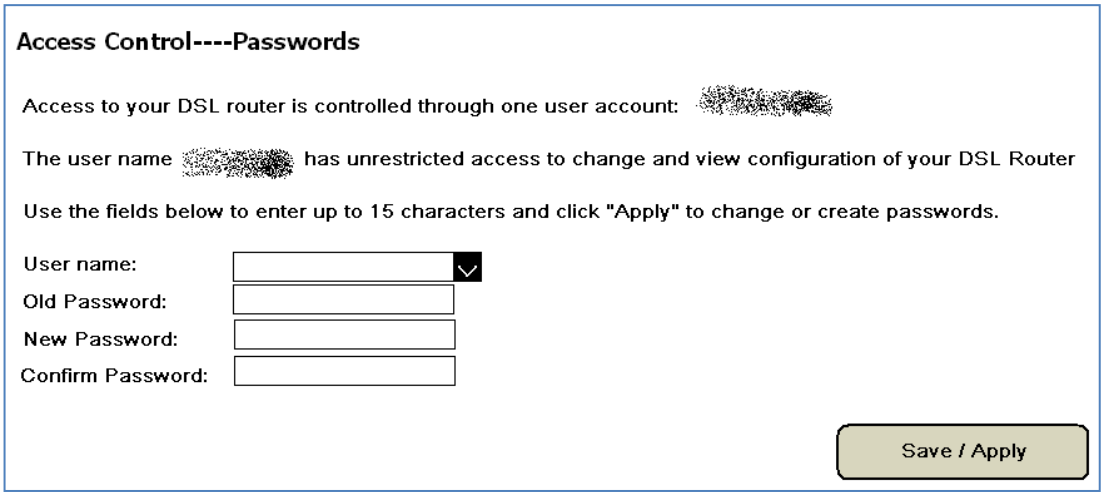
Tanto el administrador de la red como el usuario deben tomar algunas o todas las medidas de seguridad posibles para evitar ataques a la red. Las medidas mínimas de seguridad están descritas a continuación.

4.1.1. Cambiar la contraseña de fábrica

Este es el primer paso a realizar, ya que todos los productos de fábrica vienen con una contraseña estándar que es conocida e inclusive publicada en varias páginas Web; por ejemplo si se teclea en un buscador "*password router speedtouch*" se encuentra que su contraseña por defecto es 1234.

Al accesar a la configuración del router se puede cambiar su contraseña por defecto; hay que tomar en cuenta que no se debe crear claves obvias como el nombre, nombre del esposo, esposa o hijos, año de nacimiento, teléfono, etc.; tampoco escribir secuencias numéricas o alfabéticas como "12345" o "abcde". Lo mejor es crear claves alfanuméricas e intercalar letras mayúsculas, minúsculas y números.

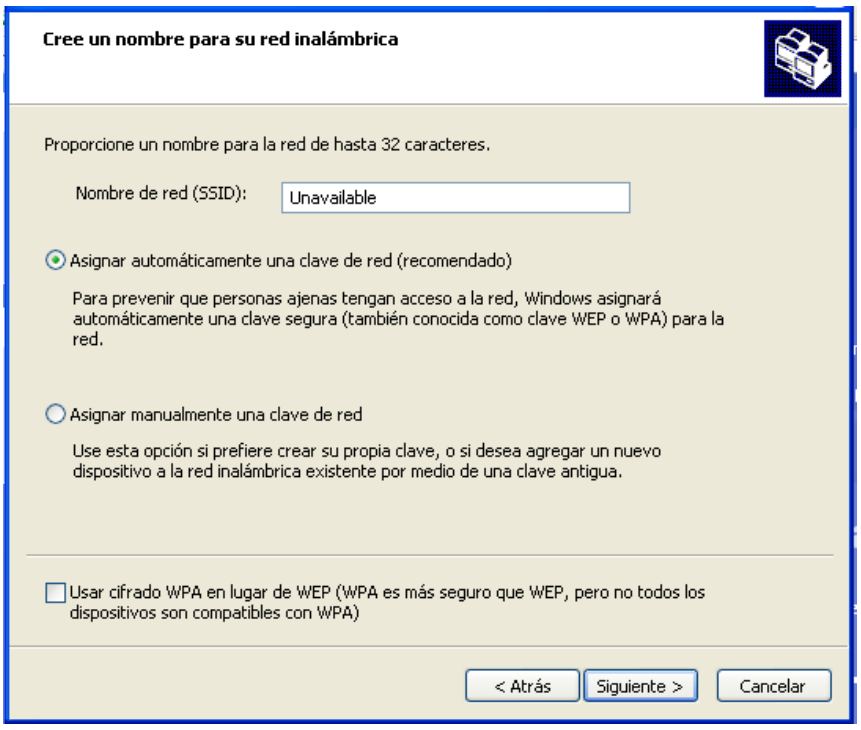
Figura 7. **Cambio de Contraseña en *Routers***



