UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGON

"Seguridad En Redes Inalámbricas"

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO MECÁNICO ELÉCTRICO

P R E S E N T A :

DANIEL SANCHEZ MEDRANO

Asesor: Ingeniero Adrián Paredes Romero

Estado de México 2006.

ÍNDICE Pag.

INTRODUCCIÓN

Dado que las redes inalámbricas están proliferando debido a su bajo costo, movilidad y su interoperabilidad con los demás tipos de redes, he dispuesto a hacer esta tesis sobre la seguridad en redes inalámbricas.

En varias plazas comerciales, hoteles así como en el aeropuerto de la ciudad, muchos comercios, ofrecen al comer u hospedarte la posibilidad de conectarse a Internet, el único requisito es contar con una laptop, notebook o PDA, en estos casos la seguridad no es tan necesaria.

Sin embargo en una empresa u oficina en la cual existe una red inalámbrica instalada y alguien trata de entrar a la red y robarse algunos documentos o datos importantes de la empresa o simplemente sabotearla, esto reduce la eficiencia o afecta el rendimiento y trabajo, sin tener idea de que esta red es insegura. Comúnmente esto ocurre cuando se instalan dispositivos (sean Access Points o Tarjetas de red inalámbricas) al desempaquetarse sin configurar nada solo conectando y usando, debido a esto la seguridad de la red esta en riesgo, no siendo culpa del software o hardware, si no que como en la mayoría de los casos de infiltración, es culpa del usuario que instala y deja todo configurado de fabrica.

En la presente tesis se pretende dar una descripción básica de una red inalámbrica segura, así como las principales técnicas de detección, configuración y mantenimiento de la misma, minimizando así el riesgo de ataque o sabotaje de la red. Brindando información que requiere conocimientos básicos en redes inalámbricas.

En el año 2004 se publico un estudio por la empresa Gartner Inc.[1] La cual es proveedor líder de investigación y análisis de la industria de TI (Tecnologías de la Información) considerada la autoridad en su ramo, en el cual asegura que el 70 % de los ataques consumados a las redes inalámbricas de área local (WLANs) se debieron a la configuración errónea o a la omisión de configuración.

Con estos datos podemos darnos cuenta de la importancia de tener el conocimiento para instalar y configurar adecuadamente los *Access Points* así como establecer políticas de seguridad y aplicarlas en ambiente de trabajo.

La aportación de este proyecto de tesis es la demostración del uso de herramientas para auditoria en redes *wireless* principalmente software libre el cual no tiene ningún costo por su uso. Estas herramientas que en ocasiones se denominan herramientas de *Hackers* son muy buenas para probar el nivel de seguridad de una red inalámbrica.

[1] Gatrner-1

CAPITULO I

CONCEPTOS BÁSICOS DE REDES INALÁMBRICAS

1.1 Sistemas De Radio Frecuencia (RF)

La Radiofrecuencia (RF) e Infrarrojo (IR) son las tecnologías principales usadas para las comunicaciones inalámbricas. Se usan RF y tecnologías de IR para aplicaciones diferentes y se han diseñado en productos con ventajas particulares.

La RF es capaz de ser usada para aplicaciones en que las comunicaciones no son de línea de vista y están en distancias largas. Las señales de RF viajan a través de las paredes y comunican donde no hay ningún camino directo entre los terminales. Para operar en la banda del espectro de licencia-libre llamada Industrial, Científica, y Médica (ISM por sus siglas en ingles), el sistema de radio debe usar una técnica de la modulación llamada de Espectro del Disperso (SS por sus siglas en ingles). En este modo se exige distribuir la señal por el espectro entero y no puede permanecer estable en una sola frecuencia. Ningún usuario puede dominar la banda, y colectivamente todos los usuarios lucen como ruido.

El hecho que las señales parecen ser ruido en la banda, hace que sean difíciles de encontrar y bloquear. Esta técnica opera bien en una aplicación de WLAN real y esta banda es difícil de interceptar, lo cual incrementa la seguridad en contra de los oyentes no autorizados. El uso del Espectro Disperso es importante porque permite muchos mas usuarios ocupar la banda en cualquier tiempo dado y lugar.

Con cualquier sistema de radio, una de las más grandes limitaciones es el ancho de banda disponible, y la habilidad de tener muchos usuarios operando simultáneamente en un ambiente dado es crítico para el despliegue exitoso de WLAN.

Hay varias bandas de licencia-libre disponibles para el uso de transmisores, las mas usadas comúnmente son las de 902 a 928 MHz, 1.4 a 1.5 GHz, y 5.7 a 5.8 GHz. De éstas, la más útil es probablemente la banda de 1.4-GHz la cual está disponible para el uso a lo largo de la mayoría de las partes del mundo. En los recientes años, casi todo el desarrollo comercial se ha basado en la nueva norma IEEE de la banda de 1.4-GHz. En las bandas de licencia-libres, hay un límite estricto en la energía de transmisión de cualquier transmisor para que el espectro pueda re usarse a una distancia corta sin la interferencia de un transmisor distante.

1.1.1 Las Radiofrecuencias

Las Radiofrecuencias son señales de alta frecuencia alternanadas que son transmitidas por un cable y son radiadas al aire por medio de una antena. La antena es el dispositivo encargado de convertir y transformar una señal alambrica en una señal inalámbrica y viceversa. Cuando la señal de alta frecuencia es transformada en forma de ondas de radio, estas ondas se propagan fuera del origen (la antena) en una línea recta en todas direcciones.

Entendiendo la conducta de propagación de las ondas de RF (Radio Frecuencia), es una parte importante de entender por qué y cómo funcionan las Redes de Area Local (LANs) inalámbricas. Sin esta base de conocimiento, un administrador sería incapaz de localizar lugares de la instalación apropiadas del equipo y no entendería cómo solucionar problemas en una red inalámbrica.

1.1.2 El Comportamiento De Las Radiofrecuencias

Las Radiofrecuencias parecen actuar erráticamente e incoherentemente bajo algunas circunstancias dadas. A Continuación se describen estos tipos de circunstancias y que pasa cuando las ondas de radio son transmitidas.

1.1.3 La Ganancia

La Ganancia es el término usado que describe un aumento en la amplitud de una señal de RF. La ganancia normalmente es un proceso activo; significando esto que se usa una fuente de poder externa para amplificar la señal, tal es el caso de un amplificador de RF, o una antena de alta-ganancia que se usa para enfocar el campo de irradiación de una señal, para aumentar su amplitud[2].

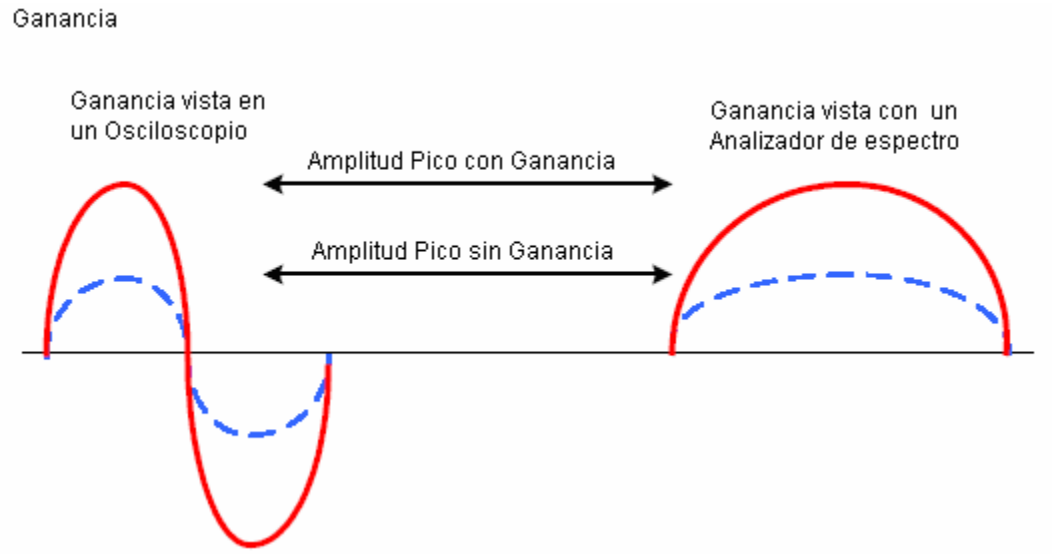


Figura 1.1: Ganancia

Sin embargo, los procesos pasivos también pueden causar ganancia. Por ejemplo, las señales de RF reflejadas pueden combinarse con la señal principal para

[2] CWNA-1

aumentar la fuerza de la señal principal, pudiendo tener un resultado positivo o negativo.

1.1.4 La Pérdida

La pérdida describe una disminución en la fuerza de la señal. Muchas cosas pueden causar perdida en una señal de RF, desde cuando la señal viaja por el cable hasta que esta es radiada por la antena.

La resistencia de cables y conectores es causa de pérdida, al convertir la señal estos se calientan. La desigualdad de impedancia en los cables y conectores puede generar energía, que llega a causar daños al ser reflejada hacia el origen de la señal. Los objetos pueden absorber directamente la onda propagada en el camino de transmisión, pueden reflejar, o pueden destruir las señales de RF.

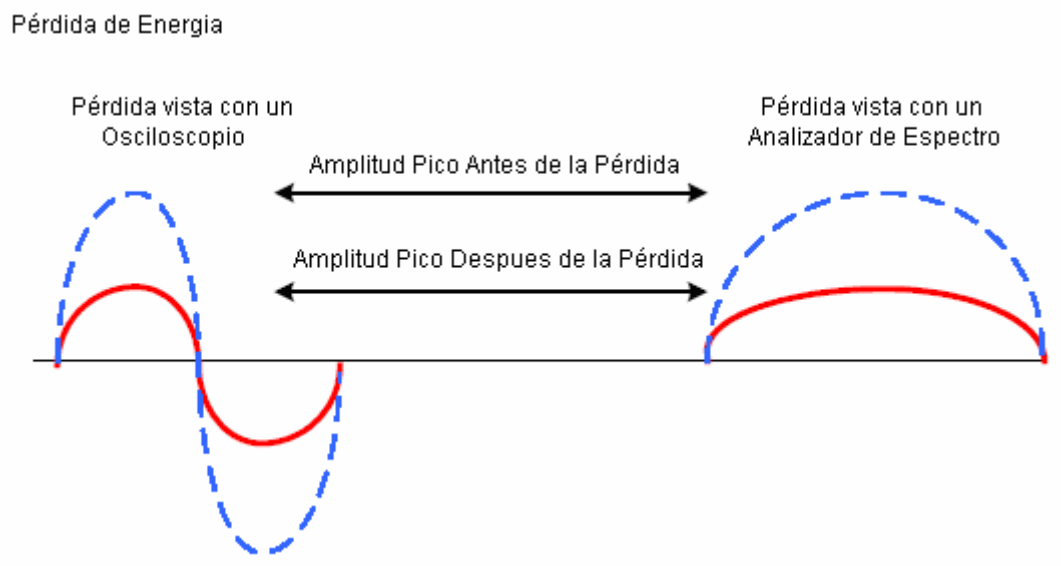


Figura 1.2: Perdida De Energía

Un umbral de sensibilidad está definido para los radiotransmisores, los cuales pueden distinguir una Señal del ruido de fondo.

1.1.5 La Reflexión

La reflexión ocurre cuando una onda electromagnética choca con un objeto que tiene una dimensión muy grande comparada con la longitud de la onda de la señal. Las reflexiones ocurren en la superficie de la tierra, edificios, paredes, y muchos otros obstáculos.

Si la superficie es lisa, la señal reflejada puede permanecer intacta, aunque hay alguna pérdida debido a la absorción y dispersión de la señal.

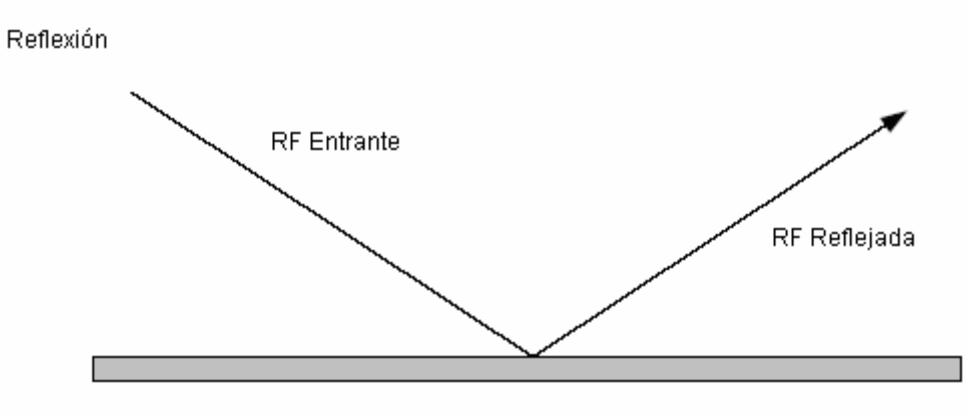


Figura 1.3: La Reflexión

La reflexión de las Radiofrecuencias puede causar problemas serios para las redes de área local LAN (Local Area Network) inalámbricas. El reflejo de la señal principal en el área de la transmisión, en muchos objetos es llamado multipath. El Multipath puede causara diversos daños en las LANs inalámbricas, como degradar o cancelar la señal principal, o causando agujeros o huecos en la RF. Las superficies como metales, blindajes de metal, puertas de metal, y otros pueden causar reflexión severa y generación de multipath.

1.1.6 La Refracción

La refracción es la división y cambio de dirección de una onda de radio al atravesar un medio de densidad diferente. Cuando una onda de RF pasa por un medio más denso (como una nube de aire frío que queda en un valle) la onda se doblará y sufrirá cambios de dirección. Al atravesar este medio, alguna parte de la onda se reflejarán fuera de la dirección señalada, y otra parte pasara a través del medio en otra dirección, como se puede observar en las siguiente figura.

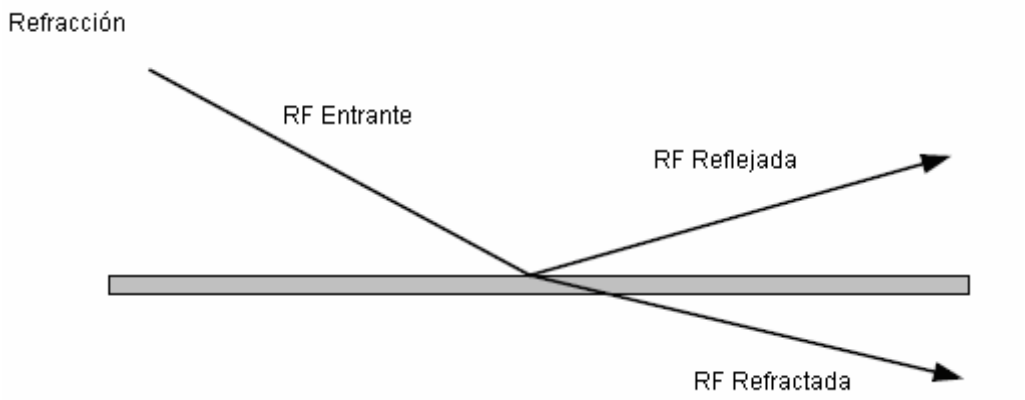


Figura 1.4: La Refracción

1.1.7 La Difracción

La difracción ocurre cuando en el camino entre el transmisor y el receptor es obstruido por una superficie que tiene irregularidades marcadas o una superficie áspera.

A frecuencias altas, la difracción actúa como reflexión, dependiendo de la geometría del objeto, la amplitud, fase, y polarización de la onda incidente al punto de difracción. La difracción es normalmente confundida e inadecuadamente, con la refracción. La difracción describe el doblamiento de la onda alrededor de un obstáculo y la refracción describe un doblamiento de onda a través de un medio.

La figura 1.5 muestra cómo la difracción actúa con los obstáculos en su camino, dependiendo de la composición del obstáculo. Si el objeto es muy grande o lo suficientemente grande, la onda no podría doblar, sino podría bloquearse.

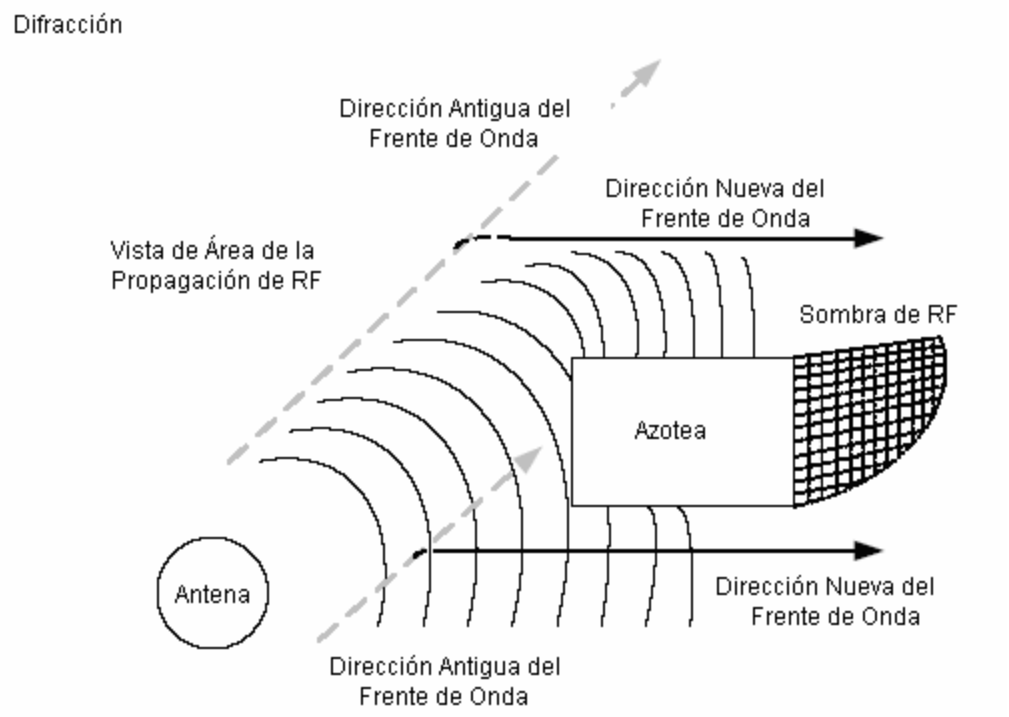


Figura 1.5: La Difracción

La difracción es el retardando de la onda en al punto dónde el frente de onda golpea el obstáculo, mientras el resto del frente de onda mantiene la misma velocidad de propagación. La difracción es el efecto en el cual las ondas doblan alrededor del obstáculo.

1.1.8 La Dispersión

La Dispersión ocurre cuando el medio a través del que viaja la onda esta formado de objetos con dimensiones pequeñas comparado con la longitud de onda de la señal, y el número de obstáculos por el volumen de la unidad es grande. Las ondas esparcidas son producidas por las superficies ásperas, los objetos pequeños, o por otras irregularidades en el camino señalado.

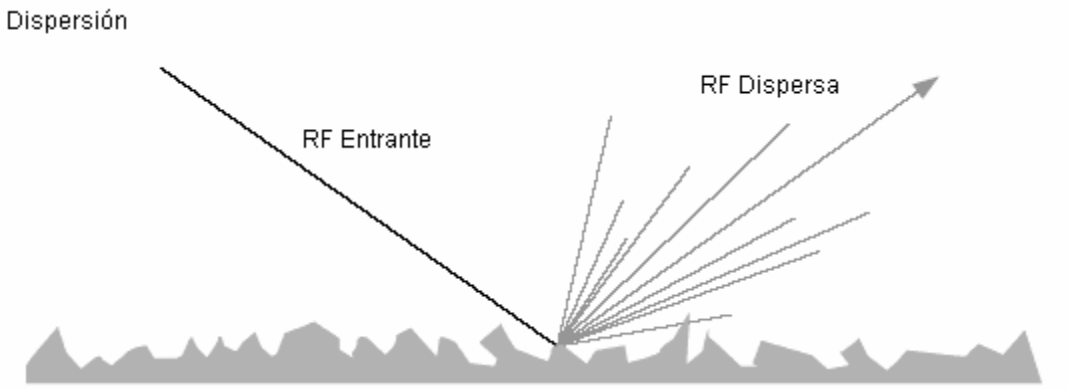


Figura 1.6: La Dispersión

La dispersión puede ocurrir cuando una onda golpea una superficie desigual y se refleja simultáneamente en muchas direcciones. La dispersión de este tipo tiene muchas reflexiones de amplitudes pequeñas que destruyen la señal principal de RF.

La dispersión de una señal de RF puede ocurrir cuando una onda se refleja fuera de arena, piedras, u otras superficies dentadas. También pueden ocurrir cuando la onda viaja a través de un medio con partículas pesadas como el polvo. En lugar de reflejarse fuera de una superficie desigual, las ondas de RF se reflejan individualmente en una parte muy pequeña fuera de las partículas diminutas. Cuando ocurre esto, la degradación de la señal de RF puede ser significante al punto de romper las comunicaciones intermitentemente o causar la pérdida completa de la señal.

1.2 Principios De Antenas

La teoría sobre antenas es una parte muy básica pero importante dentro de las redes inalámbricas. Nos puede servir para entender los principales problemas de comunicación y así escoger un tipo determinado de antena, ubicación, dirección, entre otras cosas. Los principios básicos que hay que conocer sobre las antenas son:

- Las antenas convierten la energía eléctrica en ondas de RF, en el caso de una antena transmisora, o una onda de RF en energía eléctrica en el caso de una antena receptora.

- Las dimensiones físicas de una antena se relacionan directamente con su longitud y frecuencia a la que la antena puede radiar las ondas o puede recibir las ondas radiadas.

Algunos puntos esenciales de la teoría de las antenas que se puede aplicar en las redes inalámbricas son: La línea de vista, la zona de Fresnel y la ganancia de la antena. A Continuación se dará una breve explicación de cada uno de estos conceptos.

1.2.1 La Línea De Vista

La línea de vista es la línea recta entre el transmisor y el receptor. La línea de vista es aparentemente recta, debido a que las ondas son sujetas a cambios de dirección debido a la refracción, difracción y reflexión de la misma manera que las radiofrecuencias. La línea de vista de las Radiofrecuencias puede obstruirse por algún obstáculo en la Zona de Fresnel y afectar las comunicaciones a tal grado de obstruirlas completamente.

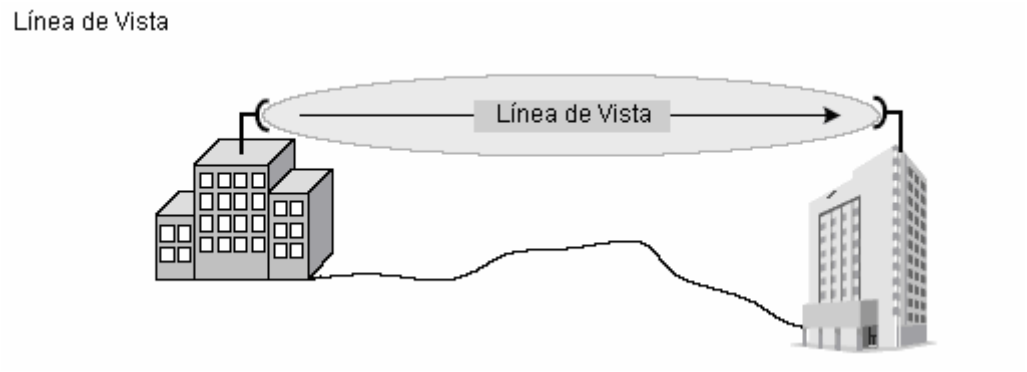


Figura 1.7: Línea de Vista

1.2.2 La Zona De Fresnel

Las zonas de Fresnel son una serie de elipsoides concéntricas alrededor del camino de la línea de vista, son muy importantes para determinar la mínima área en la que no pueden existir obstáculos para garantizar la correcta transmisión y recepción en un enlace de Radiofrecuencia. Los objetos en la Zona de Fresnel como los árboles, cúspides, y edificios pueden difractar o reflejar la señal principal fuera del receptor, cambiando la línea de vista de la RF. Estos objetos pueden absorber o dispersar la señal de RF causando la degradación o la perdida de la señal.

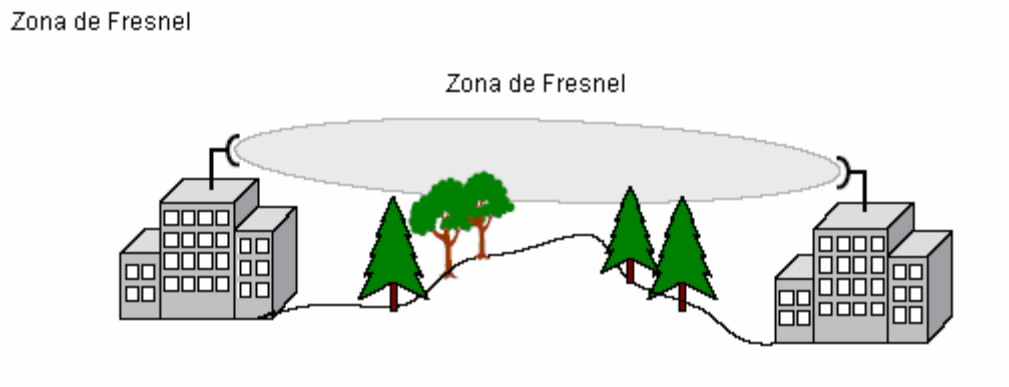


Figura 1.8: La Zona de Fresnel

El radio de la Zona de Fresnel a su punto más ancho puede calcularse por lo siguiente fórmula:

$$r = 43.3 \times \sqrt{\frac{d}{4f}}$$

Donde d es la distancia del enlace en millas, f es la frecuencia en GHz, y el resultado, r, está en pies.

1.2.3 Las Obstrucciones

Considerado la importancia de la Zona de Fresnel, es trascendente cuantificar la obstrucción a la cual puede someterse. Si se bloque una señal de RF, esta podrá doblar hasta cierto punto alrededor del obstáculo. Típicamente si se obstruye el 20% al 40% de la Zona de Fresnel el enlace presenta poca interferencia o ninguna.

Por una parte más conservadora se sugiere no permitir algún obstáculo al 20 %. Obviamente, si la obstrucción es causada por árboles u otros objetos crecientes, se debería diseñar el enlace basado en un 0%. Si el enlace activo se bloquea por una nueva construcción o el crecimiento de algún árbol, el problema se soluciona levantando la altura de las antenas.

1.2.4 La Ganancia De La Antena

La antena es un elemento pasivo (no contando los amplificadores y filtros asociados a esta). No puede amplificar o manipular la señal por si misma, pero puede crear el efecto de amplificación dada su forma física. La amplificación de la antena es el resultado de enfocar la radiación de RF en un rayo más firme.

Por ejemplo, una antena omni-direccional tiene 360 grados de zona de irradiación horizontal. Limitando la zona de irradiación de 360 grados en una zona más enfocada, de 30 grados, con la misma energía, las ondas de RF se radiarán a una distancia mayor.

1.3 Unidades De Medida

Hay unas unidades de medida estándares que son esenciales para solucionar problemas y llevar acabo la planeacion de redes LAN inalámbricas. A continuación se presenta las unidades principales así como su descripción y sus principales aplicaciones.

1.3.1 Los Watts (W)

La unidad básica de energía es el Watt. Un Watt está definido como un amperio de corriente a un voltio. La Comisión Federal de Comunicaciones (FCC) permite a una antena radiar sólo 4 Watts de energía en una conexión de LAN inalámbrica de punto a multipunto que usa una banda de 1.4 GH del espectro. Cuatro Watts no podrían parecer mucho poder, pero es bastante para enviar datos a través de señales RF a una distancia de algunos kilómetros.

1.3.2 Los MiliWatt (mW)

Al implementar LANs inalámbricas, la energía llega a ser tan pequeña como 1 miliwatt (1/1000 Watts) la cual puede usarse en una área pequeña, la energía en un segmento de una LAN inalámbrica raramente llega a superar los 100 mW, bastante para comunicar hasta 800 metros en condiciones óptimas.

Los puntos de Acceso (Access Points) generalmente tienen la habilidad de radiar de 30 a 100 mW de energía, dependiendo del fabricante. Sólo en el caso de conexiones al aire libre de punto a punto entre edificios, los niveles sobrepasarán los 100 mW. La mayoría de los niveles de energía usado por administradores de redes estará en mW o dBm. Estas dos unidades de medida representan una cantidad absoluta de poder y son ambos utilizados normalmente en la industria.

1.3.3 Los Decibeles (dB)

Cuando un receptor es muy sensible a señales de RF, puede poder recibir señales tan pequeñas como 0.000000001 Watts. Este número tan pequeño puede ser ignorado o interpretado mal. Los decibeles nos permiten representar estos números haciéndolos más manejables y entendibles. Los decibeles están basados en una relación logarítmica a la medida lineal de energía: los Watts. Un logaritmo es el exponente a que el número 10 debe elevarse para alcanzar algún valor dado.

En una medida logarítmica, la referencia no puede ser ningún cero porque el logaritmo de cero no existe. Los decibelios son una unidad de la medida relativa diferente la medida absoluta de miliWatts.

1.3.4 Las Medidas De Ganancia Y Pérdida

La ganancia y pérdida de energía son medidas en decibeles, no en watts, dado que la ganancia y pérdida son conceptos relativos y un decibel es una medida relativa. La Ganancia o pérdida en un sistema de RF pueden expresares en una medida de poder absoluta (por ejemplo diez Watt) o por una medida de energía relativa (por ejemplo la mitad de su energía).

La mitad de la energía en un sistema corresponde a perder 3 decibelios. Si un sistema pierde la mitad de su energía (-3 dB), entonces pierde de nuevo la mitad (otros -3 dB), entonces la pérdida del sistema total es ¾. Claramente, ninguna medida absoluta de watts puede cuantificar esta pérdida asimétrica de una manera sencilla, pero los decibeles hacen simplemente eso.
Como una referencia rápida y fácil, hay algunos números de ganancia y pérdida que deben recordarse constantemente. Estos números son:

-3 dB = la mitad de la energía en el mW
+3 dB = el doble de la energía en el mW
-10 dB = un décimo de la energía en el mW
+10 dB = diez veces la energía mW

Cuando se calculan la ganancia y la pérdida de energía, uno casi siempre puede dividir una cantidad de ganancia o pérdida por 10 o 3 o ambos. Con estos valores se pueden calcular la pérdida y ganancia de RF rápidamente, en una cantidad exacta sin el uso de una calculadora.

En el caso dónde el uso de este método no es posible, hay las fórmulas de conversión, que pueden usarse para estos cálculos. La siguiente es la ecuación general por convertir el mW a dBm:

$$P_{dbm} = 10 \log_{PmW}$$

Esta ecuación puede manipularse para invertir la conversión, para ahora convertir de dBm a mW:

$$Pmw = \log^{-1}\left(\frac{P_{dbm}}{10}\right)$$

1.3.5 El dBm

El punto de referencia que relaciona el dB logarítmico y la escala de Watt lineal es:

1 mW = 0 dBm

El m en dBm simplemente se refiere al hecho que la referencia es a 1 milliwatt (1 mW) y por consiguiente una medida del dBm es una medida de energia absoluta.

La Figura 1.9 muestra que el punto de la referencia siempre es el mismo, pero los niveles de energía pueden estar en cualquier dirección del punto de referencia, depende de la dirección, si ellos representan una ganancia o pérdida de energía.

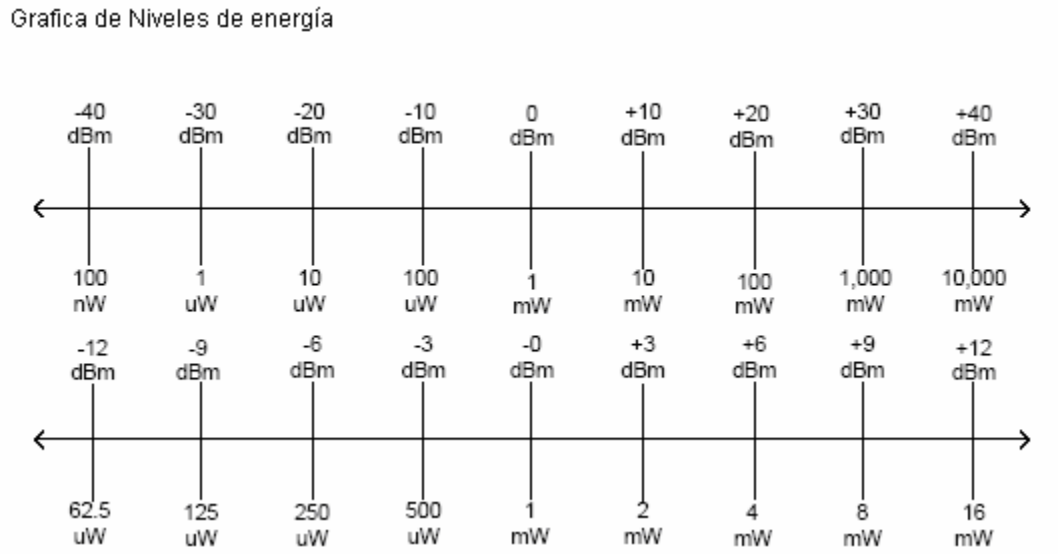


Figura 1.9: Grafica de Niveles de Energía

Estos dos diagramas representan lo mismo, sólo que uno se incrementa en las ganancias y pérdidas de 3 dB y el otro en 10 dB. Usando estas escalas, uno puede convertir niveles de energía dBm y mW fácilmente.

1.4 Introducción Al Espectro Disperso (Spread Spectrum)

El Espectro Disperso es una técnica de comunicaciones caracterizada por el gran ancho de banda a una baja energía. Usa varias técnicas de modulación en las LANs inalámbricas. Las señales del Espectro de Disperso se comportan como ruido, las cuales son muy difícil de descubrir, y aun más de interceptar o demodular sin el equipo apropiado.

Las comunicaciones de Espectro Disperso son menos susceptibles al bloqueo y a la interferencia por lo cual la comunicación es mas estable. Por estas razones, el espectro disperso ha sido en mucho tiempo el favorito del ejército.

Para conocer los distintos tipos de espectro disperso y elegir el más adecuado, primero se debe establecer una referencia discutiendo el concepto de transmisión de la banda estrecha.

1.4.1 Transmisión De Banda Estrecha

La transmisión de banda estrecha es una tecnología de comunicaciones que usa sólo la parte necesaria del espectro de frecuencia para llevar los datos. Siempre ha sido misión del FCC conservar el uso de frecuencia tanto como posible.
El Espectro Disperso está contra esa misión dado que usa una frecuencia más ancha de la que es necesaria para transmitir la información. Este es el primer requisito para considerar una señal del Espectro Disperso. Una señal de espectro disperso es aquella en la que el ancho de banda es más grande que el requerido para enviar la información.

