ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

Facultad de Ingeniería en Electricidad y Computación

Licenciatura en Sistemas de Información

"SEGURIDAD EN REDES INALÁMBRICAS"

TÓPICO DE GRADUACIÓN

Previa a la obtención del Título de:

LICENCIADO EN SISTEMAS DE INFORMACIÓN

Presentado por:

Geannina Jackeline Aguirre Briones

Ángela Isabel Sanclemente Ordóñez

Laura Alexandra Ureta Arreaga

Guayaquil - Ecuador

2005

Agradecimiento

Al Ing. Albert Espinal Santana

Director de Tópico, por su valiosa ayuda y colaboración para la realización de este trabajo.

Dedicatoria

A mi Dios, porque de Él proviene la fortaleza para seguir adelante.
A mi familia y todas aquellas personas que con su apoyo incondicional hicieron posible que culmine satisfactoriamente mi carrera profesional.

Geannina Aguirre Briones

Agradezco a Dios por darme la vida, a mi mamá Linda Celeste por haber brindando amor, comprensión y confianza, a mis hermanos por estar siempre dándome apoyo y demostrarme que con esfuerzo se puede alcanzar las metas propuestas.

Ángela Sanclemente Ordóñez

A Dios quien guía mi camino, a mis padres, a mis hermanos y a mis verdaderos amigos que siempre están conmigo por su apoyo para alcanzar las metas que me he propuesto y específicamente la culminación de mi carrera.

Laura Ureta Arreaga

Tribunal

Ing. Mónica Villavicencio
Presidente del Tribunal

Ing. Albert Espinal
Director de Tópico

CIB-ESPOL

Ing. Lorena Carló
Miembro Principal

Ing. Jaime Lucero
Miembro Principal

Declaración Expresa

La responsabilidad por los hechos, ideas y doctrinas expuesto en este proyecto, nos corresponden exclusivamente; y, el Patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

(Reglamento de Exámenes y Títulos Profesionales de la ESPOL).-

Geannina Aguirre Briones

Ángela Sanclemente Ordóñez

Laura Ureta Arreaga

RESUMEN

Las redes inalámbricas proveen a los usuarios de una LAN, acceso a la información en tiempo real en cualquier lugar dentro de la empresa. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red cableada. La instalación de una red inalámbrica puede ser tan rápida y fácil, y además que puede eliminar la posibilidad de pasar cable a través de paredes y techos. Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN cableada, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior.

Los sistemas WLANs pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

El presente proyecto tiene como objetivo, dar una visión global del estado de seguridad en las redes inalámbricas, familiarizarse con la terminología utilizada y los diferentes riegos y tipos de ataques informáticos a los cuales esta expuesta, así como también introducir niveles básicos y avanzados de seguridad en la implementación de una red de este tipo. Se describen los elementos que participan en la solución así como los protocolos de red y funcionalidades necesarias para garantizar la seguridad de la red inalámbrica.

En el capítulo 1, se describen conceptos básicos de las redes de área local inalámbricas comúnmente llamadas WLAN, se explica su definición, configuración, sus aplicaciones, sus ventajas y desventajas con relación a las redes cableadas.

El capítulo 2, se refiere al estudio de las tecnologías utilizadas en las redes inalámbricas.

En el capítulo 3, se explican los apartados de la Normalización de la IEEE que se relacionan a las redes inalámbricas.

En el capítulo 4, se describen las vulnerabilidades o debilidades a las que están expuestas las redes inalámbricas, en esta parte definimos los diferentes tipos de ataques y como se detectan las redes implementadas en un área de trabajo.

En el capítulo 5, se detallan las metodologías de seguridad que se pueden implementar en una red inalámbrica, así también se analizan cada uno de ellos y se brindan consejos para garantizar la seguridad.

En el capítulo 6, se definen de manera general los tipos de políticas que se deben considerar cuando se tiene implementada una red inalámbrica.

En el capítulo 7, se explica la gestión de seguridad de la red inalámbrica, usando el software Orinoco; además de herramientas que permiten monitorear la red.

Por ultimo en el capítulo 8 se detalla el análisis de costo beneficio de una red inalámbrica versus una red cableada.

ÍNDICE GENERAL

ÍNDICE GENERAL

CAPÍTULO 3

NORMALIZACIÓN IEEE PARA REDES INALÁMBRICAS

CAPÍTULO 4

VULNERABILIDADES EN REDES WIRELESS LAN

CAPÍTULO 5

SEGURIDAD BÁSICA Y AVANZADA EN WIRELESS LAN

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

WLAN son las siglas en inglés de Wireless Local Area Network. Es un sistema de comunicación de datos flexible muy utilizado como alternativa a la LAN cableada o como una extensión de ésta.

Las redes inalámbricas de área local (WLAN) tienen un papel cada vez más importante en las comunicaciones del mundo de hoy. Debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red cableada. La popularidad de estas redes ha crecido a tal punto que los fabricantes de computadores y motherboards están integrando dispositivos para acceso a WLAN en sus equipos.

Otra tecnología de acceso inalámbrico en áreas de pequeña extensión (WPAN/WLAN Personal Area Network) es la denominada Bluetooth, que aunque pueda parecer competencia directa de las WLAN, es más bien complementaria a ella. Bluetooth pretende la eliminación de cables, como por ejemplo todos los que se utilizan para

conectar el PC con sus periféricos, o proporcionar un medio de enlace entre dispositivos situados a muy pocos metros, sirviendo también como mando a distancia.

Las WLAN tienen su campo de aplicación específico, igual que Bluetooth, y ambas tecnologías pueden coexistir en un mismo entorno sin interferirse gracias a los métodos de salto de frecuencia que emplean. Sus aplicaciones van en aumento y, conforme su precio se vaya reduciendo, serán más y más los usuarios que las utilicen, por las innegables ventajas que supone su rápida implantación y la libertad de movimientos que permiten.

CAPÍTULO 1

CONCEPTOS Y GENERALIDADES.

1.1. Definición.

Una red de área local inalámbrica puede definirse, como a una red de alcance local que tiene como medio de transmisión el aire; también llamada Wireless LAN (WLAN), es un sistema flexible de comunicaciones que puede implementarse como una extensión o directamente como una alternativa a una red cableada. Este tipo de redes utiliza tecnología de radiofrecuencia, minimizando así la necesidad de conexiones cableadas.

Las redes WLAN se componen fundamentalmente de dos tipos de elementos, los puntos de acceso y los dispositivos de cliente. Los puntos de acceso actúan como un concentrador o hub que reciben y envían información vía radio a los dispositivos de clientes, que pueden ser de cualquier tipo, habitualmente, un PC o PDA con una

tarjeta de red inalámbrica, que se instala en uno de los slots libres o bien se enlazan a los puertos USB de los equipos.

Aún así, debido a que sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2 y los 54 Mbps, frente a los 10 y hasta los 1000 Mbps ofrecidos por una red convencional, las redes inalámbricas son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite, y en general las WLAN se utilizarán como un complemento de las redes fijas.

El uso más popular de las WLAN implica la utilización de tarjetas de red inalámbricas, cuya función es permitir al usuario conectarse a la LAN empresarial sin la necesidad de una conexión física.

1.2. Configuraciones WLAN.

La complejidad de una red de área local inalámbrica es variable, dependiendo de las necesidades a cubrir y en función de los requerimientos del sistema que se quiera implementar, se pueden utilizar diversas configuraciones de red tales como:

- Punto a Punto o Ad-Hoc.
- Extensión en celdas básicas.
- Enlaces entre varias LAN.

1.2.1. Punto a Punto o Ad-Hoc.

La configuración más básica es la llamada punto a punto o Ad–Hoc, consiste en una red de dos o más terminales móviles equipados con la correspondiente tarjeta adaptadora para comunicaciones inalámbricas; en la Figura. 1.1 se muestra un ejemplo. En esta modalidad no existe un dispositivo central encargado de concentrar y coordinar las comunicaciones, sino que cada nodo existente en la red se comunica directamente con los demás y no hay nodo preponderante alguno.

Para que la comunicación entre estas estaciones sea posible, hace falta que se vean mutuamente de manera directa, es decir, que cada una de ellas esté en el rango de cobertura radioeléctrica de la otra.

Las redes de tipo ad-hoc son muy sencillas de implementar y no requieren ningún tipo de gestión administrativa. También este tipo es conocido como **IBSS (*Independent Basic Service Set*)**

Figura. 1.1. Configuración punto a punto o Ad–Hoc.

1.2.2. Extensión en celdas básicas.

Para aumentar el alcance de una red del tipo anterior, hace falta la instalación de un **Punto de Acceso**. Con este nuevo elemento se dobla el alcance de la red inalámbrica (ahora la distancia máxima permitida no es entre estaciones, sino entre cada estación y el punto de acceso), en la Figura 1.2 se muestra un ejemplo. Además, los puntos de acceso se pueden conectar a otras redes, y en particular a una red fija, con lo cual un usuario puede tener acceso desde su terminal móvil a otros recursos. Existen muchas aplicaciones en el mundo real con entre 15 y 50 dispositivos cliente en un solo punto de acceso. Otro término con el que se conoce a una red con extensión de celdas básicas es **BSS (*Basic Service Set*).**

Figura 1.2. Cliente y punto de acceso.

Los puntos de acceso tienen un rango finito, del orden de 100m en lugares cerrados y 300m en zonas abiertas. En zonas grandes como por ejemplo un campus universitario o un edificio es probablemente necesario más de un punto de acceso, tal y como se muestra en la Figura 1.3. La meta es cubrir el área con células que solapen sus áreas

de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso. Esto es llamado "roaming".

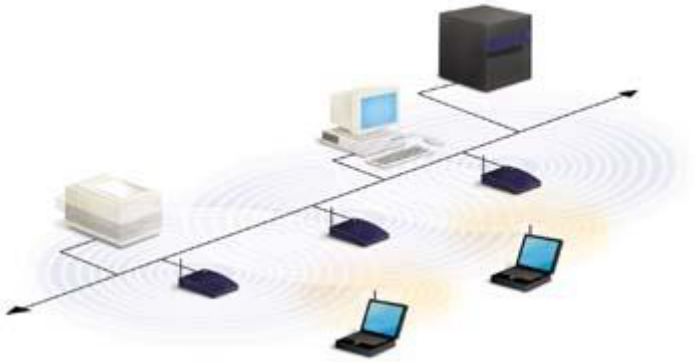

Figura 1.3. Múltiples puntos de acceso y roaming.

Para resolver problemas particulares de topología, el diseñador de la red puede elegir usar un Punto de Extensión (PE) para aumentar el número de puntos de acceso a la red, de modo que funcionan como tales pero no están enganchados a la red cableada como los puntos de acceso, así como se muestra en la Figura 1.4. Los puntos de extensión funcionan como su nombre lo indica: extienden el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión. Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos.

Figura 1.4. Uso de un punto de extensión.

1.2.3. Enlace Entre Varias LAN.

Uno de los últimos componentes a considerar en el equipo de una WLAN es la antena direccional. El objetivo de estas antenas direccionales, es el de enlazar redes que se encuentran situadas geográficamente en sitios distintos tal y como se muestra en la Figura 1.5.

Por ejemplo: se quiere una LAN sin cable a otro edificio a 1 Km. de distancia. Una solución puede ser instalar una antena en cada edificio con línea de visión directa. La antena del primer edificio está conectada a la red cableada mediante un equipo maestro. En el segundo edificio se conecta a un equipo esclavo, lo cuál permite una conexión sin cable en esta aplicación.

Es importante considerar que en la implementación de este tipo de enlaces no es recomendable el uso del estándar 802.11b, ya que éste esta especificado para interiores, y la restricción con respecto a las distancias superiores a las descritas en el estándar provocarían molestias en la conexión.

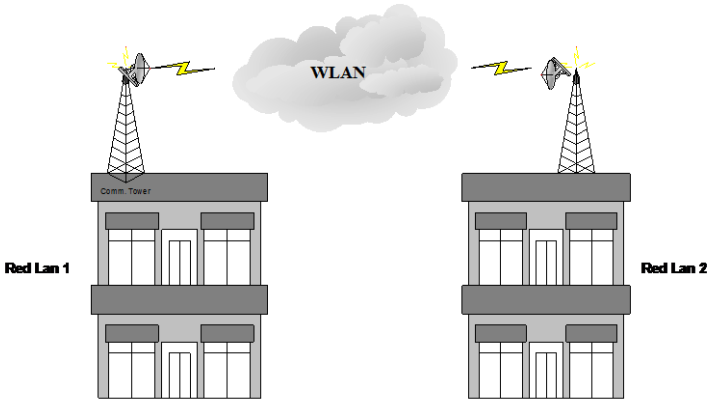

Figura 1.5. Utilización de antenas direccionales

1.3. Ventajas y Desventajas en la utilización de WLAN's

Es clara la alta dependencia en los negocios de la redes de comunicación. Por ello la posibilidad de compartir información sin que sea necesario buscar una conexión física permite mayor movilidad y comodidad.

Así mismo la red puede ser más extensa sin tener que mover o instalar cables. Respecto a la red tradicional la red sin cable ofrece las siguientes ventajas:

- **Movilidad:** Información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. El que se obtenga en tiempo real supone mayor productividad y posibilidades de servicio.
- **Facilidad de instalación:** Evita obras para tirar cable por muros y techos.
- **Flexibilidad:** Permite llegar donde el cable no puede.

- **Escalabilidad:** El cambio de topología de red es sencillo y trata igual pequeñas y un gran conjunto de redes.

Las redes WLAN también, presentan alguna desventaja, o más bien inconveniente, que es el hecho de la "baja" velocidad que alcanzan, por lo que su éxito comercial es más bien escaso y, hasta que los nuevos estándares no permitan un incremento significativo, no es de prever su uso masivo, ya que por ahora no pueden competir con las LAN basadas en cable.

1.4. Aplicaciones de los Sistemas WLAN en la Industria.

Las aplicaciones más típicas de las redes de área local que podemos encontrar actualmente son las siguientes:

- **Corporaciones:** Con WLAN los empleados pueden beneficiarse de una red móvil para el correo electrónico, compartición de archivos, y visualización de web's, independientemente de dónde se ubiquen en la oficina.
- **Educación:** Las instituciones académicas que soportan este tipo de conexión móvil permiten a los usuarios con computadoras de ordenador conectarse a la red de la universidad para intercambio de opiniones en las clases, para acceso a internet, etc.
- **Finanzas:** Mediante una PC portátil y un adaptador a la red WLAN, los representantes pueden recibir información desde una base de datos en tiempo real y mejorar la velocidad y calidad de los negocios. Los grupos de auditorias

contables incrementan su productividad con una rápida puesta a punto de una red.

- **Cuidado de la salud:** WLAN permite obtener información en tiempo real, por lo que proporciona un incremento de la productividad y calidad del cuidado del paciente eliminando el retardo en el tratamiento del paciente, los papeles redundantes, los posibles errores de trascripción, etc.
- **Restaurantes y venta al por menor:** Los servicios de restaurantes pueden utilizar WLAN para directamente entrar y enviar los pedidos de comida a la mesa. En los almacenes de ventas al por menor un WLAN se puede usar para actualizar temporalmente registros para eventos especiales.
- **Manufacturación:** WLAN ayuda al enlace entre las estaciones de trabajo de los pisos de la fábrica con los dispositivos de adquisición de datos de la red de la compañía.
- **Almacenes:** En los almacenes, terminales de datos con lectores de código de barras y enlaces con redes WLAN, son usados para introducir datos y mantener la posición de las paletas y cajas. WLAN mejora el seguimiento del inventario y reduce los costos del escrutinio de un inventario físico.

CAPÍTULO 2

TECNOLOGÍAS UTILIZADAS EN LAS REDES INALÁMBRICAS.

En esta sección se describirán dos tipos de tecnologías inalámbricas existentes definidas en el estándar 802.11:

- Espectro ensanchado.
- Infrarrojos.

2.1. Tecnologías de Espectro Ensanchado.

Un sistema de espectro ensanchado, es aquel en el cual la señal transmitida es propagada en una banda de frecuencia amplia, mucho más de hecho que el mínimo ancho de banda requerido para transmitir la información que será enviada.

Las comunicaciones de espectro ensanchado no puede decirse que sean una manera eficiente de utilizar el ancho de banda. Sin embargo, son de utilidad cuando se combinan con los sistemas existentes que ocupan la frecuencia.

La señal de espectro ensanchado**,** que es propagada en un ancho de banda grande, puede coexistir con señales de banda estrecha añadiendo únicamente un ligero incremento en el ruido de fondo que los receptores de banda estrecha pueden ver. El receptor de espectro ensanchado no ve las señales de banda estrecha, pues está escuchando en un ancho de banda mucho más amplio.