4.1.2. Modificar y ocultar el identificador de red SSID

El identificador de red SSID es el nombre de la red. Si estamos creando una red es preferible no usar nombres obvios como los descritos anteriormente; se debe escoger un nombre que no sea atractivo para los *hackers* y si es posible, que muestre indicios de un fallo simulado; podemos usar por ejemplo "Desconectado", "*Unavailable*", "Fuera_de_Línea", "Red_Abierta", etc. En la figura 8 se muestra el asistente de configuración de red inalámbrica de Windows con un ejemplo del Identificador SSID con fallo simulado.

Figura 8. **Asignación o cambio de nombre de la red**



Para ocultar este identificador únicamente se debe marcar en la casilla "Ocultar punto de acceso" (*Hide Access Point*) en la configuración del router o del punto de acceso.

4.1.3. Utilizar encriptación WEP

Hay que habilitar encriptación WEP tanto en el *router* como en la computadora. Podemos elegir una codificación de 44, 64, 76 o 128 bits (5, 10, 13 o 26 dígitos hexadecimales respectivamente). Por supuesto que si seleccionamos una codificación de 128 bits será más difícil para un intruso descifrar la clave de acceso.

Lo primero que se debe hacer es acceder a las propiedades de la red inalámbrica y seleccionar la opción "Asignar Automáticamente una clave de red", si se desea tener una clave propia se selecciona la opción "Asignar manualmente una clave de red" y en la siguiente pantalla se teclea la clave deseada como se muestra en la siguiente figura.

Figura 9. **Asignación manual de la clave WEP**

Es recomendable cambiar la clave de red cada cierto tiempo para reducir el riesgo de ataque, ya que si alguien analiza el tráfico de la red y captura paquetes de ésta podría descifrar la clave.

4.1.4. Encriptación WPA

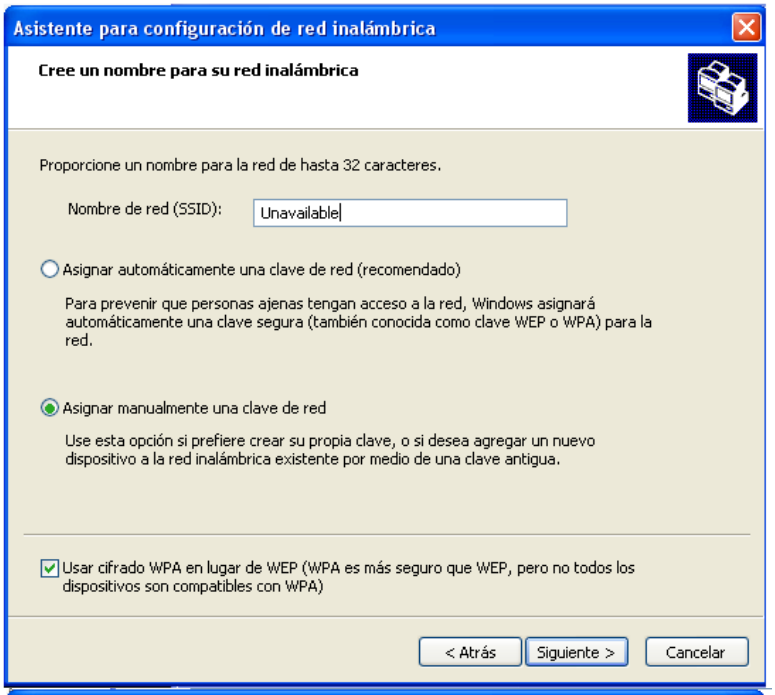
Es una opción bastante más segura que WEP ya que el cifrado es por medio de claves dinámicas que se calculan a través de una contraseña. Es importante recordar que la contraseña de la encriptación WPA, al igual que las anteriores, debe ser larga y compleja. También es recomendable cambiar la clave de red regularmente para reducir el riesgo de ataque a la misma.