1.4.2 Tecnología Del Espectro Disperso

La tecnología del espectro disperso nos permite tomar la misma cantidad de información que nosotros habríamos enviado usando una señal portadora de banda estrecha y lo habríamos extendido en un rango de frecuencia más grande. Por ejemplo, nosotros podemos usar 1 MHz a 10 Watts con la banda estrecha, pero 20 MHz a 100 mW con el Espectro Disperso.

Usando un espectro de frecuencia más ancho, se reduce la probabilidad de que los datos se alteren o se bloquen. Mientras la banda del espectro disperso es relativamente ancha, el poder máximo de la señal es bastante bajo. Este es el segundo requisito para considerar una señal del espectro disperso. Estas dos características de espectro disperso (el uso de una banda ancha de frecuencias y el poder muy bajo). Además los receptores de radio verán a la señal del espectro disperso como ruido, estos no intentarán demodular o interpretarla, por lo tanto se creara una comunicación ligeramente más segura.

1.4.3 Los Usos Del Espectro Disperso

Esta seguridad inherente es lo que le intereso al ejército de la tecnología de espectro disperso a través de los años cincuenta. Debido a sus características a parecer ruido, podian enviarse señales de espectro disperso bajo las narices de enemigos que usaban las técnicas de comunicación clásicas. Naturalmente, la seguridad de comunicación sólo era válida en tanto nadie más usara esta tecnología.

En los años ochenta, el FCC llevó a cabo un juego de reglas que hacen la tecnología de espectro disperso disponible a la investigación pública y a la comercialización de tecnología de espectro disperso. Aunque a primera vista parecio que el ejército había perdido su ventaja, que no tenía. Las bandas usadas por el ejército son diferentes de las bandas usadas por el público.

También, en los usos militares la modulación y las técnicas de codificación son muy diferente para asegurar que sus comunicaciones de espectro disperso sean más difíciles interceptar que aquéllos del público general.

Desde los años ochenta, cuando la investigación empezó fuertemente, se han usado las tecnologías de espectro disperso en los teléfonos inalámbricos, los sistemas del posicionamiento globales (GPS), la telefonía celular digital (CDMA), el sistema de comunicaciones personal (PCS), y ahora las redes de área local inalámbricas. Además de las Redes de área local inalámbricas (WLANs), las Redes de área personal inalámbrica (WPANs), las Redes de área metropolitana inalámbrica (WMANs), y las redes de área extensa inalámbricas (WWANs) también están aprovechando la tecnología de espectro de disperso.

Las WPANs usan la tecnología de Bluetooth para tomar ventaja de los requerimientos de energia muy bajos y permitir la gestión de redes inalámbrica dentro de un rango muy corto. Las WWANs y WMANs pueden usar antenas direccionales de ganancia muy alta para establecer RF a larga distancia, a gran velocidad con energía relativamente baja.

1.4.4 Las Redes De Área Local Inalámbricas (WLANs)

Las Redes de área local inalámbricas, WLANs, y WMANs usan las mismas tecnologías de espectro disperso de maneras diferentes. Por ejemplo, una LAN inalámbrica puede usarse dentro de un edificio para mantener la conectividad de los usuarios móviles, o puede usarse los puentes para proporcionar la conectividad del edificio-a-edificio por un campus. Estos son usos específicos de tecnología de espectro disperso que encaja dentro de la descripción de una Red de la Área Local (LAN).

Los usos más comunes de la tecnología del espectro disperso hoy tienen una combinación de Redes de área local inalámbricas 801.11 y dispositivos de Bluetooth dóciles 801.15. Estas dos tecnologías han capturado una tremenda participación en el mercado, lo que es irónico que la dos funcionen de forma muy diferentemente, estén dentro del la misma regla de FCC, y todavía interfieren entre sí. La investigación considerable, tiempo, y recursos han hecho estas dos tecnologías coexistir amigablemente.

1.4.5 Las Redes De Área Personal Inalámbricas (WPANs)

Bluetooth es la tecnología más popular de WPAN y esta especificada por la norma IEEE 801.15. Las regulaciones de FCC con respecto al uso de espectro disperso son extensas, permitiendo varios tipos de aplicaciones.

Algunas formas de Espectro Disperso introducen el concepto de salto de frecuencia (Frecuency Hopping), significando que el transmisor y los sistemas receptores saltan de frecuencia en frecuencia dentro de una banda de frecuencia que transmite los datos. Por ejemplo, Bluetooth salta aproximadamente 1600 veces por segundo mientras la tecnología de HomeRF (una banda ancha de tecnología WLAN) brinca aproximadamente 50 veces por segundo. Las dos tecnologías varían grandemente de las norma 801.11 WLAN que típicamente salta de 5 a 10 veces por segundo.

Cada uno de estas tecnologías tiene usos diferentes en el mercado, pero todos entran dentro de las regulaciones de la FCC. Por ejemplo, una frecuencia típica 801.11 WLAN que brinca podría llevarse a cabo como una solución de la gestión de redes inalámbrica en empresa, mientras HomeRF sólo se lleva a cabo en los ambientes de la casa debido a las restricciones de emisor de energía por la FCC.

1.4.6 Las Redes De Área Metropolitana Inalámbricas (WMANs)

Otro uso del Espectro Disperso es como enlace inalámbrico entre ciudades enteras, estas usan energía de alta potencia en enlaces punto a punto para crear una red. Este uso entra en la categoría conocido como las Redes de Área Metropolitanas Inalámbricas, o WMANs. Algunos enlaces inalámbricos punto a punto que forman una red dentro de una área geográfica muy grande es considerado una WMAN, pero todavía usa las mismas tecnologías como el WLAN.

La diferencia entre un WLAN y un WMAN, sería en muchos casos que las WMANs utilizan frecuencias licenciadas típicamente en lugar de las frecuencias sin licencia usadas por las WLANs. La razón de esta diferencia es que la organización que desarrolla la red tendrá el mando del rango de frecuencia dónde la WMAN está Implementada y no tendrá que preocuparse por que alguien implemente una red que interfiera con esta. Los mismos factores aplican a WWANs.

1.5 El Espectro Disperso De Salto De Frecuencia (FHSS)

El Salto de Frecuencia es una técnica del espectro disperso, que usa la agilidad de la frecuencia para extender los datos sobre más de 83 MHz. La agilidad de frecuencia se refiere a la habilidad del radiotransmisor para cambiar la frecuencia de la transmisión abruptamente dentro de la banda de RF utilizable. En el caso del salto de frecuencia en Redes de Área Local inalámbricas, la porción utilizable de la banda ISM de 1.4 GHz es de 83.5 MHz , la cual esta regulada por la FCC y la norma IEEE 801.11.

1.5.1 Como Funciona FHSS

En los sistemas de Salto de Frecuencia, la portadora cambia la frecuencia, o los saltos, de acuerdo a una secuencia seudo aleatoria. Esta secuencia es una lista de varias frecuencias a la que la portadora saltara a intervalos de tiempo especificados antes de repetir el modelo. El transmisor usa esta serie de saltos para seleccionar sus frecuencias de transmisión.

La portadora permanecerá a una cierta frecuencia por un tiempo especificado (conocido como el tiempo de detención), y usa una cantidad pequeña de tiempo para saltar a la próxima frecuencia (tiempo del salto). Cuando la lista de frecuencias ha sido completada, el transmisor repetirá la secuencia.

A continuación en la Figura 1.10 se muestras un sistema de salto de frecuencia que usa una secuencia del salto de cinco frecuencias sobre una banda de 5 MHz. En este ejemplo, la secuencia es:

1. 1.449 GHz
2. 1.452 GHz
3. 1.448 GHz
4. 1.450 GHz
5. 1.451 GHz

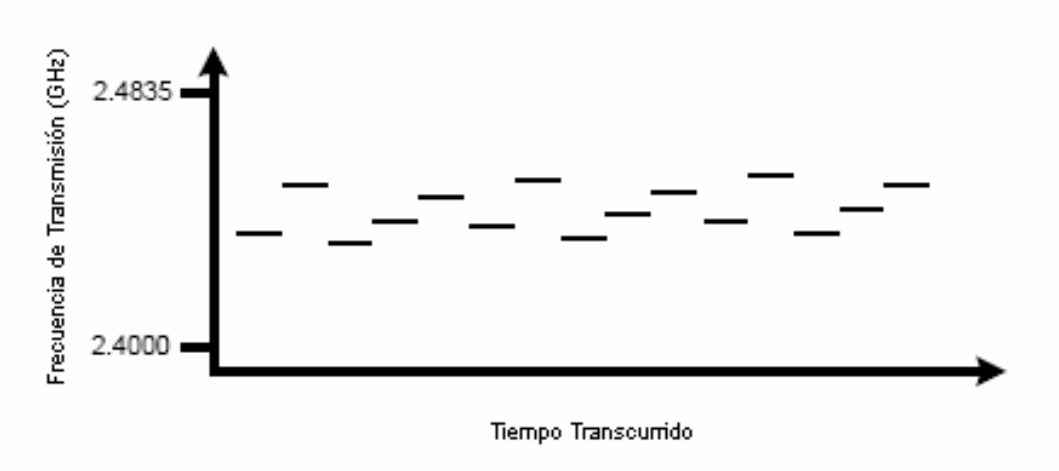


Figura 1.10: Sistema de Salto de frecuencia

Una vez que el radio ha transmitido la información sobre la portadora de 1.451 GHz, el radio repetirá la secuencia del salto, y empezara de nuevo a 1.449 GHz. El proceso de repetir la secuencia continuará, hasta que la información se reciba completamente. El receptor se sincroniza a la secuencia de salto del transmisor para recibir en la frecuencia apropiada en el momento apropiado. La señal es demodula y usada por el receptor.

1.5.2 Los Efectos De Interferencia De La Banda Estrecha

El salto de frecuencia es un método de envío de datos dónde el transmisor y los sistemas receptores saltan juntos a lo largo de un modelo repetible de frecuencias. Como es el caso con todas las tecnologías de espectro disperso, los sistemas de salto de frecuencia son resistentes pero no inmunes a la interferencia de la banda estrecha. Si una señal en una frecuencia superior fuera interferir con nuestro salto de frecuencia, por ejemplo 1.451 GHz, sólo esa parte de la señal de espectro disperso se perdería. El resto de la señal permanecería intacto, y los datos perdidos serían retransmitidos. En la realidad una interferencia de la banda estrecha puede ocupar varios megahertz de ancho de banda. Desde que un salto de frecuencia esta sobre los 83 MHz de ancho de banda, esta señal puede causar una pequeña degradación de la señal de espectro disperso

1.5.3 Sistemas De Salto De Frecuencia

El trabajo del IEEE es crear normas de operación que encajen dentro de las regulaciones creadas por la FCC. El IEEE y las normas de OpenAir con respecto a los sistemas de FHSS describen:

- Qué bandas de frecuencia pueden usarse
- Las secuencias de salto
- Tiempo de detención
- Tasas de transferencia de datos

La norma IEEE 801.11 especifica tasas de transferencia de datos de 1 Mbps y 2 Mbps. Para que un sistema de salto de frecuencia sea considerado en la norma 801.11 debe operar en los 1.4 GHz en la banda ISM (la FCC especifica que comienza de los 1.4000 GHz a los 1.5000 GHz).

1.5.4 Los Canales

Un sistema de salto de frecuencia deberá operar usando un modelo del salto especificado llamado canal. Típicamente usan 26 modelos del salto del la norma FCC o un subconjunto de estos. Algunos sistemas de salto de frecuencia permitirán crear modelos del brinco personalizados, y otros permite la sincronización entre los sistemas para eliminar completamente las colisiones en un ambiente mixto. En la Figura 1.11 se muestra un ambiente mixto y la co-relación de estos.

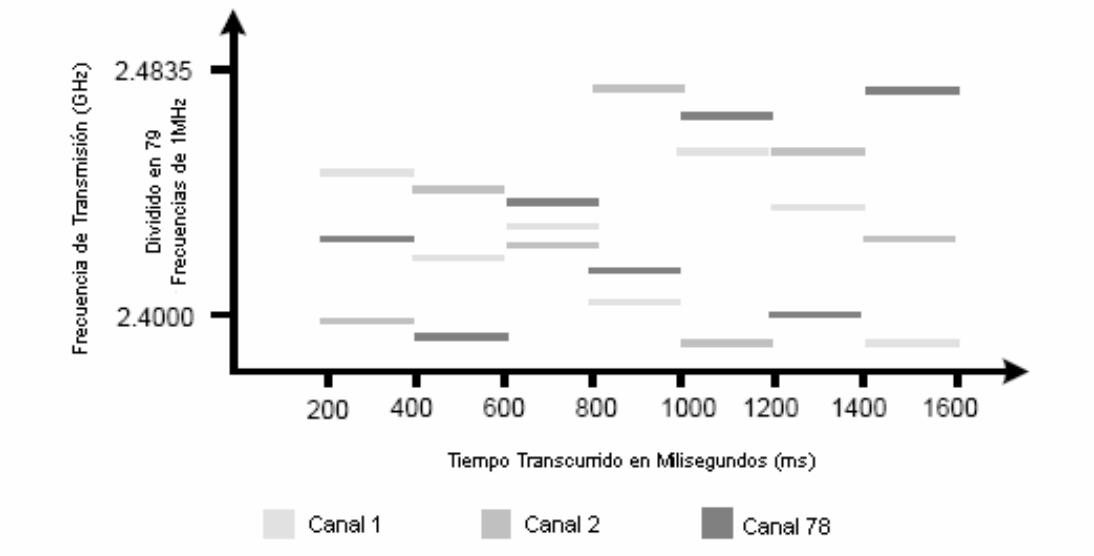


Figura 1.11: Co-Relación De Sistemas de Salto de Frecuencia

Aunque es posible tener hasta 79 Access Points sincronizados en estos sistemas, cada sistema de salto de frecuencia requeriría la sincronización precisa con todos los otros radiotransmisores para no interferir, (como transmitir en la misma frecuencia) con otro salto de frecuencia en el área. El costo de este tipo de sistemas es muy elevado y generalmente no es una opción viable.

Si se usan radios sincronizados, el gasto tiende a dictar 12 sistemas coexistentes como máximo. Si se usan radios no sincronizados entonces pueden coexistir 26 sistemas en una LAN inalámbrica; se considera que este número es el máximo en un medio LAN inalámbrico.

Aumentando el tráfico o ocasionalmente la transmisión de archivos grandes limita el número de sistemas coexistentes a 15 aproximadamente. Mas de 15 sistemas de salto de frecuencias coexistentes interferirá, a la magnitud de que las colisiones empezarán a reducir la eficiencia de la LAN inalámbrica.

1.5.5 Tiempo De Detención

Cuando un sistema de salto de frecuencia transmite, debe de permanecer en esa frecuencia por un tiempo determinado. Este tiempo se llama *tiempo de detención*. Una vez que el tiempo de detención ha expirado, el sistema cambiará a una frecuencia diferente y empezará a transmitir de nuevo.

Supongamos que un sistema de salto de frecuencia transmite en sólo dos frecuencias, 1.401 GHz y 1.402 GHz. El sistema transmitirá en la frecuencia 1.401 GHz por el tiempo de detención de 100 milisegundos (ms), por ejemplo. Después de los 100ms el radio debe cambiar su frecuencia de transmisión a 1.402 GHz y debe enviar la información a esa frecuencia por 100ms. Subsecuentemente, en nuestro ejemplo, la radio brincará atrás a 1.401 GHz y empezará el proceso de nuevo.

1.5.6 Tiempo De Salto

Cuando un sistema de salto de frecuencia salta de una frecuencia A una frecuencia B, debe cambiar la frecuencia de transmisión en uno de los dos lados. Cada uno de estos debe cambiar a un circuito de sintonización para recibir la nueva frecuencia, o debe cambiar algún elemento del circuito actual para sintonizar la nueva frecuencia. En cualquier caso, el proceso de cambiar a la nueva frecuencia debe completarse antes de que la transmisión pueda reanudarse, y este cambio toma tiempo debido a las latencias eléctricas inherente en los circuitos. Hay una cantidad pequeña de tiempo durante este cambio de frecuencia en que la radio no está transmitiendo llamado *tiempo del salto*. El tiempo del salto es en microsegundos (µs) y relativamente pequeño comparado con el tiempo de detención que es de alrededor de 100-200 ms, el tiempo del salto no es significante. Un sistema FHSS de 801.11 brinca entre los canales en un rango de 200-300 µs.

Con tiempos de detención muy cortos alrededor de 500-600µs, en sistemas de salto de frecuencia como Bluetooth, el tiempo del salto puede volverse muy significante. Si nosotros apreciamos el efecto de tiempo del salto por lo que se refiere al intercambio de datos, descubriríamos que entre mas largo sea Tiempo de Salto en relación con el tiempo de detención, más lento será la tasa de transmisión de datos. Esto traduce más largo sea el tiempo de detención = mayor será la transferencia de datos.

1.5.7 Limites De Tiempo De Detención

El FCC define el Tiempo máximo de detención de una frecuencia que salta el Sistema de Espectro Disperso a 400ms por frecuencia portadora, en un periodo de 30 segundos.

Por ejemplo, si un el transmisor usa una frecuencia por 100ms, entonces los brincos a través de la serie entera de 75 brincos, (cada brinco que tiene los mismos 100ms de tiempo) devolviendo a la frecuencia original, tiene encima de 7.5 segundos ligeramente en esta secuencia de salto. La razón que no sea exactamente 7.5 segundos son debidos a tiempo del salto. En la Secuencia de salto, cuatro tiempos consecutivo rendirían 400 ms en cada uno de las frecuencias del la portadora, durante este tiempo simplemente apenas llegaría a los 30 segundos (7.5 segundo x 4 pasos a través de la secuencia de salto) qué es aceptable por las reglas de FCC.

1.6 El Espectro Disperso De Secuencia Directa (DSSS)

La Secuencia Directa del Espectro Disperso es muy extensamente conocida y la más usada en los sistemas de Espectro Disperso, su popularidad es debido a su facilidad de aplicación y a las grandes tasas de transferencia de datos. La mayoría de los equipos LAN inalámbricos en el mercado usa la tecnología DSSS.

DSSS es un método de enviar datos en el cual los sistemas de transmisión y recepción están dentro de frecuencias los 22 MHz de ancho. El ancho de canal habilita los dispositivos para transmitir más información en una taza de transmisión de datos superior que los sistemas de FHSS actuales.

1.6.1 Como Trabaja El DSSS

DSSS combina una señal de datos que es enviada a la estación con una secuencia superior de bits con una alta tasa de transferencia, qué está llamado “chipping code“ o procesador de ganancia. Una ganancia alta aumenta la resistencia de la señal a la interferencia. La ganancia de proceso lineal mínima que el FCC permite es de 10 db, y la mayoría de los productos comerciales operan bajo 20 db.

El proceso de secuencia directa empieza con una portadora modulándose con un código de secuencia. El número de “chips” en el código determinará cuánto se extenderá, y el número de chips por bit y la velocidad del código (en chips por segundo) determinara la taza de transferencia.

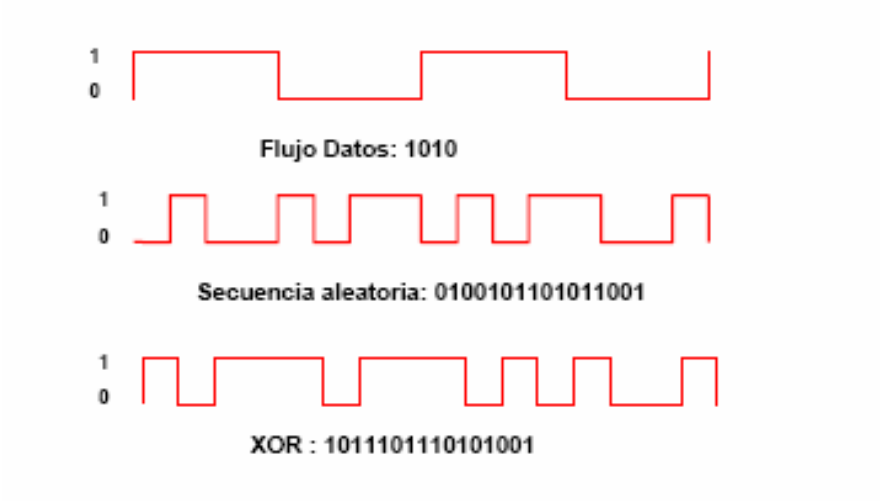


Figura 1.12: Chipping Code

El Chipping Code consiste en que para cada bit enviado se hace una operación XOR de ese bit con una secuencia de n-bit aleatorios. Estos bits son generados Pseudo aleatoriamente los n-bits del Chipping Code esparcen la señal sobre una banda de frecuencia n veces mayor. En la Figura 1.12 se muestre un ejemplo.

1.6.2 Los Sistemas De Secuencia Directa

En la banda ISM de 1.4 GHz, el IEEE especifica el uso de DSSS a una tasa transferencia de datos de 1 o 2 Mbps bajo la norma 801.11. Bajo la norma 801.11b la tasa transferencia de datos es de 5.5 y 11 Mbps.

Los dispositivos que operan en la norma IEEE 801.11b a 5.5 o 11 Mbps pueden comunicarse con dispositivos que operan en la norma 801.11 a 1 o 2 Mbps porque la norma 801.11b proporciona compatibilidad regresiva. Usuarios que emplean dispositivos 801.11 no necesitan actualizar completamente su LAN inalámbrica para usar dispositivos 801.11b su red.

Recientemente se actualizo la norma IEEE 801.11a la cual especifica lista de dispositivos que usan la tecnología de la sucesión directa y que pueden operar a 54 Mbps. Desgraciadamente para usuarios de 801.11 y 801.11b, los dispositivos 801.11a son totalmente incompatibles con 801.11b porque no usan la banda de 1.4 GHz.

Esto resulto ser un problema porque muchos usuarios querían aprovechar la tecnología de la sucesión directa la cual proporciona tasa de transmisión de datos a 54 Mbps, pero el costo el costo de una actualización de LAN inalámbrica completa era muy elevado.

Así recientemente el IEEE aprobó la norma 801.11g que especifica los sistemas de secuencia directa, que operan en la banda ISM de 1.4 GHz y que pueden entregar tasas de transferencia de 54 Mbp. La tecnología 801.11g fue la primera tecnología de 54 Mbps que era compatible hacia atrás con dispositivos 801.11 y 801.11b.

1.6.3 Los Canales

Los sistemas de salto de frecuencia, usan la secuencia del salto para definir los canales, los sistemas de secuencia directa usan una definición más convencional de canales. Cada canal es la banda contigua inmediata de frecuencias 22 MHz de ancho, y se usan frecuencias de 1 MHz para la portadora del así como con FHSS.

El canal 1, por ejemplo, opera de los 1.401 GHz a 1.423 GHz (1.412 GHz ± 11 MHz); el canal 2 opera de los 1.406 a 1.429 GHz (1.417 ± 11 MHz), y así consecutivamente.

En la Figura 1.13 se puede apreciar las asignación de canales en DSSS y la relación espectral.

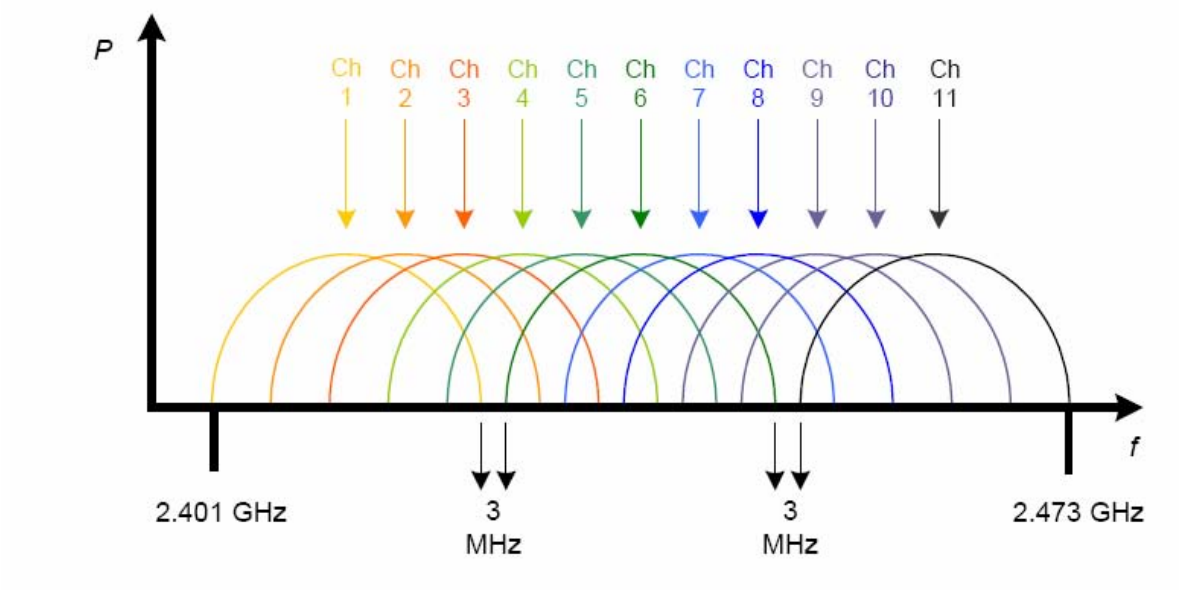


Figura 1.13: Relación Espectral Y Ubicación De Canales En DSSS

La FCC específica el uso de sólo 11 canales para la banda no licenciada en los Estados Unidos.

Nosotros podemos ver que los canales 1 y 2 se traslapan por una cantidad importante. Cada uno de las frecuencias listadas en la tabla 1.1 son consideradas frecuencias centrales. De este centro de frecuencia, 11 MHz es sumado y restado para obtener 22 MHz de ancho de banda usable.

Identificador de Canal	Frecuencias de Canales FCC GHz	Frecuencias de Canales ETSI GHz
1	2.412	N/A
2	2.417	N/A
3	2.422	2.422
4	2.427	2.427
5	2.432	2.432
6	2.437	2.437
7	2.442	2.442
8	2.447	2.447
9	2.452	2.452
10	2.457	2.457
11	2.462	2.462

Tabla 1.14: Asignaciones De Frecuencia De Canales En DSSS

El uso de sistemas de DSSS con el traslape de canales en el mismo espacio físico causaría la interferencia entre los sistemas. Los sistemas de DSSS con traslape de canales no deben implementarse porque casi siempre existiría una reducción drástica o completa en la trasmisión de datos.

Dado que las frecuencias de centro son de 5 MHz y los canales son de 22 MHz ancho, sólo deben co-localizarse los canales si los números del canales son por lo menos cinco separadamente: en los canales 1 y 6 no existe traslape, los canales 2 y 7 no se traslapan, etc. Hay un el máximo de tres sistemas de la sucesión directos co-localizados posibles porque los canales 1, 6 y 11 son los únicos teóricamente en los que no existiría traslape.

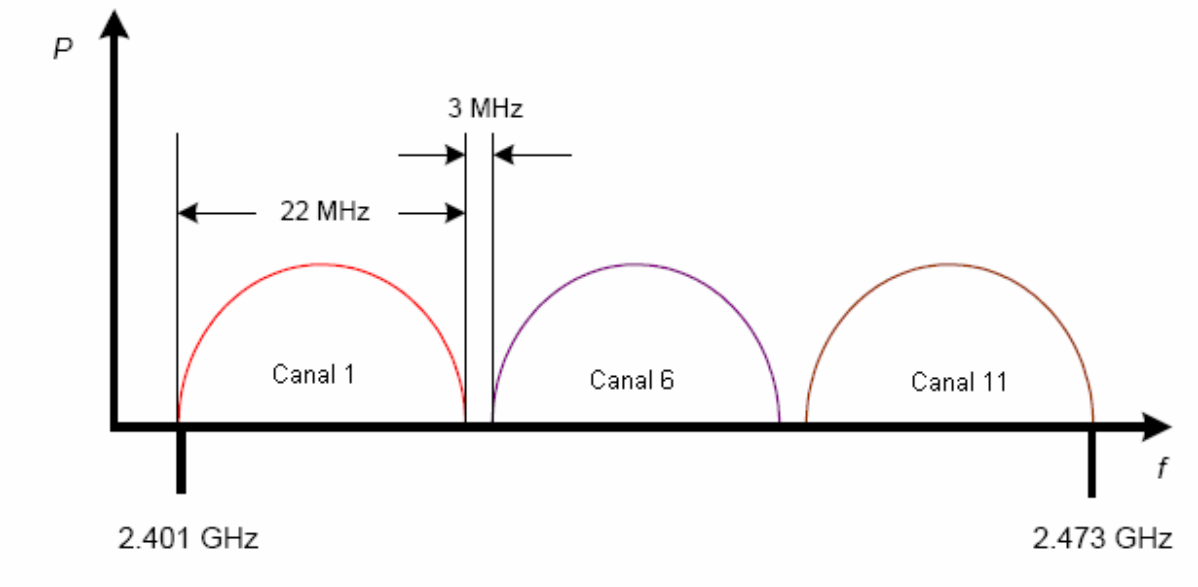


Figura 1.15: Los canales en DSSS en los cuales no existiría traslape.

1.6.4 Los Efectos De la Interferencia En La Banda Estrecha

Los sistemas de secuencia directa son resistentes ante la interferencia debido a sus características de espectro disperso.

Un señal de DSSS es más susceptible a la interferencia de la banda estrecha que FHSS dado que la banda de DSSS es mucho menor (22 MHz de ancho de banda en lugar de 79 MHz de ancho de banda usada por FHSS) y la información se transmite simultáneamente a lo largo de la banda entera en lugar de una frecuencia por tiempo.

1.6.5 Las Normas De La FCC Con Respecto A DSSS

Así como con los sistemas de FHSS, la FCC ha regulado que los sistemas de DSSS usen por lo máximo de 1 watt potencia de transmisión en las configuraciones de punto a multipunto.

1.6.6 FHSS Comparando Con DSSS

Las tecnologías FHSS y DSSS tienen sus ventajas y desventajas, el administrador de LAN inalámbricas es el que debe decidir cual usar y como implementar la red. Acontinuacion se muestran algunos de los factores que debe discutirse para determinar qué tecnología es apropiada para su organización:

- La Interferencia De La Banda Estrecha
- El Establecimiento
- El Costo
- La Compatibilidad De Equipo Y La Disponibilidad
- La Tasa De Trasferencia Y La Cantidad De Datos
- La Seguridad
- El Apoyo De Las Normas

1.6.7 La Interferencia De La Banda Estrecha

Las ventajas de FHSS incluyen una mayor resistencia a la interferencia de la banda estrecha. Los sistemas DSSS pueden ser afectados por la interferencia de la banda estrecha más que los sistemas FHSS debido al uso de bandas inmediatas de 22 MHz de ancho en lugar de 79 MHz usadas por FHSS. Este hecho puede sea una consideración importante, si el sitio de LAN inalámbrica propuesto está en un ambiente que tiene presente interferencia.

1.7 El Establecimiento De La Red

Una ventaja de FHSS sobre de DSSS es la posibilidad de situar mucho más sistemas de salto de frecuencia, que en los sistemas de la sucesión directa.

Desde que los sistemas de salto de frecuencia utilizan una “frecuencia ágil” y hacen el uso de 79 canales discretos, tiene ventaja del colocar mayor numero de sistemas conviviendo entre si que los sistemas de la sucesión directos que tienen un máximo de 3 puntos de acceso en un mismo lugar.

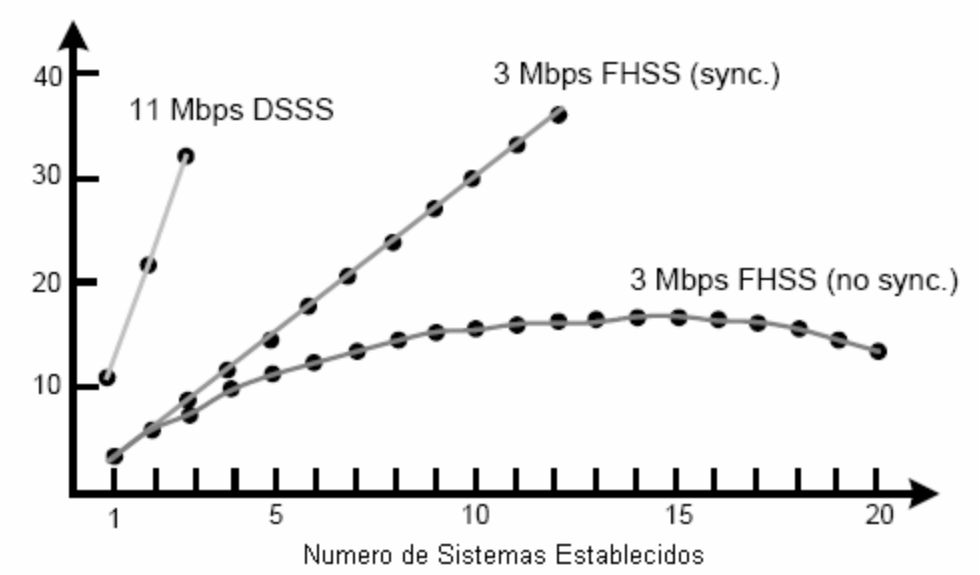


Figura 1.16: Comparación Numérica del establecimiento de sistemas en FHSS y DSSS

Sin embargo, al calcular los costos del hardware de un sistema de FHSS para conseguir la misma tasa de transferencia de datos que en sistema de DSSS, la ventaja desaparece rápidamente. Dado que un sistema de DSSS puede tener hasta 3 puntos de acceso establecidos, la tasa de transferencia para esta configuración seria:

3 puntos de acceso x 11 Mbps = 33 Mbps

En aproximadamente 50% de ancho de banda, el un sistema DSSS la transferencia real de datos estaría aproximadamente:
33 Mbps / 2 = 16.5 Mbps

Para lograr el mismo ancho de banda del sistema que cumple con la norma IEEE 801.11, el sistema de FHSS requeriría:
16 puntos de acceso x 2 Mbps = 32 Mbps

En aproximadamente 50% de ancho de banda, el un sistema FHSS la transferencia real de datos estaría aproximadamente:
32 Mbps / 2 = 16 Mbps
En esta configuración, un sistema de FHSS requeriría comprar 13 puntos de acceso adicionales para conseguir la misma tasa de transferencia de datos que un sistema de DSSS. También, la instalación adicional los servicios para estas unidades, así como comprar los cables, conectores, y antenas.