El comportamiento de la señal de banda ancha con la señal de espectro ensanchado se puede distinguir en la Figura 2.1

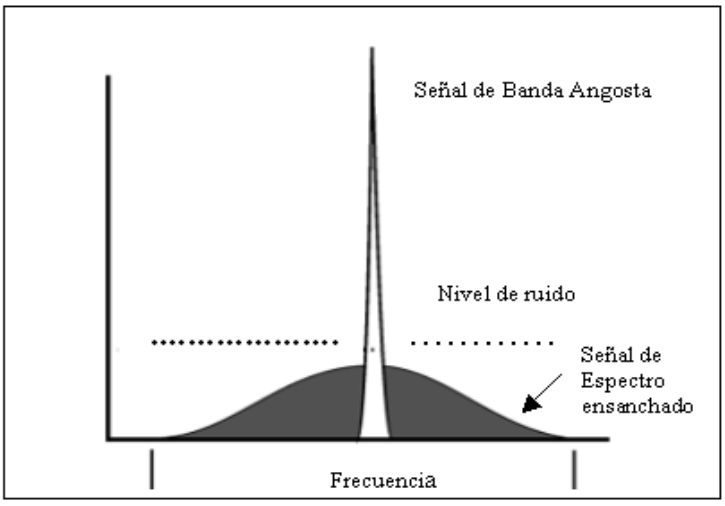

Figura 2.1. Señal de banda angosta vs. señal de espectro ensanchado.

Existen dos tipos de tecnologías de espectro ensanchado:

- Espectro Ensanchado por Secuencia Directa (DSSS).
- Espectro Ensanchado por Salto en Frecuencia (FHSS).

2.1.1. Tecnología de Espectro Ensanchado por Secuencia Directa (DSSS).

Esta técnica, opera en un canal determinado y consiste en representar cada bit de la señal original por múltiples bits en la señal transmitida. Cada bit trasmitido se modula con una secuencia de 11 bits aleatorios (Código de Barker), esta secuencia tiene propiedades matemáticas que lo hacen ideal para modular radiofrecuencias. Un ejemplo de la secuencia de Barker podría ser:

+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1

En la Figura 2.2, se muestra el aspecto de una señal de dos bits a la cual se le ha aplicado la secuencia de Barker descrita arriba.

DSSS tiene definidos dos tipos de modulaciones a aplicar a la señal resultante (señal de información luego de aplicarle la Secuencia de Barker), tal y como específica el estándar IEEE 802.11: la modulación DBPSK (Differential Binary Phase Shift Keying), y la modulación DQPSK (Differential Quadrature Phase Shift Keying), proporcionando unas velocidades de transferencia de 1 y 2 Mbps respectivamente.

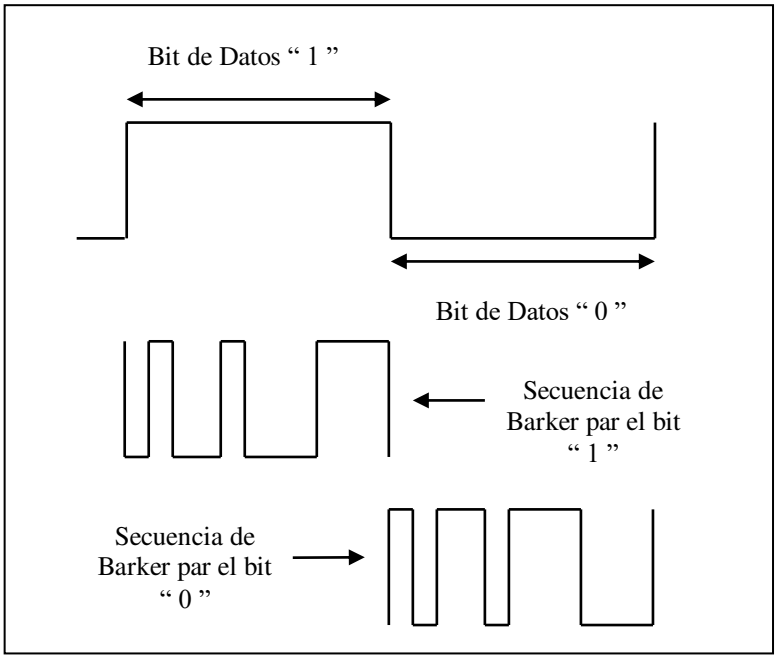

Figura 2.2. Codificación mediante la secuencia de Barker.

Para lograr velocidades de 5.5 y 11 Mbps, la codificación que se usa es CCK (Complementary Code Keying); en vez de usar el código de Barker, se usan series de secuencias complementarias que cuentan con 64 únicas palabras que pueden usarse.

En contraposición al Código de Barker, por CCK se pueden representar 6 bits de datos en una sola palabra y no 1 bit de datos por palabra como el Código Barker.

En recepción, es necesario de realizar el proceso inverso para obtener la señal de información original.

En el caso de Estados Unidos y de Europa, la tecnología de espectro ensanchado por secuencia directa (DSSS), opera en el rango que va desde los 2.4 GHz hasta los

2.4835 GHz, es decir, con un ancho de banda total disponible de 83.5 MHz. Este ancho de banda total se divide en 14 canales con un ancho de banda por canal de 5 MHz, de los cuales cada país utiliza un subconjunto de los mismos según las normas reguladoras para cada caso particular.

En el caso de Ecuador para los equipos Orinoco, se utilizan 11 canales que van desde los 2.412 GHz (canal 1) hasta los 2.462 GHz (canal 11).

En topologías de red que contengan varias celdas, ya sean solapadas o adyacentes, los canales pueden operar simultáneamente sin apreciarse interferencias en el sistema; si la separación entre las frecuencias centrales es como mínimo de 25 MHz.

Esto significa que de los 83.5 MHz de ancho de banda total disponible, podemos obtener 3 canales independientes, que pueden operar simultáneamente en una determinada zona geográfica sin que aparezca interferencia en un canal procedente del otro, así como se muestra su epración en la Figura 2.3.

Esta independencia entre canales, permite aumentar la capacidad del sistema de forma lineal con el número de puntos de acceso, operando en un canal que no se esté utilizando y hasta un máximo de tres canales, como ya se mencionó.

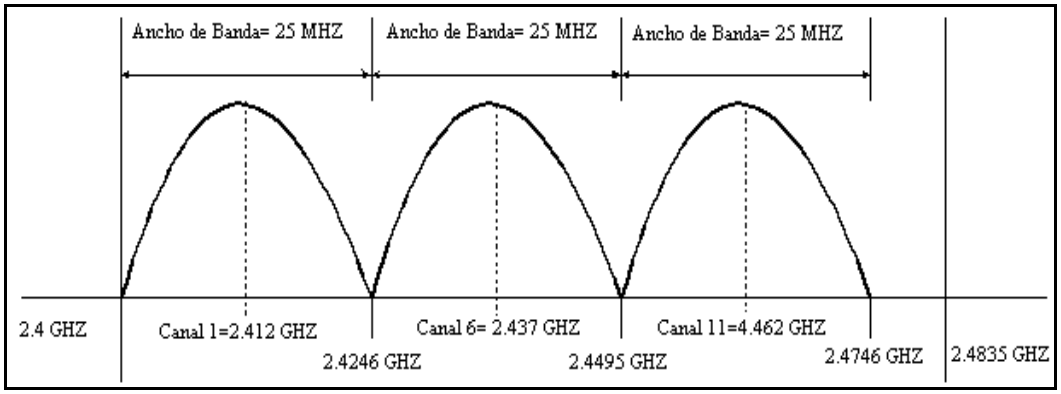

Figura 2.3. Operación de 3 canales independientes DSSS.

2.1.2. Tecnología de Espectro Ensanchado por Salto en Frecuencia (FHSS).

La tecnología de espectro ensanchado por salto en frecuencia, consiste en transmitir una parte de la información en una determinada frecuencia, durante un intervalo de tiempo llamada *dwell time e* inferior a 400 ms.

Pasado este tiempo, se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera, cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo, en la Figura 2.4, se muestra como trabaja dicha técnica.

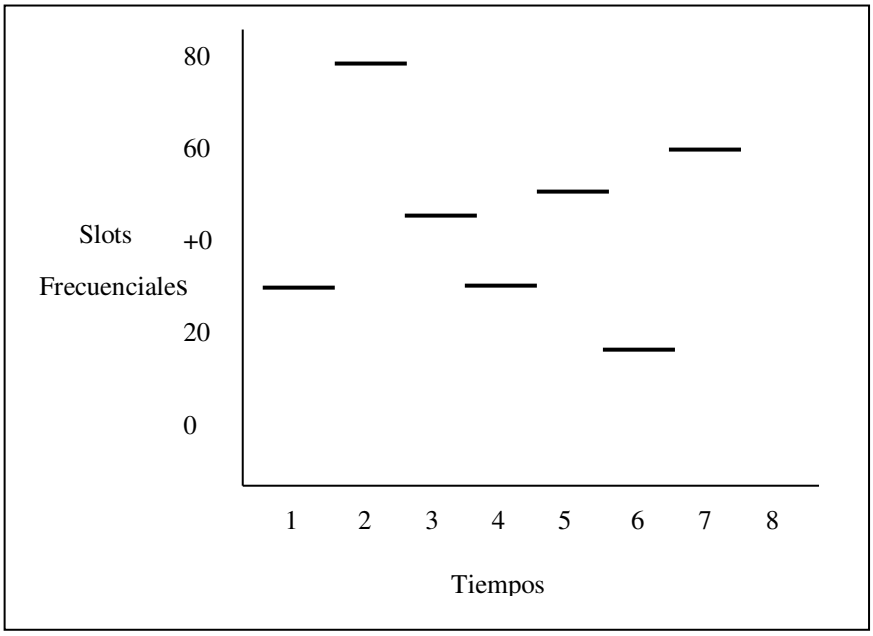

Figura 2.4. Modo de trabajo de la técnica FHSS.

Cada una de las transmisiones a una frecuencia concreta, se realizan utilizando una portadora de banda estrecha que va cambiando (saltando) a lo largo del tiempo. Este procedimiento equivale a realizar una partición de la información en el dominio temporal. El orden en los saltos en frecuencia que el emisor debe realizar viene determinado según una secuencia pseudo aleatoria, que se encuentra definida en unas tablas que tanto el emisor como el receptor deben conocer.

La ventaja de estos sistemas frente a los sistemas DSSS, es que con esta tecnología podemos tener más de un punto de acceso en la misma zona geográfica sin que existan interferencias, si se cumple que dos comunicaciones distintas no utilizan la misma frecuencia portadora en un mismo instante de tiempo.

Si se mantiene una correcta sincronización de estos saltos entre los dos extremos de la comunicación, aunque vamos cambiando de canal físico, con el tiempo se mantiene un único canal lógico a través del cual se desarrolla la comunicación.

Para un usuario externo a la comunicación, la recepción de una señal FHSS equivale a la recepción de ruido impulsivo de corta duración. El estándar IEEE 802.11 describe esta tecnología mediante la modulación en frecuencia FSK (Frequency Shift Keying), y con una velocidad de transferencia de 1Mbps ampliable a 2Mbps, bajo condiciones de operación óptimas.

2.2. Tecnología de Infrarrojos.

Una tercera tecnología definida también en el estándar 802.11 y de momento no demasiado utilizada en el ámbito comercial para implementar WLAN´s, es la de infrarrojos. Los sistemas de infrarrojos se sitúan en altas frecuencias, justo por debajo del rango de frecuencias de la luz visible. Las propiedades de los infrarrojos son, por tanto, las mismas que tiene la luz visible. De esta forma los infrarrojos no pueden pasar a través de objetos opacos, pero se pueden reflejar en determinadas superficies.

Las longitudes de onda de operación se sitúan alrededor de los 850-950 nm, es decir, a unas frecuencias de emisión que se sitúan entre los $3{,}15 \times 10e^{14}$ Hz y los $3{,}52 \times 10e^{14}$ Hz. Los sistemas que funcionan mediante infrarrojos, se clasifican según el ángulo de apertura con el que se emite la información en el emisor en:

- Sistemas de corta apertura, de haz dirigido o de visibilidad directa, que funcionan de manera similar a los mandos a distancia de los aparatos de televisión. Esto supone que el emisor y el receptor tienen que estar orientados adecuadamente antes de empezar a transmitirse información.
- Sistemas de gran apertura, reflejados o de difusión, que radian tal y como lo haría un foco; permitiendo el intercambio de información en un rango más amplio.

La Figura 2.5 muestra un transreceptor, que es el que envía el haz de luz infrarroja hacia otro que la recibe. La transmisión de luz se codifica y decodifica en el envío y recepción en un protocolo de red existente. El sistema tiene un rango de 200 mts.

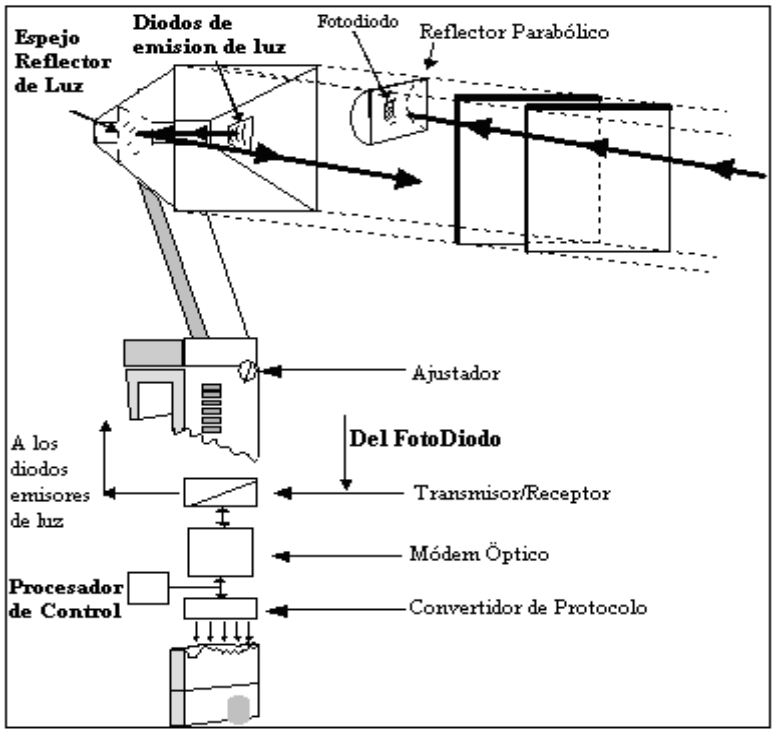

Figura 2.5. Transreceptor infrarrojo.

La norma IEEE 802.11, especifica dos modulaciones para esta tecnología: la modulación 16 ppm y la modulación 4 ppm, proporcionando unas velocidades de transmisión de 1 y 2 Mbps respectivamente.

Esta tecnología, se aplica típicamente en entornos de interior para implementar enlaces punto a punto de corto alcance, o redes locales en entornos muy localizados como puede ser un aula concreta o un laboratorio, tal y como se muestra en la Figura 2.6.

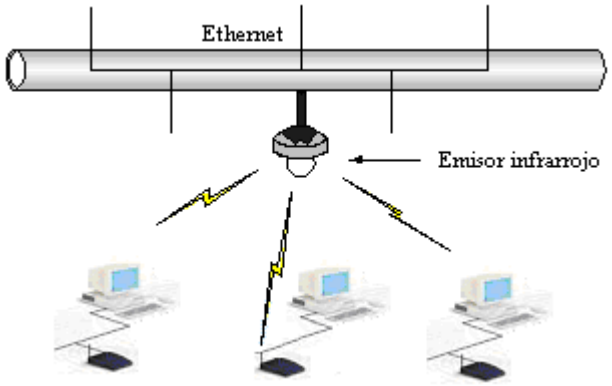

Figura 2.6. Red LAN con una célula Infrarroja.

CAPÍTULO 3

NORMALIZACIÓN IEEE PARA REDES INALÁMBRICAS.

La norma 802 fue desarrollada por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), y versa sobre la arquitectura de redes de datos LAN (Local Area Network).

Esta norma establece un estándar de tecnología en el mercado mundial, garantizando que los productos compatibles con la norma 802 sean también compatibles entre sí.
La norma posee muchos apartados, que describen y especifican las distintas funciones que se implementan en una comunicación de datos de red. Ejemplos de estos apartados se detallan en la Tabla 3.1.

Apartado	Descripción
802.1	Describe las funciones de Bridging.
802.2	Controla el enlace lógico.
802.4	Método de control de tráfico Token-Passing.
802.5	Método de control de tráfico Token-Ring.
802.10	Seguridad en comunicaciones de datos, etc.
802.11	Describe y especifica una interfase inalámbrica para comunicaciones de datos compatibles con la Norma IEEE 802.

Tabla 3.1. Norma IEEE 802.

Actualmente son cuatro los estándares reconocidos dentro de esta familia; en concreto, la especificación 802.11 original; 802.11a (evolución a 802.11 e/h), que define una conexión de alta velocidad basada en ATM; 802.11b, el que goza de una más amplia aceptación y que aumenta la tasa de transmisión de datos propia de 802.11 original, y 802.11g, compatible con él, pero que proporciona aún mayores velocidades.