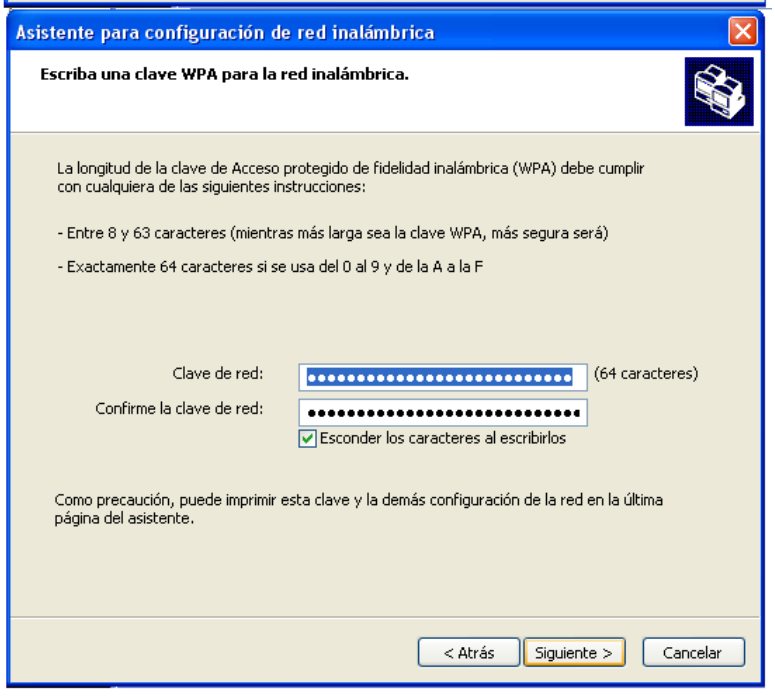
Para habilitar el encriptado WPA también se debe acceder a las propiedades de la red inalámbrica, pero ahora se selecciona la opción que habilita el cifrado WPA en lugar de WEP.

Como lo menciona la advertencia en el asistente de configuración de red inalámbrica, el problema de la encriptación WPA es que no todos los adaptadores de red inalámbricos o *routers* son compatibles con este tipo de encriptación. Lo más recomendable es buscar en la web las actualizaciones disponibles o "*codecs*" para los adaptadores de red y así descargarlas e instalarlas en la computadora. Otro punto importante es que debe de asegurarse de que la versión de Windows que se está utilizando admite la Encriptación WPA porque las versiones anteriores a Windows XP no lo hacen.

La siguiente figura muestra la habilitación del cifrado WEP y la asignación manual de su clave.