Como se puede ver, hay ventajas en la implementación de cada tipo de sistema. Si el objetivo es el bajo costo y tasas de transferencia altas, claramente la tecnología de DSSS seria la mejor opción. Si el objetivo es mantener usuarios segmentados usando diferentes puntos de acceso en un ambiente altamente denso, FHSS podrían ser una alternativa viable.

1.7.1 El Costo De Implementación

Cuando se implementa una LAN inalámbrica, las ventajas de DSSS pueden ser mas competitivas que los sistemas de FHSS, particularmente cuando se maneja por un presupuesto firme. El costo por la implementación de un sistema de secuencia directa es mucho menor que un sistema de salto de frecuencia.

Un equipo DSSS esta extensamente disponible en el mercado, y su rápida adopción ha ayudado a mantenerlo a abajo costo. Hace sólo unos años, el equipo era sólo accesible para clientes empresariales. Hoy en día, las tarjetas 801.11b ofrecen muy buena calidad y un costo por debajo de $100 dólares. Las tarjetas FHSS que cumplen con las normas 801.11 tienen un precio alrededor de los $150 y $350 dólares en el mercado dependiendo del fabricante y las normas con que cumplan las tarjetas.

1.7.2 Compatibilidad Y Disponibilidad De Los Equipos

La Alianza de Compatibilidad Inalámbrica Ethernet (WECA) proporciona comprobación del cumplimiento de 801.11b en los equipos DSSS de LAN inalámbricos, para asegurar que cada equipo operará e inter-opere con otros dispositivos 801.11b de DSSS. La norma de interoperabilidad que la WECA creó y que en este momento se usa, es llamada Fidelidad Inalámbrica o Wi-Fi™, y esos dispositivos que superan las pruebas para la interoperabilidad son dispositivos "Wi-Fi certificados".

Los dispositivos que son aprobados, se les permite pegar el logotipo de Wi-Fi en el material de publicidad y en los productos, esto muestra que estos dispositivos han sido probados y son ínter operables con otros dispositivos Wi-Fi certificados.

Figura 1.17: Logos de certificación Wi-Fi™.

En los sistemas FHSS no existe ninguna prueba para la compatibilidad del equipo que usa. Hay normas como 801.11 y OpenAir, pero ninguna organización ha avanzado para desarrollar el mismo el tipo de prueba de compatibilidad para FHSS como la WECA hace para DSSS.

Debido a la inmensa popularidad de los radios 801.11b certificados, es más fácil obtener estos dispositivos. La demanda sólo parece estar creciendo para los dispositivos Wi-Fi, mientras la demanda para los dispositivos de FHSS ha permanecido constante, pero ha ido disminuyendo durante el último año.

1.7.3 Tasa De Transferencia De Datos Y La Transferencia Real

Los últimos sistemas de salto de frecuencia, son más lentos que los últimos sistemas de DSSS porque su tasa de transferencia de datos es sólo de 2 Mbps. Aunque algunos sistemas de FHSS operan a 3 Mbps o más, estos sistemas no cumplen la norma 801.11 y no pueden ínter operar con otro sistema FHSS.

Los sistemas de FHSS y DSSS tienen una transferencia real de datos (los datos realmente enviaron) de sólo la mitad de la tasa del datos. Al probar la transferencia real de datos en una LAN inalámbrica nueva, se logran hasta 5-6 Mbps en los 11 Mbps de configuración para DSSS, y 1 Mbps en la configuración de 2 Mbps en FHSS.

HomeRF 2.0 usa sistemas de salto de frecuencia en la banda ancha para lograr 10 Mbps de trasferencia de datos que a su vez logran aproximadamente 5 Mbps de transferencia de datos real. No se puede comparar HomeRF 2.0 con sistemas 801.11 o 801.11b. La diferencia es el rendimiento de poder limitado de HomeRF (125 mW) comparado a 1 watt de los sistemas 801.11.

Cuando las tramas de datos inalámbricas son transmitidas, hay pausas entre ellas para las señales de control y encabezados de la trama. Con frecuencia en los sistemas de salto de frecuencia, este “espacio entre tramas” es más largo que el usado por los sistemas de secuencia directa, causando una disminución de datos en la proporción que realmente se envía (Tasa real de transferencia). Adicionalmente, cuando el sistema de salto de frecuencia está en el proceso de cambiar la frecuencia de transmisión, no se envía ningún dato. Esto se traduce en la disminución de tasa de transmisión real, aunque es sólo una cantidad insignificante.

Algunos sistemas LAN inalámbrico usan protocolos de la capa física propietarios para aumentar la tasa de transmisión real. Éstos métodos trabajan optimizando la tasa de transmisión real hasta o 80% de la proporción del datos, pero causando la interoperabilidad.

CAPITULO II

REDES INALÁMBRICAS

2.1 Una LAN Inalámbrica Básica

Una LAN inalámbrica básica consta de dos o más computadoras conectadas vía un enlace inalámbrico que las comunica entre sí. Un enlace en una LAN inalámbrica no consta de un cable o ningún tipo de conexión física; en vez de esto consta de una conexión vía espectros electromagnéticos viajando por el aire o el vació en los que los datos son transmitidos. Las computadoras en una red inalámbrica requieren tarjetas de interfaz de la red (adaptadores de la red), la cuales determinan y mantienen actualizada la transmisión y la recepción de la información entre las computadoras conectado a una red. También, cada computadora en una red inalámbrica debe usar la misma tecnología de conexión en red.

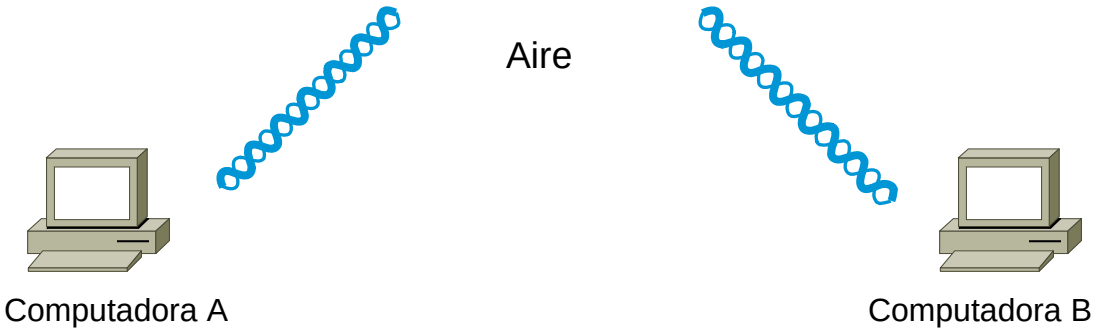


Figura 2.1 Dos Computadoras Interconectadas En Una Red Inalámbrica.

Todas computadoras en una LAN inalámbrica deben tener hardware apropiado que permita la conectividad inalámbrica. Este hardware es un componente electrónico que es fijado a una computadora que tiene que estar conectado a una LAN inalámbrica.

Estos componentes electrónicos son conocidos como los adaptadores de LAN inalámbricos o tarjetas de interfaz de la red de LAN inalámbricas (NICs por sus siglas en ingles).

Los adaptadores de la red pueden ser implementados como tarjetas de Asociación Internacional de Tarjetas de Memoria para Computadoras Personales (las PCMCIA) en computadoras portátiles, o componente de dispositivo periférico interconectan adaptadores de (PCI) en computadoras de escritorio, y son dispositivos a menudo completamente integrados dentro de computadoras portátiles.

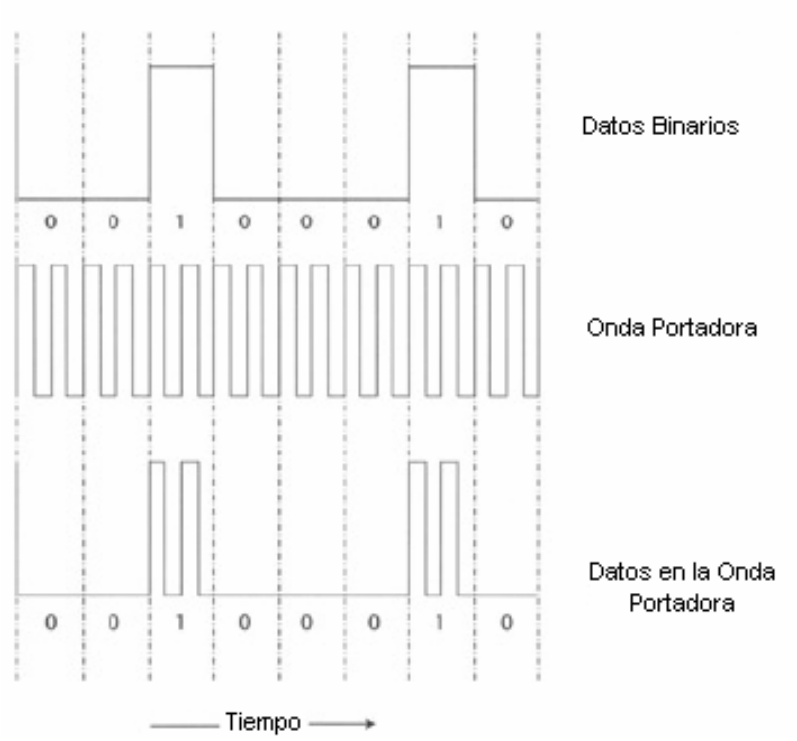


Figura 2.2 Transmisión De Datos Sobre La Onda Portadora.

En LAN inalámbricas los datos que se van a transmitir son superpuesto sobre una onda portadora electromagnética en la frecuencia especificada y transmitida sobre las ondas aéreas por el adaptador de la red inalámbrico. El adaptador de la red escucha en la misma frecuencia, y cuando recibe las ondas transmitidas, extrae los datos superpuestos de la portadora electromagnética[3].

2.2 Arquitectura Básica De Una LAN Inalámbrica

Una LAN inalámbrica puede ser desarrollada en muchos sentidos, dependiendo de la arquitectura es esta basada. Hay muchos dispositivos de radio disponibles hoy en día así que es mejor escoger los dispositivos que ínter operen entre si cuando se desarrolla una LAN inalámbrica.

A continuación se presenta una breve descripción del equipo físico y su configuración.

2.2.1 Adaptadores De LAN Inalámbricos

Todas las computadoras en una LAN inalámbrica deben tener un adaptador de la red inalámbrico. Tener este dispositivo en el sistema OSI asegura que las computadoras diferentes serán compatibles entre sí. En la conexión de una red inalámbrica solamente intervienen las dos capas inferiores del modelo OSI, la capa física y la capa de enlace de datos.

[3] BSWN-1

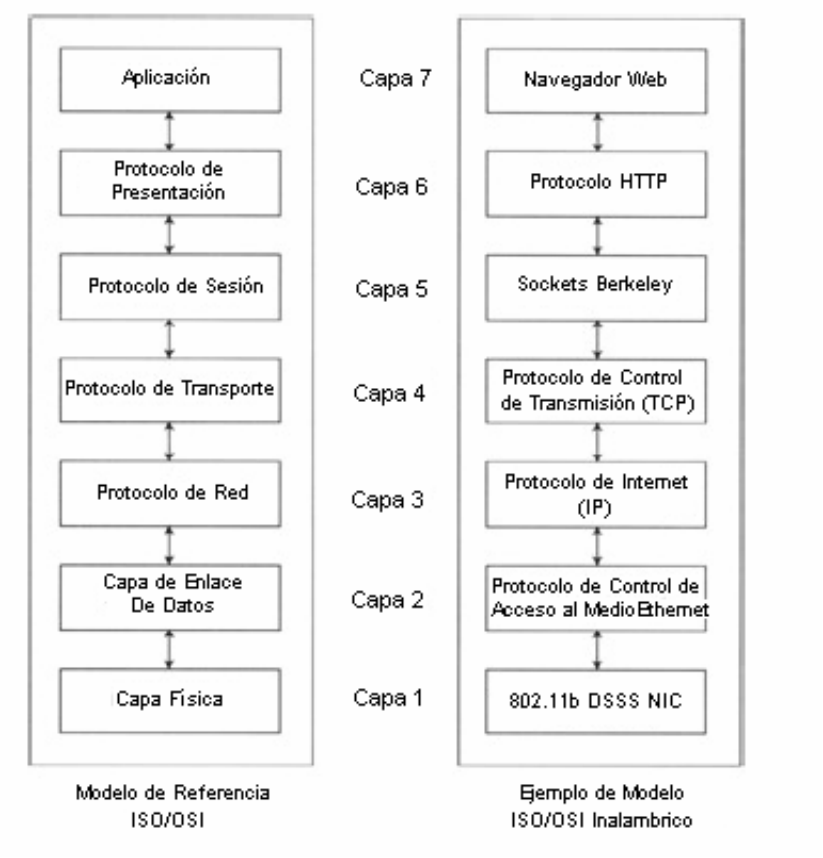


Figura 2.3 Modelo De Referencia De OSI Para Un Adaptador De LAN Inalámbrico.

Los Adaptadores de LAN inalámbricos (tarjetas de interfaz de la red) implementan la capa física del modelo de OSI y se ajustan a la capa de enlace de datos para proveer la interfaz de nivel de control de acceso media (MAC) correcta.

2.2.2 La Capa Física

La diferencia principal entre un adaptador de LAN inalámbrico y un adaptador de LAN cableado es su capa física. La capa física en adaptadores inalámbricos hace dos cosas: cuando los datos son transmitido, convierte las señales electrónicas en señales de onda al medio, y cuando las señales son recibidas del medio, los convierte en señales electrónicas para capas superiores puedan interpretarlas.

La eficiencia en una red inalámbrica va a depender del ancho de banda del espectro electromagnético, la calidad de los componentes que hacen el adaptador de la red, y los protocolos usados.

Para propagar señales eléctricas para por el aire, deben ser convertidas en ondas electromagnéticas. La distancia de alcance de la onda electromagnética depende de sus propiedades físicas. Estas propiedades incluyen la longitud y la frecuencia de la onda electromagnética.

Debido a la naturaleza muy popular de la conectividad inalámbrica y la disponibilidad limitada del espectro electromagnético, las LAN inalámbricas usan un ancho de banda limitado del espectro electromagnético para transmitir los datos en el aire. Hoy, hay tres bandas del espectro electromagnéticas básicas que son usadas para la transmisión de datos comúnmente sobre enlaces de LAN inalámbricos: infrarrojo, radio frecuencias, y microondas.

2.2.3 El Infrarrojo

Los sistemas basados en infrarrojos son las LAN inalámbricas más simples y menos costosas. Estos sistemas trabajan mejor cuando operan en línea visual (es decir los transceptores involucrados en la comunicación deben esta enfocados entre sí sin cualquier obstáculo físico).

Los sistemas infrarrojos no son de ancho de banda limitado, los dispositivos infrarrojos puede usar el ancho de banda entero para comunicarse sin ninguna interferencia con cualquier otro dispositivo. También pueden alcanzar velocidades altas en gastos relativamente bajos comparados con otras clases de sistemas.

Otro beneficio de usar un sistema basado en infrarrojo es que no requiere concesión de licencia de la Comisión Federal de Comunicaciones (FCC), que regula la porción de RF de la radiación electromagnética entre 9 kHz y 300 gHz solamente. La radiación infrarroja entra en la parte ligera del espectro electromagnético que no es regulado por el gobierno federal.

Un sistema infrarrojo puede conseguir una extensión alta, hasta una milla, que puede ser bueno para interconexión de redes. Sin embargo, cuando usted necesita conectividad omnidireccional, donde las señales son reflejadas desde objetos cercanos en todas direcciones, el rendimiento de sistema es reducido. Los sistemas infrarrojos no funcionan bien bajo tales condiciones. Los sistemas infrarrojos también padecen de la interferencia de la luz del sol y la luz artificial. Inicialmente sistemas infrarrojos eran muy populares, pero su falta de fiabilidad atribuible a las señales fácilmente obstruidas, ha limitado el uso.

2.2.4 Las Microondas

Las redes basadas en microondas operan normalmente en la banda de 5.8 GHz y usa por lo menos de 500 miliwatts de potencia. El típico alcance para un sistema de microondas en un ambiente de la oficina cerrado es aproximadamente 40 metros.

La ventaja grande para sistemas de microondas es el caudal de proceso y transferencia alta, cuando los sistemas microondas no tienen la sobrecarga involucrada con los sistemas de espectro difundidos.

2.2.5 Radio Frecuencias

Las LAN inalámbricas basadas en el radiofrecuencia son las mas populares en los últimos tiempos. Las técnicas de modulación del espectro disperso son definidas como las técnicas en las que ocurre siguiente:

1. El ancho de banda de la señal transmitida es mucho más grande que el ancho de banda del Mensaje original.

2. El ancho de banda de la señal transmitida es determinado por el mensaje transmitido y por una señal adicional conocida como código de dispersión.

El espectro difundido fue diseñado para la marina de los Estados Unidos originalmente para disfrazar las señales de control de Torpedos. El tema fue clasificado por años por el ejército, y solamente recientemente las patentes lo han hecho público. Los Sistemas que usan espectro disperso deben usar la exactamente la misma frecuencia y relación Parámetros. Estos parámetros son definidos por la tecnología montada del espectro disperso.

Actualmente hay dos tipos de la tecnología de espectro disperso mas comúnmente usados : el de espectro disperso de secuencia directa (DSSS) y el de salto de frecuencia del espectro disperso (FHSS).

2.2.6 Capa De Enlace

La capa MAC de la capa de enlace de datos controla cómo son distribuidos los datos en el Medio físico. El trabajo principal del protocolo MAC es regular el uso del medio, y esto es hecho a través de un mecanismo de acceso de canal.

Un mecanismo de acceso de canal es una manera de dividirse el recurso disponible de ancho de banda en subcanales. Cada subcanal indica cuando puede transmitir y cuando esta esperado recibir los datos. El mecanismo de acceso al canal es el núcleo del protocolo de Mac.

La productos LAN alambricos usan como protocolo MAC el Acceso Múltiple con Detección de Portadora con Detección de Colisión (CSMA/CD, también conocido como Ethernet) , los fabricantes de equipo de LAN inalámbrico lógicamente eligieron un Protocolo similar como el protocolo de MAC.

La mayoría de las puestas en funcionamiento de capa de enlace de datos usan CSMA / CD. El detector de portadora quiere decir que la estación escuchara antes de que transmita. Si hay alguien transmitiendo, entonces la estación esperan y tratan otra vez después. Si nadie está transmitiendo, entonces la estación envía el lo que tiene. Si dos estaciones envían al mismo tiempo, las transmisiones chocan y la información se perderá. Es donde la detección de colisión actúa. La estación escuchará para asegurar que su transmisión la hizo al destino sin colisiones. Si una colisión ocurre, entonces las estaciones esperan y tratan otra vez después.

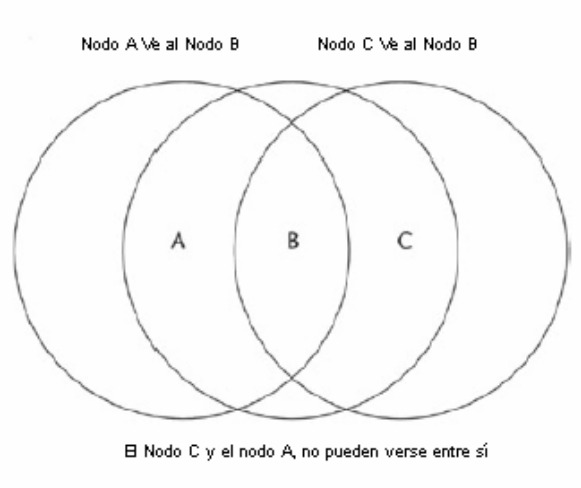


Figura 2.4 Problema de Nodo Escondido

Esta técnica trabaja bien para redes LAN alambricas, pero para redes inalámbricas esta topología puede crear un problema. Este problema es conocido como el problema de nodo escondido. El problema de nodo escondido es ilustrado en la Figura 2.4 El nodo C no puede escuchar al nodo A. Así que si el nodo A esta transmitiendo, el nodo C no lo sabrá y podrá transmitir también. Esto resultará en colisiones y pérdida de datos. La solución para este problema es el protocolo de Acceso Múltiple con Detección de Portadora con Evitación de Colisión (CSMA/CA).

CSMA/CA trabaja de la siguiente manera: la estación escucha antes de transmitir. Si alguien ya está transmitiendo, espera un período aleatorio y trata otra vez. Si nadie esta transmitiendo, entonces envía un mensaje breve. Este mensaje es llamado RTS (Ready-to-Send). Este mensaje contiene la dirección de destino y la duración de la transmisión.

Las otras estaciones ahora saben que deben esperar ese tiempo antes de que puedan transmitir. El destino envía un mensaje CTS (Clear-to-Send). Con este mensaje sabe el origen que puede enviar sin miedo de colisiones.

Cada paquete es reconocido, cada vez que el receptor recibe un paquete debe transmitir un paquete de reconocimiento ACK (Acknowledged). Si un ACK no es recibido, la capa MAC retransmite los datos. Esta secuencia entera es llamada Handshake.

2.2.7 Puntos De Acceso (APs)

Un Punto de Acceso o Access Point (AP), es un dispositivo inalámbrico centralizado que no tiene una computadora fija a el físicamente. El AP controla el tráfico en el medio inalámbrico.

Todo tráfico de la comunicación entre el las computadoras debe pasar por el punto de acceso.

Los puntos de acceso comúnmente son conectados a las LAN cableadas (redes por ejemplo, corporativas o locales) que son se conectados generalmente una Red de Area Amplia (WAN) por ejemplo, la Internet usa una conexión de alta velocidad de banda ancha.

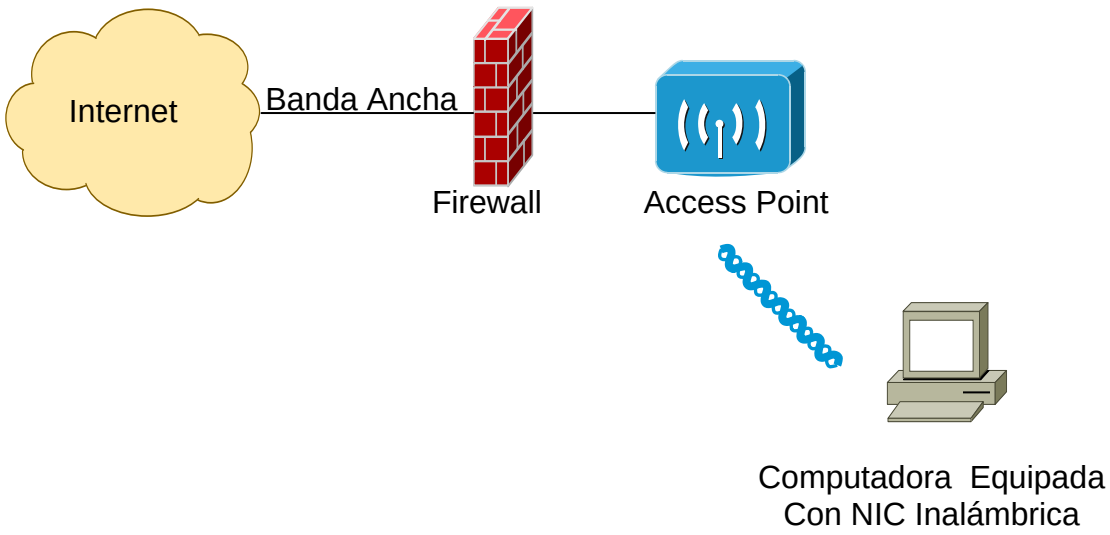


Figura 2.5 Conexión De Puntos De Acceso

Los Puntos de Acceso son puestos de este modo, para encaminar el tráfico entre la LAN inalámbrica Y la red con la que se comunica. Los Puntos de Acceso contienen un adaptador de interfaz inalámbrico exactamente como cualquier otra computadora en una LAN inalámbrica. Además, los Puntos de Acceso mantienen mucha información sobre las computadoras en la red y llevan a cabo la autentificación, la encriptación, y la sesión (la conexión) con todas las Computadoras. Dado que un Punto de Acceso puede conectar la LAN inalámbrica con cualquier otro tipo de red , también funciona como un ruter.

2.3 Configuraciones De LAN Inalámbricas

Cada computadora en una LAN inalámbrica es comúnmente llamada una estación. Una red inalámbrica puede ser configurada como una red Punto a Punto (llamada red Ad-Hoc), que es cuando dos o mas computadoras se comunican entre si directamente. El otro tipo de configuración es el modo Infraestructura donde un Punto de Acceso está involucrado y toda comunicación entre las estaciones es encaminada a través del AP central.

2.3.1 Modo Ad-Hoc

Cuando dos o más estaciones se van a comunicar entre si, forman Servicio Basico de Sets (BSS). El BSS mínimo consta de dos estaciones. Un BSS que está esperando solo y no esta conectado a un Acces Point es llamado Servicio Basico de Sets Independiente (IBSS) o una red Ad-Hoc

Un Servicio Extendido de Sets (ESS) es formado cuando dos o mas BSS operan dentro la Misma red. Una red Ad-Hoc es una red en la cual cada estación se comunica solo Punto a Punto. No hay Access Point y nadie da permiso para hablar. Principalmente estas redes son espontáneas y pueden ser montadas rápidamente.

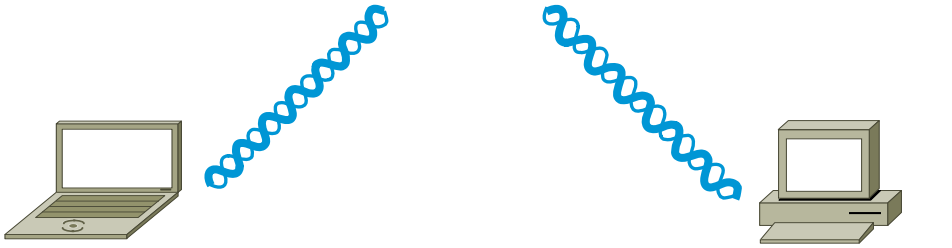


Figura 2.6 Modo Ad-Hoc

El modo Ad-Hoc no es comúnmente usado, y cuando se usa, es solamente para propósitos temporales.

2.3.2 Modo De Infraestructura

Se dice que una LAN inalámbrica esta funcionando en modo Infraestructura cuando dos o mas BSSs son interconectados usando uno Access Point. Los Access Points actúan como Hubs para estaciones inalámbricas. También rutea el Tráfico entre los dos BSSs. Cada BSS se hace un componente de una red más grande.

Uno Access Point es una estación, que direcciona los datos como un router o como una puerta de enlace y encamina el tráfico entre la red de banda ancha cableada y la rede inalámbrica y vise versa. Asi que los datos se mueven entre el BSS y la Red de banda ancha con ayuda de los Access Points.

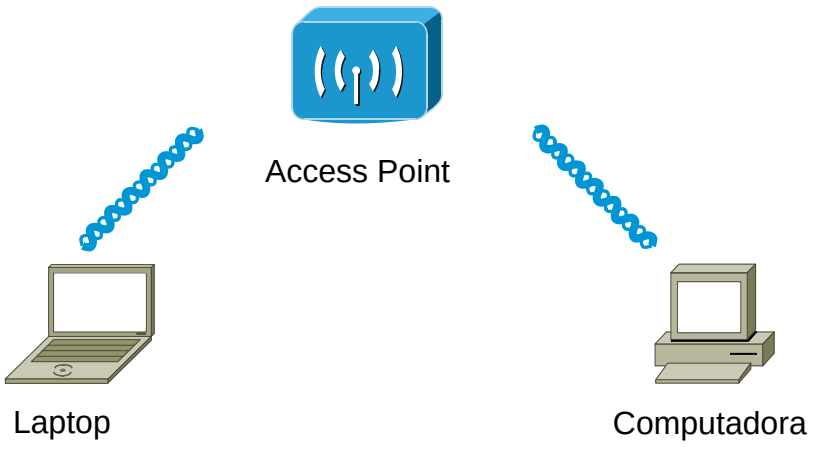


Figura 2.7 Modo Infraestructura

La mayoría de las LAN inalámbricas son construidas para operar en modo infraestructura. En redes muy grandes, el modo infraestructura puede ser usado para la distribución de sistemas.

2.3.3 Sistemas De Distribución De Servicios (DSSs)

Los Sistemas de distribución permiten a las LAN inalámbricas conectarse con el mundo cableado. Un sistema de distribución permite a los Access Points participar en una configuración de red jerárquica, que hace a las computadoras inalámbricas formar parte de LAN de la red total.

Un sistema de distribución puede ser creado a partir de existentes o nuevas tecnologías. Un puente punto a punto que conecta LANs en dos edificios distintos podría ser un sistema de distribución. Los sistema de distribución deben proveer servicios a bajo nivel a redes inalámbricas. Estos servicios son divididos en dos secciones: sistema de distribución de servicios (DSSs) y Servicios de estación (SSs).

Los DSSs proporcionan cinco servicios básicos: la relación, reasociación, desasociación, la distribución, y la Integración. Los primeros tres servicios están relacionados con la movilidad de estación. Si una estación se está moviendo dentro de un mismo BSS la estación no ejecuta ninguna transición esto es llamado no transición .Si una estación se mueve entre BSSs dentro del mismo ESS, su movilidad es llamada de transición de BSS. Si la estación se mueve entre BSSs de ESSs diferentes, esto es llamado transición de ESS. Una estación debe afiliarse el mismo con la infraestructura de BSS Si quiere usar la LAN. La estación puede hacer esto relacionándose con un AP.

Una estación puede solamente ser asociado con un AP. Esto asegura que el DS sabe siempre dónde esta la estación. El entrar en el servicio de reasociación permite que la estación cambie su asociación de un AP a otro. Tanto la asociación y reasociación es iniciado por la estación, que quiere formar parte de la red. La desasociación es cuándo la asociación entre la estación y el AP es terminada. Cualquier parte puede iniciar la desasociación. Una estación desasociada no puede enviar o recibir datos. Una estación puede moverse hacia un nuevo ESS, pero tendrá que reiniciar las conexiones.

La distribución sólo consta en que los datos sean enviados del origen al receptor destino. El mensaje es enviado al AP local (AP de entrada) y luego distribuido a través del DS al AP (AP de salida) con el que el receptor esta conectado. Si el remitente y el receptor están conectados en el mismo BSS, el AP de entrada y de salida es el mismo. Así que el servicio de distribución es llamada de manera lógica, si los datos se van a través del DS o no. La integración es cuándo es el AP de salida es un portal.

Los servicios de estación son autentificación, desautentificación, privacidad, y entrega de unidad de datos del servicio MAC (MSDU). Con un sistema inalámbrico, el entorno no es limitado como con un sistema cableado. La orden para controlar el acceso a la red, las estaciones primero deben establecer su identidad. Para entrar en la red interna primero uno debe identificarse antes de poder entrar. En redes de computadoras, antes de que sea admitida una conexión, usted debe primero pasar una serie de pruebas para asegurar que usted es quién dice ser, una vez una estación lo ha Autentificado, puede conectarse.

El proceso de autentificación puede llevarse acabo entre dos estaciones dentro de un mismo IBSS en una red de ad-hoc o entre dos APs dentro de un BSS en una red modo infraestructura. Todas las estaciones arrancan con el estado no autorizado hasta que son autentificadas. La desautentificación es cuándo la estación o el AP desea poner fin a la autentificación de una estación. Cuando esto ocurre, la estación es desasociada automáticamente y la información de conexión relacionada sobre el AP es Descartada.

La privacidad en LANs inalámbricas es conseguida a través del uso de la tecnología de encriptación. Sin la encriptación, los datos son transmitidos en texto simple. Los datos transmitidos sin encriptación son Vulnerables a la escucha por gente no autorizada.

En la mayoría de las LAN inalámbricas, la privacidad es una opción que puede ser habilitada si se desea una seguridad más alta. Para usar una LAN inalámbrica con modo seguro habilitado, las estaciones y APs deben estar configurados para usar los misma parámetros de encriptación (la tecnología, las claves de encriptación, etcétera), de otra forma no estarán habilitados para interpretar los datos.

2.3.4 Estándares Existentes De LAN Inalámbricas

Con una gran variedad de dispositivos de red inalámbricos disponibles hoy en día, y cada uno de estos producidos por una compañía diferente, los fabricantes se dieron cuenta de la necesidad hacer sus dispositivos ínter operables con otros o por lo menos que sigan un estándar en particular.

Al principio, algunos distribuidores lanzaron soluciones de LAN inalámbricas basadas en la tecnología reservada; esta solución no era ínter operable con los dispositivos de otros vendedores y requería que toda la infraestructura fuera comprada de una sola marca. El IEEE reconoció la necesidad de un estándar que utiliza el ancho de banda limitado de RF de la manera más eficiente.

2.3.4.1 IEEE 802.11

Para abordar la necesidad de un estándar de interoperabilidad de diferentes clases de LAN inalámbricas, el IEEE Comité responsable de los estándares de Redes de Área Local y Redes de Área Metropolitana, conocidos como los estándares 802 ,formo un grupo de trabajo llamado 802.11 para analizar los estándares para las LAN inalámbricas.

En 1997, el IEEE redactó el borrador de los estándares 802.11 para interconexión de redes de área local. El estándar IEEE 802.11 define la transmisión con luz infrarroja y dos tipos de la transmisión de radio dentro de la banda de 2.4 GHz sin licencia.

2.3.4.2 IEEE 802.11 b

En 1999, el estándar 802.11b fue presentado como borrador y aceptado por la industria de conexión de redes y los productos para la conexión en red inalámbrica en la banda 2.4 GHz empezaron a ser producidos.

802.11b usa la banda ISM y funciona hasta a 11Mbps con una disminución a 5.5, 2, y a 1 Mbps. 802.11b usa DSSS como tecnología de propagación de espectro. 802.11b también soporta WEP (Wired Equivalent Privacy) para garantizar la confidencialidad de los datos transmitidos en LANs inalámbricas.

2.3.4.3 IEEE 802.11 a

802.11a es uno de los resultados del grupo de trabajo IEEE 802.11.Este estándar fue desarrollado en la capa física para operar en la nueva banda UNII recién asignada. Ésta es una extensión de 802.11 que es aplicable a LAN inalámbricas y provee hasta 54 Mbps en la banda de 5 GHz.

802.11a Usa de Una frecuencia plan de codificación división multiplexar ortogonal en vez de FHSS o DSSS. Casi Todos distribuidores muy importantes han lanzado su línea de dispositivos de 802.11a.

La mayoría de los dispositivos de 802.11a son pensados para ambientes empresariales.

2.3.4.4 HomeRF

HomeRF también opera en la banda ISM de 2.4 GHz como 802.11b y los teléfonos inalámbricos. HomeRF usa FHSS como su tecnología de propagación. Las redes de HomeRF proveen uno alcance de hasta 50 metros, suficiente para cubrir una casa típica, garaje, y jardín.