3.1. WLAN 802.11.

802.11: Especificación para 1-2 Mbps en la banda de los 2.4 GHz, usando técnica de salto de frecuencias (FHSS) o secuencia directa (DSSS).

El 802.11 es una red local inalámbrica que usa la transmisión por radio en la banda de 2.4 GHz, o infrarroja, con regímenes binarios de 1 a 2 Mbit/s. El método de acceso al medio **MAC** (Media Access Control) es mediante escucha pero sin detección de colisión, **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance).

La dificultad en detectar la portadora en el acceso WLAN consiste básicamente en que la tecnología utilizada es Spread-Spectrum y con acceso por división de código (CDMA), lo que conlleva a que el medio radioeléctrico es compartido, ya sea por secuencia directa DSSS o por saltos de frecuencia en FHSS. El acceso por código CDMA implica que pueden coexistir dos señales en el mismo espectro utilizando códigos diferentes, y eso para un receptor de radio implicara que detectaría la portadora inclusive con señales distintas de las de la propia red WLAN. Hay que mencionar que la banda de 2,4 GHz está reglamentada como banda de acceso pública y en ella funcionan gran cantidad de sistemas, entre los que se incluyen los teléfonos inalámbricos Bluetooth.

3.2. WLAN 802.11b (Wi-Fi).

Extensión del 802.11 en la banda de 2.4 Ghz, con velocidades de comunicación de datos de hasta 11 Mbps usando DSSS, también conocido como Wi-Fi (Wireless Fidelity).

Un poco más tarde, en el año 1999, se aprobó el estándar 802.11b, una extensión del 802.11 para WLAN empresariales, con una velocidad de 11 Mbit/s (otras velocidades normalizadas a nivel físico son: 5,5 - 2 y 1 Mbit/s) , que al igual que Bluetooth y Home RF, también emplea la banda de ISM de 2,4 GHz, pero en lugar de una simple modulación de radio digital y salto de frecuencia (FH/Frequency Hopping), utiliza una modulación lineal compleja (DSSS). Permite mayor velocidad, pero presenta una

menor seguridad, y el alcance puede llegar a los 100 metros, suficientes para un entorno de oficina o residencial.

3.3. WLAN 802.11a (Wi-Fi 5).

Extensión del 802.11 en la banda de 5.8 Ghz, con velocidades de comunicación de datos 54 Mbps usando modulación OFDM (Orthogonal Frequency Division Multiplexing).

El IEEE ratificó en julio de 1999 el estándar en 802.11a (los productos comerciales comienzan a aparecer a mediados del 2002), que con una modulación QAM-64 y la codificación OFDM alcanza una velocidad de hasta 54 Mbit/s en la banda de 5 GHz, menos congestionada y, por ahora, con menos interferencias, pero con un alcance limitado a 50 metros, lo que implica tener que montar más puntos de acceso que si se utilizase 802.11b para cubrir el mismo área, con el coste adicional que ello supone.

La banda de 5 GHz que utiliza se denomina UNII (Infraestructura de Información Nacional sin Licencia), que en los Estados Unidos está regulada por la FCC, el cual ha asignado un total de 300 MHz, cuatro veces más de lo que tiene la banda ISM, para uso sin licencia, en tres bloques de 100 MHz, siendo en el primero la potencia máxima de 50 mW, en el segundo de 250 mW, y en el tercero puede llegar hasta 1W, por lo que se reserva para aplicaciones en el exterior.

3.4. WLAN 802.11g.

802.11 g: Extensión de 802.11 para proporcionar velocidades de 20-54 Mbps, usando DSSS y OFDM. Es compatible con el 802.11b. Tiene mayor alcance y menor consumo de potencia que el 802.11a.

El IEEE también aprobó en el año 2003 en el estándar 802.11g, compatible con el 802.11b, capaz de alcanzar una velocidad doble, es decir hasta 22 Mbit/s o llegar, incluso a 54 Mbit/s, para competir con los otros estándares que prometen velocidades mucho más elevadas pero que son incompatibles con los equipos 802.11b ya instalados, aunque pueden coexistir en el mismo entorno debido a que las bandas de frecuencias que emplean son distintas. Por extensión, también se le llama Wi-Fi.

Como se ve en las especificaciones arriba mencionadas, existe también otra subdivisión dentro de la norma 802.11. Es la referida al método de modulación de los datos. La norma describe los métodos DSSS (Direct Sequence Spread Spectrum), FHSS (Frequency Hoping Spread Spectrum), Infrared (Infrarrojo) y OFDM (Orthogonal Frecuency Division Multiplexing).

3.5. Extensiones de la Norma 802.11.

Las extensiones de las Norma de describen a continuación en la Tabla 3.2.

Extensión	Descripción
802.11e	Su objetivo es proporcionar soporte de QoS (Calidad de Servicio) para aplicaciones de redes LAN. Se aplicará a los estándares físicos a, b y g de 802.11. La finalidad es proporcionar claves de servicio con niveles gestionados de QoS para aplicaciones de datos, voz y video.
802.11i	Su objetivo es la seguridad. Se aplicará a los estándares físicos a, b y g de 802.11. Proporciona una alternativa a la Privacidad Equivalente Cableada (WEP) con nuevos métodos de encriptación y procedimientos de autentificación. IEEE 802.1x constituye una parte clave de 802.11i.
802.11d	Constituye un complemento al nivel de Control de Acceso al Medio (MAC) en 802.11. para proporcionar el uso, a escala mundial, de las redes WLAN del estándar 802.11 permitirá a los Puntos de Acceso comunicar información sobre los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios.
802.11f	Su objetivo es lograr la interoperabilidad del Punto de Acceso dentro de una red WLAN multiproveedor. El estándar define el registro del Punto de Acceso dentro de una red y el intercambio de información entre dichos Punto de Acceso cuando un usuario se traslada desde un punto de acceso a otro.
802.11h	El objetivo es cumplir los reglamentos europeos para redes WLAN a 5 GHz. requieren que los productos tengan control de la potencia de transmisión (TPC) y selección de frecuencia dinámica (DFS). El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el Punto de Acceso para reducir al mínimo la interferencia con otros sistemas Ej.: radar.

Tabla 3.2. Extensiones de la Norma 802.11.

Cabe mencionar que la banda de frecuencia 2.4 Ghz, utilizada por la tecnología 802.11b, es una banda **No Licenciada** lo que significa que su uso es libre.

La norma 802.11b, es la que actualmente se comercializa en forma masiva a través de una gran variedad de productos y aplicaciones. La norma 802.11a está evolucionando, y se supone que en un futuro cercano también ofrecerá soluciones económicas al mercado de datos inalámbricos al igual que el 802.11g.

Resumiendo los conceptos más relevantes de la norma 802.11b:

- Es un estándar internacional en comunicaciones de datos.
- Tecnología probada por muchos años a nivel mundial.
- Existe gran variedad de productos orientados a distintas aplicaciones.
- Opera en una banda No Licenciada.

CAPÍTULO 4

VULNERABILIDADES EN REDES WIRELESS LAN.

¿Qué es lo que hace que las redes inalámbricas sean más vulnerables que las redes de cable?

La respuesta es sencilla: desconocimiento de las herramientas de seguridad disponibles para redes inalámbricas. El término “seguridad inalámbrica” no tiene porque ser una expresión contradictoria. De hecho son muchas las personas que piensan que es más difícil “pinchar” un cable que el aire. Hoy en día existen las herramientas de seguridad, funciones y protocolos adecuados para proporcionar una adecuada protección en las LAN’s inalámbricas.

4.1. Debilidades de Implementación en Wireless LAN.

Además de las debilidades propias inherentes, la puesta en práctica de los estándares nunca es ideal, y siempre puede haber defectos y no adhesiones al mismo, hasta en los fabricantes más prestigiosos.

Existen ataques particulares a redes wireless, que aprovechan algunas de las debilidades comentadas, y que pueden ser agrupados en varias categorías:

4.1.1. Ataques de escucha/monitorización pasiva *(eavesdropping*).

Las redes *wireless* son especialmente vulnerables a los ataques de monitorización, siendo el único requisito para su realización la conectividad, es decir, la posibilidad de acceso al flujo de datos.

El primer paso para poder obtener acceso a un sistema es conseguir una asociación con el mismo. En las redes que utilizan autenticación *Open Syste*m, el proceso es transparente, aumentando su complejidad en los sistemas con autenticación *Shared Ke*y. En estos casos, la autenticación es posible tras la captura y *cracking* de cierto número de paquetes, existiendo diversas herramientas que facilitan dicha tarea. Tras ello, es posible el acceso y monitorización del tráfico presente en el entorno como cualquier cliente autenticado. También es posible realizar inyección y modificación de mensajes en este tipo de redes, sin necesidad de descifrar claves, SSID y demás.

Cómo utilizar esta posibilidad queda a la imaginación de cada cual. La implementación práctica de los ataques de escucha se conoce como *wardriving* (con su evolución de *drive-in hackin*g), y consiste en localizar e identificar puntos de acceso a lo largo del territorio. Carreteras, calles, aeropuertos, palacios de congresos… cualquier ubicación puede ser rastreada. Adicionalmente, existen programas que pueden trabajar de forma conjunta con un receptor GPS (Global Positioning System), lo que permite localizar de manera muy precisa (latitud, longitud, datos adicionales como SSID) la ubicación de distintos Puntos de Acceso.

4.1.2. Ataques de Intercepción/Inserción *(man-in- the-middle*).

Los entornos que operan sobre el protocolo 802.11b facilitan la captura y redirección de sesiones, ya que una estación que transmite no es capaz de detectar la presencia de estaciones adyacentes con la misma dirección MAC o IP.

Esto permite que se lleve a cabo un ataque de secuestro de sesión mediante el uso de dos estaciones hostiles diferentes, por ejemplo. En el inicio del ataque, la estación legítima (L) se encuentra conectada con el Punto de Acceso. La primera estación hostil (H1) adopta la misma dirección MAC e IP que el cliente L. Entonces la segunda estación hostil (H2) comienza a enviar gran cantidad de tráfico, saturando las conexiones de L. La consecuencia de esta saturación es que H1 recibiría cada vez mas cantidad de tráfico legítimo enviado por el PUNTO DE ACCESO hacia L, dado que los *buffer* de recepción de L estarían llenos constantemente, consiguiendo finalmente suplantar H1 a L. Sencillo.

Algo más complicado son los ataques de suplantación de Puntos de Acceso. Para ello, y basándose en las deficiencias de autenticación de Puntos de Acceso del protocolo y de sus implementaciones, es posible colocar un Punto de Acceso más cercano al usuario con los mismos datos de configuración de red. En este caso, los clientes se conectan al Punto de Acceso intruso, permitiendo al elemento hostil la captura y redirección del tráfico de red de los usuarios legítimos. Este ataque se conoce como *evil-twi*n, y aunque la incidencia es baja actualmente, se prevé su incremento en el futuro.

4.1.3. Ataques de denegación de servicio *(jam-ming).*

Por las características propias del medio, es sencillo realizar ataques que afecten a la disponibilidad en los entornos *wireless.* Dichos ataques pueden ser abordados desde varios enfoques, siendo los más sencillos aquellos que utilizan un dispositivo de radiofrecuencia (RF) de alta potencia para generar interferencias, lo que prevendría que el usuario legitimo pudiera utilizar el servicio.

Esto es consecuencia de la implementación de la capa MAC de 802.11b, que no transmitirá mientras detecte otra actividad de RF. Dentro de los dispositivos de RF de alta potencia podemos clasificar a los hornos microondas.

Para evitar las colisiones inherentes al protocolo CSMA/CD, el estándar utiliza paquetes de reserva de bandas de tiempo (RST) a los que el Punto de Acceso contesta

(CTS), obligando al resto de estaciones a no transmitir durante el intervalo definido en CTS.

Otro tipo factible de DOS, probado en entornos de laboratorio, se produce cuando una estación hostil envía mediante *spoofing* de forma ininterrumpida tramas CTS con los datos de origen (MAC e IP) del Punto de Acceso, y desemboca en una paralización gradual de las comunicaciones de la red.

4.1.4. Interferencia y Atenuación.

Debido a la naturaleza de la tecnología de radio, las señales de radio frecuencia pueden desvanecerse o bloquearse por materiales medioambientales. La inspección nos ayudará a identificar los elementos que afecten negativamente a la señal inalámbrica, algunos elementos y su grado de interferencia se muestra en la Tabla 4.1.

Material	Ejemplo	Interferencia
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Árboles y plantas	Media
Agua	Lluvia	Alta
Papel	Rollos de papel	Alta
Vidrio con plomo	Ventanas	Alta
Metal	Vigas, armarios	Muy Alta

Tabla 4.1. Interferencia y Atenuación.

Debido a que las redes inalámbricas operan en un espectro de frecuencias utilizado por otras tecnologías, pueden existir interferencias que pueden afectar negativamente al rendimiento. Las tecnologías que pueden producir interferencias son las siguientes:

- Bluetooth.
- Hornos Microondas.
- Algunos teléfonos DECT inalámbricos.
- Otras redes WLAN.

4.2. El Problema de la Seguridad.

El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere.

Cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podría tener acceso a la red inalámbrica. Por ejemplo, si varias empresas tienen sede en un mismo edificio, y todas ellas poseen red inalámbrica, el equipo de un empleado podría encontrarse en cierto momento en el área de influencia de dos o más redes diferentes, y dicho empleado podría conectarse (intencionalmente o no) a la red de una compañía que no es la suya. Aún peor, como las ondas de radio pueden salir del edificio, cualquier persona que posea un equipo móvil y entre en el área de influencia de la red, podría conectarse a la red de la empresa.

En la Figura 4.1, se muestra como un vehículo que contenga el equipo necesario puede recibir las ondas de frecuencia de la red inalámbrica, y si no se han tomado las medidas necesarias de seguridad puede ingresar a la red sin ningún inconveniente.

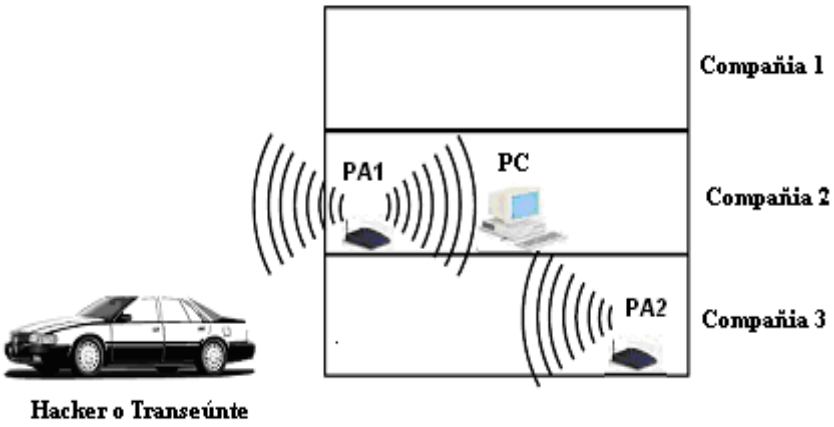

Figura 4.1. Acceso no autorizado a una red inalámbrica.

4.3. Localizando Redes Inalámbricas.

4.3.1. Warchalking.

El **warchalking,** que consiste en caminar por la calle con un computador portátil dotado de una tarjeta WLAN, buscando la señal de puntos de acceso. Cuando se encuentra uno, se pinta con tiza un símbolo especial en la acera o en un muro, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no.

De este modo, otras personas pueden conocer la localización de la red y hacer uso de esta. Dicha simbología se muestra en la Figura 4.1.

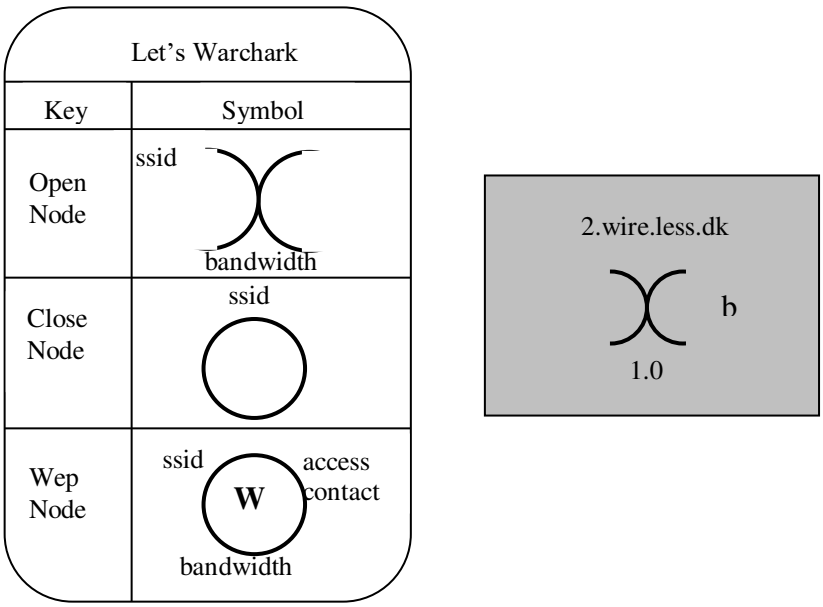

Figura 4.2. Warchalking y su simbología.