Figura 10. **Asignación manual de la clave WPA**



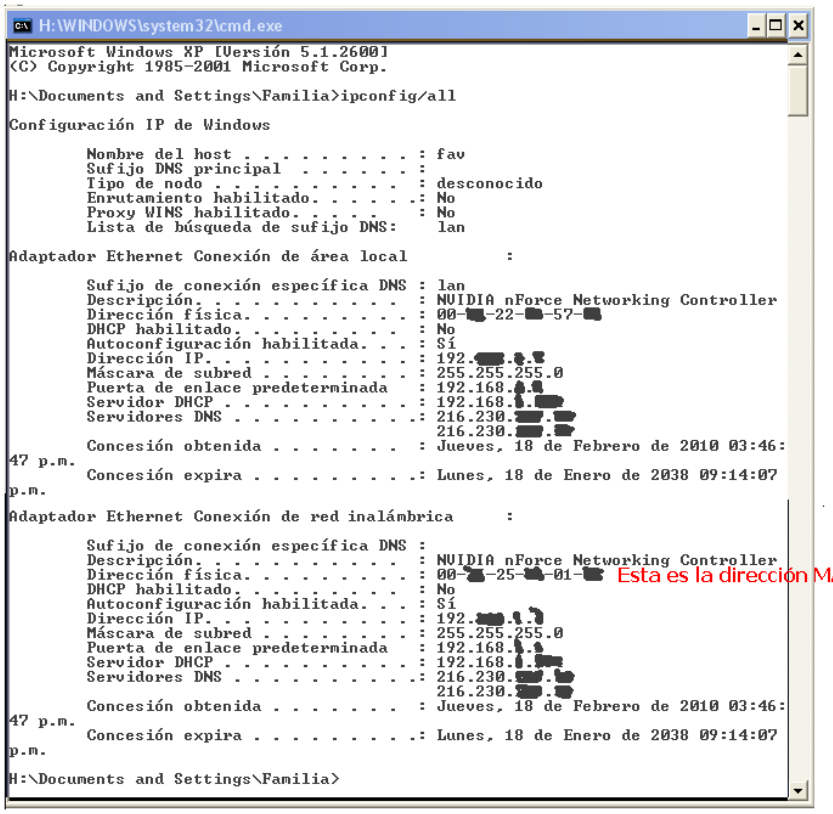


4.1.5. Activar el filtrado de direcciones MAC

Este filtrado se hace con el objeto de restringir los equipos que se conectarán a la red, pues como se sabe, las direcciones MAC son fijas y están grabadas en las tarjetas. La primera parte de ella identifica al fabricante y la última es el número secuencial asignado al equipo.

Para averiguar la dirección MAC del equipo se puede escribir el comando "ipconfig/all" en el símbolo del sistema. En la siguiente figura se muestra la información que devuelve este comando.

Figura 11. **Identificación de la dirección MAC del equipo inalámbrico**

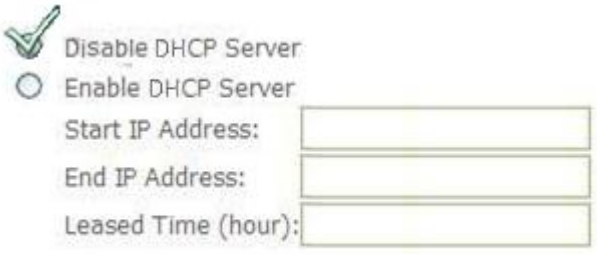


Cuando se tengan las direcciones MAC que se desean agregar a la red, se accesa al *router* o punto de acceso y se escribe en la lista de direcciones permitidas. Inclusive se puede escribir una lista de direcciones MAC no permitidas si fuera necesario denegar el acceso a algunos equipos.

4.1.6. Desactivar el servidor DHCP

Debido a que el DHCP integrado en el *router* es el encargado de distribuir las direcciones IP a cada PC, entonces un buen método para detener a alguien que desee irrumpir nuestra red es reducir el número de direcciones IP únicamente a las que realmente van a acceder a la red. Para desactivar el servidor DHCP se debe marcar la casilla "*Disable DHCP Server*" en el *router*, pero la dirección IP, la puerta de enlace de datos y los identificadores se deben ingresar directamente en cada equipo de la red.

Figura 12. **Deshabilitación del servidor DHCP en el *router***



4.1.7. Deshabilitar la red

Esta medida puede ser tomada si la red inalámbrica no se va a utilizar durante cierto tiempo.

4.2 Medidas de seguridad aplicadas por proveedores de servicio

Actualmente es posible encontrar redes WI-FI abiertas, por lo que el único requisito para conectarse a ellas es tener una computadora portátil, un PDA o un teléfono celular con el *hardware* adecuado; ejemplos de estas redes abiertas pueden encontrarse en el Parque Central de Antigua Guatemala, el campus de la Universidad de San Carlos, restaurantes como McDonalds, Pollo Campero o Nais, por mencionar algunas. Al utilizar en estos lugares el servicio de internet se puede ser blanco de ataques, principalmente de *sniffing,* ya que la única medida de seguridad que aplican en estas redes es que la zona de cobertura se limita únicamente al área del local.