2.3.4.5 Bluetooth

Bluetooth es uno de los estándares mas recientes. Bluetooth es un candidato fuerte para las redes de área personal o PAN . LA PAN es definida como una red inalámbrica de alcance desde centimetros hasta 5 metros. Bluetooth también opera en la banda ISM.

Las aplicaciones existentes de Bluetooth incluyen la sincronización de datos para ordenadores de mano, asistentes personales digitales (PDAs), auriculares inalámbricos, y dispositivos similares.

2.3.5 ¿Las LAN Inalámbricas Son Los Riesgos A La Salud?

Los quipos de LAN inalámbricos irradian energía electromagnética. La salud de un ser vivo puede ser afectada por tales ondas adversamente. Antes de comprar o usar cualquier dispositivo que use energía electromagnética, lea el Manual del equipo cuidadosamente y busque la información respecto a la energía que irradia tal dispositivo.

Si un dispositivo Viene con una identificación de la FCC., usted puede obtener la información respecto a la emisión de ondas y frecuencia de uso, en el sitio web de la FCC. Y su dirección electrónica es www.fcc.gov/oet/fccid. En este sitio, sólo debe ingresa el numero de identificación de la FCC. del Dispositivo, que consta de tres claves, la primera clave de licencia que son los tres primeros caracteres, el código de producto de equipo, y el EPC (hasta catorce caracteres de largo) por ejemplo:
Documento de identidad de la FCC.: ABC12345678901234

2.3.6 Riesgos De Seguridad

Las redes inalámbricas normalmente usan el protocolo de privacidad (WEP) para garantizar la confidencialidad de los datos transmitidos. WEP es un protocolo de seguridad, especificado en norma Wi-Fi del IEEE, esta diseñado para suministrar un nivel de seguridad y privacidad comparable con una LAN cableada.

Una LAN alambrica es protegida por medio de mecanismos de seguridad física (por ejemplo el acceso controlado a un edificio) que es eficaz para un Ambiente físico controlado, pero podría ser inútil para las LAN inalámbricas dado que las ondas de radio no son necesariamente contenidas por las paredes . WEP trata de proteger cifrando los datos transmitidos sobre la red inalámbrica. De esta manera incluso si alguien escucha los paquetes de radio, él o ella no lo serán capaces de entender el contenido de los datos Transmitido sobre la LAN inalámbrica.

Sin embargo, un grupo de investigación del la Universidad de Berkeley en California, publicó recientemente un informe en los que explica defectos de seguridad muy importantes en el protocolo WEP que deja a las LAN inalámbricas vulnerables a ataques malintencionados.Pero la alianza de compatibilidad de Ethernet inalámbrica (WECA), una organización constituida por 802.11 y los Fabricantes de equipo, afirmaron que WEP no era la única forma de seguridad.

2.4 Organizaciones Internacionales

La mayoría del hardware y de las tecnologías computacionales se basan en algunos estándares, las redes inalámbricas también. Existen algunas organizaciones que definen y apoyan estándares que permiten que el hardware de diversos fabricantes sea compatible así como la interconexión entre ellos. Conociendo las leyes y los estándares que rigen a las redes inalámbricas nos podemos asegurar que cualquier red que se ponga en ejecución sea ínter operable.

2.4.1 Comisión Federal De Comunicaciones (FCC)

La Comisión Federal de Comunicaciones (FCC) es una agencia estatal de los Estados Unidos, la cual se encarga de la regulación de comunicaciones vía radio, televisión, cable y satélite.

La jurisdicción de la FCC no sólo cubre los 50 estados si no también todas las posesiones de los Estados Unidos por ejemplo Puerto Rico, Guam, y las Islas Vírgenes.

La FCC establece las leyes dentro de las cuales los dispositivos de redes inalámbricas deben funcionar especificando la radiofrecuencia, las tecnologías de transmisión así como del hardware que puede ser utilizado

La dirección del sitio de Internet de la FCC es www.fcc.gov

2.4.2 Instituto De Ingenieros Eléctricos Electrónicos (IEEE)

El instituto de Ingenieros Eléctricos y Electrónicos es el fabricante dominante de los estándares para la mayoría de las cosas relacionadas con la tecnología de información en los Estados Unidos.
El IEEE crea sus estándares dentro de las leyes creadas por la FCC. Es parte de la misión del IEEE desarrollar los estándares para la operación de redes inalámbricas en el marco de las reglas y de las regulaciones de la FCC.

Los Estándares de IEEE para Redes Inalámbricas mas comúnmente usados son:

- 802.11
- 802.11b
- 802.11a
- 802.11g

La dirección del sitio de Internet del IEEE es www.ieee.org

2.4.3 Alianza De Compatibilidad Entre Redes Inalámbricas Ethernet (WECA)

La Alianza De Compatibilidad entre Redes Inalámbricas Ethernet (WECA) promueve y prueba la Interoperabilidad de dispositivos 802.11b y de los dispositivos 802.11a y 802.11g.

La misión de WECA es certificar la interoperabilidad de los productos Wi-Fi™ (IEEE 802.11) y promover Wi-Fi como estándar global del redes LAN inalámbricas a través de todos los segmentos de mercado.

Cuando un producto cumple con los requisitos de la interoperabilidad según lo descrito en las pruebas realizada por WECA , esta concede al producto una certificación de la interoperabilidad, la cual permite al vendedor utilizar la insignia Wi-Fi en la publicidad y el empaquetado del producto certificado. El sello Wi-Fi asegura al usuario final la interoperabilidad con otros dispositivos que también llevan la insignia Wi-Fi (no importando la marca de estos).

La dirección del sitio de Internet de la WECA es www.wirelessethernet.org

2.4.4 Asociación De Redes Inalámbricas De Área Local (WLANA)

La misión de la asociación de redes inalámbricas de área local es educar y difundir el conocimiento al consumidor en relación con al uso y disponibilidad de LANs inalámbricas y así como promover las redes inalámbricas en la industria. La WLANA es un recurso educativo para personas intentan aprender más sobre LANs inalámbricas. WLANA puede también ayudar si usted busca un producto específico o servicio de redes inalámbricas brindando información así como comparación de productos.

La dirección del sitio de Internet de la WLANA es www.wlana.org.

CAPITULO III

SEGURIDAD EN REDES

Desde que ha existido la posibilidad de acceso remoto a las computadoras, la tentación para el acceso no autorizado a los datos y recursos ha sido una realidad dolorosa. Muchas empresas son amenazadas constantemente en sus activos lo que pudiera representar miles o millones de dólares en pérdidas. Las vulnerabilidades en nuestros sistemas de información pueden representar problemas graves, por ello es muy importante comprender los conceptos necesarios para combatirlos y defendernos de posibles ataques a nuestra información.

La seguridad de red tiene dos tipos básicos: seguridad operacional de la red y seguridad de datos de la red. La seguridad operacional de la red se refiere a salvaguardar y asegurar una operación sin defectos de una red de ordenadores. La seguridad operacional de la red se encarga del aseguramiento de la información, la seguridad del control de acceso de personal (controla quién puede tener acceso a la red), definiendo los papeles de autorización (restringe que cosas pueden hacer en la red los usuarios), y la seguridad física del equipo de la red.

La seguridad de datos de red se ocupa de tres áreas principales: confidencialidad, integridad, y disponibilidad. La Confidencialidad significa que solamente las personas que tienen acceso legítimo deben poder utilizar la información y los recursos. La integridad implica que solamente quienes están autorizados pueden modificar la información. La disponibilidad se refiere a que aquellas personas que necesitan la información y los recursos puedan tener acceso cuando lo necesitan.

3.1 Seguridad Operacional De La Red

La seguridad operacional es aquella que se encarga de que una red esté equipada de las medidas más conocidas y apropiadas que garanticen un entorno confiable, esta se asegura de que los datos dentro de la red nunca estén comprometidos y estén libres de la posibilidad de acceso no autorizado de los intrusos o de los hackers.

Para permitir una operación sin problemas, la seguridad operacional incluye las medidas activas para la creación de políticas que definen el acceso físico a los dispositivos de una red. Esta define y restringe el acceso a la red no permitiendo el acceso a un individuo sin prueba de su identidad usando control de acceso o autentificación de la red. El propósito de la seguridad de red es prevenir y detectar el uso no autorizado de los recursos de la red. Las medidas preventivas necesitan ser desarrolladas para poder prevenir que usuarios no autorizados tengan acceso a la red de computadoras. Es necesaria la detección de intentos de infiltración e infiltraciones logradas así como determinar cuales sistemas y datos se han comprometido.

Para asegurar adecuadamente una red, necesitamos tener un plan bien estructurado. Al formular el plan, necesitamos considerar la seguridad física así como la autentificación y el control de acceso a la red, también necesitamos tener en cuenta las políticas de usuarios en cuanto al acceso a los sitios de trabajo, a los servidores, al espacio en disco, y a las impresoras.

A continuación se hablara más a detalle de los tipos de seguridad que debemos tomar en cuenta así como las recomendaciones comunes.

3.1.1 Seguridad Física

La seguridad física de la red se ocupa de asegurar activos y recursos físicos en contra de adversarios. La mayoría de las políticas de seguridad físicas comunes incluyen el robo de equipo y la penetración en el cable físico de la red.

Par proteger el robo de redes cableadas, en la mayoría de los casos es necesario proteger la intrusión de personal no autorizado con guardias de seguridad y cámaras de video. Esto incluye un ambiente seguro donde los ordenadores y las redes están situados en un ambiente libre de peligro.

Los recursos centrales del establecimiento de una red, tales como servidores, routers, y los recursos de la comunicación de la red, se deben proveer de los sistemas de energía condicionados y redundantes tales como usar reguladores de energía y fuente de alimentación continua (UPS) para proteger el equipo en contra de problemas de energía eléctrica.

3.1.2 Puntos Débiles

Los puntos débiles de orden físico son aquellos presentes en los ambientes en los cuales la información se está almacenando o manejando.

Como ejemplos de este tipo de vulnerabilidad se distinguen:

– Instalaciones inadecuadas del espacio de trabajo.
– Ausencia de recursos para el combate a incendios.
– Disposición desorganizada de cables de energía y de red.
– Ausencia de identificación de personas y de equipo, entre otros.

Estos puntos débiles, al ser explotados por amenazas, afectan directamente los principios básicos de la seguridad de la información, principalmente la disponibilidad.

3.1.3 Vulnerabilidades Naturales

Los puntos débiles naturales son aquellos relacionados con las condiciones de la naturaleza que puedan colocar en riesgo la información. Muchas veces, la humedad, el polvo y la contaminación podrán causar daños a los activos. Por ello, los mismos deberán estar protegidos para poder garantizar sus funciones.

La probabilidad de estar expuestos a las amenazas naturales es determinante en la elección y montaje de un ambiente de trabajo. Se deberán tomar en cuenta cuidados especiales con la ubicación del lugar de trabajo, de acuerdo con el tipo de amenaza natural que pueda ocurrir en una determinada región geográfica.

Entre las amenazas naturales más comunes podemos citar:

– Ambientes sin protección contra incendios.
– Locales próximos a ríos propensos a inundaciones.
– Infraestructura incapaz de resistir a las manifestaciones de la naturaleza como terremotos, maremotos, huracanes etc.

3.1.4 Autentificación Y Control De Acceso De La Red

En la mayoría de los casos, el primer punto de entrada a una red está a través de un sitio de trabajo del Usuario. El mecanismo para asegurarse de que un Usuario legítimo esté teniendo acceso a la red es validando la autenticidad de un Usuario y comúnmente se conoce como autentificación de conexión.

La autentificación de conexión es un proceso que identifica la autenticidad de un Usuario basado en las credenciales que él proporciona (por ejemplo, Nombre de Usuario y Contraseña).

Una vez que la conexión es acertada, se concede acceso al Usuario a los recursos de la red (por ejemplo, servidores de archivos y las impresoras). La prevención del acceso no autorizado a una red es de importancia primaria al discutir seguridad del LAN.

La figura 3.1 muestra un ejemplo de una conexión de la red bajo Windows XP.

Figura 3.1 Autentificación De La Red Usando Nombre Y Palabra De Paso Del Usuario.

En la mayoría de las LAN, los sitios de trabajo del Usuario están instalados sistemas operativos (OS) con varios niveles de autentificación. La mayoría de las computadoras permiten que Usuarios múltiples abran una sesión y utilicen los recursos de sistema. Dependiendo del OS, el Usuario puede abrir una sesión localmente (conectado físicamente con la red), o remotamente (por ejemplo, conectado sobre el Internet) Autentificándose sobre la red.

En cualquier caso, el Usuario que desea tener acceso el sitio de trabajo debe estar autorizado para abrir una sesión. La autentificación de Usuarios se realiza vía un servidor central llamado servidor de la conexión. Cada Usuario autorizado a tener acceso a una red debe tener una cuenta en este servidor de conexión.

El administrador de la red crea generalmente estas cuentas. Los privilegios y los niveles de la autorización se conceden a cada Usuario cuando se crea una cuenta de Usuario[4].

En términos del LAN, un “privilegio” se relaciona normalmente con el tipo de acceso que tiene un Usuario a la red (por ejemplo, administración de cuentas del Usuario), mientras que la autorización refiere a un conjunto de permisos que se conceden a un Usuario para utilizar los servicios de red (por ejemplo, de autorización de tener acceso a una base de datos interna de los recursos humanos).

Las conexiones con todos los privilegios, designadas comúnmente de usuario root o de Administrador, se deben limitar a una pequeña cantidad de usuarios autorizados. El acceso a los recursos se debe asociar a través de grupos de usuarios agregados en conexiones lógicas. Por ejemplo, en una configuración de una empresa, los Usuarios de estadísticas deben pertenecer a un grupo que consiste solamente en los empleados que trabajan en el servicio y los recursos de contabilidad como los servidores de las estadísticas se deben restringir a ese grupo.

La información de la autentificación del usuario se salva de diversas maneras, que varía en cada sistema operativo. Sin embargo, el estándar en las compañías son los ambientes de UNIX y Windows 2003 y en estos se conoce como Protocolo de Acceso a Directorio Ligero (LDAP). LDAP es un protocolo basado en TCP/IP usado para tener acceso a la información del Usuario salvada en una base de datos especializada conocida como directorio de LDAP. Este directorio contiene la información necesaria para validar la autenticidad del Usuario del la red.

[4] BSWN-1

3.1.5 Autentificación De Usuarios De Red

El mecanismo de uso general para validar la identidad de un Usuario se llama autentificación de Usuario de Red. La autentificación de Usuario de red se utiliza para asegurarse de que solamente ese personal que ha sido autorizado pueda acceder a la red. Generalmente, para ser Autentificado se le pide al usuario un Nombre de Usuario y una Contraseña, las cueles solo deben de ser conocidas por el. La información de la autentificación se comunica normalmente del sitio de trabajo del Usuario al servidor de una manera segura. En la mayoría de los sistemas, las Contraseñas se guardan en el servidor en un formato cifrado. Dependiendo de las necesidades de seguridad y del sistema operativo, puede haber varios niveles de Contraseñas que son solicitadas por el servidor antes de que se permita a un Usuario tener acceso a un servicio.

Aunque la combinación del Nombre de Usuario y de Contraseña sigue siendo el método más utilizado de autentificación, existen otros medios de autentificación tales como los biométricos (por ejemplo, exploración de la retina o de huella digital). Los mecanismos de autentificación en los cuales se requiere más información que solamente el Nombre de Usuario y Contraseña se llaman autentificación de n-factor, donde n es el número de partes de información adicionales que se requiere para iniciar una sesión. Por ejemplo, si además del Nombre de Usuario y de Contraseña es requerida una exploración retina, esta seria una autentificación de dos-factor.

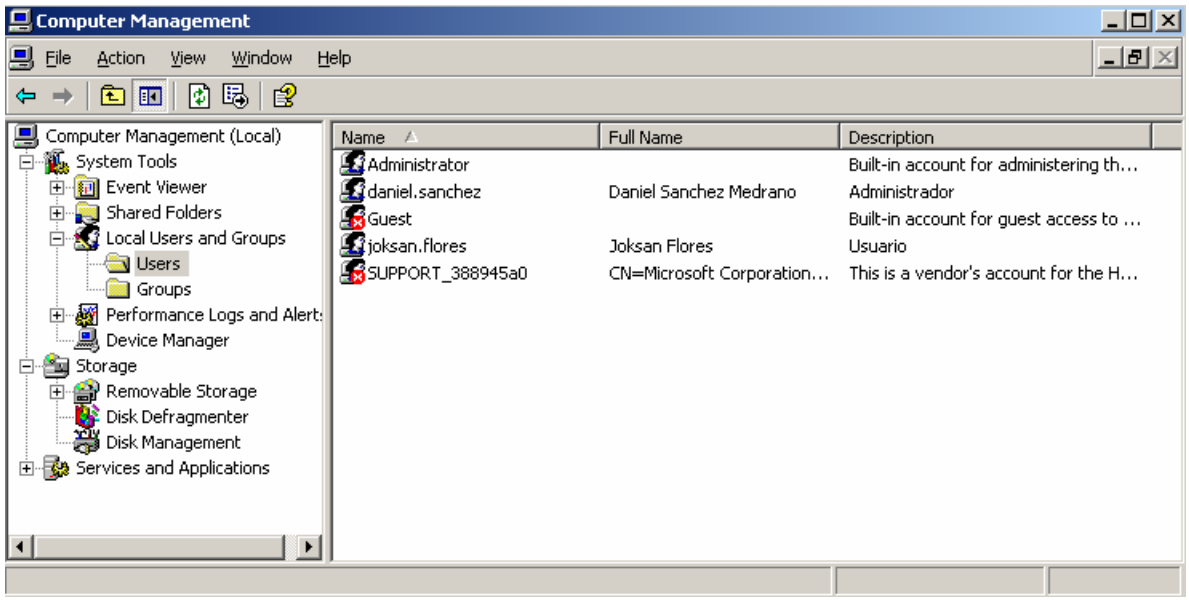
3.1.5.1 Grupos De Usuarios

En la mayoría de las empresas los privilegios usuarios de la red depende directamente de los permisos que tiene el departamento en el cual forman parte, dado que normalmente no se realiza la misma tarea del trabajo, ni una misma operación de la red.

Por ejemplo, una red de una empresa de estadísticas cuenta con 100 empleados, de los cuales tiene 60 contables, 20 personas de soporte administrativo, 10 ejecutivos, 5 coordinadores del recurso, y un departamento de la tecnología de información de 5 personas.

Cada grupo de Usuarios puede necesitar un diverso conjunto de servicios por ejemplo, los contables puede necesitar el acceso al software de las estadísticas y email, los ejecutivos a los datos confidenciales, y el departamento de tecnología de información a la red entera poder manejarla. Manejar y asegurar el acceso a un conjunto dado de servicios a un conjunto de Usuarios es una construcción común en los esquemas de la seguridad conocidos como Grupos de Usuario.
Un Grupo de Usuarios consiste en una colección de unos o más Usuarios con un identificador único conocido como nombre de grupo. Se agrupan los Usuarios en base a su función o papel de trabajo dentro del ambiente de la red, y a ellos se le asignan los permisos apropiado de tener acceso a varios recursos de la red.

Por ejemplo, todos los Usuarios del área de estadísticas pueden pertenecer a un grupo llamado estadística, asimismo todos los Usuarios en el departamento del recurso humanos pueden formar un grupo llamado recursos y los administradores de los sistemas informáticos pueden pertenecer a un grupo llamado administradores, con el permiso de tener acceso a todos los sistemas excepto los servidores que contienen secretos comerciales confidenciales y ésos que contienen la información de recursos humanos.



La Figura 3.2 Muestra Los Usuarios Y El Grupo Al Que Pertenecen Bajo Windows 2003.

En algunos sistemas, los grupos de Usuario pueden contener a otros grupos, dando por resultado una jerarquía, por ejemplo a los contables que traten de los clientes en Europa puedan pertenecer a un grupo conocido como eu−accountants como subgrupo de contables.

La Figura 3.3 Muestra un ejemplo de los grupos de Usuario jerárquicos.

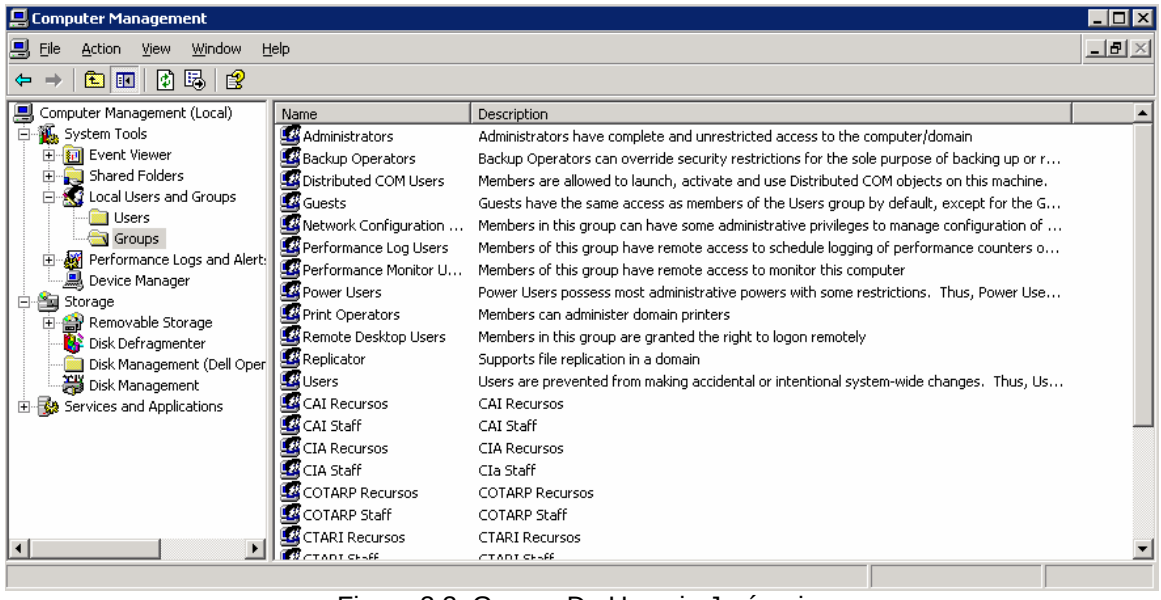


Figura 3.3 Grupos De Usuario Jerárquicos.

Esencialmente, los grupos de Usuario proporcionan un alto nivel de la seguridad de red y mejoran su funcionamiento, permitiendo acceso a los recursos protegidos de la red solamente a los Usuarios en Grupos especificados.

3.1.5.2 Servidores De Autentificación Y Listas De Control De Acceso (Acls)

Los servidores de autentificación son las computadoras que realizan la autentificación de todos los Usuarios que deseen tener acceso a la red. Los servidores de autentificación mantienen una lista de Usuarios, grupos, y Contraseñas, así como los privilegios que tiene cada usuario. Esta lista se conoce como Access Control List (ACL) o lista de control de acceso. Las listas de control de acceso son solamente manejadas por una pequeña cantidad de Usuarios que normalmente son los administradores de la red. Además de tener un servidor de autentificación, cada computadora en una red puede tener su propio mecanismo de autentificación y ACLs si desea permitir que otros Usuarios de la red tengan acceso a su información.

3.1.5.3 Autentificación Remota De Usuarios

Si los Usuarios no se encuentran actualmente en el sitio donde existe la red física de computadoras y estos requieren acceso a la red de sitios externos por ejemplo, sitio del cliente, o en el hogar, entonces son necesarias medidas de seguridad adicionales para permitirle abrir una sesión a la red remotamente.

Los Usuarios locales se encuentran en un ambiente seguro dado que están conectados directamente en la red. Los Usuarios remotos tienen acceso a la red a través de medios poco seguros por ejemplo, líneas telefónicas o el Internet y presentan riesgos más altos de seguridad. Típicamente, los usuarios remotos se autentican usando un nivel de seguridad adicional además de nombre de usuario y contraseña tales como protocolos de red especiales por ejemplo IPsec o una VPN.

3.2 Ataques Comunes Contra La Seguridad Operacional De La Red

Un ataque de red contra seguridad operacional normalmente se refiere las actividades que están dirigidas a interrumpir una operación normal o total de la red, reduciendo su funcionamiento, o destruyendo totalmente la parte física de la red. Los ataques que se originan fuera de la red se llaman ataques externos, mientras que los que se originan dentro de la red se llaman ataques internos.

3.2.1 Ataques Externos De Red

Conectando una red local con una red externa, especialmente Internet, abre un mundo de oportunidades a los Usuario internos que utilicen una conectividad más alta y más rápidamente para el intercambio de información, así como el posible acceso a la red de usuarios no autorizados. Los ataques externos de red a menudo son hechos por posibles fallas de seguridad o ausencia de esta. Cada tipo de ataque intenta capitalizar cierta debilidad que una red sufra.

Algunos de los ataques externos comunes de la red son ataques basados en contraseñas, ataques basados en tráfico de red, ataques basados en aplicaciones y virus, ataques basados en vulnerabilidades de sistema, entre otros.

3.2.2 Ataques Basados En Contraseñas (Password−Based).

Dado que la mayoría de las redes utilizan nombres de personas como Nombre De Usuario para su identificador de cuenta, hay solamente un conjunto limitado de los Nombres De Usuario que un Hacker tiene que intentar cuando desea penetrar una red basada en autentificación usando la combinación del *Nombre De Usuario* y de *Contraseña*. Además de las limitaciones del *Nombre De Usuario*, los Usuario eligen *Contraseñas* fáciles de recordar que incluyen a menudo nombres de sus hijos , nombres de sus mascotas, o su número de Seguridad Social, Tales *Contraseñas* son fáciles deducir y aumentan la vulnerabilidad de la red.

La mayoría las organizaciones utiliza el nombre del Usuario para crear su cuenta de red. Los ataques basados en contraseñas utilizan esta homologación o estándar para tratar de acceder a la red.

Los Hackers utilizan a menudo un ataque de diccionario (dictionary attack) el cual consiste en conocer un nombre de usuario valido y recorrer todos las Contraseñas más posiblemente usados, es decir, las palabras que dependiendo del lenguaje usado se piensa pueden ser las mas elegidas como contraseñas, como por ejemplo nombres, colores, números, ciudades etc.

Otro ataque se conoce como ataque de Fuerza Bruta (brute−force), en el cual un hacker intenta todas las combinaciones posibles de caracteres hasta encontrar una contraseña que permite el acceso. Los ataques de fuerza bruta son muy costosos en tiempo computacional, tardando incluso años. Es por eso importante asegurarse que los Usuarios utilicen Contraseñas difíciles de adivinar, pudiendo utilizar una contraseña que incluya números, letras y caracteres especiales, añadiendo una longitud amplia. Muchas organizaciones requieren a sus empleados cambiar con frecuencia sus Contraseñas para reducir los riesgos asociados a ataques de Fuerza Bruta.

3.2.3 Ataques De Tráfico De Red (Traffic−Based).

Los recorridos de los datos a partir de una computadora a otra en una red o entre redes se realizan mediante paquetes. Estos paquetes son normalmente visibles a todos los ordenadores que tengan acceso a la red. En los ataques de tráfico de red el intruso intenta evitar que usuarios legítimos accedan a información o servicios.

Para ello, el intruso apunta a su computador o a conexión de red, o la red del sitio que usted quiere usar, entonces el atacante "inunda" la red con información, evitando así que usted pueda acceder a su correo electrónico, ver una página web, una cuenta en línea, u otro servicio, incluso a la red. El más común es el ataque de denegación de servicio o DOS (Denial-of-Service) .

Por ejemplo, cuando usted ingresa una dirección web, está haciendo una solicitud a través de Internet para que una computadora le envíe información (una página web). Dicha computadora puede procesar un cierto número de solicitudes a la vez, de manera que si un atacante puede sobrecargar al servidor con solicitudes, no podrá procesar más requerimientos. Ese es un ataque de "denegación de servicios", porque usted ya no puede acceder al sitio.

3.2.4 Intercepción De Paquetes (Packet−Sniffing)

Para conducir un ataque de intercepción de paquetes, un hacker utiliza un programa llamado Sniffer. Un Sniffer de paquetes es un programa que captura o intercepta datos de los paquetes mientras que viajan en la red. Por ejemplo, durante la fase de la autentificación, un hacker puede interceptar los datos transmitidos por un sitio de trabajo. Los datos interceptados en este caso pueden incluir los Nombres de usuario, las contraseñas, y la información propietaria del usuario que viaja sobre la red en texto plano (sin encriptar). Obteniendo estos datos el atacante puede usarlos para acceder a la red con ese nombre de usuario y contraseña robado.

3.2.5 Ataques Vía Aplicación O Virus (Virus−Based)

Un hacker efectúa ataques vía aplicación o virus escribiendo programas de computadora que pueden afectar el funcionamiento de una red o de un ordenador individual. Estos programas se propagan a menudo vía correo electrónico o utilizando las vulnerabilidades del sistema operativo para dañar datos y el equipo.

Los ejemplos de tales virus y programas de aplicación incluyen programas de administración remota tales como Caballos de Troya (Trojan Horse). Usando estas aplicaciones, un hacker puede también utilizar la computadora del Usuario infectado para atacar otras computadoras o redes, inculpando al Usuario por el ataque.

3.2.6 Los Caballos De Troya (Trojan Horse)

Los Caballos de Troya mejor conocidos como Troyanos son una manera común en la que los hackers toman el control de una maquina victima. Los troyanos son pequeños programas que se instalan en el sistema operativo y no realizan ninguna acción destructiva. Estos tipos de programas sirven para obtener información y espiar a los usuarios pudiendo grabar todo lo que escriben así obteniendo Contraseñas y números de cuenta de banco. También pueden permitir a los intrusos fácil acceso a su computadora sin su conocimiento, cambiar sus configuraciones del sistema, o infectar su ordenador con un virus.

Para evitar ser infectado por un troyano se debe de evitar abrir archivos de los cuales no se tenga idea de la procedencia, así como actualizar el antivirus y el sistema operativo

3.2.7 Programas de Administración Remota

Muchos sistemas operativos proporcionan administración remota del equipo. Aunque éstos son muy provechosos para los administradores del sistema, éstos proporcionan a una puerta trasera para que los hackers puedan controlar una red.

Por ejemplo, en los sistemas Windows, los más comunes son el Remote Administrator, Pc Anywhere, VNC, así como el Escritorio remoto de Windows. Estos programas pueden tener vulnerabilidades lo mas recomendable es que se actualicen constantemente para evitar que sean una via de acceso al sistema o la red y de este modo comprometer el sistema.

3.2.8 Intermediarios De Un Ataque

Los intrusos utilizan con frecuencia los ordenadores comprometidos (ésos que se han atacado y están con éxito bajo control de un intruso) como plataformas de lanzamiento para atacar otros sistemas. Un ejemplo de esto es cómo se utilizan las herramientas distribuidas de denegación de servicios (DOS).

Los intrusos instalan un agente (con frecuencia con un programa tipo troyano) y cuando varios agentes se están ejecutando en diversos ordenadores, un solo programa piloto puede mandar a todos para lanzar un ataque del DOS contra otro sistema. Para asegurarse de que una red sea segura de tales ataques, los Usuarios de la red deben ser desalentados de usar los programas que no se obtienen de una fuente segura.

Asimismo, todos los Usuarios deben de señalar cualquier comportamiento extraño de la red a los administradores de esta, y el software antivirus se debe ejecutar en las computadoras con análisis programados automáticamente.

3.2.9 Ataques Basado En Programas De Mensajería

Para que un código malicioso pueda ejecutarse en un ordenador en una red, debe primero llegar del ordenador del atacante. El mecanismo más fácil que está disponible para un hacker envié este archivo es vía sistemas de la mensajería incluyendo el email y los programas de chat.

3.2.10 Virus De Archivos Adjuntos De Correo Electrónico

Los virus y otros tipos de código malicioso se envían a menudo como archivos adjuntos a los mensajes de email. Los Hackers envían emails que contienen virus a los Usuarios una red que deseen atacar. No es basta con que el origen del correo sea de alguien que usted conoce o de algun familiar. Este puede ser un virus. También, el código malicioso se puede distribuir en programas de entretenimiento o juegos. Muchos virus recientes utilizan estas técnicas de ingeniería social para propagarse.

3.2.11 Falsificación De Correo Electrónico (Email Spoofing)

El email spoofing es cuando un mensaje de correo electrónico parece haber sido originado a partir de una fuente cuando fue realmente fue enviado de otro lugar. El email spoofing es comúnmente usado para obtener contraseñas. Por ejemplo un correo presuntamente enviado por el administrador de sistema el cual solicita a los usuarios que le envíen sus contraseñas para reiterar que ese correo esta siendo usado de lo contrario se dará de baja la cuenta.

Para evitar caer en este tipo de ataques se recomienda no enviar contraseñas ni números de cuenta por correo electrónico, la mayoría de los proveedores de servicios así como bancos nunca le pedirán información vía el email.

3.2.12 Programas De Charla En Internet (Chat)

Las aplicaciones de Chat vía Internet, tales como aplicaciones de la mensajería proporcionan un mecanismo para que la información sea transmitida bidireccional mente entre ordenadores en Internet. Los clientes de Chat proveen medios para intercambiar información, Web URLs, y en muchos casos, ficheros de cualquier tipo, los cuales presentan riesgos similares a los de clientes de email.

Por lo tanto se debe de tener cuidado y limitar la capacidad del cliente de la Chat de ejecutar ficheros descargados.

3.2.13 Navegadores Web Y Código Móvil (Java/Javascript/Activex)

Los Navegadores Web han abierto una nueva área para los hackers y los creadores de virus. Un cliente que navega en Internet puede ejecutar accidentalmente un programa que puede tener efectos negativos en la computadora y la red. Ha habido informes de problemas con código móvil (por ejemplo, Java, Javascript, y ActiveX).

Estos lenguajes de programación son capaces de ejecutar código cuando el navegador abre determinada página de Internet. Aunque el código generalmente es útil, puede ser utilizado por intrusos para recopilar la información (tal como que paginas de Internet visita) o para ejecutar código malévolo en su ordenador.

3.2.14 Extensiones De Fichero Ocultas

Muchos sistemas operativos utilizan extensiones del nombre del archivo para distinguir un tipo de fichero de otros. Microsoft Windows utiliza las extensiones de tres letras para identificar un determinado tipo de Archivo. Los sistemas operativos Windows contienen una opción para ocultar las extensiones de archivo de determinados tipos. La opción es activada por defecto, pero un Usuario puede elegir inhabilitar esta opción para hacer que las extensiones de archivo sean visualizadas por Windows.