4.3.2. Wardriving.

El wardriving, propio para localizar puntos de acceso inalámbrico desde un automóvil. Para este fin se necesita de un computador portátil con una tarjeta WLAN, una antena adecuada (que se puede elaborar fácilmente con una lata de conservas) un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas, que se consigue libremente en Internet.

Figura 4.3. Wardriving.

En la Figura 4.3 se observa a la izquierda el equipo necesario (computador, y lata que simula antena); a la derecha, el GPS (Global Positioning System) que es un sistema satelitario basado en señales de radio que indica la ubicación de redes inalámbricas.

Una vez localizada una red inalámbrica, una persona podría llevar a cabo dos tipos de ataques:

- Ingresar a la red y hacer uso ilegítimo de sus recursos.
- Configurar un punto de acceso propio, orientando la antena de tal modo que los computadores que son clientes legítimos de la red atacada se conecten a la red del atacante. Una vez hecho esto, el atacante podría robar la información de dichos computadores, instalarles software maligno o dañar la información.

CAPÍTULO 5

SEGURIDAD BÁSICA Y AVANZADA EN WIRELESS LAN.

5.1. Metodologías de Defensa en Redes Wireless LAN.

Existen varios métodos para lograr la configuración segura de una red inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas. Se hará a continuación una presentación de cada uno de ellos.

5.1.1. Método 1: Filtrado de direcciones MAC.

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de

acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

- No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.
- El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.
- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales como AirJack 6 o WellenRei-ter, entre otros. De este modo, el atacante puede hacerse pasar por un cliente válido.
- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, porque el punto de

acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

5.1.2. Método 2: Wired Equivalent Privacy (WEP).

El nivel más básico de seguridad para redes inalámbricas es WEP, o Wired Equivalent Privacy, una característica estándar de todas las redes LAN inalámbricas certificadas con la norma Wi-Fi. WEP, creado por el Instituto de Ingenieros en Electricidad y Electrónica (IEEE), ha sido diseñado para proporcionar un nivel de seguridad, prevenir posibles escuchas de la información y proteger la red mediante la encriptación de todos los datos que se envíen de forma inalámbrica

El algoritmo WEP forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

El algoritmo WEP cifra de la siguiente manera (Ver Figura 5.1):

- A la trama en claro se le computa un código de integridad (Integrity Check Value, ICV) mediante el algoritmo CRC-32. Dicho ICV se concatena con la

trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.

- Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.
- Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas en claro iguales producirían tramas cifradas similares. Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.
- La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números seudo aleatorios. El generador RC4 es capaz de generar una secuencia seudo aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.
- El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el ICV).
- Se hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada.
- El IV y la trama se transmiten juntos.

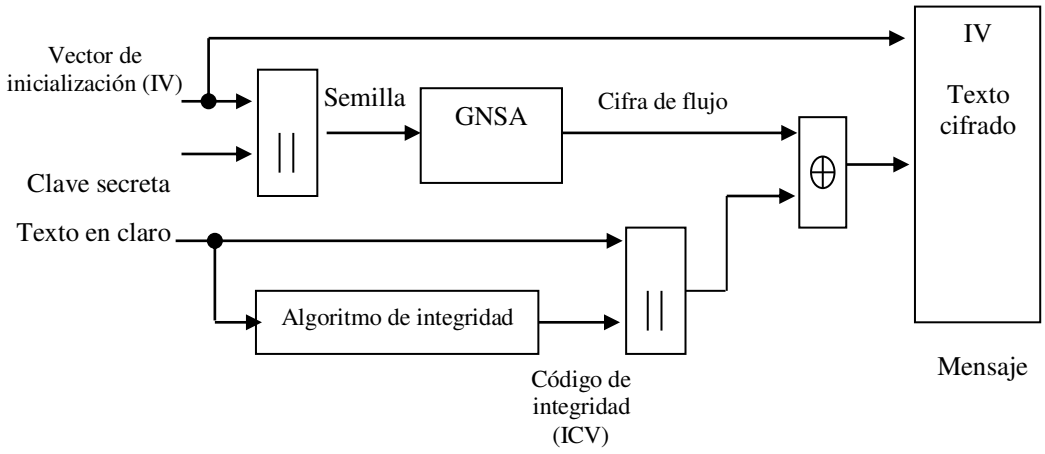

Figura 5.1. Funcionamiento del algoritmo WEP en modalidad de cifrado.

En el receptor se lleva a cabo el proceso de descifrado (Ver Figura 5.2):

- Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.
- Un generador RC4 produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.
- Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrado, obteniéndose de esta manera la trama en claro y el ICV.
- A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.
- Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

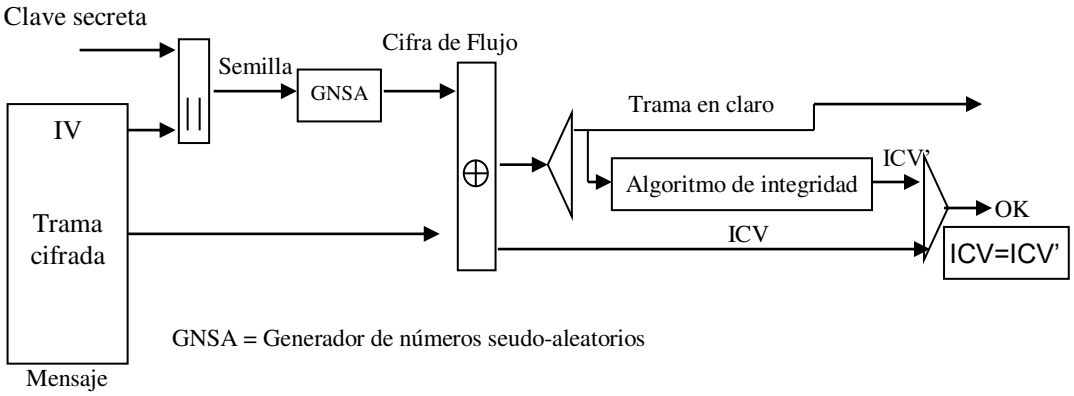

Figura 5.2. Funcionamiento algoritmo WEP en modalidad de descifrado.

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro en la manera que es empleado en la mayoría de aplicaciones:

- La mayoría de instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.
- WEP no es en absoluto una solución de cifrado extremo a extremo, sino que sólo cubre el segmento *wireless* de la comunicación.
- El IV que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio de 2^{24} IV distintos. Esto no es problemático en una red casera con bajo tráfico, pero en una red que posea alto tráfico se puede agotar

el espacio de los IV en más o menos 5 horas. Si el atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener los textos en claro de ambas tramas mediante un ataque estadístico. Con el texto en claro de una trama y su respectivo texto cifrado se puede obtener la cifra de flujo; conociendo el funcionamiento del algoritmo RC4 es posible entonces obtener la clave secreta y descifrar toda la conversación.

- WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP. El primer programa que hizo esto posible fue WEPCrack, que consiste en una serie de scripts escritos en lenguaje Perl diseñados para analizar un archivo de captura de paquetes de un sniffer. La herramienta AirSnort9 hace lo mismo, pero integra las funciones de sniffer y rompedor de claves, y por lo tanto es más fácil de usar. Airsnort captura paquetes pasivamente, y rompe la clave WEP cuando ha capturado suficientes datos.

Los mecanismos de seguridad que ofrece el protocolo 802.11b pueden ser clasificados en las siguientes categorías:

- **Autenticación.** Cuando se desea establecer una comunicación entre dos dispositivos, debe primero establecerse una *asociació*n. Para ello el cliente

solicita la autenticación y el Punto de Acceso responde identificando el tipo de autenticación presente en la red. Posteriormente, el cliente procede con la autenticación y, si es satisfactoria, se lleva a cabo la asociación.

El primer paso para poder autenticar un cliente en una red *wireless* es el conocimiento del SSID *(Service Set Identifie*r), que funciona de forma similar al concepto de comunidad en SNMP, es decir, para obtener acceso al sistema es necesario conocer el SSID.

El estándar 802.11b plantea dos posibles formas de autenticación:

- **Open System:** Es el mecanismo de autenticación por defecto, y permite que cualquier estación se una al sistema tras la negociación de los parámetros de red necesarios, es decir, se utiliza autenticación NULA, en la que cualquier dispositivo puede obtener acceso a la red.
- **Shared Key:** Se lleva a cabo mediante un mecanismo de desafío/respuesta cifrado, siendo necesario durante el proceso que ambas estaciones posean una clave común (autenticación simétrica). Para que una red 802.11b pueda utilizar este tipo de autenticación, debe emplear el protocolo WEP.

- **Confidencialida**d. La confidencialidad en las redes wireless se obtiene mediante el uso de WEP como protocolo de cifrado.

- **Control de Acces**o. Cuando está activada la autenticación *shared ke*y, todos los paquetes deben estar correctamente cifrados, siendo descartados en caso contrario. Otra forma complementaria de control de acceso y autenticación se apoya en filtrado de tráfico por direcciones MAC en los puntos de acceso.
- **Integridad de dato**s. WEP utiliza un simple CRC32 (Código de Redundancia Cíclica) para asegurar la integridad de los datos, siendo insuficiente la utilidad y eficiencia de este control.

5.1.3. Método 3: Las VPN.

Una red privada virtual (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP.

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN.

Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado. La Figura 5.3 muestra la estructura de la red con la utilización de VPN.

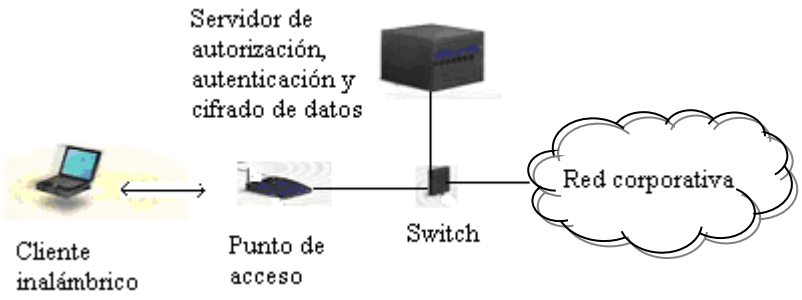

Figura 5.3. Estructura de una VPN para acceso inalámbrico seguro.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes.

Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.

5.1.4. Método 4: 802.1x.

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local cableadas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x.

El protocolo 802.1x involucra tres participantes (Ver Figura 5.4):

- El suplicante, o equipo del cliente, que desea conectarse con la red.
- El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS (Remote Authentication Dial-In User Service), cuya especificación se puede consultar en la RFC 2058. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las LAN.
- El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto, etc.) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

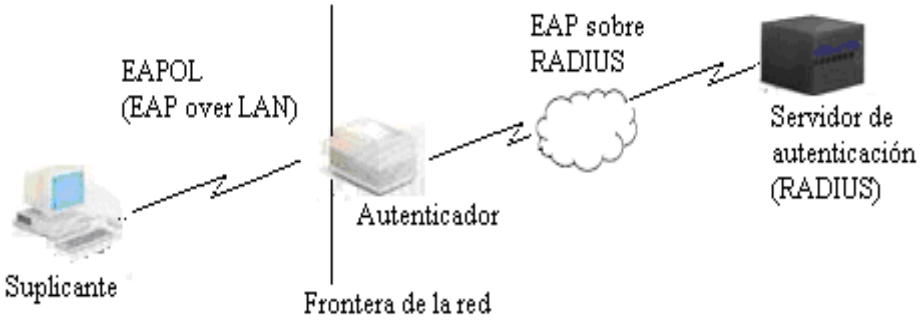

Figura 5.4. Arquitectura de un sistema de autenticación 802.1x.

La autenticación del cliente se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocol) y el servicio RADIUS, de la siguiente manera (Ver Figura 5.5):

- El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red (en el caso alambrado) o logra enlazarse o asociarse con un punto de acceso (en el caso inalámbrico). En ese momento, la interfaz de red tiene el acceso bloqueado para tráfico normal, y lo único que admite es el tráfico EAPOL (EAP over LAN), que es el requerido para efectuar la autenticación.
- La estación de trabajo envía un mensaje EAPOL-Start al autenticador, indicando que desea iniciar el proceso de autenticación.
- El autenticador solicita a la estación que se identifique, mediante un mensaje EAP-Request/ Identity.
- La estación se identifica mediante un mensaje EAP-Response/ Identity.
- Una vez recibida la información de identidad, el autenticador envía un mensaje RADIUS-Access-Request al servidor de autenticación, y le pasa los datos básicos de identificación del cliente.
- El servidor de autenticación responde con un mensaje RADIUS Access-Challenge, en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso. Dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función

criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje EAP-Request.

- El cliente da respuesta al desafío mediante un mensaje EAP-Response (Credentials) dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje RADIUS-Access-Response.
- Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje RADIUS-Access-Accept, que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red.
- El autenticador envía un mensaje EAP-Success al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS.

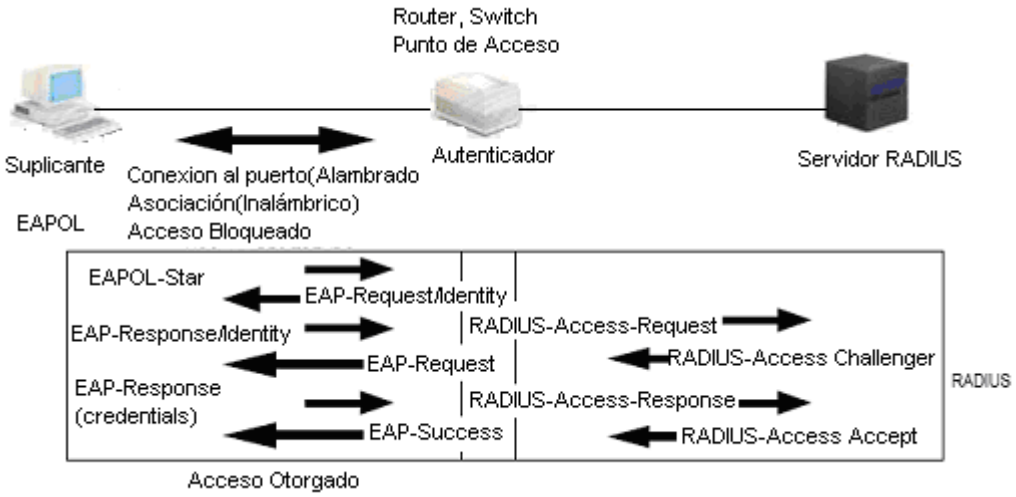

Figura 5.5. Diálogo EAPOL-RADIUS.

En el caso del acceso inalámbrico, el servidor RADIUS despacha en el mensaje RADIUS-Access-Accept un juego de claves WEP dinámicas, que se usarán para cifrar la conexión entre el cliente y el punto de acceso. El servidor RADIUS se encarga de cambiar esta clave dinámica periódicamente (por ejemplo, cada cinco minutos), para evitar el ataque de rompimiento de la clave descrito en la sección referente a WEP.

Existen varias variantes del protocolo EAP, según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas.

Las variantes de EAP que emplean certificados de seguridad son las siguientes:

- EAP-TLS: Requiere de instalación de certificados en los clientes y en el servidor. Proporciona autenticación mutua fuerte (es decir, el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEP. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Transparent Layer Substrate).
- EAP-TTLS: Desarrollada por Funk Software y Certicom. Proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor. Esto garantiza la autenticación fuerte del servidor por parte del cliente; la autenticación del cliente por parte

del servidor se efectúa una vez que se establece la sesión TLS, utilizando otro método tal como PAP, CHAP, MS-CHAP ó MS-CHAP v2.

- PEAP: Desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAPTTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

El empleo de certificados permite una autenticación fuerte entre cliente y servidor, sin embargo posee también varias desventajas:

- La administración de los certificados de seguridad puede ser costosa y complicada, especialmente en los esquemas donde se necesitan certificados en los clientes y en el servidor. Es necesario comprar los certificados a una autoridad de certificación (CA) conocida, o montar una CA propia.
- El diálogo de autenticación es largo. Esto ocasiona que el proceso sea algo demorado, siendo especialmente molesto para usuarios que tienen que reautenticarse con mucha frecuencia (por ejemplo, usuarios en movimiento que cambien de un punto de acceso a otro).
- La manipulación del certificado puede ser engorrosa para el usuario. En muchos casos se elige instalar el certificado en la terminal del usuario, con lo cual, si la terminal es robada y el certificado es el único nivel de seguridad que se posee, la seguridad de la red estaría en riesgo. Otra solución sería llevar

el certificado en una tarjeta inteligente (smart card), lo que obligaría a instalar hardware adicional en las terminales para leer dichas tarjetas.