Las empresas de telefonía que proveen este tipo de servicio de red inalámbrico y las grandes corporaciones que poseen redes privadas tales como instituciones financieras, bancarias, ingenios y empresas con un banco de datos o "secretos" importantes, no están anuentes a brindar la información sobre los mecanismos de seguridad que utilizan en sus redes; por el temor de ser blanco de algún tipo de ataque informático diseñado especialmente para romper las barreras de seguridad que aplican.

Sin embargo, con el fin de conocer e investigar las medidas de seguridad aplicadas en una red privada; el administrador y encargado de la red inalámbrica interna del Liceo Guatemala, Pedro Arrivillaga, amablemente respondió las siguientes preguntas:

Pregunta No. 1. ¿Por qué acá en el Liceo Guatemala utilizan una red segura y no una red abierta?

Respuesta:

Una red segura permite que solamente ciertas personas a través de ciertos equipos se puedan conectar. Las personas a quienes se les ha dado el privilegio de conectarse lo hacen a través de una clave de acceso o con la habilitación de su computadora en la lista de direcciones MAC en el punto de acceso. De esta forma también es posible salvaguardar la información que reside en los equipos conectados.

Esto no quiere decir que el método sea 100% seguro, ya que como se sabe, existen diferentes métodos por medio de los cuales personas no autorizados pueden conectar sus equipos a la red.

Pregunta No. 2. ¿Qué topología tiene esta red?

Respuesta:

La topología de nuestra red es modo infraestructura, ya que no deseamos que los usuarios tengan acceso a la información de otros.

Pregunta No. 3. ¿A qué tipo de ataques está expuesta esta red?

Respuesta:

Se puede dar un secuestro de sesión, una suplantación de dirección MAC, denegar servicio, retransmisión, etc.

Quizá la mas común y de lo que se puede encontrar más fácilmente son secuestros de sesiones, existen programas que se pueden descargar de internet y realizan dicho trabajo. La suplantación de dirección MAC quizá sea un tanto más complicada, debido a que requiere de mayores conocimientos para realizar dicha tarea.

Redes que tienen una configuración de Dirección MAC son redes que seguramente tienen dentro de la arquitectura de red servidores que realizan diferentes funciones (Servidor de privilegios de usuarios - *Active Directory*, servidor Proxy, etc.), no es tan fácil ya entonces infiltrarse en la red.

Pregunta No. 4. ¿Qué medidas de seguridad que aplica en la red?

Respuesta:

Las medidas de seguridad varían dependiendo de las necesidades que se tengan y de los conocimientos que tienen los administradores de la red para poner en marcha diferentes sistemas de seguridad. Todos los sistemas de seguridad necesitan de un amplio control de parte del administrador de la red.

Las medidas de seguridad pueden ir de dos formas. A) desde accesos por clave a usuarios y B) accesos a servicios por parte de los usuarios a través de un sistema de control de privilegios de usuarios.

La primera se configura directamente en el punto de acceso a la red inalámbrica (entiéndase clave WEP, o registro de dirección MAC). Esta permite cierta seguridad, pero depende del buen uso que le de el usuario de la terminal o de la computadora. La segunda se puede implementar sobre la primera y proporciona niveles de seguridad para cada usuario de la red. Esto quiere decir que clasifica a los usuarios en niveles de acceso a la red y servicios que se les puedan habilitar, tales como servicio de internet, manipulación de archivos, uso de impresoras, etc)

En el Liceo Guatemala utilizamos la configuración de direcciones MAC, esta nos permite tener un mejor control de las personas y los equipos que se han conectado a la red. Previamente a configurar la dirección MAC nos aseguramos de que los equipos cuenten con ciertas garantías mínimas que permitan la tranquilidad de todos y cada uno de los usuarios; por ejemplo, deben contar con un software anti-virus, además hacemos énfasis en que al momento de crear las claves de acceso, estas sean alfanuméricas.

El servicio que mayormente utilizan los equipos conectados a la red inalámbrica es el del acceso a Internet, es por eso que tenemos configurado un servidor proxy que controla los servicios y las páginas Web a las que pueden accesar, dependiendo de los privilegios de cada usuario dentro de la red.

Pregunta No. 5. ¿Por qué utiliza esta técnica y no WEP o WPA?