Muchos virus de correo electrónico se aprovechan esta opción de extensiones de archivos ocultas. El primer ataque principal que se aprovechó de una extensión de fichero oculta fue el gusano I Love You, que tenía un archivo nombrado “LOVE−LETTER−FOR−YOU.TXT.vbs”.

Cuando un Usuario ve este fichero, el piensa que es un archivo de texto y trata de abrir el archivo, pero dado que es un archivo de virus escrito en Visual Basic, comienza a ejecutarse en el ordenador del Usuario y envía un correo electronico a todos los contactos enumerados en la libreta de direcciones de Microsoft Outlook.

3.3 Asegurar Una Red De Ataques Externos

Al conectar un LAN privada con una red externa, ciertos ordenadores vitales se deben colocar en una zona desmilitarizada (DMZ). Un DMZ es esa parte de la red que está conectada directamente con una red externa o Internet. Los ordenadores en la DMZ están en riesgo más alto de ser atacados, así que deben ser conectados con la LAN privada a través de un Firewall.

Los Firewalls se aseguran de que solamente los ordenadores autorizados en la DMZ o la red externa tengan acceso a la LAN privada. Los Routers se aseguran de que solamente el tráfico tratado en la red privada fluya del DMZ al LAN privado. Esto asegura que nadie de exterior pueda tener acceso a los ordenadores dentro del LAN privada y también de que nadie desde adentro pueda realizar conexiones que no se permiten.

3.3.1 Ataques Internos De Red

Los ataques internos de redes se originan dentro de estas, debido a intenciones malévolas o de un error de una persona no autorizada a tener acceso a la red. En cualquier caso, tales ataques deben ser prevenidos correctamente salvaguardando los recursos de la red.

Aunque la mayor parte de los ataques internos de la red son debidos al uso incorrecto o desautorizado de un privilegio, la mayoría de los ataques que se puedan lanzar contra una red del exterior se pueden también lanzar dentro de la red.

Esto significa que aislar una red interna de redes externas no elimina la posibilidad de un ataque de la red.

Los servidores de fichero y espacio de disco compartidos, las aplicaciones de la red incluyendo las impresoras y los sistemas de comunicación externos, los programas de aplicación de la red, y las bases de datos, son a menudo los blancos de los hackers y los adversarios en los ataques que tienen origen dentro de la red.

3.3.2 Seguridad En Los Servidores De Archivos Y De Espacio Compartido

Los Servidores de Archivos almacenan grandes cantidades de datos para uno o varios usuarios en una red. El espacio disponible para los Usuarios en los servidores de archivos se conoce como espacio de disco. El espacio es asegurado dividiendo el disco en particiones llamadas directorios de usuario.

Para asegurar que solo el usuario autorizado tenga acceso a estos directorios, son usadas las listas de acceso las cuales permiten o restringen el acceso a los directorios. También estas se encargan de proporcionar privilegios de lectura, escritura, ejecución y eliminación.

Los ataques comúnmente posibles a los servidores de archivos son originados por virus, los cuales tratan de llenar el disco duro con información basura, o por empleados internos curiosos que desean obtener información de documentos secretos no autorizados.

3.3.3 Seguridad De Programas De Red

En una red basada en autentificación se puede restringir el acceso a las aplicaciones de red a ciertos usuarios. Tales aplicaciones pueden incluir las impresoras, los sistemas de entrada a las salas de cómputo, y los dispositivos de red.

Por ejemplo, solamente los usuarios que manejen la nómina de pago deben poder imprimir en una impresora que imprima cheques.

Típicamente, las impresoras compartidas son asociadas a los servidores de red conocidos como Servidores de Impresión. Estos servidores de impresión utilizan la autentificación de red para asegurarse de que un Usuario pueda utilizar la impresora. Asimismo, se maneja un sistema físico de acceso (por ejemplo, un sistema que usa huellas digitales o tarjetas magnéticas) para permitir acceder a los recursos de red físicamente.

3.3.4 Seguridad De Ejecución De Aplicaciones

La seguridad ejecución de aplicaciones se ocupa de que solamente el personal señalado tenga acceso a un programa en específico. Por ejemplo, solamente los empleados que trabajan haciendo la nómina de pago en una compañía deben tener acceso al programa que genere o maneje la información de la nómina.

Una aplicación puede trabajar en conjunto con la seguridad del sistema operativo, o puede confiar en una base de datos (donde se almacenan los datos de sesión) para autentificar la seguridad.

Los programas que se ejecutan en un servidor están diseñados especialmente para funcionar en modo autenticado, porque se ejecutan en un servidor central. Los Usuarios de software en red deben ser concientes de evitar compartir contraseñas con otros individuos. Además, el acceso a las aplicaciones en red se debe conceder a un número mínimo del personal.

3.3.5 Seguridad De Bases De Datos

Las bases de datos proporcionan una gran cantidad de datos a programas de aplicación. Estas bases de datos podrían contener la información sensible sobre clientes o expedientes de recursos humanos que se deben mantener privados.

La mayoría de las bases de datos cuentan con sus propios esquemas de la autentificación de Usuario y Contraseña. Dado que las bases de datos son normalmente programas de aplicación y los datos se salvan en el disco, se pueden aplicar medidas de seguridad orientadas a conexión de red y a nivel de aplicación a las bases de datos.

3.4 Seguridad De Conexión Y Transmisión De Datos

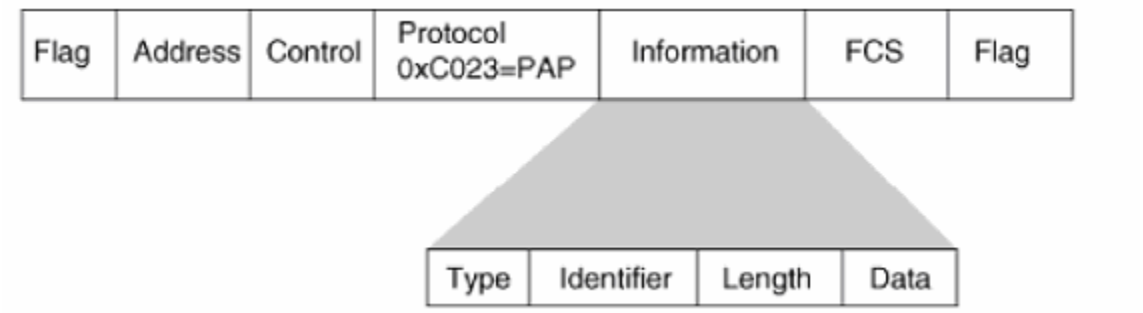
3.4.1Autentificación Sobre Un Medio Inseguro

Un medio de comunicación de red se considera inseguro si los Usuarios con quienes se comparte el medio no pueden ser autentificados. La autentificación implica el presentar las credenciales (por ejemplo, nombre de usuario y contraseña) para verificar su identidad. Si estas credenciales se transmiten sobre un medio inseguro sin codificar, el resultado es equivalente a decirles a todos los usuarios el nombre de usuario y contraseña. Para confiar en la seguridad de un mecanismo de autentificación, se deben usar protocolos de autentificación para asegurar que el intercambio de datos a la hora de autentificarse sea seguro.

Dependiendo del protocolo de la autentificación usado, las credenciales se transmiten normalmente en forma cifrada. Los protocolos de uso general de autentificación son: PAP/CHAP protocolo extensible de la autentificación (EAP), y Kerberos entre otros.

3.4.2 El Protocolo De Autentificación De Contraseña (PAP)

El protocolo PAP (Password Authentication Protocol) provee una manera simple de establecer la identidad de un usuario utilizando 2 pasos. Esto es realizado solo al iniciar el enlace de establecimiento. En la figura 3.4 se muestra el Frame de PAP.



Type Code: 1) Requerimiento De Autentificación
2) Ack De Autentificación
3) Nak De Autentificación

Identifier: Este Octeto Debe Coincidir En Los Requerimientos Y Respuestas.

Length: 2 Octetos Los Cuales Indican La Longitud Del Paquete PAP Incluyendo Los Campos De Código, Identificador, Longitud Y Campo De Datos.

Data: 0 O Mas Octetos.

Figura 3.4 Frame de PAP.

Después de que la fase de establecimiento esta completa, un paquete de requerimiento de autentificación es enviado para iniciar la autentificación PAP. Este paquete contiene el nombre de usuario y contraseña como se muestra en la figura 3.5.

Figura 3.5 Requerimiento De Autentificación PAP.

Este paquete es enviado separadamente hasta que un paquete de respuesta de validación es recibido o un contador opcional expire. Si el autentificador recibe el identificador de usuario y su contraseña (Peer-ID/Password) y estos son reconocidos y aceptados, entonces responde con un autentificado de aceptación (Authenticate-Ack). Si el identificador de usuario y contraseña no es reconocido o aceptado, el autentificador debe responder con un autentificado de no aceptación (Authenticate-Nak).

La Figura 3.6 muestra la secuencia de negociación de PPP en el router “R1mex” el cual esta tratándose de autentificar para obtener acceso al servidor NAS (Network Access Server) el cual es el autentificador.

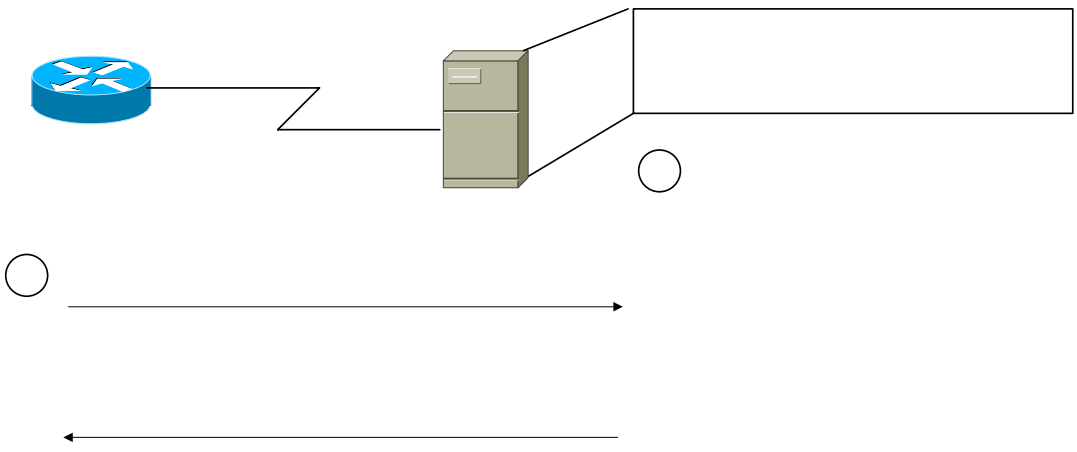
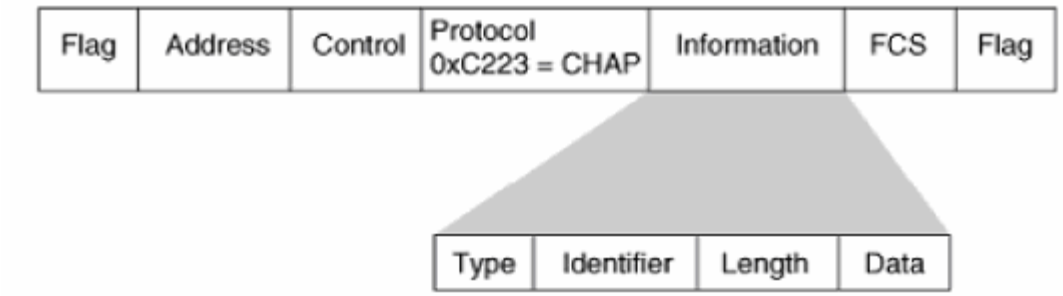


Figura 3.6 Autentificación PPP PAP.

El protocolo PAP no es un método robusto de autentificación. PAP solo autentifica el usuario y la contraseña que son enviados en el medio sin codificar. No hay protección para ataques basados en contraseñas. El usuario es el encargado de la frecuencia de intentos y el tiempo de estos. PAP asume que el medio es seguro, no es recomendable su uso en redes inalámbricas.

3.4.3 El Protocolo CHAP

El Protocolo CHAP (Challenge Handshake Authentication Protocol) es usado periódicamente para confirmar la identidad de un usuario o un dispositivo usando una comunicación de tres pasos. CHAP ejecuta un enlace de datos inicial y puede se ejecutado en cualquier momento una vez que el enlace es establecido. Los tipos de Frames de CHAP son mostrados a continuación en la figura 3.7.



Type:
1. Reto
2. Respuesta
3. Éxito
4. Falla

Identifier: Este Octeto Debe Coincidir En Los Requerimientos Y Respuestas.

Length: 2 Octetos Los Cuales Indican La Longitud Del Paquete CHAP Incluyendo Los Campos De Código, Identificador, Longitud Y Campo De Datos.

Data: 0 O Mas Octetos.

Figura 3.7 Frame de CHAP.

La Figura 3.8 muestra un escenario en el que el router “R1mex” trata de autentificarse en el servidor NAS.

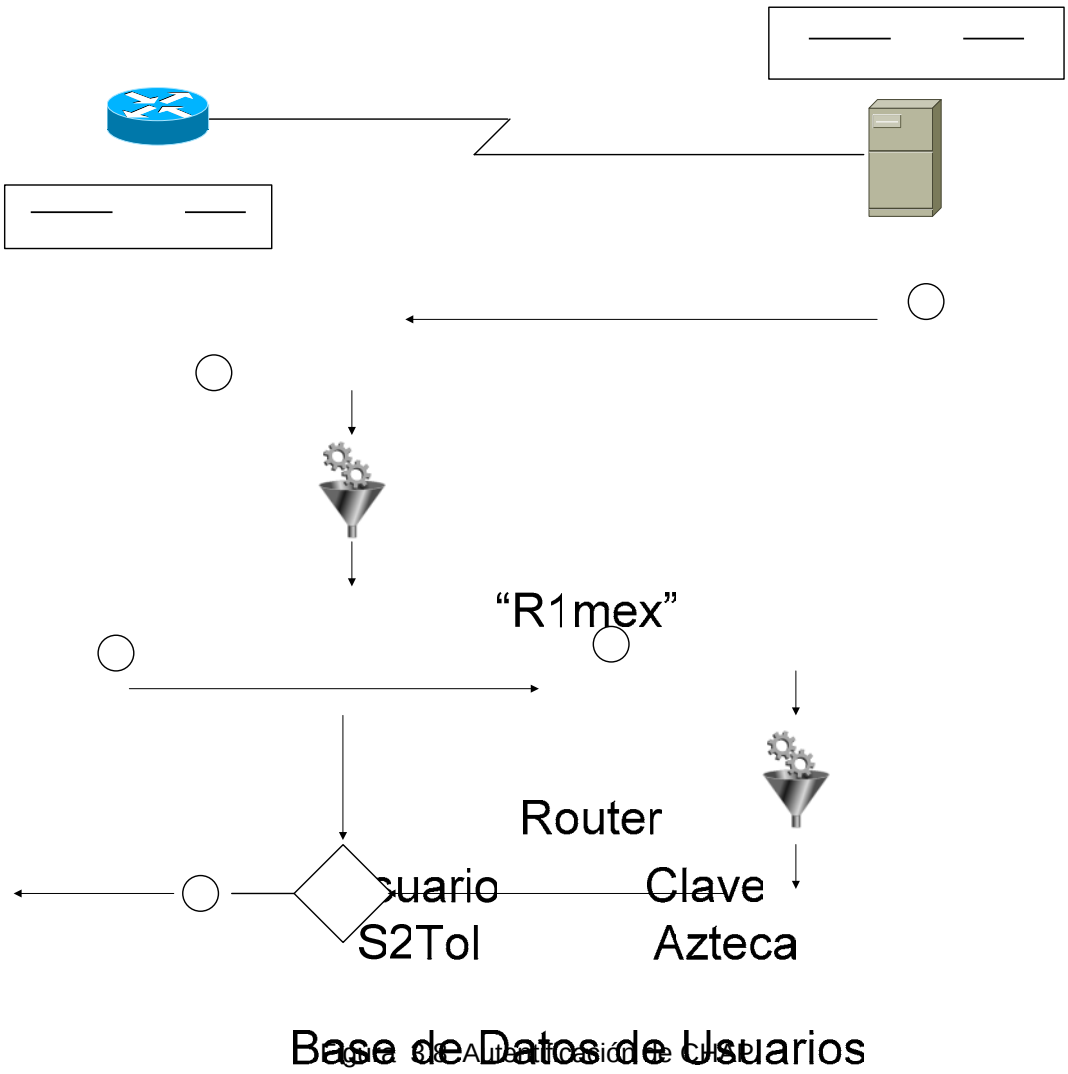


Figura 3.8 Autenticación de CHAP

La clave nunca es enviada sobre el enlace. En la figura 3.8 la palabra “Azteca” es la clave. Los pasos siguientes describen el proceso de autentificación de CHAP:

Paso 1 Una ves que la fase de establecimiento es completada el autentificador envía un mensaje de reto al cliente. El reto (challenge) consiste en un identificador (ID), un número aleatorio y el nombre del dispositivo local o el nombre de usuario en el dispositivo remoto.

Paso 2 El cliente que recibe el reto calcula el valor hash del numero aleatorio, la clave en este caso Azteca es también resultado de la función de hash.

Paso 3 El cliente envía la respuesta de reto, la cual consiste en lo siguiente:
- Una versión codificada del identificador (ID).
- La clave secreta (en este caso la palabra “0A483F6D” la cual es el resultado del proceso de hash).
- El numero aleatorio.
-También incluye el nombre del dispositivo remoto asi como el nombre de usuario de este.

Paso 4 Cuando el autentificador recibe la respuesta de reto, este verifica la clave utilizando el nombre de dispositivo, que también se envió calculando el valor hash. El autentificador compara la respuesta con el valor que el mismo calculo del proceso de hash.

Paso 5 Si el valor concuerda, el autentificador acepta la autentificación y envía un mensaje de éxito y el protocolo de control de enlace LCP establece la comunicación.

Como se puede ver en la figura la clave jamás es transmitida sobre el medio solo la respuesta al proceso de hash. La Clave o Password debe ser idéntica en ambos lados tanto en el dispositivo local como en el remoto. Este password debe ser configurado y generado de manera segura en ambos dispositivos.

Dado que esta clave nunca es transmitida en el medio se previene el robo de identidad por parte de otros dispositivos. Sin la respuesta correcta, el dispositivo remoto no se podrá conectar al dispositivo local.

El protocolo CHAP provee protección contra el uso de ataques tipo intercepción de paquetes (Packet-Sniffing) a través del uso de cambio incremental del identificador. El uso frecuente de retos (challenges) es utilizado para limitar el tiempo de exposición de cualquier ataque. El dispositivo autentificador es el que controla la frecuencia y el tiempo de los retos.

3.4.4 El Protocolo EAP

El protocolo extensible de autentificación (EAP) es en general un protocolo diseñado para trabajar con PPP, este soporta múltiples métodos de autentificación. EAP no selecciona un mecanismo de autentificación en específico en la fase de enlace, sin embargo esto se pospone hasta la fase de autentificación en la cual el autentificador requiere más información antes de determinar el mecanismo de autentificación. Este arreglo permite el uso de otro servidor el cual actúa implementando los mecanismos de autentificación.

En la Figura 3.9 el router (el cliente) esta tratando de autentificarse con el servidor NAS (el autentificador). La secuencia de pasos es la siguiente:

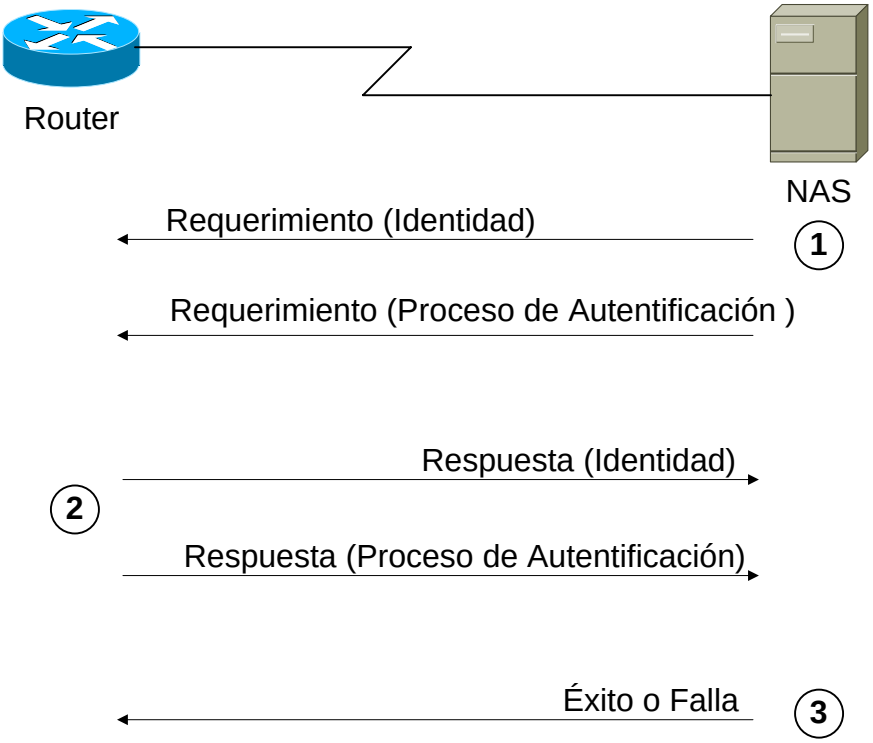


Figura 3.9 Autentificación EAP.

Paso 1 Cuando la fase de establecimiento de enlace esta completa, el autentificador envía uno o más requerimientos de autentificación al cliente. El requerimiento tienen un valor en el campo de tipo que indica que es un requerimiento: Los ejemplos de estos tipos de requerimientos incluyen identificadores MD5 , S/Key, tarjeta de token genérica entre otros. El tipo de requerimiento MD5 es el más parecido al del protocolo de autentificación CHAP.

Paso 2 El usuario envía un paquete de respuesta a cada requerimiento. Como cada paquete de requerimiento, la respuesta contiene un valor en el campo de tipo que corresponde.

Paso 3 El autentificador termina la fase de autentificación con un envió de paquete completo o con una falla.
El protocolo EAP agrega más flexibilidad a la autenticación PPP y provee la capacidad de uso de nuevas tecnologías tales como uso de certificados y firmas digitales cuando estos estén disponibles.

3.4.5 Kerberos

Kerberos es un protocolo de autentificación libre desarrollado e inventado por el Instituto Tecnológico de Massachusetts (MIT) como solución a los problemas de seguridad en redes. El Protocolo kerberos utiliza el algoritmo DES para encriptar la autenticación.

El uso principal de Kerberos es asegurarse de que los usuarios y los servicios de red sean realmente quien dicen ser. Para cumplir con esta meta Kerberos otorga tickets a los usuarios. Estos tickets tienen un tiempo de vida y son almacenados en el cache de identificación de los usuarios y puede ser usado posterior mente por el mecanismo estándar de autentificación, proporcionando el nombre de usuario y la contraseña. El protocolo de kerberos utiliza un servidor de autentificación comúnmente llamado KDC (Key Distrubution Center) centro de distribución de llaves.

3.4.5.1 Requerimiento De Autentificación Y Respuesta En Kerberos

Inicialmente el cliente de kerberos conoce la llave de encriptación la cual solamente es conocida por el cliente y el KDC. También de manera similar cada aplicación del servidor comparte una llave de encriptación con el KDC.

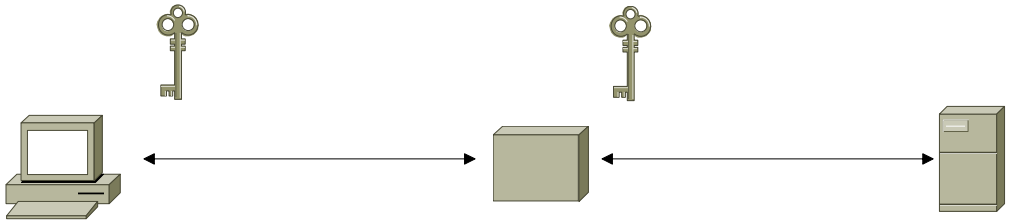


Figura 3..10 Llaves De Encriptación en Kerberos.

Cuando el cliente quiere crear una conexión con una aplicación en particular en el servidor, el cliente utiliza un requerimiento de autentificación para primero obtener un ticket y una llave de sesión del KDC.

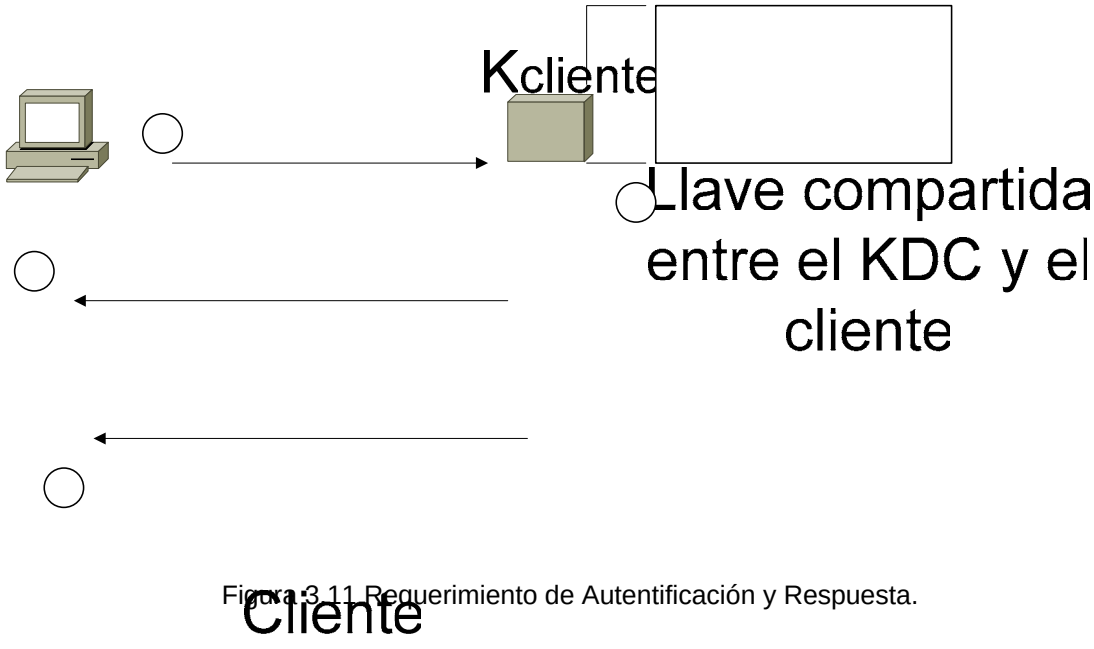


Figura 3.11 Requerimiento de Autentificación y Respuesta.

Paso 1 El cliente envía un requerimiento de autentificación al KDC. Este requerimiento contiene la siguiente información:

- Su supuesta identidad.
- El nombre del servidor de aplicaciones.
- El tiempo de expiración del ticket.
- Un número aleatorio que será usado para comparar la respuesta de autentificación con el requerimiento.

Paso 2 El KDC verifica los permisos del cliente y crea una respuesta de autentificación.

Paso 3 El KDC envía la respuesta al cliente. La respuesta de autentificación contiene la siguiente información.

- La llave de sesión, Ksesión.
- El tiempo asignado de expiración.
- El numero aleatorio del requerimiento.
- El nombre del servidor de aplicaciones.
- Información adicional del ticket.

Toda esta información es codificada con la llave del usuario (K_{client}), la cual fue registrada con el servidor de autentificación. El KCD también envía el ticket de kerberos que contiene la llave aleatoria de sesión ($K_{sesión}$) que será usada para autentificar el cliente con el servidor de aplicaciones, en este se envía el nombre del cliente y el tiempo de expiración en el cual esa llave es valida. El Ticket de kerberos es codificado usando K_{server}.

Paso 4 Cuando el cliente recibe a respuesta de autentificación, tiene que introducir la llave. Esta llave K_{client} es usada para decodificar la llave de sesión $K_{sesión}$.
Ahora el cliente esta listo para comunicarse con el servidor de aplicaciones.

3.4.5.2 Requerimiento De Aplicación Y Respuesta En Kerberos

El requerimiento de Aplicación y respuesta es intercambiando del cliente al servidor de aplicaciones el cual conoce la llave del ticket de Kerberos. El intercambio es mostrado en la Figura 3.12.

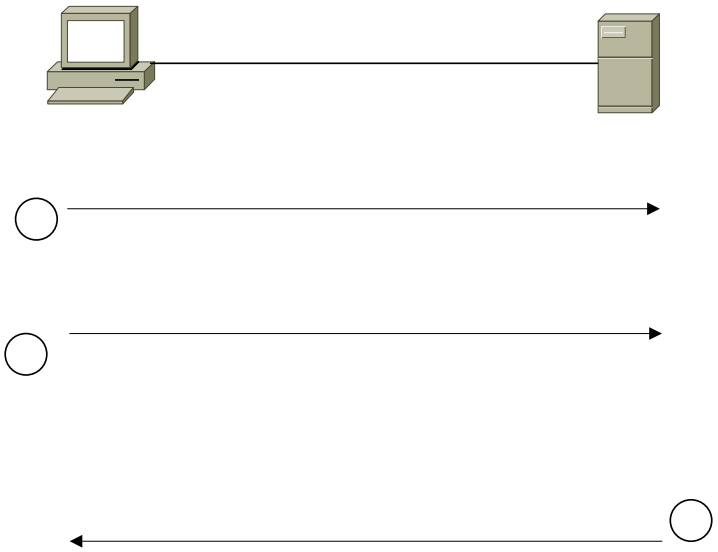


Figura 3.12 Llaves De Encriptación En Kerberos.

Paso 1 El cliente envía 2 cosas al servidor de aplicaciones como parte del requerimiento de aplicación:

- El Ticket de Kerberos
- Un Autentificador el cual incluye
    - La Hora Actual
    - La secuencia de chequeo
    - Una llave de codificación opcional.

Todos estos elementos son codificados con la llave de sesión Ksesión la cual acompaña al ticket.

Paso 2 después de recibir el requerimiento de aplicación el servidor de aplicaciones decodifica el ticket con Kserver, obtiene la llave de sesión y la usas para decodificar el autentificador.

Si la misma llave ha sido usada para codificar el autenficador y decodificarlo el numero de chequeo debe coincidir y el verificador puede asumir que el auntetificador fue generado por el cliente que el ticket envio.

Por si mismo esto no es suficiente para autentificar dado que cualquier atacante puede interceptar el autentificador y enviarlo después al usuario. Por esta razón el verificador también checa la marca de tiempo (timestamp). Si la timestamp no ha sido usada en otros requerimientos el verificador acepta el requerimiento como autentico.

En este instante el servidor ha verificado la identidad del cliente. Para algunas aplicaciones el cliente quiere estar seguro de la identidad del Servidor. Si esto es requerido un tercer paso es necesario.

Paso 3 El servidor de aplicaciones genera una respuesta extrayendo el tiempo del cliente del autentificador y lo reenvía al cliente con otra información, todo usando la llave de sesión Ksesión.

3.4.6 Conexión Por Medio De Encriptadores A Nivel Hardware

Los encriptadores de conexión funcionan como traductores. Cada extremo que necesita cifrar los datos se asocia con un dispositivo fisico de encriptación. Todos los datos que salen de la estación de trabajo se cifran usando un clave criptográfica que esta preestablecida (por un media seguro por ejemplo, via telefónica o personalmente) entre las dos entidades que establecen la transmisión cifrada.

Los dispositivos de encriptación utilizan normalmente un algoritmo simétrico para cifrar los datos antes de transmitirlos sobre la red. El dispositivo que recibe los datos utiliza la clave previamente compartida para desencriptar los datos y los envía a la estación de trabajo. El estándar equivalente a este procedimiento en redes inalámbricas es el protocolo WEP que utiliza la norma IEEE 802.11 para mantener la privacidad.

3.4.7 Redes Privadas Virtuales (VPNs)

Hoy, las redes privadas virtuales (VPNs) son el medio mas utilizado para asegurar la confidencialidad en transmisiones sobre redes. Las VPNs permiten a una entidad (que puede ser un sitio de trabajo, una laptop o un router) establecer una conexión segura con una red alejada usando TCP/IP sobre un medio inseguro.

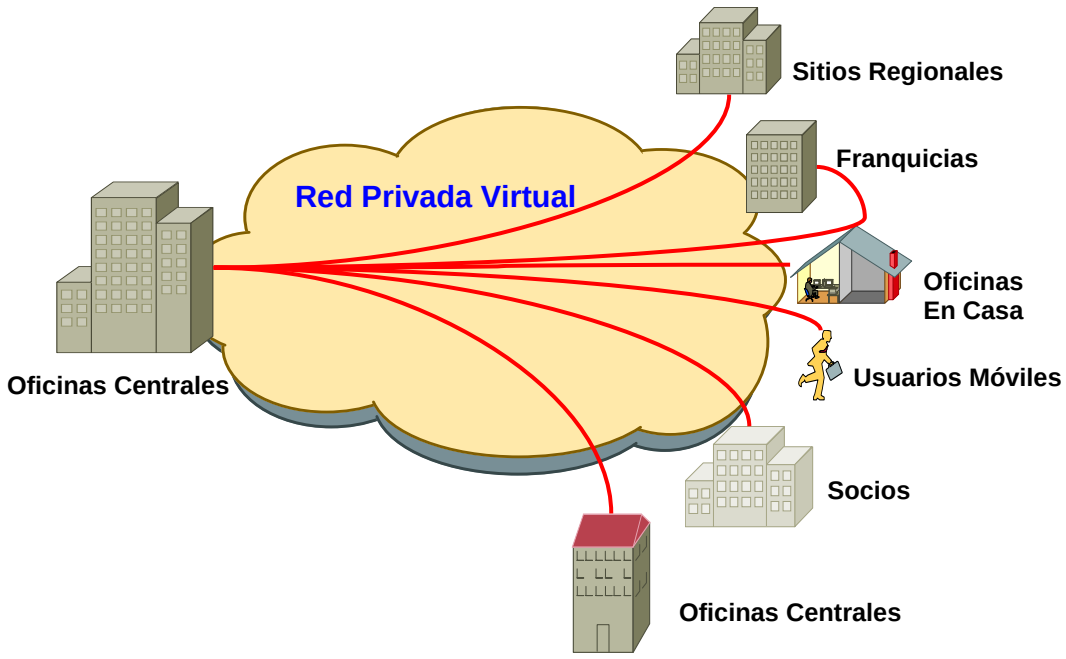


Figura 3.13 Red VPN.