Las variantes de EAP que utilizan contraseñas son las siguientes:

- EAP-MD5: Emplea un nombre de usuario y una contraseña para la autenticación. La contraseña se transmite cifrada con el algoritmo MD5. Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede ensayar a cifrar múltiples contraseñas con MD5 hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente). Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está conectando a la red adecuada), y el esquema no es capaz de generar claves WEP dinámicas. Por estos problemas, EAP-MD5 ha caído en desuso.
- LEAP: Esta variante es propietaria de Cisco. Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP. Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.
- EAP-SPEKE: Esta variante emplea el método SPEKE (Simple Password-authenticated Exponential Key Exchange), que permite verificar que tanto cliente como servidor comparten una información secreta (en este caso, una

contraseña) a través de un medio inseguro. Se ha comprobado que el método es muy seguro, aun con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servicio de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

5.1.5. Método 5: WPA (Wi-Fi Protected Access).

WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. TKIP amplía la longitud de la clave de 40 a 128 bits. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP. El protocolo TKIP está compuesto por los siguientes elementos:

- Un código de integración de mensajes (MIC), encripta el checksum incluyendo las direcciones físicas (MAC) del origen, del destino y los datos en

texto claro de la trama 802.11. Esta medida protege contra los ataques por falsificación.

- Contramedidas para reducir la probabilidad de que un ataque pueda aprender o utilizar una determinada llave.
- Utilización de un IV (vector de inicialización) de 48 bits llamada TSC (TKIP Séquense Counter) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden.

La estructura de encriptación TKIP propuesta por 802.11i sería la siguiente:

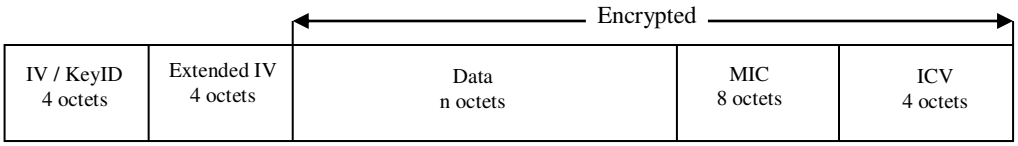

Figura 5.6. Estructura de encriptación de TKIP.

La utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de redecodificar la llave temporal durante una sola asociación. Pueden intercambiar 2^{48} paquetes utilizado una sola llave temporal antes de ser rehusada.

El proceso de encapsulación TKIP se muestra a continuación:

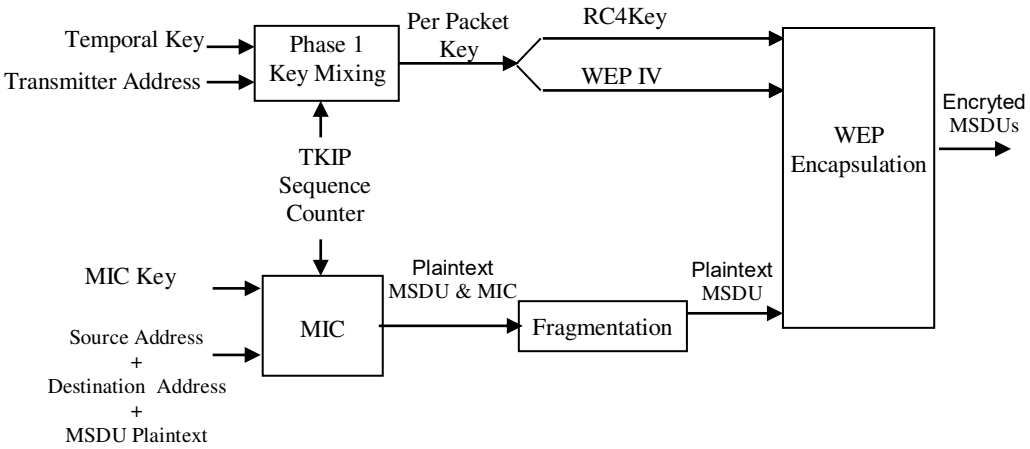

Figura 5.7. Proceso de encapsulación TKIP.

Se combinan en dos fases la llave temporal, la dirección del emisor y el TSC para la obtención de una llave de 128 bits por paquete, dividiendo en una llave RC4 de 104 bits y en una IV de 24 bits para su posterior encapsulación WEP.

El MIC final se calcula sobre la dirección física origen y destino y el MSDU (MAC Service Data Unit o texto plano de los datos en la trama 802.11) después de ser segmentado por la llave MIC y TSC.

La función MIC utiliza una función hash unidireccional, si es necesario, el MSDU se fragmenta incrementando el TSC para cada fragmento antes de la encriptación WEP.

En la desencriptación se examina el TSC para asegurar que el paquete recibido tiene el valor TSC mayor que el anterior. Sino el paquete de descartará para prevenir posibles ataques por repetición. Después de que el valor del MIC sea calculado

basado en el MSDU recibido y desencriptado, el valor calculado del MIC se compara con el valor recibido.

Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

1. **Modalidad de red empresarial:** Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.
2. **Modalidad de red casera, o PSK (Pre-Shared Key):** WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

La norma WPA data de abril de 2003, y es de obligatorio cumplimiento para todos los miembros de la Wi-Fi Alliance a partir de finales de 2003. Según la Wi-Fi

Alliance, todo equipo de red inalámbrica que posea el sello “Wi-Fi Certified” podrá ser actualizado por software para que cumpla con la especificación WPA.

5.2. Análisis de Métodos.

La seguridad en las redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite. Sin embargo, la gran cantidad de las redes inalámbricas actualmente instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, con lo cual se está poniendo en peligro la confidencialidad e integridad de dicha información.

Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas. Su implementación depende del uso que se vaya a dar a la red (casera o empresarial), de si es una red ya existente o una nueva, y del presupuesto del que se disponga para implantarla, entre otros factores.

La restricción de acceso mediante direcciones MAC es insuficiente para cualquier red, dado el gran número de herramientas disponibles libremente para cambiar la dirección MAC de una tarjeta cualquiera.

El método mediante WEP con clave estática es el mínimo nivel de protección que existe. En una red casera puede ser suficiente; en una corporativa, el uso de WEP está

formalmente desaconsejado, por la facilidad con la que se pueden romper las claves WEP en un entorno de alto tráfico.

El uso de las VPN es una alternativa interesante cuando ya se tiene una red inalámbrica, y no se posee hardware inalámbrico que soporte el protocolo 802.1x.

Requiere de la instalación de software especializado en los clientes inalámbricos, y de un servidor o una serie de servidores que manejen las tareas de cifrado de datos, autenticación y autorización de acceso.

La alternativa de 802.1x y EAP es la adecuada si los equipos de la red inalámbrica se pueden actualizar, o si se va a montar una red nueva. Puede usarse la solución de WEP con clave dinámica, o la de WPA; ambas ofrecen un excelente grado de protección.

Finalmente, todo mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada. El seguimiento de una política consistente evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, y garantiza la calidad y confidencialidad de la información presente en los sistemas de la empresa.

En la Tabla 5.1. se resumen las características 802.11 y WPA antes mencionadas.

Características			802.11	WPA
Cifrado	**Sistema (Algoritmo) de cifrado**		WEP (RC4)	TKIP (RC4)
	Longitud		40 bits	128 bits
	Gestión de claves	**Generación clave**	Estática: la misma para todos los dispositivos	Dinámica: por usuario, por sesión, por paquete
		Distribución clave	Manual en cada dispositivo.	Automática gestionada por 802.1x/EAP
Autenticación	**Entorno**		Definido por 802.11	802.1x/EAP
	Método		Abierta clave compartida (autentifica el equipo)	EAP-TLS, PEAP, EAP-TTLS (autentifican al usuario)

Tabla 5.1. Características de seguridad IEEE 802.11 y WPA.

5.3. Garantizando la Seguridad de una Red Inalámbrica.

Para poder considerar una red inalámbrica como segura, debería cumplir con los siguientes requisitos:

- Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas

direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.

- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

5.4. Consejos de Seguridad.

Para que un intruso se pueda meter a nuestra red inalámbrica tiene que ser nodo o usuario, pero el peligro radica en poder escuchar nuestra transmisión. Vamos a dar unos pequeños consejos para poder estar más tranquilos con nuestra red inalámbrica.

1. **Haga más sencilla la seguridad:** Integre las políticas inalámbricas y las de cable. La seguridad inalámbrica no es una infraestructura de red aparte cuyos procedimientos o protocolos son completamente distintos. Desarrolle una política de seguridad que combine tanto seguridad inalámbrica como seguridad para la red de cable, para impulsar las ventajas de gestión y de ahorro de costos. Por ejemplo, integrando la petición de nombre de usuario y contraseña para todos los usuarios que accedan a la red ya sea mediante infraestructura de cable o inalámbrica.

2. **Situar el punto de acceso en el lugar adecuado:** Comience con lo más básico: en la configuración de la red de su empresa, asegúrese de que los puntos de acceso están fuera de su firewall perimetral en el caso de que su solución inalámbrica no cuente con los sistemas de encriptación y autenticación requeridos, de esta manera su firewall perimetral controlará los accesos. Además se debe cambiar las claves por defecto cuando instalemos el software del Punto de Acceso
3. **Utilizar una dirección MAC para evitar ataques:** Utilizar una dirección MAC basada en ACLs (Access Control Lists) hará que sólo los dispositivos registrados puedan acceder a la red. El filtro mediante direcciones MAC es como añadir otro cerrojo a la puerta principal, y cuantos más obstáculos encuentre un hacker, más rápidamente desistirá en sus intenciones de intrusión a nuestra red.
4. **Administrar su nombre de red:** Todas las redes inalámbricas tienen asignado por defecto un nombre de red o SSID (Service Set Identifier). Cámbielo, inmediatamente, por un código alfanumérico. Si su organización puede encargarse de la administración de la red, cambie del SSID de forma regular, e inutilice la función de reconocimiento automático de la contraseña en su ordenador, para evitar que el SSID sea identificado fácilmente.
5. **Impulsar los servidores RADIUS existentes:** Los usuarios remotos de las compañías más grandes son a veces autenticados para utilizar la red a través de un servidor RADIUS (Remote Authentication Dial-In User Service). Los

directores de TI pueden integrar las redes LAN inalámbricas en la infraestructura RADIUS ya establecida para hacer más sencilla su gestión. Esto no sólo hace posible la autenticación inalámbrica, sino que además asegura que los usuarios de la red inalámbrica siguen el mismo proceso de y aprobaciones que los usuarios remotos.

6. **Instalar el Protocolo de seguridad WEP:** WEP (Wired Equivalent Privacy) es el protocolo de seguridad inalámbrico del estándar 802.11b. Se ha diseñado para proporcionar protección mediante encriptación de datos al tiempo en que se transmite la información, exactamente igual que se hace en las redes de cable. Sólo tiene que instalarlo, habilitarlo y cambiar de forma inmediata la clave WEP, ya que aparecerá una por defecto. Lo ideal es que genere sus claves WEP de forma dinámica cuando un usuario se identifique, haciendo que la clave de acceso a la red inalámbrica sea diferente para cada usuario y en cada ocasión, de esta manera se consigue una mejor protección.
7. **VPN:** Si cada opción de seguridad es un impedimento que un hacker debe salvar (cambiar el SSID, habilitar filtros mediante direcciones MAC y generar claves WEP de forma dinámica) una red privada virtual o VPN es una cámara acorazada. Las VPN ofrecen un nivel más de seguridad basado en la creación de un túnel seguro entre el usuario y la red.
8. **No todas las Redes Inalámbricas son iguales:** Mientras que 802.11b es un protocolo estándar y todos los equipos que lleven la acreditación Wi-Fi operan con la misma funcionalidad base, no todos los dispositivos inalámbricos han

sido creados de la misma manera. Wi-Fi asegura interoperabilidad, mientras que los productos de muchos fabricantes no incluyen prestaciones avanzadas de seguridad.

9. **No permita que cualquier "usuario avanzado" configure su red inalámbrica:** La configuración de una WLAN es lo suficientemente sencilla como para que no haga falta que el personal técnico instale los puntos de acceso en su propio departamento, sin pararse a pensar demasiado en el aspecto de la seguridad. Antes debe analizarse la red regularmente, con herramientas de detección de intrusos para evitar que la red pueda convertirse en un punto potencial susceptible de ser atacado por un hacker. Por tanto, se debe establecer una política que restrinja que las WLANs puedan ser implementadas sin el desarrollo y aprobación del administrador de la red.
10. **Utilizar opciones no compatibles,** si nuestra red es de una misma marca podemos escoger esta opción para tener un punto mas de seguridad, esto hará que nuestro posible intruso tenga que trabajar con un modelo compatible al nuestro.

CAPÍTULO 6

POLÍTICAS GENERALES EN REDES WLAN.

Las políticas de seguridad documentadas permiten a una organización definir arquitecturas aceptables para la aplicación y uso de tecnologías inalámbricas.

Un programa de conocimiento de seguridad ayuda que los usuarios establezcan una buena práctica de la seguridad para prevenir ataques ya que entendiendo el valor de los recursos orgánicos y el nivel de protección requerido es posible habilitar más soluciones inalámbricas rentables que proporcionan un el nivel apropiado de seguridad.

6.1 Tipos de Políticas.

La definición de políticas va a depender de cada empresa, de manera general las hemos clasificado de la siguiente forma:

- Políticas de Administración.
- Políticas Técnicas.
- Políticas de Operación.

6.1.1. Políticas de Administración.

1. Desarrolle políticas de seguridad dirigidas al uso de tecnología inalámbrica, incluyendo el 802.11.
2. Asegurar que los usuarios en la red tengan el conocimiento de la seguridad y los riesgos asociados con la tecnología inalámbrica.
3. Realizar una valoración de riesgo para conocer el valor de los recursos que necesitan protección.
4. Asegure que el cliente NIC y Punto de Acceso tengan las licencias respectivas para actualizar los parches de seguridad cuando ellos ya estén disponibles.
5. Realizar las valoraciones de seguridad regularmente y en intervalos aleatorio para entender la red inalámbrica totalmente.
6. Asegurar los límites y alrededores del perímetro del edificio.
7. Controlar los accesos físicos al edificio y otras áreas por ejemplo con el uso de identificaciones, lectores de tarjetas de asistencia, etc.
8. Realice un completo estudio del sitio para establecer la posible ubicación de los Puntos de Acceso.

9. Se debe contar con un completo inventario de todos los Puntos de Acceso y dispositivos inalámbricos.
10. Asegurar que las redes inalámbricas no se usen hasta que se cumplan con las políticas de seguridad.
11. Localizar los Puntos de Acceso en el interior del edificio en lugar de en las paredes exteriores y lugares cercanos a las ventanas.
12. Colocar los Puntos de Acceso en las áreas aseguradas para prevenir el acceso físico y la manipulación por parte de usuarios desautorizados.

6.1.2. Políticas Técnicas

1. Realizar las pruebas a los Puntos de Acceso para determinar la magnitud precisa de los límites de la red inalámbrica.
2. Asegúrese que los Puntos de Acceso están apagados cuando ellos no se usan por ejemplo, los fines de semana.
3. Para restablecer la función en los Puntos de Acceso sólo se realizará por un grupo de personas autorizadas.
4. Restaure los Puntos de Acceso a las últimas escenas de seguridad después de que se restablezca la función.
5. Cambie el SSID predefinido en los Puntos de Acceso.
6. Desactive la transmisión que SSID ofrece para al cliente.
7. Valide que el SSID no refleje el nombre de la empresa, la división, departamento, la calle, productos, etc.

8. Asegurar que los canales de los Puntos de Acceso esta por lo menos a cinco canales diferentes de cualquier otro de las redes inalámbricas cercanas para prevenir la interferencia.
9. Cambiar todos los parámetros predeterminados.
10. Desactive todo los protocolos inseguros que no son esenciales en los Puntos de Acceso.
11. Habilitar todas las seguridades que ofrecen los productos WLAN, incluso la autenticación criptográfica y la privacidad que ofrece WEP.
12. Asegúrese que el tamaño de encriptación sea de por lo menos 128 bits o tan grande como sea posible.
13. Remplace periódicamente las claves.
14. Instale un firewall propiamente configurado entre la infraestructura cableada y la red inalámbrica (Punto de Acceso o hub a otros Puntos de Acceso).
15. Instale software antivirus en los clientes inalámbricos.
16. Instale un firewall personalizado en todos los clientes inalámbricos.
17. Desactive los archivos compartidos en los clientes inalámbricos.
18. Despliegue las listas de control de acceso MAC.
19. Considere instalación de Switches en lugar de los hubs para la conectividad de los Puntos deAcceso.
20. Despliegue las IPsec basadas en VPN la tecnología para comunicaciones inalámbricas.