Respuesta:

Debido a las necesidades de la institución educativa y a los avances de la tecnología, las medidas de seguridad que utilizamos en el Liceo Guatemala son especiales, debido a dos factores. El primero es que tenemos un promedio de 1500 usuarios que podrían hacer uso en cualquier momento de la red inalámbrica. Es conocido por muchos que ahora los diferentes teléfonos celulares ya cuentan con una interfaz WI-FI lo que permitiría conectarse a la red en cualquier instante. Si tuviéramos una clave única de acceso WEP o WAP podría ser mal utilizada y se podría accesar a los archivos de control de notas o navegar en internet a las horas de clase, sin que se sepa exactamente quién está haciendo uso de la red.

El segundo factor es que los servicios a la red muchas veces no son de carácter educativo para los alumnos, debido a que comúnmente lo que frecuentan son espacios de ocio y entretenimiento.

Pregunta No. 6. ¿Cómo autentica a los usuarios?

Respuesta:

Todos los maestros pueden solicitar el conectarse a la red. Los alumnos tienen denegado dicho privilegio. En caso de que sea necesario deberá contar con la solicitud escrita y los permisos para esto.

En el colegio solamente hay dos personas autorizadas para configurar la autenticación de usuarios; una de ellas es el administrador de la red (Coordinador de Tecnología del colegio), el cual es designado por las autoridades del colegio; la otra es el auxiliar de red, elegido por el administrador.

Los usuarios deben de seguir un procedimiento para conectarse a la red.

a. Dependiendo a la ubicación en donde se encuentran laborando se les registra la Dirección MAC en los puntos de acceso de la red inalámbrica a donde pertenezcan.

b. Se hace una inspección visual para ver si la computadora cuenta con lo necesario para conectarse a la red. Esto es: Sistema operativo compatible y software de control de virus.

c. Se les da la inducción necesaria para que puedan realizar correctamente la conexión al punto de acceso.

d. Se les dan los lineamientos para hacer uso de la red.

Pregunta No. 7. Como administrador de la red, ¿cada cuanto tiempo analiza el tráfico de red para detectar intentos de *hackeo*?

Respuesta:

El control se realiza de forma periódica, dos veces por semana, los diferentes puntos de acceso guardan un registro de las conexiones que se han realizado a cada punto de acceso, este se guarda cada vez. Allí es donde se puede observar que ha sucedido en cada punto de acceso. Al momento de ver algún inconveniente ya en repetidas ocasiones se analiza la información y se toman las medidas.

Las respuestas brindadas por el administrador de esta red son básicamente las que responderían los administradores de otras redes donde no se maneje un tipo de información especial o secreta, en este caso en especial el acceso WI-FI se utiliza para que los profesores tengan acceso al Internet o para poder accesar al control de notas, sanciones, circulares e información proveniente de la Dirección o Rectoría del Colegio; quedando claro que cada usuario solamente puede accesar a la información que le concierne y no a la de los demás.

CONCLUSIONES

1. Las principales ventajas de las redes WI-FI son la movilidad que ofrecen a los usuarios, ya que no los ata a un punto en específico, y también la facilidad de acceso a redes abiertas e inclusive redes semiseguras o seguras utilizando los permisos necesarios.

2. La desventaja más notoria de las redes WI-FI es que las ondas de radiofrecuencia no pueden ser detenidas, por lo que la información transmitida en ellas puede ser interceptada y analizada por *hackers*.

3. Los mecanismos más utilizados para brindar seguridad a redes inalámbricas son: autenticación de usuario, claves de acceso a la red, listas de control de acceso en puntos de acceso y cifrado WEP o WPA para los paquetes de datos.

4. Los tipos de ataques que puede sufrir una red WI-FI pueden ser pasivos o activos; en el primer caso el intruso solamente husmea la red para obtener información, en el segundo caso la situación es más delicado ya que el intruso puede alterar la información o inclusive puede impedir que un usuario autorizado haga uso de la red.

5. Un grave problema que afrontan las redes inalámbricas es que en Internet se pueden encontrar programas especialmente diseñados para romper la seguridad de estas redes, ya que existen programas falsificadores de puntos de acceso, programas para analizar el tráfico de redes, programas desencriptadores e inclusive programas falsificadores de direcciones MAC.