Las VPNs utilizan tecnología de túnel (tunneling) para la transmisión de datos mediante un proceso de encapsulación o encriptación. Una de las principales ventajas de una VPN es la seguridad, los paquetes viajan a través de infraestructuras publicas (Internet) en forma encriptada y a través del túnel de manera que sea prácticamente ilegible para quien intercepte estos paquetes.

Esta tecnología es muy útil para establecer redes que se extienden sobre áreas geográficas extensas, por ejemplo diferentes ciudades y a veces hasta piases y continentes. Las VPNs no sólo se utilizan para permitir a sitios de trabajo alejados conectarse con una LAN sobre un medio inseguro, también se pueden utilizar para interconectar dos redes separadas para formar una sola red privada virtual.

3.4.7.1 Beneficios De Las Redes Privadas Virtuales

Las VPNs son una alternativa a la infraestructura de una red privada convencional en la cual se renta un enlace dedicado Punto a Punto, las VPNs utilizan la red publica eliminando los costos de la renta de infraestructura utilizando la red publica como medio de transmisión. Las VPNs Utilizan las tecnologías de transmisión disponibles hoy en día, así como la calidad de servicios para asegurar le confiabilidad del transporte de datos. Las VPNs aparte de Seguridad ofrecen bajo costo en su implementación así como también la facilidad para conectarse a las redes corporativas trasfiriendo datos de forma segura.

3.4.7.2 Configuración Básica De Una VPN

Los componentes que se requieren implementar en una VPN dependen de la complejidad de la misma así como el uso que se le va a dar.

Una VPN básica consiste normalmente en un sitio de trabajo con un cliente de VPN instalado, de una red TCP/IP, de un Gateway VPN (puede consistir en software o de un dispositivo físico) y una conexión de red (la cual puede ser una conexión vía telefónica, Internet, o línea privada) que conecte al cliente VPN con el Gateway VPN.

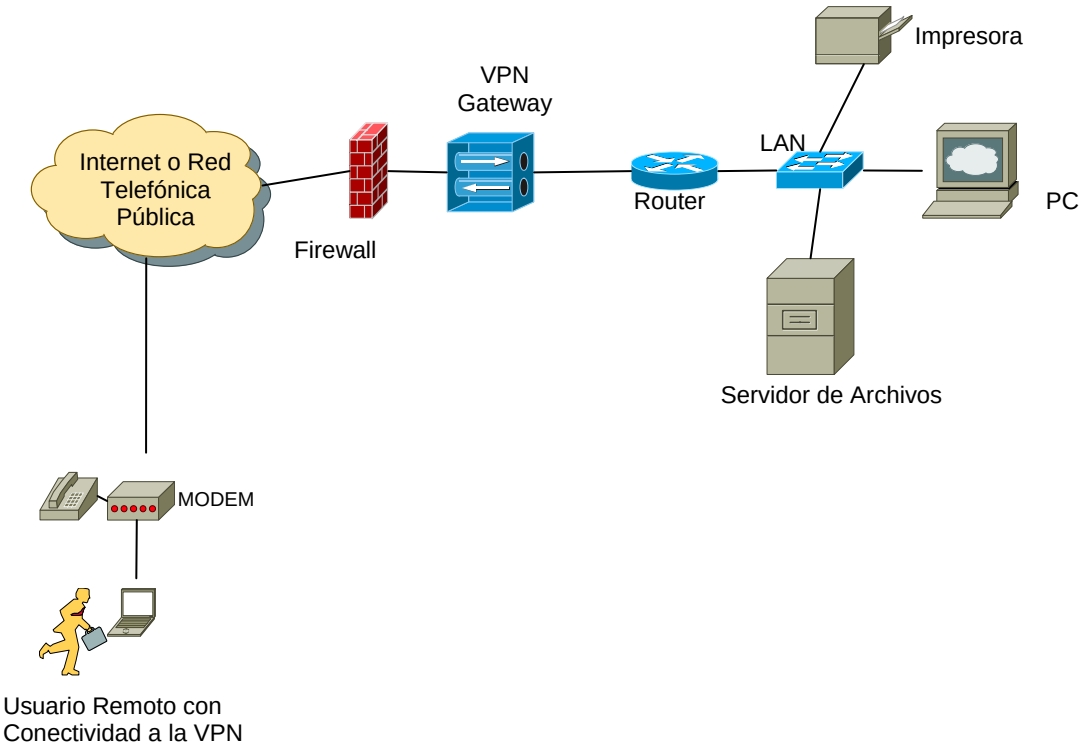


Figura 3.14 Conectividad de VPN sobre el Internet.

El software del cliente VPN normalmente contiene módulos criptográficos y el software de red necesario para establecer una sesión de VPN con un Gateway VPN. Un Gateway VPN contiene los módulos y software de red criptográficos, pero también contiene la base de datos de la autentificación que el Gateway VPN utiliza para autenticar a los clientes. Los Gateways VPN están conectados con la red que el Usuario remoto desea acceder al autentificarse. Los Gateways VPN se protegen casi siempre con un cortafuego para evitar ataques tipo DOS.

3.4.7.3 Operación Básica De VPN

La configuración mas comúnmente usada de una VPN es donde una red corporativa se equipa de un Gateway VPN que esté conectado con Internet y la red corporativa, Un usuario móvil instalo un software de cliente VPN y se conecta con Internet vía una conexión telefónica.

Al tratar de establecer la conexión el cliente VPN utiliza los datos que proporciona el Usuario (comúnmente nombre de usuario y contraseña), para Autenticarlo con el Gateway VPN. Una ves que se comprobaron los datos y son validos se acierta en la conexión, el Gateway VPN intercambia una serie de algoritmos y claves criptográficos de cifrado con el software cliente VPN de una manera segura.El Gateway VPN asigna una dirección IP al cliente VPN. El cliente VPN utiliza esta IP para identificarse al comunicarse con la red remota. En este momento inicia una sesión cifrada entre el cliente y el servidor. El cliente en este momento puede tener acceso al recurso de la red detrás del Gateway VPN mientras que el Gateway VPN permite que el cliente VPN reciba cualquier transmisión desde la red corporativa asegurada.

3.4.7.4 Protocolos VPN

Los tipos de las VPN se basan principalmente en dos protocolos importantes: Protocolo de Túnel Punto a Punto (PPTP) y Protocolo de Internet Seguro (IPSec).

3.4.7.5 Protocolo De Túnel Punto A Punto (PPTP)

PPTP es básicamente una extensión del PPP y permite que una red sea encaminada sobre otra red para conectar con un espacio privado de direcciones IP en un ambiente de VPN.

Por ejemplo, una organización determinada puede utilizar un conjunto de direcciones IP privadas de 10.168.0.1 a 10.168.0.254 en sus oficinas principales pero puede requerir que sus empleados remotos se puedan conectar con ella a través del Internet usando las direcciones IP 192.168.0.1 a 192.168.0.254.

En tal caso el empleado primero se conectaría con un ISP local y sería afectado con una dirección IP para esa sesión. Este dirección IP por supuesto estaría en el rango de los direccionamiento mantenidos por ése ISP, para comunicarse con éxito con el resto de los ordenadores en su oficina, las necesidades de este Usuario de una dirección IP sera asignada en el rango de direccionamientos establecido por la oficina central. Usando una conexión PPTP, este Usuario establecerá una conexión con los ordenadores en su oficina. PPTP no utiliza cifrado, pero un protocolo separado de cifrado se puede utilizar con PPTP.

3.4.7.6 Seguridad De Protocolo de Internet (IPSec)

El protocolo (IPSec) es un estándar del Internet Engineering Task Force (IETF), y él se documenta en el Request For Comments (RFC) rfc2401. Este protocolo es de una forma similar usado a PPTP. IPSec es un protocolo mucho más robusto y tiene mayor flexibilidad y características que PPTP. Los niveles de la seguridad en IPSec son muy altos, y permite una variedad de mecanismos criptográficos y de tamaño de claves que varían. Al igual que PPTP, antes de establecer una conexión entre los ordenadores se debe previamente intercambiar las claves de la seguridad y las palabras secretas entre el cliente y los servidores. IPSec es el protocolo más extensamente utilizado en VPNs.

CAPITULO IV

Asegurando Una Red Inalámbrica

Debido a la popularidad y facilidad de empleo que las redes inalámbricas proporcionan, las empresas y los usuarios domésticos están implementando rápidamente estas redes, también debido a que en muchos lugares públicos se están empleando tales como parques, centros comerciales, supermercados, cafeterías, restoranes, aeropuertos etc. Desafortunadamente la mayoría de estas implementaciones no cumplen con las normas básicas de seguridad que se relacionan con las tecnologías actualmente disponibles de redes inalámbricas.

El punto critico de la seguridad en las redes inalámbricas, basadas en radio frecuencia (por ejemplo, redes 802.11) es que estas irradian intencionalmente datos sobre un área que pueda exceder los límites físicos de las instalaciones de los usuarios. Por ejemplo, las ondas de radio 802.11b en 2.4 Gigahertz traspasan fácilmente las paredes de un edificio y pueden ser captadas en el estacionamiento de este. Alguien ajeno al personal autorizado puede extraer información sensible de una compañía usando la red inalámbrica a una distancia considerable o desde un automóvil sin ser notado por el personal de seguridad de la red.

Estas vulnerabilidades han convertido a las redes inalámbricas en uno de los blancos principales de los Hackers. Los problemas de seguridad aumentan cuando estas redes están conectadas a Internet. En este caso, los Hackers no solo están interesados en el acceso a LAN inalámbrica si no que también están interesados en tener acceso a Internet para contar con una conexión con gran ancho de banda.

Es por eso importante comprender los riesgos y vulnerabilidades antes de implementar una conexión inalámbrica.

4.1 Requisitos De Una Red Inalámbrica Segura

La seguridad de una red inalámbrica es establecida en base a las características físicas de esta, así como por los métodos usados para transmitir los datos, los protocolos que se utilizan para controlar la seguridad, y las políticas de seguridad que utiliza la red.

Las redes inalámbricas se consideran altamente inseguras por que el medio de transmisión de datos no esta limitado físicamente. Al ser transmitidos los datos via radiofrecuencia, estas redes permiten a los usuarios contar con un amplio margen de movimiento en todas direcciones. Lo cual significa que los atacantes no requieren una conexión física a la red. En lugar de esto necesitan estar presentes en el rango físico donde las señales de radio pueden ser interceptadas. Por ejemplo si una red tiene una señal de alcance de 300 metros, los Hackers dentro de un radio de 300 metros pueden interceptar la señal y producir un ataque contra la red[5].

4.1.2 Requisitos Operacionales De Una Red Inalámbrica Segura

La seguridad operacional de las redes inalámbricas se ocupa de proporcionar una operación segura y sin defectos. La seguridad operacional se debe poner en ejecución para evitar cualquier amenaza que pueda afectar la operación normal de la red inalámbrica. La mayoría de estas amenazas son posibles debido a la implementación de una red inalámbrica mal configurada, interferencia en la radiofrecuencia, errores en protocolos usados para transmitir datos o una autentificación nula de la red.

[5] BSWN-1

4.1.2.1 Seguridad En Puntos De Acceso (Access Point)

La mayoría de las redes inalámbricas funciona en modo de la infraestructura en la cual los Access Point coordinan la comunicación entre los usuarios actuando como un hub transmitiendo los datos de los usuarios.

La función de los Access Points es de encaminar todo el tráfico de los usuarios, lo cual lo convierte en una pieza fundamental en la red. Por ejemplo, si un AP esta saturado o ha sido vulnerado, esto afecta el funcionamiento de la red entera. Además de que la mayoría de los Access Point pueden ser administrados y configurados vía Internet. Esta característica aunque es extremadamente útil, permite que gente no autorizada, al romper la seguridad del Access Point asuma el control total de la red inalámbrica.

El número y los tipos de ataques contra los Access Points han crecido constantemente y continuaran debido a la popularidad de las redes inalámbricas. Estos ataques son fáciles ejecutar y difíciles de detectar en la red vía medios tradicionales. El ataque más común a un Access Point es conducido por un adaptador de red inalámbrica el cual envía mensajes constantes a un AP, Saturando al Access Point e impidiendo que este conteste los mensajes enviados por otros adaptadores de red. Además de ataque de inundación, hay otro tipo de ataques, los ataques de administración del AP en los cuales un AP es controlado por un adversario el cual controla todo el tráfico de la red.

Es importante utilizar APs que incluye medidas de seguridad contra ataques conocidos. Por ejemplo una red inalámbrica segura debe contar con Access Points que cuenten con mecanismos de autentificación integrados. Los APs más complejos incluyen protección contra ataques DOS, además de contar con un Router y un Firewall integrados para prevenir trafico no autorizado en las redes inalámbricas.

4.1.2.2 Método De Radiofrecuencia (RF)

Los datos en un LAN inalámbrica viajan sobre las ondas de aire usando radiofrecuencias como portadoras. Esto significa que el dispositivo transmisor sobrepone los datos en una radiofrecuencia predefinida y luego los trasmite en el aire. El dispositivo receptor separa los datos de la onda portadora y los convierte en una señal digital la cual se interpreta. La seguridad de los datos transmitidos sobre el aire se puede afectar de muchas maneras, algunas de las cuales incluyen: el bailoteo de frecuencia debida a un a interferencia la cual hace inoperable a una red inalámbrica.

Una red inalámbrica comúnmente tienen un rango de 100 metros por Access Point y en la mayoría de los casos puede atravesar las paredes por eso es importante ubicar el Access Point en un lugar estratégico para evitar que la seña pueda ser interceptada. Es muy importante considerar en el método usado para transmitir los datos sobre ondas de aire para poder asegurar una red inalámbrica. Existen muchos métodos de transmisión de datos usados en redes inalámbricas. Los más comunes DSSS y FHSS. FHSS se considera más seguro y resistente a los ataques comparados a DSSS. En FHSS, el canal en el cual se transmiten los datos cambia frecuentemente, mientras que en DSSS los datos se transmiten en un canal fijo. Al elegir una tecnología inalámbrica, es importante elegir una tecnología que proporcione los mejores métodos de seguridad de RF.

4.1.2.3 Autentificación En La Capa De Enlace

Muchas redes inalámbricas autentifican a los usuarios basados en la capa de enlace, en la cual un adaptador inalámbrico se comunica con un Access Point u otro dispositivo y se identifica usando su dirección MAC (Media Access Control).

Las direcciones MAC son de longitud de 48 bits, expresado como 12 dígitos hexadecimales. Estos seis primeros dígitos deben corresponder con el fabricante de la interfaz y los otros seis dígitos, especifican el número de serie del interfaz.

La autentificación basada en la dirección MAC se considera compleja e incómoda porque requiere que cada AP en la red tenga todas las direcciones MAC de los dispositivos autorizados, complicando el proceso de configuración.

La autentificación basada en direcciones MAC se considera débil debido a la disponibilidad de adaptadores de red inalámbricos que tienen la capacidad de cambiar la dirección MAC. Un Hacker puede lanzar un ataque sabiendo que direcciones MAC acepta el Access Point y programando su tarjeta inalámbrica con esa MAC. Al tratarse de conectar al Access Point este confirma la identidad del usuario basado en su dirección MAC, al coincidir esta el usuario puede acceder con éxito a la red y a sus recursos. La autentificación basada en MAC debe utilizar solamente como método de autentificación adicional. Dado que existe la posibilidad que un atacante puede utilizar la identidad de una MAC autorizada para acceder a la red.

4.1.2.4 Autentificación De La Red

Desafortunadamente, la mayoría de las tecnologías actualmente disponibles de redes inalámbricas LAN no incluyen un mecanismo robusto de autentificación de usuarios. La mayoría de las tecnologías como el estándar 802.11 solo permite la autentificación de identificador de conjunto de servicios (SSID), en la cual se le asigna a cada Access Point un identificador único el cual consiste un una serie de letras y números que son transmitidos para notar su existencia y así los usuarios encuentren esa red. La autentificación basada en el SSID es extremadamente débil y solamente proporciona identificación al Access Point.

El ataque contra Access Points mas común es el Rogue Attack en el cual un usuario mal intencionado pone un AP con el mismo nombre de SSID que comúnmente utilizan los usuarios. Al conectarse los usuarios a este AP pirata todo el trafico de red que pasa por el es escuchado y grabado lo cual representa un problema grave de seguridad. La mayoría de los ataques contra de las redes LAN inalámbricas son efectuados analizando el trafico de datos en la red. Si los datos no se transmiten de manera codificada cualquier persona podría escucharlos, alterarlos o dañarlos. Por lo cual es muy importante que en todo tipo de redes inalámbricas el tráfico sea codificado.

La seguridad en redes inalámbricas se ve afectada dado que la mayoría de los equipos en el mercado no cuenta con características de seguridad habilitadas por defecto. El Usuario tiene que configurar manualmente los parámetros de seguridad y principalmente los de encriptación. Es también importante educar a los consumidores y que ellos mismos se mantengan actualizados sobre los posibles riesgos de seguridad de usar las redes inalámbricas así como las soluciones para corregirlas.

4.2 El Protocolo WEP

El Wired Equivalent Privacy (WEP) es un algoritmo de cifrado usado por el proceso de autentificación de claves para autentificar usuarios y para codificar datos en redes inalámbricas. El estándar de IEEE 802.11 especifica el uso de WEP.

WEP es un algoritmo simple que utiliza un generador de números seudo aleatorios (PRNG) y el código de cifrado de flujo RC4. Por varios años este algoritmo era considerado un secreto comercial y las especificaciones no estaban disponibles, pero en septiembre de 1994, alguien filtro el código fuente en la lista de correo de un grupo de Hackers. Hoy en día el código fuente esta disponible, aunque es propiedad de RSA Security Inc.

El funcionamiento de la tecnología del cifrado WEP fue desarrollado a una longitud de codificación más baja debido a las regulaciones del control de la exportación de Estados Unidos que no permitieron que ninguna tecnología de cifrado sobre 40 dígitos binarios (5 caracteres de largo) fuera exportada fuera de los Estados Unidos. Para evitar este conflicto con los controles de exportación, IEEE 802.11 utilizo llaves de cifrado de 40−bits, aunque muchos vendedores hoy en día utilizan el estándar opcional de 128−bit[6].

El cifrado de flujo RC4 es muy rápido tanto como para codificar y decodificar, lo cual ahorra ciclos de procesamiento de CPU, RC4 también es muy fácil de implementar lo cual lo hace muy popular en programas de software. Cuando se describe a WEP como simple, significa que es débil. El algoritmo RC4 fue mal implementado en WEP, brindando una solución no adecuada de seguridad para la redes 802.11. En los dos tipos disponibles de WEP, 64-bits y 128-bits ambos tienen el mismo defecto en el vector de inicialización (IV) el cual es de 24-bits y utiliza el mismo proceso de codificación.

[6] CWNA-1

4.2.1 Debilidades Y Defectos Del Protocolo WEP

El defecto del proceso en la mayoría de las implementaciones WEP es que el vector de inicialización (IV) empieza en 0 y se va incrementando en 1 por cada paquete que es enviado. El vector de inicialización llega hasta el valor de 2^{24} (16,777,216), en una red con mucho tráfico este valor será superado lo cual significa que el Vector de inicialización tendrá que ser reiniciado a 0 por lo menos una ves al día.

Cuando WEP es usado, el vector de inicialización es transmitido en plano (sin codificar), con cada paquete cifrado. La manera en que el vector de inicialización (IV) es incrementado y enviado sin codificar permite los siguientes agujeros de seguridad:

- Ataques activos para inyectar tráfico nuevo. Estaciones no autorizadas pueden inyectar paquetes en la red basados en el vector de inicialización sin codificar.

- Ataques activos para decodificar el tráfico. Basado en el engaño al Access Point.

- Ataques basados en diccionario. Después de suficiente flujo de tráfico, la llave WEP puede ser descubierta usando herramientas gratuitas. Una vez que se conoce la clave WEP se puede decodificar todos los paquetes y escuchar todo el tráfico de la red. Así como acceder a ella.

- Ataques pasivos para decodificar el tráfico. Usando análisis estático, el trafico WEP puede ser decodificado.

4.2.2 Porque Fue Elegido WEP

Dado que WEP no es seguro, por qué fue elegido e implementado en el estándar 802.11?. Una vez que el estándar 802.11 fuera aprobado y terminado, los fabricantes de equipo wireless sacaron sus productos a la venta. El estándar 802.11 especifica los siguientes criterios de seguridad:

- Exportable.
- Razonablemente Fuerte.
- Auto Sincronización.
- Computacional Mente Eficiente.
- Opcional.

WEP cumple estos requisitos. Cuando WEP fue implementado, fue pensado para cumplir con los objetivos de seguridad como confidencialidad, control de acceso, y de integridad de datos. Lo que paso fue que se fabricaron demasiados adaptadores inalámbricos y se pensó que utilizando WEP se podría brindar seguridad a las redes inalámbricas. Afortunadamente para la industria, los dispositivos de redes inalámbricas ganaron inmensa popularidad antes de que este problema fuera ampliamente conocido. Esta serie de eventos guiaron a algunos fabricantes así como a terceros a crear soluciones de seguridad para redes inalámbricas.

El estándar 802.11 permite la implementación abierta de WEP a los fabricantes, así la implementación de cada fabricante de llaves WEP puede no ser la misma, agregando otra debilidad a WEP. Incluso las pruebas de interoperabilidad de Wi-Fi de WECA incluyen solo llaves WEP de 40 bits. Algunos fabricantes de dispositivos inalámbricos han optado por corregir WEP, mientras otros han usado nuevos estándares como 802.1x con EAP o VPNs.

4.2.3 Autentificación WEP

WEP proporciona a dos modos de autentificación: llave compartida y sistema abierto.

Autentificación Sistema Abierto

La autentificación de sistema abierto (open−system) también se conoce como autentificación nula porque un adaptador LAN Inalámbrico puede conectarse a cualquier Access Point y escuchar todos los datos que se envíen si codificar. Este tipo se implementa generalmente donde la facilidad de uso es el objetivo principal y el administrador de la red no desea preocuparse de cosas de seguridad. Éste tipo servicio no tiene autentificación.

Autentificación de Llave Compartida

Esto implica compartir una llave secreta para autentificar el adaptador LAN Inalámbrico al Access Point. La autentificación de llave compartida (shared−key) proporciona un mejor grado de autentificación que el sistema abierto. Para que una estación utilice la autentificación de llave compartida, debe utilizar el protocolo de codificación WEP.

La figura 4.1 ilustra la operación de la autentificación de llave compartida. El estándar 802.11 no especifica cómo distribuir las llaves a cada estación, sin embargo el proceso es el siguiente:

Paso 1 Un adaptador LAN Inalámbrico envía un Frame de petición de autentificación (un Frame de longitud fija) al AP que desean autentificarse.

Paso 2 Cuando el AP recibe un Frame inicial de la autentificación, el AP contestará con un frame de reto de autentificación que contiene 128 bytes de texto aleatorio generado por el motor de WEP en forma de estándar.

Paso 3 El adaptador LAN Inalámbrico copiará el texto del reto en un frame de autentificación, lo codificara con la llave compartida y enviara al AP.

Paso 4 El AP recibe el frame y decodifica el valor del texto del reto, usando la llave compartida y lo compara al texto de reto que el envió anteriormente.

Paso 5 Si el texto del reto coincide, el adaptador LAN Inalámbrico será notificado que la autentificación fue exitosa. Si no, el AP enviará una autentificación negativa.

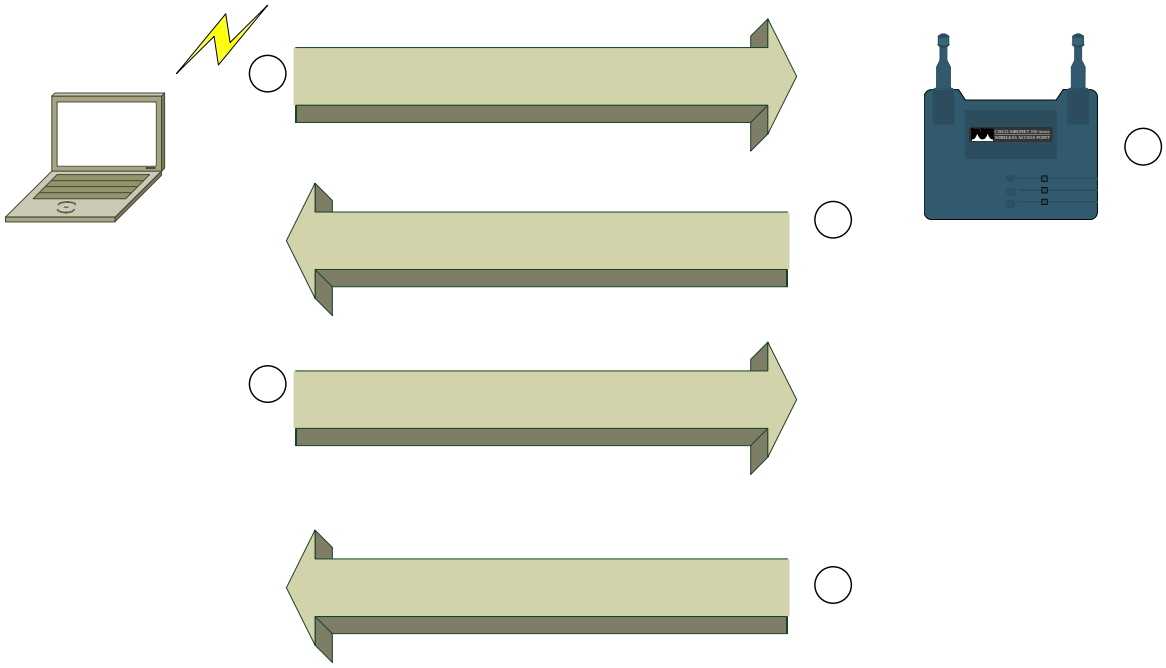


Figura 4.1 Autentificación WEP De Llave Compartida.

4.2.4 Llaves WEP

Las llaves WEP son utilizadas en los dispositivos cliente y de infraestructura en las LANs inalámbricas. Una llave de WEP es conjunto de caracteres alfanuméricos usados dos maneras en una LAN inalámbrica. Primero, una llave de WEP se puede utilizar para verificar la identidad de una estación. En segundo lugar, las llaves WEP pueden ser utilizadas para la codificación de datos.

Cuando un cliente con habilitación WEP trata de autentificarse y establecer comunicación con un Access Point este determinará si el cliente cuenta con la llave WEP valida. Esta llave de ve ser la misma usada en la implementación de la red. Las llaves deben coincidir en ambos lados de la conexión de la LAN inalámbrica.

El administrador de redes LANs Inalámbricas, puede distribuir las llaves de WEP manualmente, o usando un método mas avanzado de distribución. Los sistemas de distribución puede ser tan simples como utilizar llaves estáticas o tan avanzados como usar servidores de llaves de codificación.

Las llaves WEP están disponibles en dos tipos, las de 64-bits y las de 128-bits. Muchas veces aparecen como de 40-bits y de 104 bits. La razón es que ambas utilizan 24-bits para el vector de inicialización y lo demás para la llave codificada. La longitud de la llave codificada es de 40-bits o de 104 bits dando el la longitud total WEP de 64-bits y 128-bits.

Configurar las llaves WEP en dispositivos como Access Points y tarjetas inalámbricas cliente es relativamente fácil.

En la figura 4.2 se muestra un ejemplo de una ventana de configuración. Primero hay que seleccionar el formato de la llave si va a ser en formato ASCII alfa numérico o si va a ser en formato hexadecimal.

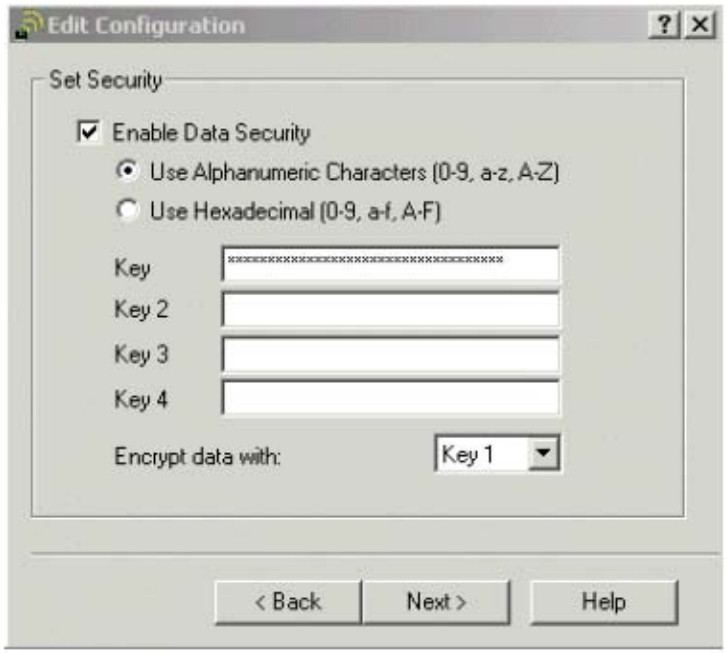


Figura 4.2 Configuración De Llaves WEP En Dispositivo Cliente.

El número de caracteres de la llave depende de la configuración, si se manejan caracteres ASCII o Hexadecimales y si es de 64-bits o 128-bits.

Si una tarjeta inalámbrica soporta 128-bits, entonces es compatible con los 64-bits. Cuando se utiliza una llave WEP en formato ASCII, esta será de una longitud de 5 caracteres para una llave WEP de 64-bits y 13 caracteres para una llave WEP de 128-bits. Para utilizar una llave WEP en formato hexadecimal se requieren 10 caracteres para una llave de 64-bits y 26 para una llave de 128-bits.

4.2.5 Uso De Llaves WEP Estáticas

Al elegir utilizar llaves WEP estáticas, estas se deberán asignar manualmente a los Access Points y a sus clientes. Estas llaves WEP nunca cambiarían, haciendo este segmento de la red susceptible a ataques de Hackers que pueden obtener la llave WEP utilizada. Por esta razón el uso de llaves WEP estáticas es apropiado para redes inalámbricas simples o caseras, pero no se recomienda su uso en redes inalámbricas empresariales.

Cuando implementan llaves estáticas WEP, es fácil que la seguridad de la red sea comprometida. Si un empleado llega a perder su tarjeta Inalámbrica también pierde las llaves ya que esta configuración se guarda en las tarjetas. Si alguien encuentra la tarjeta puede tener acceso a la red inalámbrica hasta que se cambien las llaves. La mayoría de los Access Point y clientes de acceso, soportan 4 llaves WEP simultáneamente, como se puede ver en la figura 4.3. Una razón útil para poder introducir hasta 4 llaves WEP es la segmentación de la red.

Otra razón para utilizar múltiples llaves WEP es en caso de que haya una mezcla de tarjetas que utilicen 64-bits y 128-bits. Esto puede aplicarse para dividir en grupos de 64-bits y 128-bits respectivamente para usar el cifrado máximo en un grupo sin afectar el otro.

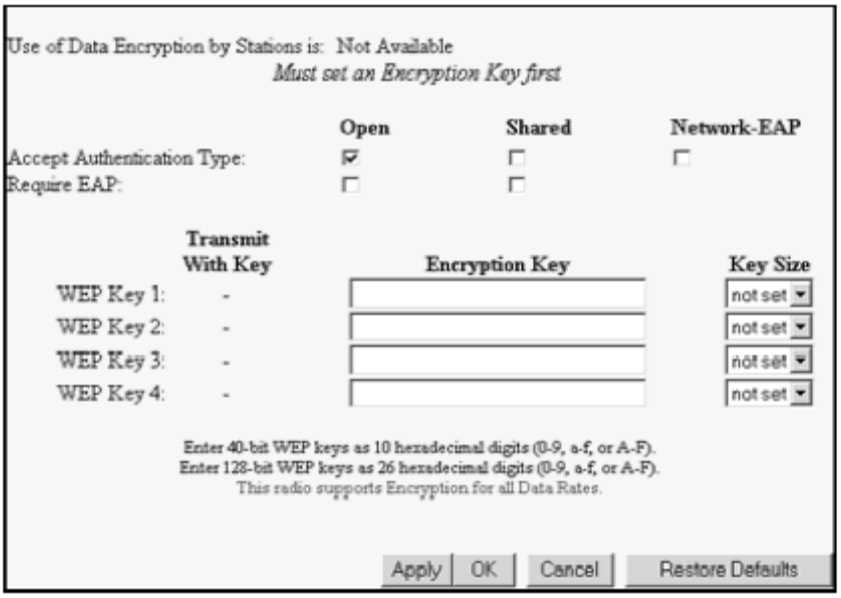


Figura 4.3 Cuadro de Configuración de llaves WEP en Access Point.

4.2.6 Servidor Centralizado De Llaves De Codificacion

Para LANs inalámbricas empresariales usar WEP es un mecanismo básico, por lo cual se deben de utilizar servidores de llaves de codificaron por los siguientes motivos:

- Generación Centralizada De Llaves.
- Distribución Centralizada De Llaves.
- Rotación Constante De Llaves.
- Reducción De Tráfico De Administración De Llaves.

Existen diversos tipos de dispositivos que son usados como servidores centralizados de llaves. Generalmente se usan servidores del tipo RADIUS u otro tipo de servidores especializados con el fin de distribuir nuevas llaves en un intervalo corto.

Normalmente cuando se usan llaves WEP el administrador debe introducirlas manualmente en las estaciones y Access Points.

Con el uso de servidores centralizados de llaves, se lleva acabo un proceso automatizado de asignación de llaves WEP entre estaciones, Access Points y servidores de llaves. La figura 4.4 muestra la común implementación de un servidor de llaves de codificación.

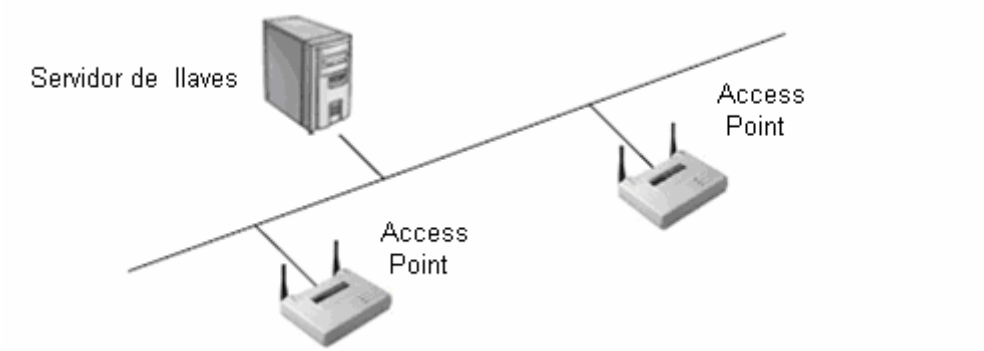


Figura 4.4 Servidor Centralizado de llaves de codificación.