21. La encriptación usada debe ser suficiente para la sensibilidad de los datos en la red y el procesador de las computadoras.
22. Realizar pruebas y actualizaciones regulares al software.
23. Todos los Puntos de Acceso deben tener una contraseñas administrativas que contenga una combinación que no se fácil de descifrar.
24. Todas las contraseñas deben cambiarse regularmente.
25. Controlar la autenticación del usuario con el uso de métodos biométricos, tarjetas inteligentes, PKI, etc.
26. El modo ad hoc para 802.11 será deshabilitado cuando exista riesgo.
27. Use IP estático en la red.
28. Desactivar DHCP.
29. Habilitar los mecanismos de autenticación de usuario para las interfaces de los Puntos de Acceso.
30. Asegurar que el tráfico de dirección destinado para Puntos de Acceso esta conectado adelante a la red.
31. Use SNMP V.3 y/o SSL/TLS para la administración Web basado en Puntos de Acceso.

6.1.3. Políticas Operacionales

1. Configurar SNMP en los Puntos de Acceso para el menor privilegio (es decir, sólo lectura).
2. Desactive SNMP si no se usa.

3. Reforzar la seguridad de la administración de Puntos de Acceso usando SNMP V3 o equivalentes.
4. Usar la interfaz del puerto serial local para la configuración de Puntos de Acceso para minimizar la exposición de información sensible.
5. Utilizar otras formas de autenticación como RADIUS y Kerberos.
6. Utilizar agentes de detección de intrusión en la parte inalámbrica de la red, para descubrir conductas sospechosas o acceso desautorizado.
7. Despliegue interviniendo la tecnología para analizar los archivos producidos por Radius para la actividad sospechosa.
8. Utilizar producto de seguridad 802.11 que ofrecen otras seguridades tal como protección criptográfica reforzada o de autorización de usuario.
9. Habilitar utilización de claves (802.1X) en lugar de las claves predefinidas para sesiones WEP distintas.
10. Verificar los impactos de desplegar cualquier producto de seguridad antes de su utilización.
11. Designar a una persona para rastrear el progreso de seguridad de los productos 802.11 y normas (IETF, IEEE, etc.), las amenazas y vulnerabilidades con la tecnología.
12. Esperar hasta que las actualizaciones de la tecnologías 802.11 WLAN proporcione seguridad.
13. Los Puntos de Acceso que ya no se usarán eliminar la configuración para prevenir descubrimiento de red la configuración, las contraseñas, etc.

CAPÍTULO 7

HERRAMIENTAS DE GESTIÓN.

7.1. Generalidades.

Existen en el mercado diferentes tipos de dispositivos inalámbricos y herramientas para la Administración de redes inalámbricas, los cuales presentan diferentes técnicas para asegurar la red.

En este caso hemos seleccionado la marca Lucent Technologies con su línea inalámbrica Orinoco.

Los productos de la familia Orinoco, son un sistema de equipos de red que permiten la construcción de cualquier tipo de configuración de red, desde una pequeña red inalámbrica hasta una completa y gran infraestructura inalámbrica.

Los productos de la familia Orinoco consisten de:

- Tarjetas de red inalámbricas.
- Adaptadores USB.
- Puntos de Acceso.
- Antenas extensoras de rango.

En cuanto a software, Orinoco consiste en un sistema de herramientas de gestión que permiten:

- Mostrar y modificar la configuración (remota) de los componentes de la red.
- Configurar los componentes de red, tal como los puntos de acceso.
- Diagnosticar el funcionamiento de la red y, si es necesario, identificar y resolver errores en la misma.
- Administrar y optimizar el funcionamiento de la red.

El software Orinoco consiste de las siguientes herramientas:

- Administrador del cliente Orinoco (Client Manager).
- Administrador OR Orinoco (OR Manager).
- Administrador PRO Orinoco.
- Administrador de Punto de Acceso Orinoco.

Estas herramientas pueden ser instaladas en estaciones que corran Microsoft Windows 95, 98, NT 4.0, o 2000.

En este caso vamos a detallar los niveles de seguridad que los dispositivos y herramientas que ORINOCO implementan para redes inalámbricas, comparando con las metodologías existentes descritas en capítulos anteriores.

7.2. Seguridad.

La seguridad que incluye los equipos Orinoco e implementando las metodologías descritas anteriormente en el capítulo 5 se resumen en lo siguiente:

- Seguridad en el acceso a los datos inalámbricos.
- Encriptación de los Datos inalámbricos.
- Seguridad en la configuración de los puntos de acceso.

7.2.1. Seguridad en el Acceso a los datos inalámbricos.

Para prevenir el acceso no autorizado a los datos que se transmiten sobre la red, los equipos Orinoco cuentan con los siguientes niveles de seguridad:

- Restricción del acceso inalámbrico a la red.
- Encriptación de los datos.

Estas medidas de seguridad, que se aplican a las comunicaciones en la capa física, complementan la validación del nombre de usuario y contraseña en la capa de red, además de que algunos equipos dan soporte para RADIUS.

7.2.1.1. Restricción del Acceso Inalámbrico a la Red.

Para excluir a dispositivos de cómputo no autorizados y desconocidos del establecimiento de una conexión inalámbrica a la red, se pueden utilizar las siguientes opciones (Ver Figura 7.1):

1. **Close Wireless System:** Esta opción cierra la red a todas las estaciones que no han sido configuradas correctamente con el nombre red (network name).

   Cerrar la red inalámbrica previene el acceso de usuarios no autorizados a los puntos de acceso. Si un usuario trata de accesar a la red sin configurar su estación con el correcto nombre de red, la estación no será capaz de verse con los Puntos de Acceso.

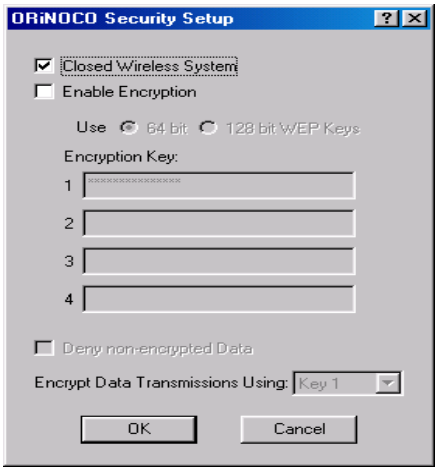

Figura 7.1. Cerrando la red inalámbrica

Hay 2 opciones para este tipo de seguridad de acceso: Abierto y Cerrado

- Configuración abierta: Es una de las aplicaciones del estándar IEEE 802.11, modo que permitirá accesar a los Puntos de Acceso desde:

  - Todas las estaciones que tengan el correcto nombre de red.
  - Todas las estaciones que tenga como nombre de red **"Any".**

- Configuración cerrada: Es el modo propietario que usa Lucent Technologies; que cierra la red para todas las estaciones que no han sido configuradas con el nombre correcto de red. Esta opción denegará el acceso a:

  - Todas las estaciones que tengan configuradas como nombre de red "Any" y
  - Todas las estaciones que no sean Orinoco.

Para habilitar esto, se ingresa al Punto de Acceso que desee y se selecciona **Setup/Interface Setup/Setup2/Security**, del Administrador OR , luego marcar la opción **Close Wireless System**; si esta opción no es marcada la red permanecerá abierta.

2. **Access Control:** Esta opción permite usar tablas de control de acceso, para construir una lista de estaciones autorizadas permitidas y así establecer una conexión inalámbrica a la red.

Otro método para restringir el acceso inalámbrico a los Puntos de Acceso es el uso de las tablas de control de acceso, contenidas en la opción **Setup/Access Control** del Administrador OR (Ver Figura 7.2) .

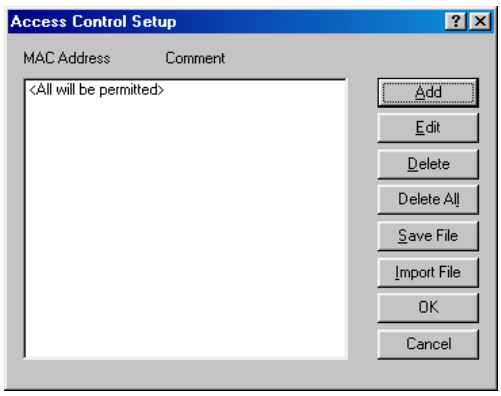

Figura 7.2. Control de Acceso por direcciones MAC

Si se decide habilitar la tabla de control de acceso, entonces el Punto de Acceso:

- Solamente permitirá el paso de mensajes, desde/hacia estaciones autorizadas que han sido identificadas en la tabla de control de acceso.
- Ignorará todas las demandas de reenviar los datos desde/hacia estaciones no listadas.

Habilitar el control de acceso es un mecanismo de seguridad más rígido que el de "Cerrar la Red Inalámbrica", ya que requiere que el administrador de la LAN autorice a cada tarjeta PC.

Para autorizar el acceso a la red de las estaciones inalámbricas el administrador de la LAN debe:

- Agregar la dirección MAC de cada tarjeta PC, correspondiente a cada estación en el archivo de la tabla de control de acceso.
- Descargar el archivo de la tabla de control de acceso para todos los Puntos de Acceso.

7.2.2. Encriptación de los Datos Inalámbricos.

Para proveer un nivel más alto de seguridad para la transmisión de los datos, se puede usar la encriptación de datos WEP (Wired Equivalent Privacy) que permite encriptar todos los datos que serán transmitidos por el medio LAN inalámbrico.

Se pueden especificar hasta 4 diferentes llaves para desencriptar los datos inalámbricos, y seleccionar una de las llaves para encriptarlos. La opción de usar las cuatro diferentes llaves para desencriptar los datos inalámbricos, permite cambiar sus llaves WEP en intervalos regulares sin afectar el desempeño de la red.

Para habilitar la encriptación en el Punto de Acceso, se selecciona la opción **Setup / Setup Interface / Setup 2/ Security** del Administrador OR (Ver Figura7.3).

.

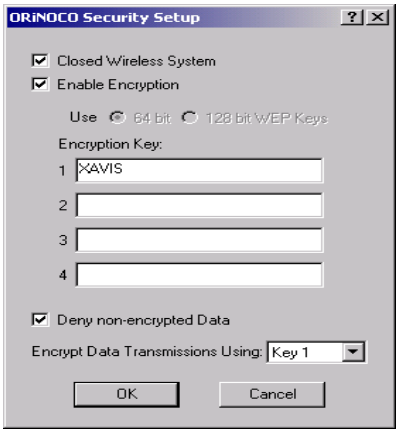

Figura 7.3. Configurando la Encriptación

Luego seguir los siguientes pasos:

- Seleccione la opción **Enable Encryption.**
- Ingrese 4 diferentes llaves para desencriptar los datos recibidos vía la interfase inalámbrica.
- Seleccione una de estas claves, para encriptar los datos inalámbricos que están siendo transmitidos vía la interfase inalámbrica.

Esta misma configuración de encriptación debe ser también cargada en las estaciones. Para la tarjeta Orinoco Silver los valores válidos (llaves para encriptar) son:

- 5 dígitos de valor alfanuméricos en el rango de “a-z” y “0-9” .
- 10 dígitos de valor hexadecimal, precedido por los caracteres “0x” (zero x), por ejemplo: 0xABCD1234FE

Para la tarjeta Orinoco Gold los valores válidos (llaves para encriptar) son:

- 13 dígitos de valor alfanuméricos en el rango de “a-z” y “0-9”, por ejemplo: SECURE1234567.
- 26 dígitos de valor hexadecimal, precedidos por los caracteres “0x” (zero x), por ejemplo: 0xABCD1234FE.
- Opcionalmente se pueden también usar los valores de la tarjeta Silver.

Las cadenas hexadecimales que no estén precedidas de “0x” serán interpretadas como una cadena alfanumérica.

Como se muestra en la Figura 7.3, existe otra opción **Deny non-Encrypted data**, que siempre debería estar habilitada, ya que permite que el Punto de Acceso sólo procese mensajes recibidos en la interfaz inalámbrica cuando éstos han sido encriptados con una de las 4 llaves de identificación. Esto brinda una óptima seguridad contra accesos no autorizados en la red.

Si la opción **Deny non-Encrypted data** no es habilitada, entonces el punto de acceso procesará todos los mensajes recibidos en la interfaz inalámbrica, indiferentemente si el mensaje ha sido encriptado con una de las llaves de identificación o no.

7.2.3. Seguridad en la Configuración de los Puntos de Acceso.

Medidas de seguridad, como el control de acceso, llegan a hacer inefectivas cuando personas no autorizadas pueden ver y modificar la configuración de los puntos de acceso.

Para proteger la configuración de red de modificaciones indeseadas, se recomiendan implementar las siguientes medidas:

- Contraseñas de lectura y lectura/escritura.
- Lista de accesos de direcciones IP SNMP.
- Mecanismo de Alerta de mensajes traps a la estación (opcional).

7.2.3.1. Contraseñas de Lectura y Lectura / Escritura.

Para restringir el acceso a la información de configuración del Punto de Acceso, se pueden crear 2 niveles de autorización de contraseñas:

1. **Contraseña de Lectura:** La contraseña de lectura, sólo proveerá acceso a los Puntos de Acceso para monitorear la información de diagnóstico, encontrada en la opción de Monitoreo en la ventana principal del Administrador OR.

   Para definir una contraseña de lectura:

   1. Seleccione la opción **Setup / Parámetros SNMP** (Ver Figura 7.4).

2. En el campo contraseña de lectura se ingresa la contraseña. El valor por defecto es public (dicho valor debe ser cambiado por una contraseña personalizada).

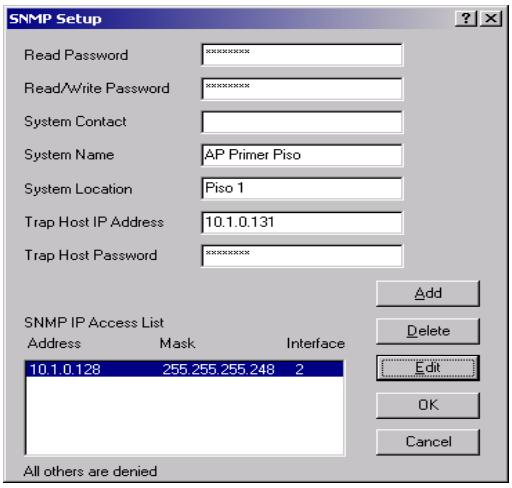

Figura 7.4. Configurando la Seguridad SNMP.

2. **Contraseña de lectura/escritura.-** La contraseña de lectura / escritura, proveerá de un acceso total para visualizar la información de diagnóstico del Punto de Acceso, es decir no solo permitirá monitorear la red, si no también configurar el punto de acceso. Si se ingresa una contraseña errónea resultará un **error fuera de tiempo**, o "**error SNMP**".

Para definir una contraseña de lectura/escritura, se siguen los mismos pasos descritos en el parámetro contraseña de lectura, y se escribe en el campo **read-write password** la contraseña deseada (de igual forma esta contraseña de acceso total debe ser personalizada).

7.2.3.2. Lista de Acceso IP SNMP.

Se puede usar las listas de acceso SNMP para crear un nivel extra de seguridad en adición a las contraseñas de lectura y lectura /escritura. Esto permitirá a un número limitado de estaciones de gestión visualizar y/o modificar los parámetros de los Puntos de Acceso, basándose en las direcciones IP de estas estaciones.

En el campo de listas de acceso, típicamente deberían incluir todas las direcciones IP de las estaciones de gestión que usarán el administrador OR para configurar y/o monitorear los puntos de acceso.

Para autorizar las estaciones de gestión se debe ingresar:

- La dirección IP de la estación y,
- La interfaz de red del Punto de Acceso a través de la cual se ingresará al mismo.

Para indicar la interfaz se usa:

- "1" para la ethernet.
- "2" para la interfaz de red inalámbrica A.
- "3" para la interfaz de red inalámbrica B.

Alternativamente se puede usar el valor “X”, para permitir el acceso al punto de acceso por cualquiera de las interfaces disponibles.

Para permitir que múltiples estaciones de gestión accedan a la configuración y/o monitoreo de los Puntos de Acceso, se puede asignar también un rango de direcciones IP. Para esto, se ingresa la máscara de subred que indicarán las estaciones autorizadas para modificar los parámetros.

Cuando la dirección IP o interfaces no concuerde con el listado, en la lista de acceso SNMP IP el solicitante recibirá un error fuera de tiempo.

Para autorizar a una estación administradora, vía lista de acceso SNMP IP, se selecciona la opción **Setup / Parámetros SNMP**, (Ver Figura 7.4).

Usar los siguientes botones para modificar la lista de acceso SNMP IP:

- Agregar: Para añadir una dirección IP a la lista.
- Borrar: Para quitar la dirección IP de la lista.
- Edit: para cambiar entradas en la lista.

El valor por defecto es <Todos serán permitidos>.

7.2.3.3 Mecanismo de Alertas de mensajes Trap hacia la estación.

Se puede usar el mecanismo de traps a la estación de gestión, para informar al administrador de la red cuando alguien resetea el Punto de Acceso, o si hay una autentificación fallida, o cuando un enlace se levanta o se cae; es decir cuando ocurren eventos.

La alerta de traps a la estación, permite al administrador de red verificar si estos eventos fueron originados por usuarios autorizados o no.