6. La aplicación de medidas mínimas de seguridad, tales como cambiar la contraseña por defecto, usar un nombre no significativo para la red, usar una contraseña difícil de adivinar, habilitar el encriptado WEP o WPA, desactivar el servidor DHCP o deshabilitar la red el tiempo que no se está utilizando, reduce el riesgo de que la red sea atacada.

RECOMENDACIONES

1. Al crear una red inalámbrica en ambiente Windows es mejor asignar la clave manualmente, ya que de esta manera se pueden mezclar letras y números.

2. Para la encriptación de datos en redes inalámbricas es preferible utilizar cifrado WPA; esto debido a que el largo de la clave de encriptación del cifrado WPA es mayor que el largo de la clave de encriptación del cifrado WEP (32 caracteres máximo para encriptado WEP contra 64 caracteres máximo para encriptado WPA).

3. Realizar un monitoreo constante en las redes inalámbricas ayudaría a prevenir los ataques a ellas, ya que se podrían encontrar las deficiencias de estas redes y se corregiría el problema antes de cualquier ataque externo.

REFERENCIAS

[1] **WI-FI**. http://es.wikipedia.org/wiki/WI-FI

[2] **Introducción a WI-FI.** www.es.kioskea.net/contents/WI-FI

[3] Ponce, Tortosa y Maicas. **Redes Inalambricas: IEEE 802.11**

[4] **Capa Mac.** http://es.kioskea.net/contents/WI-FI

[5] **IEEE 802.11.** http://es.wikipedia.org/wiki/802.11

[6] Luis Carlos Fernández. **Las Tecnologías WI-FI. (**España: CEDITEC, 2003), p. 7

[7] Ibid., p. 9

[8] Ibid., p 9-10

[9] **Ventajas y Desventajas**. http://es.wikipedia.org/wiki/WI-FI

[10] **Autenticación.** http://www.ordenadores-y-portatiles.com/encriptacion.html

[11] Stewart Millar, ***WI-FI Security*** (USA: McGraw-Hill), p 4-5

[12] **Seguridad de Red Inalámbrica WI-FI (802.11 o WI-FI).** http://es.kioskea.net/contents/WI-FI/WI-FIsecu.php3

[13] **Servidor RADIUS.** www.virusprot.com/cursos/Redes-Inalámbricas-Curso-gratis10.htm#Servidor_RADIUS

[14] Stewart Millar, *op. cit.*, p 5

[15] **Seguridad de Red Inalámbrica WI-FI (802.11 o WI-FI).** http://es.kioskea.net/contents/WI-FI/WI-FIsecu.php3

[16] **Filtrado de Direcciones MAC**.http://www.virusprot.com/cursos/Redes-Inalámbricas-Curso-gratis7.htm

[17] **Filtrado de Direcciones MAC**. http://es.kioskea.net/contents/WI-FI/WI-FIsecu.php3

[18] **WPA – Acceso Inalámbrico Protegido.** es.kioskea.net/contents/WI-FI/WI-FI-wpa.php3

[19] **Hacking de Redes Inalámbricas WI-FI.** www.virusprot.com/cursos/Redes-Inalámbricas-Curso-gratis21.htm

[20] **Seguridad en Redes WI-FI.** www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridad_en_redes_inalambricas_WI-FI.shtml

[21] **Proteger una red WI-FI**. http://www.ayuda-internet.net/tutoriales/proteger-red-WI-FI/proteger-red-WI-FI.html

BIBLIOGRAFÍA

1. Carballar Falcón, José Antonio. **WI-FI, instalación, seguridad y aplicaciones.** España: Ra-ma, 2007. 336 pág.

2. Carballar Falcón, José Antonio. **WI-FI. Cómo construir una red inalámbrica.** 2ª Edición. España: Ra-ma, 2004. 272 pág.

3. Curran, Kevin. **WI-FI Security**. Estados Unidos de Norteamérica: Booksurge.com, 2004. 132 pág.

4. Fernández González, Luis Carlos. **Las tecnologías WI-FI: Aplicaciones, modelos de negocio y tendencias.** [on line]. España: CEDITEC [consultado 16 septiembre 2009]

5. Miller, Stewart S. **WiFi security**. Nueva York: McGraw Hill, 2003. 309 pág.