Los servidores centralizados de llaves de cifrado permiten la generación de llaves por paquete, por sesión u otro método, dependiendo de la configuración o tipo de equipo. En la asignación de nuevas llaves por paquete, las llaves WEP deben ser asignadas a ambos lados de la conexión por cada paquete enviado. Mientras que la asignación por sesión se utiliza una nueva llave WEP por cada sesión en ambos nodos.

4.2.7 Uso De WEP

Cuando se inicializa WEP, la carga de los datos del paquete que es enviado es codificado usando WEP, sin embargo la parte de la cabecera incluyendo la dirección MAC no es cifrada. Toda la información de la capa 3 incluyendo dirección origen y destino es codificada con WEP. Cuando un Access Point envía la señales SSID (Beacon Frames) en una LAN inalámbrica usando WEP estas señales no son codificadas dado que los Beacon Frames no pertenecen a la capa 3.

Cuando se envían paquetes usando el cifrado de WEP, esos paquetes deben ser decodificados. Este proceso de decodificación consume ciclos de CPU y reduce el rendimiento en ancho de banda en una LAN inalámbrica, a veces significativamente. Algunos fabricantes introducen CPUs adicionales en los Access Points para realizar los procesos de codificación y decodificación WEP. Muchos fabricantes implementan la codificación y decodificación WEP utilizando software el cual ocupa la misma CPU que es usada para reenvió de paquetes, administración de Access Point, etc. Estos Access Points son los que mas recienten el uso de WEP. Implementando WEP vía hardware es muy probable que un Access Point 802.11b pueda mantener su rendimiento en 5Mbps. La desventaja de esto es el precio más alto de este tipo de Access Points.

Se puede implementar WEP como un mecanismo básico de seguridad, pero los administradores de la red deben conocer las debilidades de WEP y cómo compensarlas. También se debe de tomar en cuenta que cada fabricante puede utilizar WEP de diferente manera, y la compatibilidad entre varias marcas de hardware puede ser disminuida. Se recomienda utilizar una misma marca para evitar este tipo de problemas.

4.2.8 La Operación Del Protocolo De WEP

El algoritmo WEP proporciona autentificación y codificación a dispositivos LAN 802.11. WEP utiliza llaves compartidas, y la misma llave es usada para codificar y decodificar los datos. El algoritmo de cifrado WEP trabaja según los siguientes pasos:

Paso 1 Generación de la clave de codificación de la llave compartida.

El llave compartida de 40−bits concatenada con el vector de inicialización de 24−bits (IV) que es un dato generado aleatoria mente, dando por resultado una longitud total de 64−bit. La llave resultante alimenta al algoritmo RC4 para crear la llave de codificación. La figura 4.5 muestra una generación teórica usando el algoritmo de WEP.

```
Concatenated-Key = Shared-Key + IV

Encryption-Key = RC4(Concatenated-Key)
```

Figura 4.5 Generación de llave WEP.

Paso 2 Codificación de datos usando la llave de codificación.

Una operación de Chequeo de redundancia cíclica de 32−bits (CRC32) es realizado para asegurar la integridad de la información y prevenir la modificación desautorizada de los datos. El CRC es un valor numérico computado de los dígitos binarios en el mensaje que se transmitirá. El valor calculado se añade al final del fichero a la cola del mensaje antes de la transmisión, el receptor después detecta la presencia de errores en el mensaje, calculando un nuevo CRC y comparando con el CRC que se envió con los datos.

Los 4 octetos del CRC que resultan se concatenan al mensaje original. La secuencia que resulta entonces se codifica usando la llave de cifrado generado en el paso1 realizando una operación matemática or exclusiva (XOR).Or esclusiva es una operación matemática que compara 2 dígitos binarios en cada posición de dos valores dados, por ejemplo el valor A y el valor B. Si el dígito binario en la posición especifica de A o B es 1, pero no en ambos, el resultado de esa operación será un 1.

XOR es de uso frecuente en algoritmos criptográficos simétricos, donde se utiliza la operación XOR a los datos que serán codificados por una clave del cifrado y para recuperar los datos originales, los datos son descifrados con XOR y con la llave de cifrado.

El resultado es un mensaje cifrado de igual en longitud al los datos originales más 4 octetos. El mensaje final, (el mensaje cifrado) se envía a ambos extremos (es decir, del AP al adaptador) con el vector de inicialización (IV) precediendo al mensaje codificado. Los pasos de cifrado se muestran en la figura 4.6.

```
CRC-Value = CRC32(Original-Message)

Message-with-CRCCheck = Original-Message + CRC-Value

Encrypted-Message = (Message-with-CRCCheck) XOR Encryption-Key

MessageSentToPeer = IV + Encrypted-Message
```

Figura 4.6 Codificación De Datos Usando WEP.

Paso 3 Decodificación de datos y autentificación del mensaje.

El Access Point o el adaptador realizan los pasos contrarios para recuperar los datos originales y para autentificar que el mensaje fue enviado por alguien con quién se ha compartido una llave. En el proceso de decodificación, el vector de inicialización acompaña al mensaje junto con la llave compartida y se utiliza para generar la llave de cifrado (como en el paso 1), la cual es usada para decodificar el mensaje utilizando la operación XOR y la llave de encriptación. Los pasos se muestran el la figura 4.7.

```
MessageReceived = POLOJMNB

EncryptedMessage = MessageReceived - First-24-bits

IV = MessageReceived - Last-40-bits

Concatenated-Key = Shared-Key + IV

Decryption-Key = RC4(Concatenated-Key)

Decrypted-Message = (EncryptedMessage) XOR Decryption-Key
```

Figura 4.7 Decodificación De Datos Usando WEP.

Paso 4 Autentificación del mensaje recibido.

LA autentificación y descodificación de los datos transmitidos se realiza aplicando el algoritmo de chequeo al mensaje decodificado y comparando con el resultado del algoritmo CRC32. Si el CRC calculado no es igual al valor del CRC recibido en el mensaje, el mensaje recibido tiene un error, y se envía una notificación a la administración de control de medio la cual lo reenvía a la estación que envió el mensaje.

Las unidades móviles con mensajes erróneos no sea autentifican. A continuación se muestra este proceso en la figura 4.8

```
CRC-Value = CRC32(Decrypted-Message)
```

Figura 4.8 Autentificación Del Mensaje Recibido.

Si la misma llave que se utiliza para codificar y decodificar los mensajes también se utiliza para autentificar la estación, se considera un riesgo de seguridad hacer que las claves del cifrado y los claves de autentificación sean iguales.

4.3 El Protocolo De Autentificación 802.1X

El protocolo 802.1X fue diseñado originalmente para redes LANs Ethernet, pero también puede ser implementado en redes inalámbricas 802.11, el protocolo 802.11 no requiere que todos los dispositivos LAN utilicen las mismas llaves WEP, y permite que un dispositivo tengo un conjunto de llaves compartidas: una llave para sesión unicast y otra llave global multicast. Actualmente la aplicación en 802.11 solamente soporta llaves compartidas multicast pero se espera que en un futuro soporte llaves por sesión unicast. La configuración y actualización de todas las llaves puede ser un proceso difícil y puede no trabajar bien en una red con infraestructura larga. A demás la carencia de una implementación en protocolo para intercomunicación entre los Access Points (IAPP) dificulta el romming y necesita autentificarse de nuevo con un Access Point nuevo.

4.3.1 La Operación Básica 802.1X

Existen tres dispositivos que interactúan entre si en la operación básica del protocolo 802.1X, estos son el autentificador, el dispositivo a autentificar y el servidor de autentificación. Un autentificador es un dispositivo que requiere cumplir la autentificación antes de permitir el acceso a los servicios. El dispositivo a autentificar solicita el acceso a los servicios disponibles vía el autentificador. Un servidor de autentificación realiza la función de autentificación: Controla las credenciales del dispositivo a autentificar en nombre del autentificador.

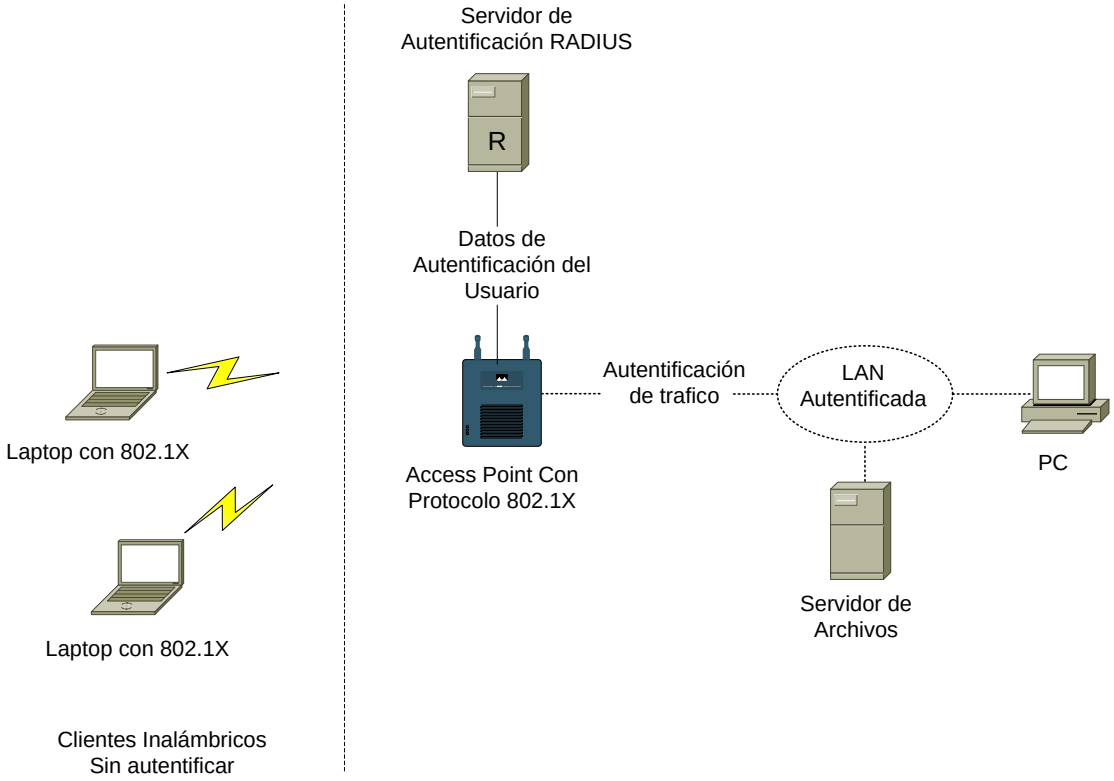


Figura 4.9 Dispositivos Básicos En 802.1X.

El servidor de la autentificación entonces responde al autentificador y le indica si dispositivo a autentificar está autorizado o no, a tener acceso a los servicios del autentificador. El servidor de la autentificación puede ser una entidad separada, o sus funciones pueden ser colocadas con el autentificador. El servidor mas utilizado de autentificación remota es RADIUS (Remote Authentication Dial−in User Service). La Figura 4.9 muestra una configuración común de 802.1X.

El acceso LAN puede desempeñar dos papeles en una interacción del control de acceso de la red: autentificador o dispositivo a autentificar. El control de acceso de autentificador define dos puntos de acceso lógicos a la LAN física. El primer punto de acceso lógico es el no controlado, el cual permite un intercambio no controlado entre el autentificador y otros sistemas en la LAN sin importar el estado de autorización del sistema. El segundo punto de acceso lógico es el controlado en el cual se permite el intercambio entre un sistema en la LAN y el autentificador, solo si el sistema es autorizado.

El estado de autorización de acceso controlado determina si el tráfico puede fluir del dispositivo a autentificar a la LAN. Este empezara como no autorizado y entonces cambiara a autorizado una vez que el dispositivo sea autentificado.

EL protocolo 802.1X utiliza típicamente el protocolo de extensión de autentificación (EAP) para el intercambio de información entre el dispositivo a auntentificar y el servidor de autentificación. Esto significa que los mensajes EAP necesitan ser encapsulados directamente sobre la LAN. Otro protocolo es elegido para este uso el protocolo EAP sobre LAN (EAPOL),

4.3.2 Uso De 802.1X Para Solucionar Los Problemas De Seguridad WEP

El protocolo 802.1X es usado para extender la seguridad al protocolo WEP. Esto se logra enviando una llave de autentificación al cliente y al Access Point como parte del proceso de autentificación. Solo un cliente autentificado conoce la llave de autentificación y esta llave codifica todos los paquetes enviados por el cliente como lo establece WEP. 802.1X ayuda a corregir la inseguridad en WEP brindando llaves por estación o sesión, para limitar el número de paquetes que usan la misma llave asegurándose de que las llaves cambian constantemente entre 5 y 10 minutos o cada 4 millones de paquetes, limitando el uso de llaves iguales, corrigiendo la debilidad de WEP. Después de la autentificación, se debe de configurar 802.1X para que pida a una estación que se reautentifique periódicamente en un intervalo especifico, para asegurar de que las llaves WEP cambien constantemente.

Es importante recordar que todo el tráfico de la autentificación es transmitido a través de un acceso no controlado, mientras que toda la transferencia autorizada de datos ocurre en el acceso controlado una ves que se ha autentificado al usuario. La autentificación de un adaptador LAN inalámbrico que usa el protocolo 802.1X consiste en los siguientes pasos:

Paso 1 Sin una llave de autentificación valida, el Access Point bloquea todo el trafico a través de el.

Paso 2 Cuando un adaptador LAN inalámbrico entra en el rango de alcance de un Access Point autentificador, el AP envía un reto de autentificación a la estación inalámbrica.

Paso 3 Una vez que la estación inalámbrica recibe el reto del Access Point, esta responde identificándose.

Paso 4 El Access Point envía la identificación de la estación inalámbrica al servidor RADIUS para iniciar el servicio de autentificación.

Paso 5 El servidor RADIUS solicita las credenciales a la estación inalámbrica especificando el tipo de credenciales que necesita para confirmar la identidad de esta.

Paso 6 La estación inalámbrica envía las credenciales al servidor RADIUS.

Paso 7 Una ves validadas las credenciales de la estación inalámbrica, el servidor RADIUS envía una llave de autentificación al Access Point, esta llave es codificada para que solo el Access Point pueda conocerla.

Paso 8 El Access Point utiliza la llave recibida del servidor RADIUS para asegurar la transmisión con la estación inalámbrica. Esta llave es siempre es transmitida en forma codificada.

4.4 WPA, TKIP, 802.11i y AES

Las debilidades del protocolo WEP limitaron su uso en un ambiente empresarial. Por lo cual el comité 802.11i de IEEE, trabajo duro para crear un protocolo sucesor de WEP. Originalmente llamado WEP2 pero fue renombrado a WPA (Wi-Fi Protected Access). El 31 de octubre de 2002, la alianza Wi-Fi anunció WPA, esencialmente una solución rápida, dado que el protocolo 802.11i no estaba totalmente listo, solo algunas partes las cuales fueron aplicadas en WPA por ejemplo 802.1X y el protocolo de integridad de llaves temporales TKIP.

Esencialmente, WPA es un subconjunto de 802.11i que se puede implementar via mejoras del software y firmwares. Aplicando TKIP para codificar el trafico y 802.1X para control de acceso. Desde una perspectiva de seguridad, estas tecnologías tienen gran importancia porque solucionan numerosas debilidades y vulnerabilidades encontradas en WEP y en el protocolo 802.11[7].

4.4.1 WPA

Hay que recordar que la principal debilidad de WEP es que el vector de inicialización se repite frecuentemente después de determinado tiempo o de mucho flujo de tráfico. Cuando el mismo vector de inicialización (IV) es usado dos veces, comúnmente llamado colisión IV, WEP es vulnerable de ataques tipo inyección de datos.

Actualmente existen varios programas que utilizan este principio para descifrar la llave WEP capturando grandes cantidades de información de la red. Entre estos se encuentran WEPCrack, AirSnort entre otros.

Finalmente la función de chequeo de valor de integridad (ICV) usa 32-bits CRC que puede ser forzado utilizando una técnica de inyección de paquetes. Esto permite al atacante modificar el paquete cambiando el valor ICV haciendo la alteración indetectable. WPA Soluciona estos problemas usando TKIP y 802.1X.

TKIP Corrige estas debilidades:

- Ataques de Replica: el valor de IV puede usarse en fuera de orden.
- Ataques de Falsificación: ICV usa 32-bits lineales y puede ser manipulado.
- Ataques de Colisión de llaves: Colisiones IV.
- Ataques de Debilidad de LLaves: el cifrado RCP es vulnerable a ataques escucha en los cuales se puede encontrar la llave.

[7] HSIYN-1

802.1x Corrige las siguientes debilidades:

- Carencias de Administración de llaves.
- Soporte inexistente de métodos de autentificación mejorados (tarjetas inteligentes, certificados digitales, contraseñas desechables, dispositivos biométricos, etc.).
- Identificación y autenticación de usuarios nula.
- Soporte inexistente para Autentificación y Autorización centralizada.

Los primeros productos que implementaron WPA comenzaron a venderse en mayo del 2003. Sin embargo las implementaciones no son aplicables a redes Ad-hoc solamente a redes modo infraestructura usando un Access Point.

4.4.1.1 El Protocolo De Integridad De Llaves Temporales (TKIP)

TKIP tiene tres elementos principales para mejorar el cifrado:

- Una función de mezcla de llaves por paquete.
- Una adición de un código de control de mensajes (MIC).
- Una mejora del IV que incluye reglas de secuencia.

Básicamente TKIP es una corrección al protocolo WEP, desarrollado como una actualización basada en software y hardware. El diseño fue planeado para mantener la retro compatibilidad con el hardware existente. Actualmente TKIP corrige todas las vulnerabilidades conocidas de WEP

4.4.1.2 TKIP En Detalle

El cliente comienza con dos llaves de cifrado: una de integridad de datos de 64-bits y otra de codificación de datos de 128-bits obtenidas en la negociación con 802.1X. La llave de cifrado de datos se llama llave temporal (TK). La llave de integridad es llamada código de integridad del mensaje (MIC).

Paso 1 La dirección MAC proveniente del dispositivo se le aplica una operación XOR junto con llave temporal (TK) para crear la llave de fase 1 (muchas veces llamada llave de fase intermedia).
Paso 2 La llave de la fase 1 es mezclada con la llave por paquete producida en este paso.
Paso 3 La salida del paso 2 se entrega al motor WEP como una llave normal de 128-bits (IV + llave compartida).

El resto del proceso ocurre como una transacción WEP normal. La diferencia es que no todos los clientes usan la misma llave WEP (dado la fase 1) y no se cuenta con la relación entre el IV (en este caso el número de secuencia) y la llave por paquete (dado la fase 2). En la figura numero 4.10 se muestra en detalle el proceso:

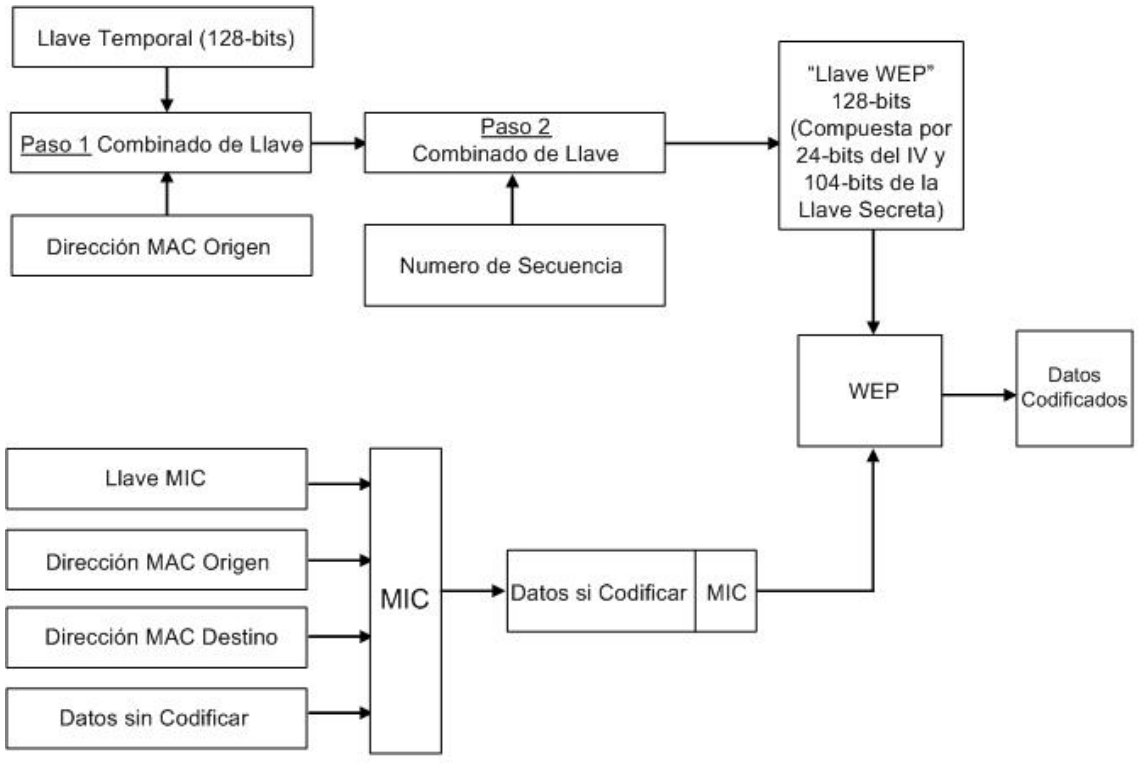


Figura 4.10 Codificación TKIP.

4.4.1.3 Combinación De Llave Por Paquete

El problema con el diseño original de WEP es que el vector de inicialización (IV) dependía de la llave secreta y era puesto directamente en RC4. En TKIP el paso 1 se asegura que cada cliente tenga una llave intermedia diferente. Luego el paso 2 combina la llave con el número de secuencia y finalmente lo introduce en RC4. Este proceso implica un proceso más elaborado que solo introducirlo a RC4. TKIP usa llaves por paquete corrigiendo la implementación incorrecta de RC4 en WEP.

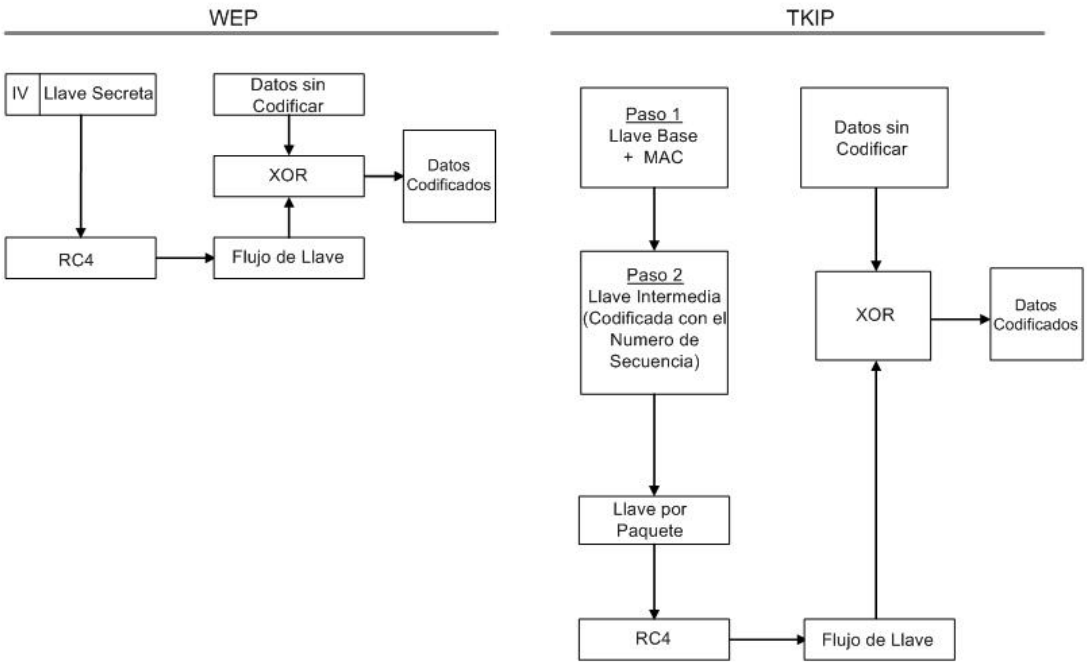


Figura 4.11 Combinación de llave Por Paquete.

4.4.1.4 Función De Código De Integridad Del Mensaje (MIC) De TKIP

En vez de usar un CRC de 32-bits la nueva función de código de integridad del mensaje (MIC), utiliza una función de codificación unidireccional diseñada por Neils Ferguson.

Al ser no linear dificulta la posibilidad de modificar el paquete mientras es enviado. La función MIC requiere de los siguientes elementos: La llave MIC, la dirección origen, la dirección destino, y los datos sin codificar.
Incorporando las direcciones origen y destino se puede verificar la dirección MAC. El resultado del MIC es agregado al campo de datos de la trama.

4.4.1.5 Mejoras En La Longitud Del Vector De Inicialización (IV)

TKIP supera los problemas de colisión IV de WEP siguiendo dos reglas simples. La primera es que el espacio del vector de inicialización (IV) ha sido incrementado de 24-bits a 48-bits, a una velocidad de transmisión de 54Mbps se requieren 1000 años para que se repita el IV. Segundo TKIP requiere que el IV se incremente de cero a otro número sin seguir una secuencia específica. En términos de seguridad esta implementación evita las colisiones IV y los ataques asociados al IV.

4.4.1.6 WPA Para El Hogar

Según lo descrito anterior, TKIP y WPA confían en una infraestructura 802.1x (Como servidores RADIUS) para la distribución de llaves. No todos los usuarios caseros cuentan con la infraestructura necesaria para la implementación de WPA, por lo tanto se introdujo un modo especial llamado llave precompartida PSK.
En este modo especial todos lo usuarios deben de contar con una llave compartida secreta (llamada llave maestra) en cada cliente y en el Access Point, esta trabaja de una forma similar a WEP. TKIP utiliza la llave maestra como punto de partida para generar matemáticamente otras llaves de codificación. A diferencia de WEP, TKIP cambia las llaves de codificación para asegurarse de nunca usar una llave dos veces.

4.4.2 AES y 802.11i

WPA fue el resultado de una medida de diseño apresurada para implementar las partes que estaban listas de 802.11i y sacarlas al mercado a mediados del 2003. Por lo tanto WPA era un subconjunto de 802.11i. El componente primario de 802.11i no estaba totalmente listo, el cual era el estándar de cifrado avanzado AES (Advanced Encryption Standard). En la especificación 802.11i la codificación AES es obligatoria mientras que TKIP es opcional.

4.4.2.1 Una Nueva Llave De Cifrado AES-CCMP

AES es un motor de codificación que cumple con las normas de los estándares federales para el procesamiento de información (FIPS) en los Estados Unidos y fue diseñado para remplazar a RC4. La adopción origina de AES por el gobierno de los Estados Unidos fue el resultado de un proceso de investigación.

AES tiene una variedad de modos, pero la especificación 802.11i ha seleccionado el modo de conteo el protocolo CBC-MAC (CCM), comúnmente llamado AES-CCMP. El modo de conteo provee la codificación mientras CBC-MAC provee la autentificación y la protección a la integridad de datos.

AES igual que RC4 fue diseñado como un algoritmo de llave simétrico, dado que los datos son codificados y decodificados con la misma llave compartida. Sin embargo el cifrado AES trabaja con pedazos de 128-bits a diferencia de RC4 que lo hace con un solo bit utilizando un proceso de XOR, de ahí que AES se conozca como cifrado de bloque. CCMP y TKIP comparten muchas características. Ambos usan llaves temporales de cifrado derivadas de una llave maestra obtenida de la negociación con 802.1X. CCMP usas un IV de 48-bits conocido número de paquete (PN).

4.4.2.2 Uso De Un MIC Nuevo

Al igual que TKIP, CCMP tiene un algoritmo de código de integridad de mensaje (MIC), para asegurarse de que el paquete no ha sido alterado. Sin embargo el MIC usado en CCMP trabaja de diferente manera al MIC de TKIP. El cálculo de MIC de CCMP se basa en los datos del IV y otros datos de la cabecera del paquete. También trabaja con las partes del bloque 128-bits para calcular el valor final.

4.4.2.3 Un Motor Nuevo Del Cifrado

El proceso de codificación AES es diferente al proceso WEP/TKIP. Primero el cifrado AES procesa 128-bits antes de poner el IV y otra información en la cabecera del paquete. Los datos sin codificar son divididos en paquetes de 128-bits, se procesan en una operación XOR y se cifran al mismo tiempo con AES. La codificación repite el proceso mientras incrementa el contador de bloque cada 128-bits hasta que todos los datos son codificados. Finalmente el contador se pone en 0 y se aplica una operación XOR al valor MIC el cual se agrega al final del Frame. El resultado de este proceso es un cifrado fuerte. Sin embargo esto implico gastos adicionales al requerir más procesamiento del CPU que con el motor de WEP. Por lo tanto AES no es compatible con el equipo inalámbrico de primera generación requiriendo hardware nuevo.

4.5 Descuidos Comunes De Seguridad

La mayoría del equipo de redes LAN inalámbricas se venden con las opciones de seguridad deshabilitadas. Para implementar la seguridad en dispositivos 802.11 se debe tener cuidado en elegir apropiadamente la tecnología a usar así como configurar solo las opciones que se vallan a usar.

4.5.1 Uso De Valores Por Defecto

Una red desprotegida puede también proporcionar acceso libre a desconocidos a su ancho de banda. Hay Hackers que se dedican a encontrar redes inalámbricas desprotegidas y ocupar los servicios de Internet para hospedar paginas o archivos ilegales. Para proteger las redes LAN inalámbricas de los hackers y otras amenazas se debe de trabajar con datos codificados y en modo de autentificación.

4.5.1.2 Uso De Llaves Compartidas Fijas

La mayoría de los dispositivos actualmente disponibles de redes inalámbricas utilizan más de una llave compartida. Estas llaves compartidas son usadas para propósitos de autentificación y codificación. Si estas llaves no se actualizan constantemente pueden ser descifradas. Por eso es importante asegurarse que la red sea segura y que las llaves deben actualizarse frecuentemente para evitar ataques de hackeo de llaves.

4.5.1.3 Uso De Señales De Radio Muy Fuertes

La fuerza de las señales de radio usadas en redes inalámbricas define el rango de el cual un dispositivo LAN inalámbrica puede acceder a la red. El uso de los dispositivos que producen señales de radio muy fuertes agregan inseguridad a la LAN inalámbrica al ser mas accesibles a personas no autorizadas a distancias lejanas. Es importante utilizar dispositivos inalámbricos que emitan señales de radio que no sean demasiado fuertes.

4.5.2 Aseguramiento De La Red

Lo primero que hay que recordar es que la mayoría de dispositivos de redes inalámbricas 802.11 son vendidos con las opciones de seguridad deshabilitadas. Es responsabilidad de los administradores y usuarios de la red, asegurarse de que se implementaran estas medidas de seguridad. Así como contar con una forma de autentificar los usuarios que requieran conectarse a la red y configurar los Access Points para cifrar todos los datos que se transmiten en la red.

4.5.2.1 Autentificación Del Usuario

Todos los usuarios de la LAN inalámbrica segura deben ser autentificados. Pueden usarse las técnicas de autentificación WEP para seguridad mínima, 802.1X para seguridad media y VPNs para seguridad de alto nivel.

Se pueden combinar el protocolo 802.1X y VPNs para proporcionar seguridad a redes inalámbricas que se conectan a redes cableadas y LAN remotas.

En este caso todos los dispositivos inalámbricos se autentifican usando el protocolo 802.1X, y se utiliza VPN para proporcionar a seguridad de alto nivel a los dispositivos inalámbricos, la red local y redes LAN remotas.

Es necesario también la autentificación a nivel sistema operativo para proveer seguridad a los diferentes recursos de red compartidos, por ejemplo un servidor de archivos.

4.5.2.2 Confidencialidad De Datos Y Privacidad

Para que una red inalámbrica sea llamada segura, todo el tráfico en la LAN se debe transmitir correctamente en forma cifrada. Los datos entre dispositivos inalámbricos se pueden proteger usando WEP para brindar una la seguridad mínima y con tecnología VPN para proporcionar una seguridad de alto nivel.

El protocolo 802.1X soluciona los problemas de seguridad del protocolo WEP proporcionando un mecanismo mejorado para actualizar las llaves y autentificar usuarios. Para necesidades de seguridad mínimas la codificación WEP se puede utilizar con precaución, Pero si se desea seguridad de nivel medio se puede utilizar 801.1X para estos fines. Se deben de usar VPNs para un alto nivel de confidencialidad de datos y privacidad. Las VPNs proporcionan confidencialidad codificando todos los datos que se transmiten entre los dispositivos. Las VPNs se pueden utilizar junto con el protocolo 802.1X para restringir el acceso de usuarios autorizados a redes inalámbricas

4.5.2.3 Políticas De Uso De Contraseñas

Los administradores y usuarios de cualquier tipo de redes, especialmente redes inalámbricas se les deben de pedir cambiar sus contraseñas regularmente. Así como utilizar contraseñas difíciles de descifrar. Los usuarios deben ser desalentados fuertemente de compartir sus contraseñas con otros usuarios. El acceso a los recursos de alta importancia debe ser restringido y no se debe permitir conectarse a la red a usuarios que no cuenten con opciones de seguridad habilitadas.

4.5.2.4 Análisis De Trafico De Red Y Frecuencia De Uso

Los administradores de LANs inalámbricas deben vigilar el tráfico y uso de la red regularmente para asegurarse que la red no esta comprometida. Se deben observar los registros de autentificación con frecuencia para identificar cualquier agujero de seguridad o cualquier intento de vulnerar la seguridad.

CAPITULO V

Auditoria En Redes Inalámbricas

5.1 Etapas De La Auditoria

Los hackers y los auditores de seguridad realizan los mismos pasos para tratar de acceder a una red. Estos pasos incluyen los siguientes:

1. Definir Una Meta
2. Investigación Y Descubrimiento
3. Planeamiento Del Ataque
4. Ejecución Del Ataque
5. Limpieza De Rastros

Cada paso se realiza comúnmente en el orden descrito, pero las habilidades de cada persona y el objetivo determinan el grado y la duración de cada paso. Es decir un Script Kiddie que trata de buscar zombis para realizar un ataque distribuido de denegación de servicios (DDOS), ocupa unos segundos en definir la meta y en buscar computadoras vulnerables para realizar su ataque. Esto es por que utilizara herramientas automatizadas para buscar cientos de computadoras encontrando algunas vulnerables. Un Script Kiddie no selecciona un blanco en especifico simplemente elige una que sea vulnerable de la lista. Un Auditor de seguridad tendrá un método diferente de ataque, principalmente porque la meta es realizar un servicio en vez de encontrar computadoras vulnerables para su beneficio personal[8].