Para activar el mecanismo de traps a la estación:

1. Se selecciona la opción **Setup / Parámetros SNMP** (Ver Figura 7.4).
2. En el campo **Trap Host IP Address**, se ingresa:
    - La dirección IP de la estación de gestión, a esta dirección se enviarán los mensajes, por ejemplo si el Punto de Acceso es reseteado.
    - (Valor inicial, 0.0.0.0) – Para deshabilitar el agente Trap SNMP.
3. Se ingresa una contraseña en el campo **Trap Host Password**. Se escoge una contraseña que corresponda a la contraseña ingresada en la estación trap, para filtrar mensajes no solicitados o no autorizados en esta estación.

La contraseña será incluida en el mensaje trap SNMP enviados por este Punto de Acceso. Si la estación trap recibe un mensaje sin contraseña o con una contraseña desconocida, el mensaje trap será ignorado.

- Valores válidos: Cualquier valor alfanumérico en el rango de a-z, 0-9 con un mínimo de 2 y un máximo de 31 caracteres.
- Valor inicial: **public**.

7.3. Herramientas de Auditoria.

En el mercado se pueden conseguir herramientas que fácilmente detectan una red inalámbrica y pueden ser utilizadas para emitir algún tipo de ataque a la red, sin embargo estas herramientas pueden ser utilizadas para hacer un seguimiento de la red, y poder realizar auditorias, detección de intrusos, etc.

Algunas de estas herramientas están orientadas a realizar scanneos de la red, hasta crakear las claves. A continuación mencionaremos algunos tipos de herramientas:

- **Sniffers WLAN:** Un sniffer es un programa para monitorear y analizar el tráfico de una red, pueden ser utilizados para capturar lícitamente o no los datos que son transmitidos en la red.

  La Tabla 7.1 lista algunos sniffers utilizados en diferentes plataformas.

NOMBRE	PLATAFORMA
Mognet	Java VM
Kismet	Linux, iPaq, Zaurus
Ethereal	Unix, Windows
TCPDump	Unix
PrismDump	Unix
PrismDump2	BSD
AiroPeek	Windows
Gifit	Windows, Linux
Sniffer Wireless	Windows

Tabla 7.1. Sniffers WLAN.

- **Ethereal:** Esta herramienta gratuita permite capturar tráfico de redes, fue desarrollado en sistemas UNIX pero se encuentra disponible para otros sistemas operativos como Windows, es ideal para averiguar la dirección ip del punto de acceso del cual se recibe la señal, además de filtrar capturas es muy fácil de utilizar. (Ver Figura 7.5.).

  Puede leer más de 20 tipos de formatos distintos y se destaca por su impresionante soporte de más de 300 protocolos, entre los cuales podemos mencionar: TCP(Transmission Control Protocol), ICMP(Internet Control Messagging Protocol), UDP(User Datagram Protocol), DHCP(Dynamic Host Configuration Protocol), ARP(Address Resolution Protocol), VTP(Virtual Trunking Protocol), SMTP(Simple Mail Transfer Protocol),etc.

Brinda soporte para los siguientes tipos de redes: Ethernet, FDDI, Token-ring, IEEE 802.11, ATM, etc.

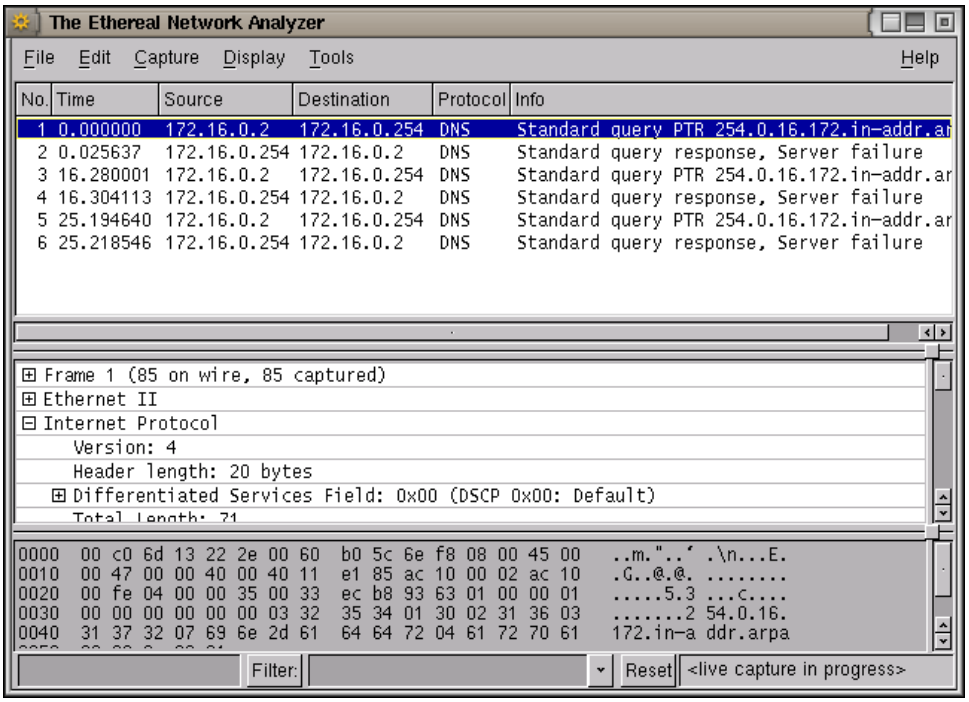

Figura 7.5. Herramienta de monitoreo Ethereal.

- **Getif:** Es un visor de datos SNMP, el cual permite visualizar datos en algunos casos comprometedores de ciertos dispositivos, inclusive topologías de red, por defecto utiliza las comunidades "public y private". (Ver Figura 7.6.).

  Otra aplicación interesante de este gestor es la posibilidad de visualizar respuestas de rangos de IP, indicando que direcciones IP están respondiendo al escaneo de la red.

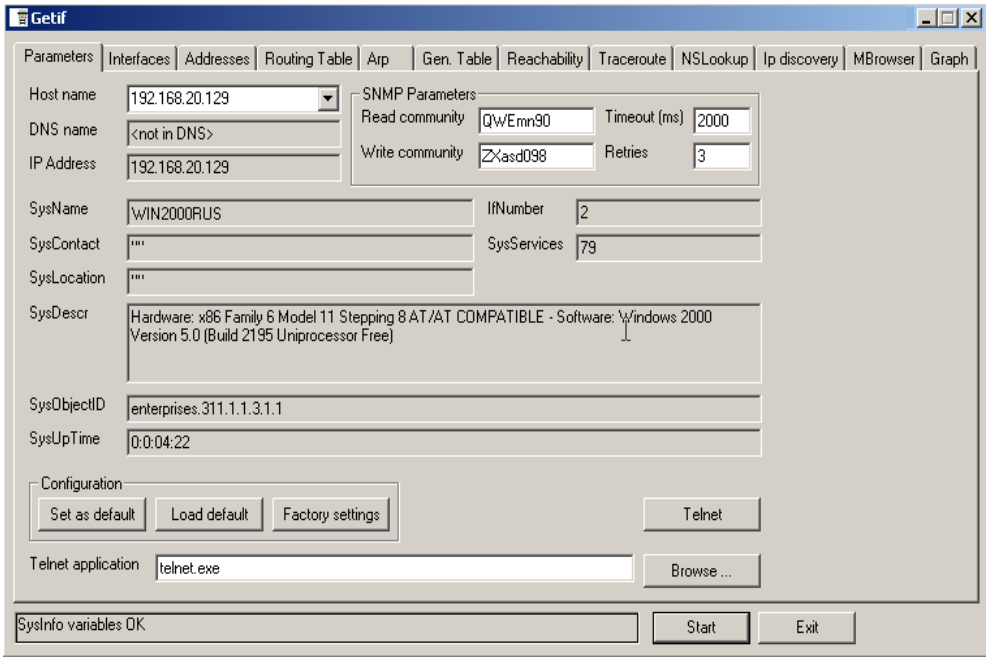

Figura 7.6. Herramienta de Monitoreo Getif.

- **Scanners WLAN:** La Tabla 7.2. listas algunos scanners y también conocidos como sniffers, que también detectan las actividades de la red.

NOMBRE	PLATAFORMA
NetStumbler	Windows
MacStumbler	Macintosh
SSIDSniff	Unix
AP Scanner	Macintosh
Wavemon	Linux
WLAN Expert	Windows
Wavelan-tools	Linux
Sniffer Wireless	Windows
TCH-Wardrive	Linux

Tabla 7.2. Scanners WLAN.

- **Network Stumbler:** La principal virtud de esta herramienta radica en su sencillez de manejo, además de realizar una muy buena descripción de los tipos de infraestructura y niveles de seguridad que se encuentran en los dispositivos. Con esta herramienta es posible establecer la posición exacta de los Puntos de Acceso y permite reconfigurar automáticamente la tarjeta de red wireless para obtener servicio del Punto de Acceso. (Ver Figura 7.7).

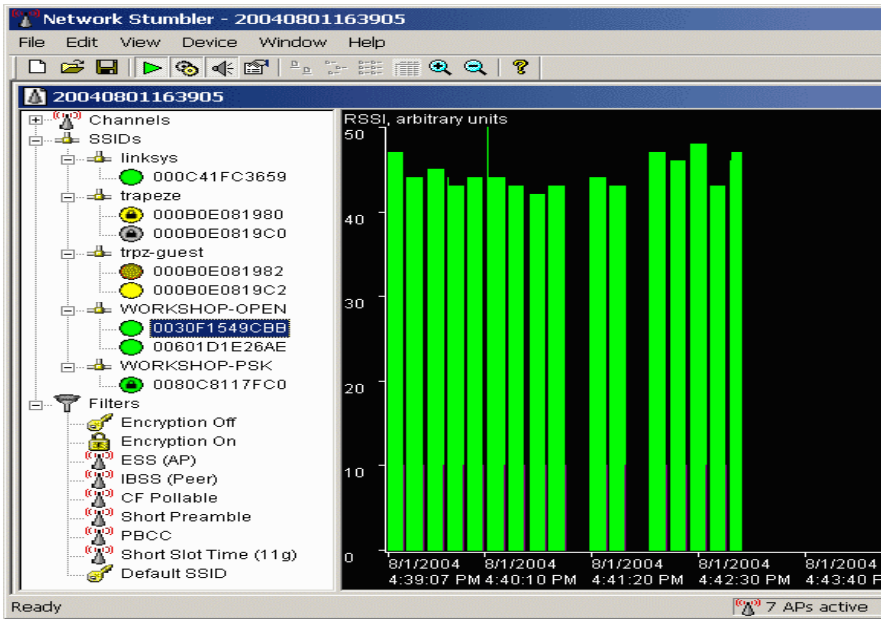

Figura 7.7. Herramienta de monitoreo Network Stumbler.

- **WEP key crackers:** Permite obtener la clave WEP modificando el firmware de las tarjetas. La Tabla 7.3. lista algunos de los programas utilizados para este propósito.

NOMBRE	PLATAFORMA
WEPCracker	Linux
Airsnort	Windows, Linux
Airsnort for BSD	BSD

Tabla 7.3. WEP key crackers.

- **AirSnort:** Este software es capaz de recuperar las claves del cifrado WEP de las redes wireless, el principal problema reside principalmente en el tipo de tarjeta que se utiliza para activar el tipo monitor, el chipset debería ser Orinoco o PRISM.

  Funciona pasivamente controlando las transmisiones, y procesando las claves de codificación, una vez que ha acumulado 100 Megas de datos puede descifrar las contraseñas de encriptación en menos de un segundo.(Ver Figura 7.8.)

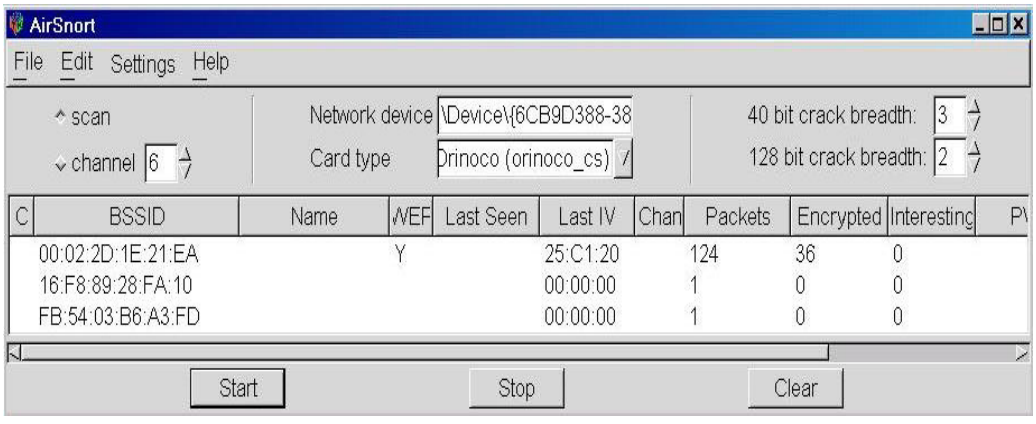

Figura 7.8. Herramienta de monitoreo AirSnort.

CAPITULO 8

COSTO Y BENEFICIO DE IMPLEMENTACIÓN WLAN.

Descripción del Caso de Estudio: Una compañía industrial, desea automatizar sus procesos entre el área de producción y el de distribución y almacenaje.

Para esto, es necesario realizar la evaluación de las posibilidades de infraestructura de red, mediante un análisis de costo beneficio y conocer así la mejor opción para la implementación de la red.

La compañía cuenta para éstas áreas con 20 estaciones de trabajo divididas en la siguiente forma:

- 15 estaciones para el área de producción que comprendidos por la gerencia, control de calidad, laboratorio e investigación y desarrollo; éstos se encuentran en el primer piso alto de la empresa.

- 5 estaciones para el área de distribución y almacenaje, repartidos en las bodegas de productos terminados, materia prima y material de empaque, además del área de despacho y distribución de los productos; éstas áreas están localizadas en la planta baja.

8.1. Análisis de Costo.

A continuación se realiza un análisis de costo para la implementación de una red, pudiendo ser ésta WLAN, LAN cableada o mixta.

8.1.1. Costo de Implementación.

8.1.1.1. Costo de Implementación WLAN.

A continuación, en la Tabla 8.1., se detallan los costos de todo el hardware requerido, incluyendo los costos de configuración de los puntos de red; para la puesta en marcha de la WLAN. En el costo del Punto de Acceso está incluido el software de administración y seguridad.

Cant.	Descripción	Costo Unitario	Costo Total
2	ORINOCO PA-1000 802.11 a/b Punto de Acceso (incluye herramienta de gestión)	687.00	1374.00
2	ORINOCO 802.11a/b USB Adapter GOLD	85.00	170.00
5	ORINOCO 802.11a/b Cardbus GOLD	105.00	525.00
15	ORINOCO 802.11a/b PCI Card GOLD	120.00	1800.00
2	ORINOCO 20" IEEE Pigtail Assembly	70.00	140.00
2	ORINOCO Range Extender Antenna	80.00	160.00
Total Costo de Hardware			**$ 4,169.00**
20	Configuración de puntos de red	30.00	600.00
Total General			**$ 4,769.00**

Tabla 8.1. Costo de implementación WLAN.

La Figura 8.1. muestra el esquema de red y ubicación de los equipos.

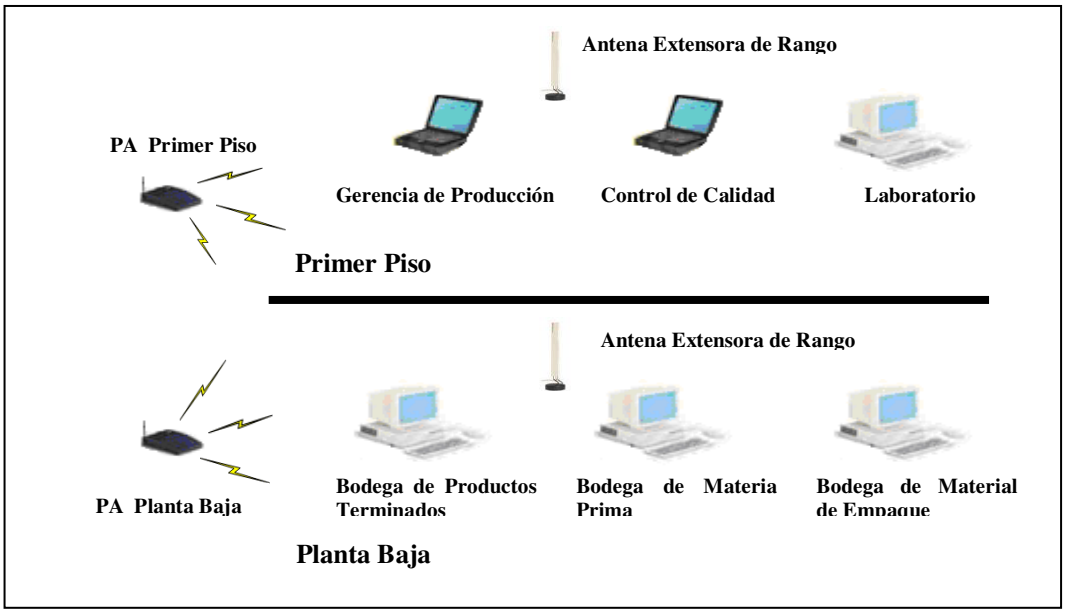

Figura 8.1. Diseño de la WLAN.

8.1.1.2. Costo de Implementación LAN Cableada.

La Tabla 8.2 detalla los costos del hardware para la implementación de una LAN cableada, costos de configuración de los puntos de red y la colocación de los cables en las instalaciones del edificio, cabe resaltar que en los costos de cableado está incluida la mano de obra.

Cant.	Descripción	Costo Unitario	Costo Total
1	3Com Switch 3300 24 Port 10/100 BaseT	1,095.00	1,095.00
1	3Com 3C16610 SuperStack II 12 Port DS Hub 500 10/100 Base T Auto-Sensing	438.00	438.00
5	Cardbus Ethernet PC card	30.00	150.00
15	Ethernet PCI adapter	20.00	300.00
50	Conectores RJ 45	0.45	22.50
50	Canaleta con cinta doble fast (2 metros por unidad)	2.50	125.00
1	Cross Connect 24 Port	70.00	70.00
1	Cross Connect 16 Port	50.00	50.00
5	Jack doble	7.00	35.00
10	Jack simple	5.00	50.00
300 mts	UTP Cat 5 (por metro instalado)	1.50	450.00
Total Costo de Hardware			**$ 2,785.50**
20	Configuración de puntos de red	25.00	**$ 500.00**
Total General			**$ 3,285.50**

Tabla 8.2. Costo de implementación LAN cableada.

La Figura 8.2. muestra el esquema de LAN cableada que tendrían las instalaciones, y la distribución de los equipos.

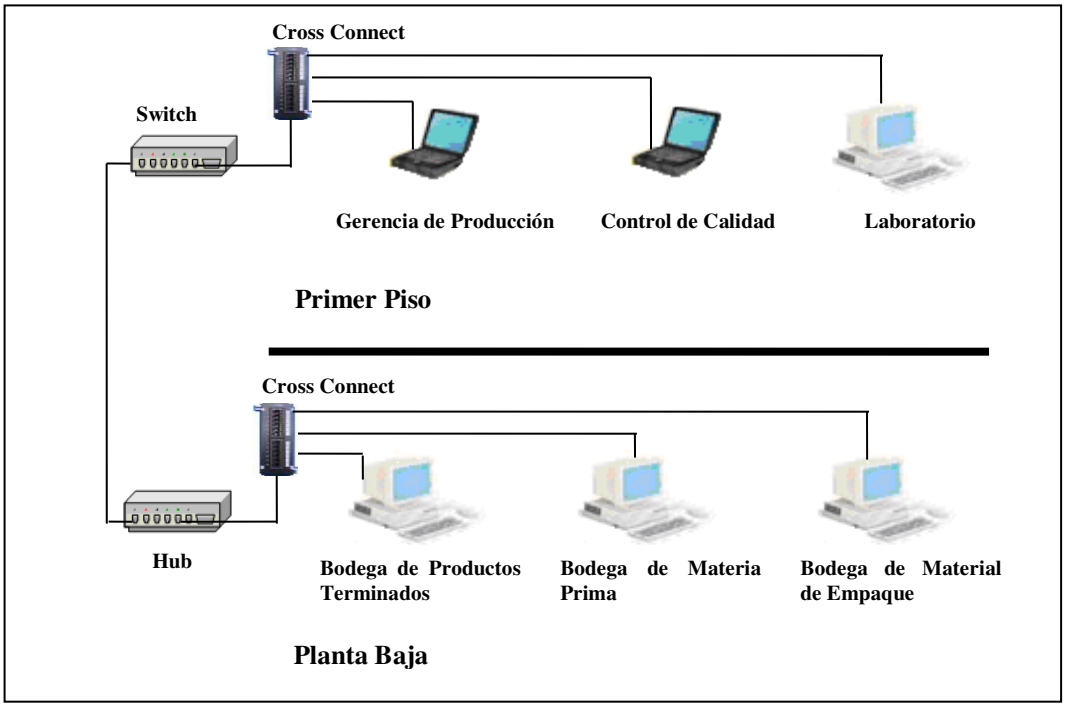

Figura 8.2. Diseño de la LAN cableada.

8.1.1.3 Costo de Implementación WLAN - LAN Cableada.

En la Tabla 8.3. adjunta, se especifican los costos para la implementación de una red WLAN – LAN, a la que denominaremos red mixta.

En ésta se detalla hardware wireless y wired, así como también los costos de configuración para cada uno de ellos.

Cant.	Descripción	Costo Unitario	Costo Total
1	ORINOCO PA-1000 802.11 a/b Punto de Acceso (incluye herramienta de gestión)	687.00	687.00
1	ORINOCO 802.11a/b USB Adapter GOLD	85.00	85.00
5	ORINOCO 802.11a/b Cardbus GOLD	105.00	525.00
10	ORINOCO 802.11a/b PCI Card GOLD	120.00	1200.00
1	ORINOCO 20" IEEE Pigtail Assembly	70.00	70.00
1	ORINOCO Range Extender Antenna	80.00	80.00
Total Costo de Hardware Wireless			**$ 2,647.00**
1	3Com 3C16610 SuperStack II 12 Port DS Hub 500 10/100 Base T Auto-Sensing	438.00	438.00
5	Ethernet PCI adapter	20.00	100.00
15	Conectores RJ 45	0.45	6.75
10	Canaleta con cinta doble fast (2 metros por unidad)	2.50	12.5
1	Cross Connect 16 Port	50.00	50.00
5	Jack simple	5.00	25.00
100 mts	UTP Cat 5 (por metro instalado)	1.50	150.00
Total Costo de Hardware LAN cableada			**$ 782.25**
5	Configuración de puntos LAN	25.00	125.00
15	Configuración de puntos WLAN	30.00	450.00
Total General			**$ 4,004.25**

Tabla 8.3. Costo de implementación WLAN - LAN cableada.

La Figura 8.3. muestra el esquema de WLAN - LAN.

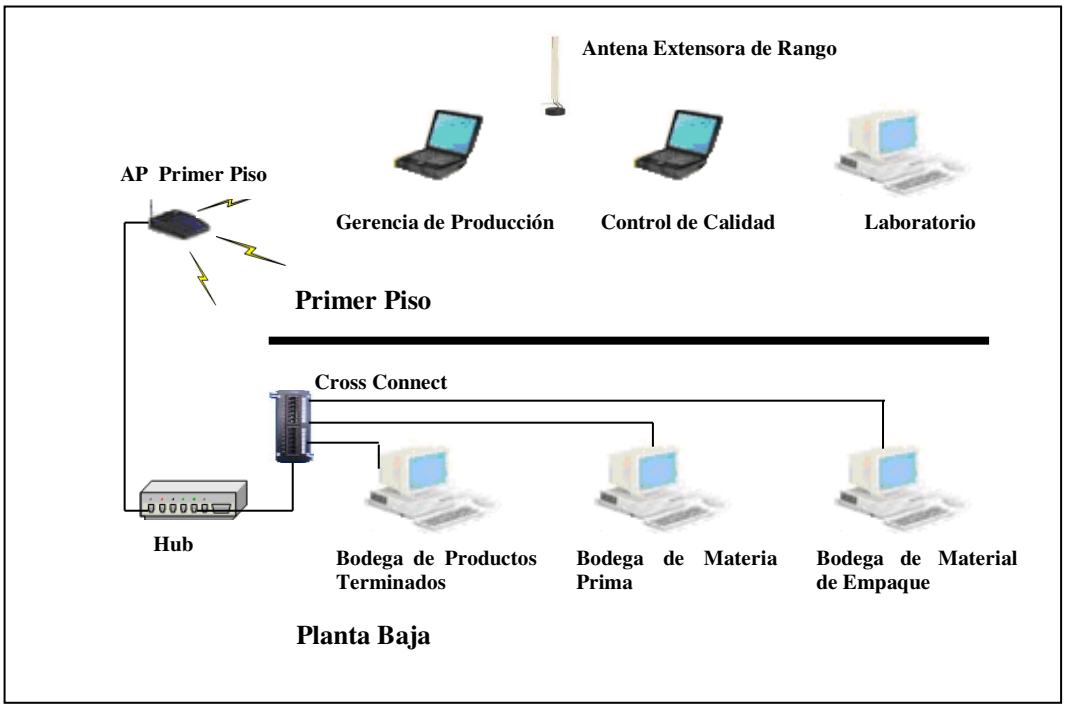

Figura 8.3. Diseño de la WLAN - LAN cableada.

8.1.2. Análisis Comparativo de Costos.

Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN, la inversión de toda la instalación y el costo durante el ciclo de vida puede ser significativamente inferior.

Como se muestra en la Tabla 8.3. la relación de costos que existe entre la implementación de una red WLAN y el de una red LAN cableada; muestra un incremento en la inversión del proyecto del 45.15% entre un costo y otro.

Descripción	Costo
Total Costo WLAN	**$ 4,769.00**
Total Costo WLAN - LAN Cableada	**$ 4,004.25**
Total Costo LAN Cableada	**$ 3,285.50**

Tabla 8.4. Resumen costo de implementación.

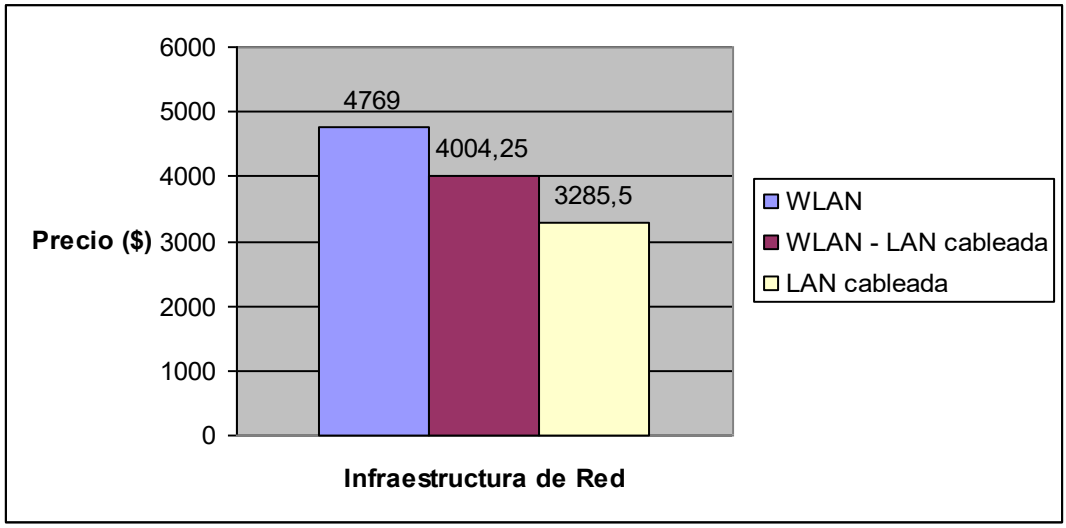

Figura 8.4. Gráfico comparativo de costo.

8.2. Beneficios WLAN.

Los beneficios de una WLAN, son superiores a largo plazo sobretodo en ambientes dinámicos que requieren acciones y movimientos frecuentes.

El valor que agrega esta infraestructura de red varía según el tipo de negocio donde se utiliza, y su análisis de beneficios radica en la ponderación según el orden de importancia que éstos puedan aportar para el desarrollo de las actividades de la compañía. A continuación se detallan los beneficios que se logran:

- **Movilidad dentro de un edificio o un complejo de edificios:** Facilita la implementación de aplicaciones que requieren una conexión continua a la red, especialmente aquellas aplicaciones en tiempo real y de apoyo a empleados en movimiento dentro del un complejo industrial.

  La implementación de LAN cableadas dificultan la reubicación ágil y oportuna que necesitan frecuentemente los empleados o futuras readecuaciones de las oficinas.

- **Flexibilidad:** La tecnología inalámbrica permite a la red llegar a puntos de difícil acceso para una LAN cableada, facilita la instalación y lo hace del modo mas apropiado, en lugar que la ubicación de cada estación la dicte el conector de punto de red del dispositivo (PC) del usuario.

- **Escalabilidad:** Los sistemas de WLAN pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además resulta muy fácil la incorporación de nuevos usuarios a la red.

- **Simplicidad de instalación en espacios temporales:** La instalación de una WLAN es rápida y fácil, elimina la necesidad de tirar cables a través de paredes y techos. Simplifica la instalación de redes en grandes espacios abiertos. Permite dar acceso a la red de datos desde oficinas temporales como son las salas de reuniones. La instalación de redes cableadas, ameritan más tiempo y esfuerzo para su adecuación.

- **Reducción de los costos de cableado:** Reduce dramáticamente los requerimientos de cableado y permite cubrir áreas sin acceso. Facilita dar acceso a la red a nuevos empleados o empleados temporales a más bajo costo de operación y mantenimiento. Redes temporarias se pueden instalar rápidamente evitando costosas actualizaciones.
- **Aumento de eficiencias:** Estudios han demostrado que los usuarios conectados a un WLAN aumentan su eficiencia promedio a un equivalente de 1.75 horas semanales de trabajo, que aquellos conectados a redes cableadas, debido a que optimizan tiempos de espera y otros tiempos muertos.
- **Aumentos de productividad:** El estar conectado todo el tiempo, permite el uso de herramientas de productividad desde cualquier lugar de la empresa.
- **Facilita la colaboración:** Facilita el acceso a herramientas de colaboración desde cualquier lugar (Ej. sala de reuniones, etc.). Archivos pueden ser compartidos en el momento que surge la necesidad y pedidos de información se pueden satisfacer instantáneamente.

  Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbit/s, o superiores.
- **Mejor imagen corporativa:** Mejora la percepción de una empresa debido a que aumenta su nivel de conectividad y participación en una nueva economía.

- **Uso más eficiente de los espacios de oficina:** Aumento de la flexibilidad en la administración de los espacios de oficina por incremento de personal temporal o debido a reuniones con muchos invitados.
- **Reducción de errores:** Datos e información pueden ser ingresados al sistema en el mismo lugar y en el mismo momento que la información es disponible, reemplazando la necesidad de transcripciones temporarias en papel, ingresándolos en red cuando se cuenta la disponibilidad de conexión a la red.

8.3. Conclusión.

Al realizar una comparación de costos para la implementación de una red LAN cableada, una mixta y una red WLAN, se puede ver que la adquisición de hardware y configuración para una WLAN es superior en costos, aunque en el largo plazo se logra minimizar los costos de mantenimiento, además de que los beneficios son significativos en cuanto al rendimiento y optimización de los recursos; considerando que la maximización de los beneficios que ofrece una red inalámbrica dependerán de la actividad el negocio.

Con respecto al caso de estudio que se plantea en este capítulo, se propone como solución, la implementación de una red inalámbrica ya que las necesidades del negocio ameritan la inversión. Para esto se han tomado en consideración los siguientes puntos.

- La estructura del edificio y la ubicación de las áreas de trabajo dificultarían la instalación de cableado.
- Los espacios de las áreas de trabajo serían optimizados con una red WLAN.
- La seguridad ha sido uno de los criterios decisivos para la toma de decisiones ya que mediante ésta, se suministrarán elementos de seguridad, tales como algoritmos de cifrado que autenticarán el tráfico de la red.
- La interconexión de la fábrica con las instalaciones de administración se verán altamente beneficiados, ya que el uso de cableado dificulta la optimización de transferencia, entre un edificio y otro.
- La administración del inventario se verá beneficiado, debido a que las bodegas manejan un ambiente dinámico; esto es que siempre están en un constante cambio y reorganización.

Referencias.

1. Libros:

- C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, 2000.
- N. Borisov, I. Goldberg, D. Wagner, "Intercepting mobile communications: The insecurity of 802.11", 2001
- W. A. Arbaugh, N. Shankar, Y.C. Justin Wan, "Your 802.11 Wireless Network has No Clothes", 2001.
- "Port-Based Network Access Control", IEEE Std 802.1X-2001, 2001
- Eduardo Tabacman. Seguridad en Redes Wireless. En las memorias de la I Jornada de Telemática"Comunicaciones Inalámbricas, Computación Móvil". ACIS, Bogotá (Colombia), 2003.

2. Páginas Web:

- Institute of Electrical and Electronics Engineers: http://www.ieee.org
- Grupo de trabajo de IEEE 802.11: http://grouper.ieee.org/groups/802/11/
- Wireless Fidelity Alliance: http://www.wi-fi.org
- The Wireless LAN Association www.wlana.com
- Warchalking http://www.warchalking.org/
- Seguridad en Redes Inalámbricas http://www.securitywireless.info/