[8] MWS-1

5.1.1 Definir Una Meta

Existen dos tipos de hackers: los que solo están buscando una red inalámbrica desprotegida, y aquellos que esta auditando una red en específico por una razón ética o no ética.

En el primer caso la meta será conducida por la curiosidad o por malas intenciones. Típicamente este grupo esta formado por Script Kiddies o Hackers novatos que solo les interesa descubrir cuantas redes inalámbricas están desprotegidas en un área cercana. La diferencia es en lo que pasa cuando una red inalámbrica insegura es descubierta. Un Script Kiddie inmediatamente tratara de descubrir las computadoras conectadas a esa red e instalara un caballo de Troya u otros programas para tomar ventaja de la situación.

Por otro lado, un Auditor o un Hacker Ético tendrá una meta bien definida. El hecho de atacar una red inalámbrica es solo parte de la auditoria de seguridad, la cual incluirá también probar la red vía Internet, realizar llamadas telefónicas e intentar ingeniería social. En este caso la meta es solo probar la seguridad de la red inalámbrica y determinar si es vulnerable a un ataque.

La diferencia entre los dos, son las intenciones. Un Script Kiddie solo buscara una forma de entrar a la red. Una vez descubierta, la usara para su beneficio. Sin embargo un Auditor encontrara la misma debilidad pero descubrirá otros métodos de ataque y brindara una descripción detallada de las debilidades en la red inalámbrica.

5.1.2 Investigación Y Descubrimiento

Ya que se tiene un objetivo definido, puede empezar la auditoria. En esta parte de la auditoria se tendrán que investigar y realizar pruebas para ver que información se puede obtener y que sirva para poder entrar en la red. Esta es una parte importante del proceso ya que probar todos los aspectos de la red nos puede llevar varios días o semanas.

Solo cuando el ataque es exitoso se puede decir que se realizo una investigación sobre el blanco. Se tendrán que efectuar dos etapas de investigación a la red, una a la red inalámbrica y otra a la red cableada.

Para recabar datos se puede apuntar al Access Point con una antena Yagi. Una ves que el equipo esta listo se ejecuta el programa AirSnort y se esperara a que los datos sean recolectados. Basados en la tasa de captura de datos se podrá estimar el tiempo suficiente para romper la llave WEP. Una ves teniendo la llave WEP se puede empezar a espiar los paquetes y así obtener mas datos de los usuarios de la red como contraseñas, direcciones MAC validas, configuraciones IP, direcciones de correo u otras cosas.

Esta parte del proceso se efectuara varias veces por que es poco probable que se obtenga la suficiente información para penetrar la red la primera vez.

5.1.3 Planeación Del Ataque

Cuando se planea un ataque a una red inalámbrica se deben de tomar en cuenta ciertos factores. Una ves que se tiene el blanco se debe de planear la forma en que se va a acceder a el. También se debe de contar con todas las herramientas necesarias para efectuar el ataque, esto puede consistir en el hardware, programas y datos conocidos de la red.

Planear el ataque puede tomar minutos o meses. Si la red es un sitio altamente asegurado, el hacker debe crear una red semejante a la que se quiere atacar con el mismo software y hardware que tiene para practicar y encontrar las debilidades y no cometer errores.

La audición puede tomar tiempo dado que muchas veces se requiere de grandes cantidades tráfico para poder descifrar las claves. Es importante ser paciente y no apresurar las cosas para no ser detectado.

5.1.4 La Ejecución Del Ataque

La parte de la ejecución es el proceso donde se hackea el sistema vulnerable. Un hacker quiere asegurarse de salir y entrar a la red sin alertar a un sistema de detención de intrusos o ser descubierto por el administrador de la red. Una ves que se conoce la dirección IP del Access Point y si esta configurada por defecto, posiblemente todos las demás configuraciones también estén así. En caso de ser afirmativo se pueden modificar los parámetros, re-direccionar las conexiones, controlar los servicios y más. Si el Access Point esta conectado la red via DSL esto puede ser un problema serio en el cual también se puede controlar el ancho de banda a Internet.

Usando las configuración de fábrica, un hacker fácilmente puede conocer la configuración de la red y así modificar los datos del Access Point o realizar un ataque de denegación de servicios. Por lo cual es importante cambiar la configuración de fábrica una vez que se ha instalado el equipo.

5.1.5 Limpieza De Rastros

La parte de limpieza es en la cual el hacker limpia cualquier modificación al sistema hecha por el y elimina los archivos de registro que fueron creados como resultado del ataque. Esta parte es la mas importante en cualquier proceso de Hackeo, si el hacker logra limpiar todos sus rastros, el propietario de la red jamás sabrá que el hacker penetro en su red y no establecerá o modificara medidas de seguridad garantizando esto que el hacker pueda volver a entrar a la red sin ser esperado.

En el caso de hackeo a redes LAN inalámbricas se crean varios archivos de registro en el Access Point los cuales puede revelar la identidad del atacante. La dirección MAC puede ser grabada y dependiendo de la configuración, el hacker tendrá que borrar o modificar la información con datos validos. Esto se puede hacer controlando las sesiones de usuarios validos o cambiando la dirección MAC por una dirección de un cliente valido.

Otros posibles puntos donde se puede crear archivos de registro son en un Firewall, en una VPN, en un servidor RADIUS o en un monitor de tráfico de red instalado. Es por esto que es peligroso tratar de acceder a redes dado que nunca se sabe que dispositivos existan.

5.2 Wardriving

Las redes inalámbricas se han vuelto parte de nuestras vidas en los pasados años. En este capitulo se muestra una parte de la historia del WarDriving y la terminología necesaria para entender de que se trata.

Esto incluye información acerca de las herramientas, los programas y la terminología que se maneja comúnmente. Muchas de la herramientas que usa un WarDriver son las mismas herramientas que usa una persona para obtener acceso no autorizado a una red inalámbrica. Dado que estas no son las intenciones de de un WarDriver la metodología que se usa aquí es ética solo con fines educativos.

5.2.1 El Origen Del Wardriving

El Wardriving es una actividad mal entendida por la gente y los medios. Dado que el nombre suena como una actividad criminal. Por eso es importante comprender el origen del nombre. El Wardriving es el acto de moverse alrededor de un área en específico descubriendo y apuntando en un mapa la cantidad de Access Points que existen para fines estadísticos. Después estas estadísticas son usadas para levantar reportes de problemas de seguridad en este tipo de redes. La definición de Wardriving no solamente incluye realizar las investigaciones en automóvil, si no que incluye cualquier tipo de investigación moviéndose alrededor de cierta área para recabar los datos, como caminando o en bicicleta.

El termino Wardriving proviene de la palabra Wardialing, un termino que fue introducido al publico en general por el personaje de Matthew Broderick (David Lighman) en la película Juegos de Guerra[9] en 1983. Wardialing es el uso de un MODEM para marcar números secuencialmente para encontrar computadoras conectadas y acceder a ellas. En esos tiempos era la forma mas practica de conectar 2 computadoras en red. Actualmente es una tecnología obsoleta y muy poco usada.

[9] IMDB-1

El Wardriving emplea el mismo concepto pero usando la tecnología actual: las redes inalámbricas. El concepto de Wardriving talvez comenzó al siguiente día en que la primera red LAN inalámbrica fue desarrollada. El nombre de Wardriving se dio a conocer ampliamente cuando el proceso fue automatizado por un consultor de seguridad informática llamado Peter Shipley en Berkeley California. En el otoño del año 2000, Shipley condujo una auditoria de redes inalámbricas en Berkeley y dio a conocer sus resultados en la conferencia anual de Hackers DefCon en Julio del 2001.

La realidad de Wardriving es simple. Los profesionales de seguridad en Internet y la gente en general esta interesada en proveer información al público acerca de las vulnerabilidades que están presentes en las configuraciones de fábrica de los Access Points.

De acuerdo con el FBI no es ilegal buscar Access Points, pero robar el servicio, hacer ataques de negación de servicios y robo de información, si.

5.2.2 Herramientas Necesarias

En esta sección se muestran las herramientas requeridas para efectuar auditoria en base a WarDriving[10]. Existen diferentes tipos de configuraciones que pueden ser usadas en la inspección de las redes entre las cuales incluyen las siguientes:

- Obtener El Hardware Requerido
- Elegir Una Tarjeta De Red Inalámbrica
- Decidir Si Se Usara Una Antena Externa
- Conectar Una Antena Externa A La Tarjeta Inalámbrica

[10] WDDD-1

5.2.3 Obteniendo El Hardware

La configuración mas usada de Wardriving utiliza una computadora portátil (laptop). Para auditar con una laptop se necesitan otros dispositivos hardware y al menos un software especializado. Los principales componentes incluyen:

- Una Laptop
- Una Tarjeta Inalámbrica
- Una Antena Externa
- Un Conector Externo Para La Antena
- Un Dispositivo GPS (Opcional)
- Software Para Wardriving

Dado que el equipo usado por el software para Wardriving no requiere un procesador muy poderoso se puede escoger una laptop de modelo viejo. Una vez que se escogió una laptop se necesita elegir que software se va utilizar. Existen 2 opciones una maquina con el OS Linux o con Windows, depende de la experiencia personal para elegir el sistema operativo y a su ves la herramientas disponibles en este. En la figura 5.1 se muestra una laptop elegida para este fin.

Figura 5.1 Computadora Típica Para Wardriving

5.2.4 Escogiendo La Tarjeta Inalámbrica

Una vez que se escogió la computadora lo siguiente es elegir la tarjeta inalámbrica. La mayoría de las redes implementadas hoy en día son 802.11b. Por lo tanto esta seria la elección conveniente de tarjeta.

También existe redes 802.11g las cuales superan por 5 veces la velocidad de una tarjeta 802.11b (54MBps contra 11MBps). Pero por el momento son muy costosas y existe muy poco software Wardriving para estas, dado que este estándar utiliza WPA, y una buena implementación de WPA elimina casi por completo los problemas de inseguridad de las redes inalámbricas.

Algunas tarjetas 802.11a son soportadas también por software Wardriving bajo ciertas condiciones. Pero en general las tarjetas 802.11a o cualquier tarjeta combo 802.11a/b/g no son recomendadas para Wardriving debido a que el estándar 802.11a maneja tres rangos de frecuencia UNII y bajo las regulaciones de la FCC no pueden contar con antenas removibles.

Cuando fue creado el software Kismet y NetStrumbler solamente existían dos tipos de chipsets en las tarjetas inalámbricas: el Hermes y el Prism2. Aunque existen otros chipsets disponibles en el mercado, la mayoría del software es diseñado basado en estos dos chipsets. Como regla el NetSumbler (OS Windows) trabaja con tarjetas basadas en chipsets Hermes y Kismet (OS Linux) con tarjetas basadas en chipsets Prism2. En algunos casos las tarjetas Prism2 pueden trabajar con Netstrumbler y las Hermes pueden trabajar bajo Linux modificando el kernel y ser usadas en Kismet.

5.2.4.1 Tipos De Tarjetas Inalámbricas

Antes de comprar una tarjeta para Wardriving es importante asegurarnos que el software que vallamos a utilizar sea compatible con esta.

NetStumbler (el cual se vera mas adelante) ofrece pre-configuraciones para tarjetas basadas en chipsets Hermes como por ejemplo las tarjetas Orinoco. NetStrumbler ofrece soporte para las siguientes tarjetas:

- Lucent Technologies WaveLAN/IEEE (Agere ORiNOCO)
- Dell TrueMobile 1150 Series
- Avaya Wireless PC Card
- Toshiba Wireless LAN Card
- Compaq WL110
- Cabletron/Enterasys Roamabout
- Elsa Airlancer MC-11
- ARtem ComCard 11Mbps
- IBM High Rate Wireless LAN PC Card
- 1stWave 1ST-PC-DSS11IS, DSS11IG, DSS11ES, DSS11EG
- Algunas tarjetas Prism2 trabajan bajo Windows XP.

Algunas distribuciones Linux requieren una modificación en su Kernel para trabajar con tarjetas Hermes y entrar en modo monitor el cual es requerido por Kismet.
Kismet ofrece soporte para las siguientes tarjetas:

- Cisco

1. Aironet 340
2. Aironet 350

- Prism 2

1. Linksys
2. D-Link
3. Zoom
4. Demarctech
5. Microsoft

- ORiNOCO

1. WaveLAN basadas en Lucent ORiNOCO
2. Airport

- AIRPORT

1. Airport cards under Mac OS X using the Viha drivers

- ACX100

1. Dlink 650+

Para mejorar los resultados se requieren tarjetas que cuenten con conectores para antenas externas como la que se muestra en la figura 5.2. Esta característica ayuda a extender el rango de alcance agregando una antena.

Figura 5.2 Conector Para Antena Externa En Una Tarjeta Orinoco.

Mucha gente en el mundo del Wardriving prefiere la tarjeta ORiNOCO Gold 802.11b producida por Agere o Lucent (mostrada en la figura 5.3) dado que es compatible tanto con Netstrumbler y con Kismet y también cuenta con conector para antena externa. Esta tarjeta actualmente esta descontinuada y se producen modelos nuevos que no usan el chip Hermes pero cuentan con el conector para antena. Existen en el mercado algunas de las viejas tarjetas basadas en el chipset Hermes pero son conocidas como ORiNOCO Gold Classic[11].

Figura 5.3 Tarjeta Inalámbrica Orinoco Gold Classic

Es recomendada la tarjeta ORiNOCO Gold Classic ya que es compatible con casi todo el software para Wardriving y puede ser usada tanto en Linux como en Windows.

5.2.5 Antenas Externas

Para mejorar los resultados mientras se buscan y se analizan redes inalámbricas es recomendable utilizar antenas externas. Una antena sirve para radiar o recibir ondas de RF, la mayoría de las tarjetas inalámbricas cuentan con una pequeña antena integrada. Una antena externa conectada a una tarjeta inalámbrica incrementa el rango de detección de las señales de redes inalámbricas.

[11] EBAY-1 Se puede conseguir vía ebay por 79 dólares.

Existen diferentes tipos de antenas que se pueden conectar a las tarjetas inalámbricas: parabólicas, direccionales y omni-direccionales. Las antenas parabólicas son poco recomendadas dado su tamaño y no son prácticas para el Wardriving.

Figura 5.4 Antena Parabólica.

Mucha gente en el mundo de Wardriving utiliza una antena direccional o una omni-direccional conectada a su tarjeta inalámbrica. Ambas se encuentran disponibles en diferentes tamaños y fuerza de señal. Se necesita considerar varios aspectos para determinar el tipo de antena a usar. La liga amateur de radio repetidoras (www.arrl.org) puede proveer algunos datos importantes así como teoría de antenas.

5.2.5.1 Antenas Omni-Direccionales

Las antenas omni-direccionales irradian y reciben señales de todas direcciones y pueden comprarse desde 50 usd dependiendo del mecanismo de colocación. Un error común es creer que con una antena de ganancia fuerte serán mejores los resultados de recepción de señales inalámbricas.

Lo cual no es cierto dado que al aumentar la ganancia (en decibeles isotropitos dBi) el ángulo de cobertura será más agudo. En la figura 5.5 se muestra la comparación entre los radios de cobertura de una antena omni-direccional de 5dBi comparada con otra de 8 dBi. También se muestra una vista lateral de la cobertura total.

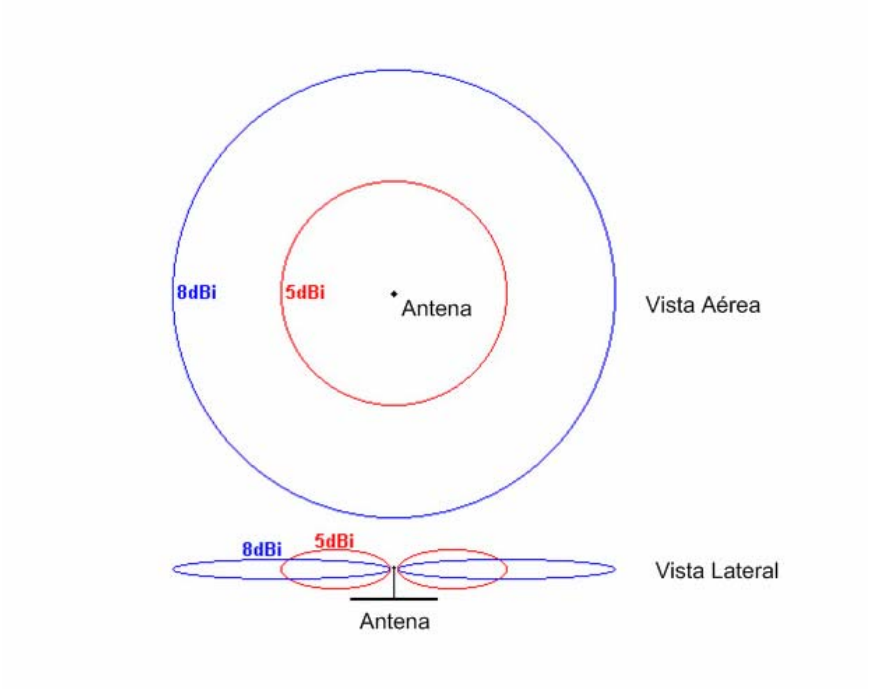


Figura 5.5 Comparación De Las Señales De Las Antenas.

Por lo visto en la figura se puede concluir que una antena omni-direccional de 5 dBi provee mejores resultados en un vecindario con edificios altos como en el centro de la ciudad. También provee mejor cobertura en zonas donde existen obstáculos entre la antena y el Access Point como casas y edificios. Otro beneficio de las antenas de 5 dBi es que la mayoría cuenta con soporte magnético que puede ser colocado fácilmente en el techo de automóvil sin que se requiera un dispositivo para colocarla como se muestra en la figura 5.6.

Figura 5.6 Antena De 5 dBi Con Soporte Magnético.

Las antenas de ganancia de 8 dBi como la que se muestra en la figura 5.7 es excelente para áreas con pocos obstáculos como autopistas. Estas antenas son muy efectivas cuando las residencias o negocios se encuentran lejos de la computadora como por ejemplo un estacionamiento. Estas antenas comúnmente requieren dispositivos para montarlas.

Figura 5.7 Antena De 8 dBi.

5.2.5.2 Antenas Direccionales

Las antenas direccionales se basan en el principio de línea de vista para transmitir y recibir señales inalámbricas, estas solo pueden recibir señales de la dirección a donde son apuntadas. Estas Antenas son excelentes para usar en áreas con edificios altos. Se pueden colocar cerca del edificio e ir apuntando en busca de Access Points. Las antenas direccionales pueden tener más ganancia para recibir señales en un tamaño menor. Por ejemplo una antena de ganancia de 14.5 dBi (como la de la figura 5.8) es un poco mas grande que la antena omni-direccional de 8 dBi mostrada en la figura 5.7.

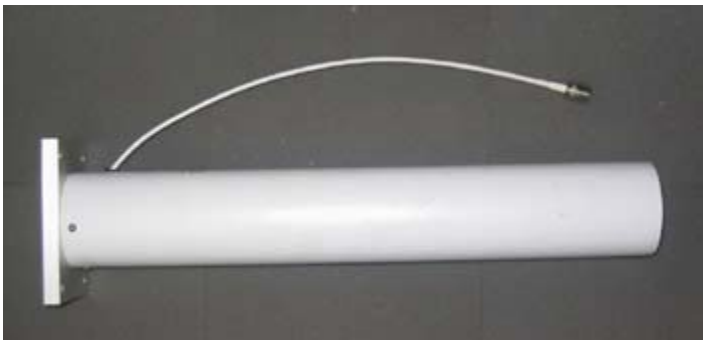


Figura 5.8 Antena Direccional De 14.5 dBi.

Existen varios tipos de antenas direccionales, las más comunes son: la yagi y la de maya parabólica. Pero la mas usada es la yagi y por ello es la mas barata, ofreciendo una muy buena ganancia a un precio accesible[12].

Usualmente la antena omni-direccional es la mejor elección para el Wardriving, esto es porque puede escuchar las señales de radio en todas direcciones y no es necesario apuntarlas a un punto especifico para buscar redes inalámbricas. Pero existen condiciones en las cual una antena direccional es mas efectiva.

[12] EBAY-2 Se puede conseguir el kit con tarjeta inalámbrica en ebay por 95 dólares.

5.2.6 Conectando La Antena A La Tarjeta De Red Inalámbrica

Una ves que se han elegido la tarjeta de red y la antena externa es necesario un cable especial para conectarlas apropiadamente, comúnmente estos cables reciben el nombre de cola de cochino (pigtail). La mayoría de las antenas cuentan con un conector tipo N (N-type) pero las tarjetas inalámbricas tienen un conector en específico que cambian con el fabricante, al comprar la tarjeta es importante verificar el tipo de conector con el que cuenta, en algunos casos el adaptador viene incluido con las tarjetas inalámbricas. Esto permitirá conectar exitosamente la antena al conector de la tarjeta de red.

Figura 5.9 Conectores Para Antena Externa

5.2.7 Iniciando El Proceso De Auditoria

Una ves que se cuenta con todo el hardware necesario, se esta casi listo para empezar a buscar los Access Points. Antes de hacer esto es necesario asegurarse de no conectarse inadvertidamente a la red encontrada, dado que algunos Access Points están configurados para que los clientes se conecten automáticamente. Esto es debido a que el Access Point permite conectar a cualquier tarjeta inalámbrica sin configurar ningún parámetro debido a como esta configurado. El rotuer tiene habilitado el protocolo de configuración dinámica de host (DHCP).

El servidor DHCP asigna automáticamente una dirección IP valida a cualquier host que lo requiera, una ves que se establece la conexión el DHCP completa el proceso.

Esto no pasa con los programas de Linux como Kismet o AirSnort dado que operan en modo monitor. Un dispositivo en modo monitor solamente escucha el tráfico si establecer una conexión. Para prevenir las conexiones accidentales a las redes encontradas usando Windows, se necesitan hacer unos cambios a la configuración.

5.2.8 Deshabilitando La Pila De TCP/IP En Windows

Deshabilitando la pila TCP/IP de Windows la laptop no será capas de conectarse a la red. Este es un proceso censillo que se necesita realizar antes de empezar a buscar redes vía Wardriving.

Paso 1 En Windows XP/2000 Seleccionar el icono de panel de control.

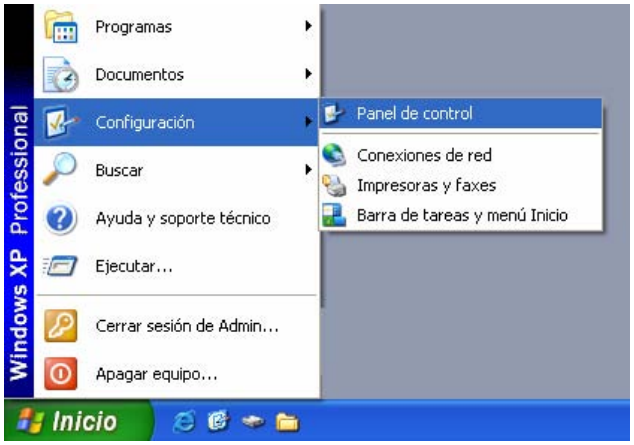


Figura 5.10 Paso 1 Para Deshabilitar TCP/IP En Windows.

Paso 2 ya que se esta en el panel de control seleccionar el icono de conexiones de red.

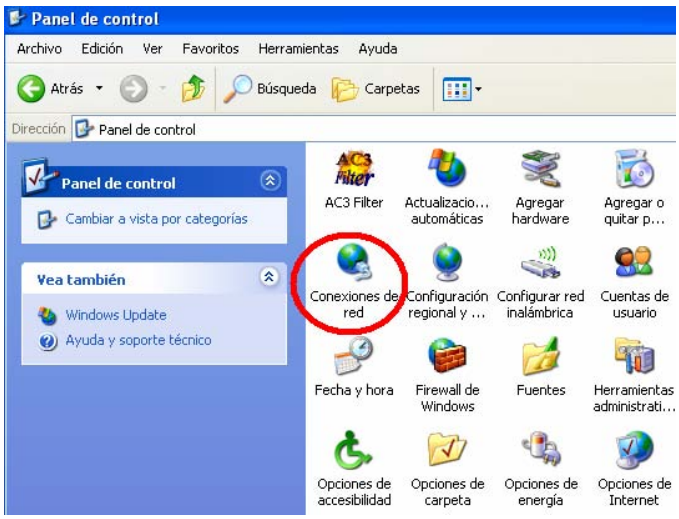


Figura 5.11 Paso 2 Para Deshabilitar TCP/IP En Windows.

Paso 3 Seleccionar Propiedades de la conexión.

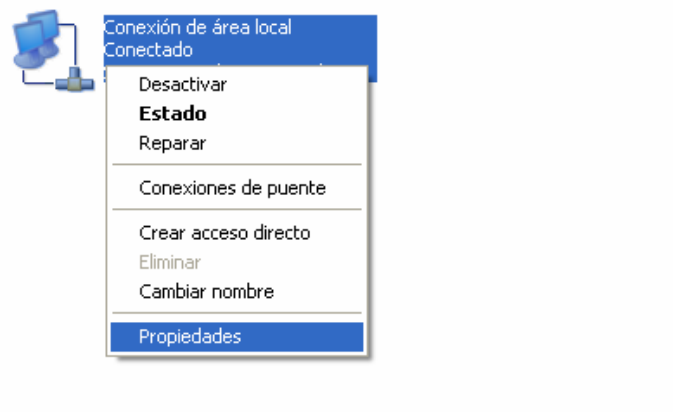


Figura 5.12 Paso 3 Para Deshabilitar TCP/IP En Windows

Paso 4 Des-seleccionar la casilla del protocolo IP y con esto se finaliza el proceso.

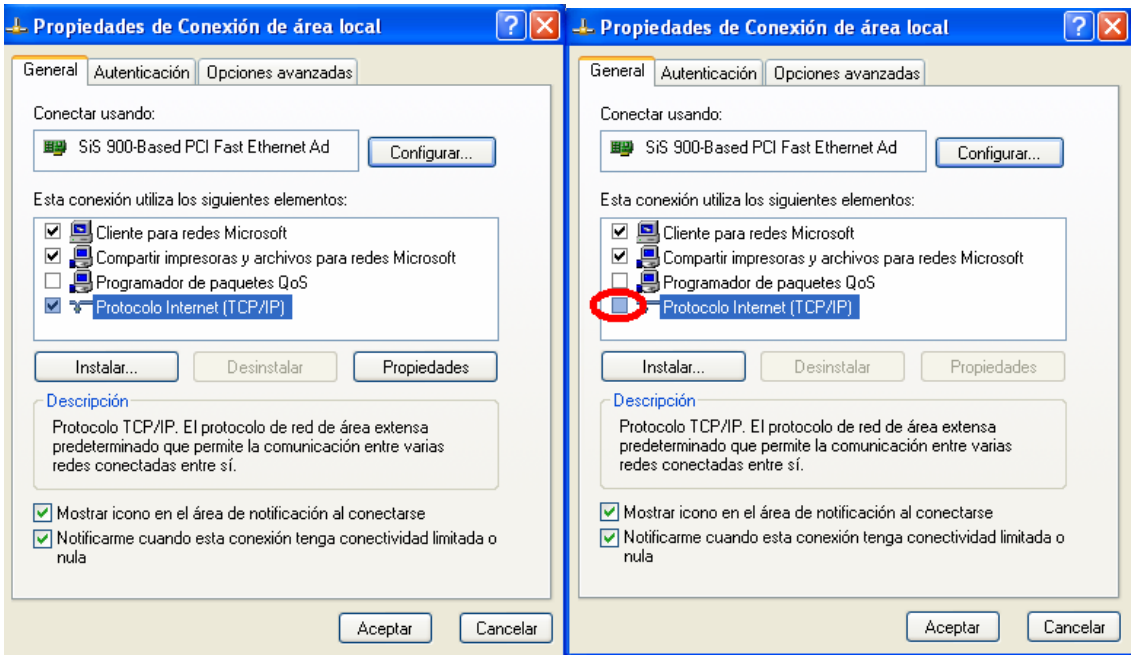


Figura 5.13 Paso 4 Para Deshabilitar TCP/IP En Windows.

Hay que tomar en que existe una herramienta llamada FakeAP (www.blackalchemy.to/project/fakeap/). FakeAP puede ser configurado para generar cientos de Access Points falsos. Una persona que este cerca de un sistema configurado con FakeAP podrá detectar cientos de Access Points, dado que FakeAP genera frames con SSIDs y direcciones MAC creadas virtualmente. Para una persona es virtualmente imposible saber si un Access Point es real o es generado vía FakeAP.

Ahora que TCP/IP esta deshabilitado la tarjeta inalámbrica no se podrá conectar a ninguna red. Por lo que el software para Wardriving trabajara perfectamente sin conectarse a una red y a si no ser detectado. Una ves que se requiera conectarse a una red solo hay que habilitar otra vez el protocolo TCP/IP y asi trabajar de manera normal.

.

5.3 Software de Auditoria

5.3.1 Ethereal

Ethereal es uno de los analizadores de paquetes de red más populares. Un analizador de paquetes de red tratara de capturar los paquetes de la red y mostrara los datos del paquete lo más detalladamente posible. Se puede decir que un analizador de paquetes de red es un dispositivo de medición que es usado para saber que pasa dentro del cable de red. En el pasado este tipo de herramientas era muy costosas o propietarias. La ventaja de Ethereal es que es totalmente gratuito.

Usos comunes de Ethereal:

- Los Administradores de red lo usan para investigar problemas existentes.
- Los ingenieros en seguridad lo usan para examinar problemas de seguridad.
- Los desarrolladores lo usan para corregir implementaciones de protocolos.
- La gente lo usa para aprender el funcionamiento interno de los protocolos de red.

Estos son algunos usos y puede usarse en otras situaciones.

Entre las características de Ethereal estas son las más importantes:

- Disponible para sistemas operativos Unix y Windows.
- Captura en tiempo real de interfaces de red.
- Muestra los paquetes con información detallada.
- Pude guardar y abrir datos de paquetes capturados.
- Filtrado de paquetes por criterios establecidos.
- Búsqueda de paquetes por criterios.
- Muestra los paquetes en diferentes colores basado en el filtrado de paquetes.
- Crea varias estadísticas etc.

5.3.1.1 Usando Ethereal

Usar Ethereal es básicamente lo mismo no importando el sistema operativo, dado que esta basado en una interfaz grafica GUI. Una vez que Ethereal es iniciado se vera la siguiente pantalla (figura 5.14), en la cual se muestra la siguiente información.

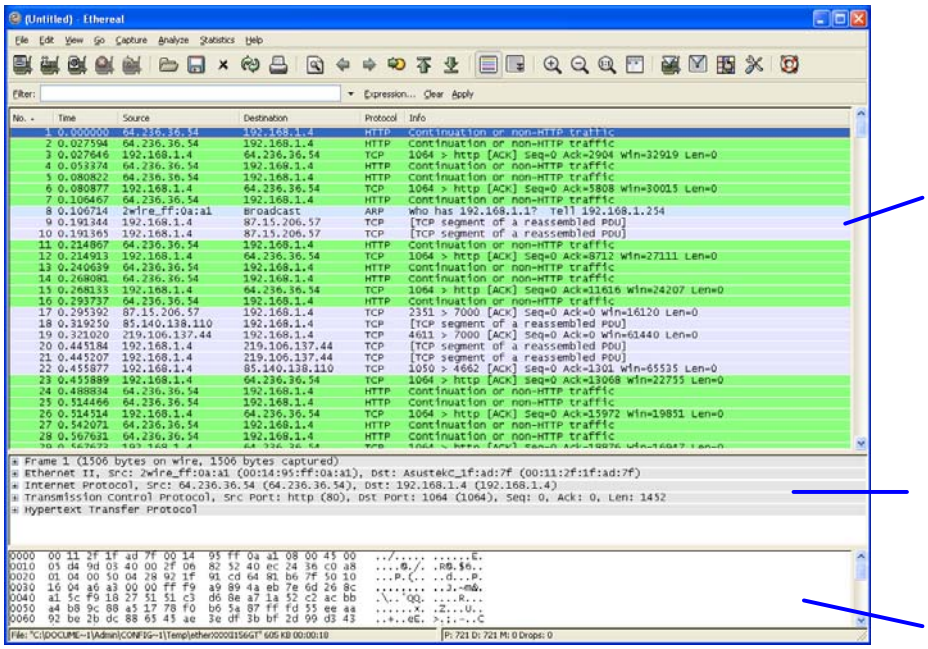


Figura 5.14 Pantalla De Ethereal.

- Resumen del Paquete: Aquí se muestra una lista de los paquetes capturados en el cual se incluye el numero de paquete, la dirección origen y destino, el protocolo y otra información del paquete.

- Detalle del Paquete: Esta ventana contiene la información mas detallada del paquete, dirección MAC, dirección IP, información de la cabecera del paquete, tamaño del paquete, entre otros. Aquí se puede ver lo mas importante, el contenido del paquete.

- Hex Dump: Este campo contiene tres campos de información más comunes en los analizadores de paquetes. El campo de la izquierda muestra el valor de memoria del paquete, el campo de en medio muestra los datos en valor hexadecimal y el campo de la derecha muestra los datos en código ASCII. En esta sección se puede ver tal y como es enviada la información carácter por carácter.

5.3.1.2 Configuración De Ethereal

El uso de Ethereal puede ser muy simple. Al instalar Ethereal ya esta pre-configurado para analizar paquetes lo único que se tiene que configurar es seleccionar el dispositivo de red de donde se desean capturar los paquetes.

Para empezar a capturar los paquetes, la tarjeta de red debe estar instalada. Si se esta utilizando una tarjeta inalámbrica se tendrá que estar cerca del Access Point o utilizar una antena externa para poder capturar los paquetes. Si se usa Linux es más probable que se puedan capturar los paquetes de los Access Points o de routers inalámbricos. Si se usa Windows solo se podrán capturar datos locales de la tarjeta inalámbrica.

5.3.1.3 Flujo De TCP

Ethereal cuenta con una opción que puede reconstruir los datos del flujo TCP capturado. Para hacer esto tenemos que empezar a capturar paquetes, después de contar con algunos paquetes capturados podemos ver el flujo de TCP. En la figura 5.15 se muestra un flujo TCP de una conversación de Messenger en la cual podemos ver todos los datos escritos en esta. Esto puede ser útil una vez que se tenga la clave WEP de la red inalámbrica, se puede empezar a recabar información como contraseñas, nombres de usuario, información de cuentas etc[13].

[13] EUG-1

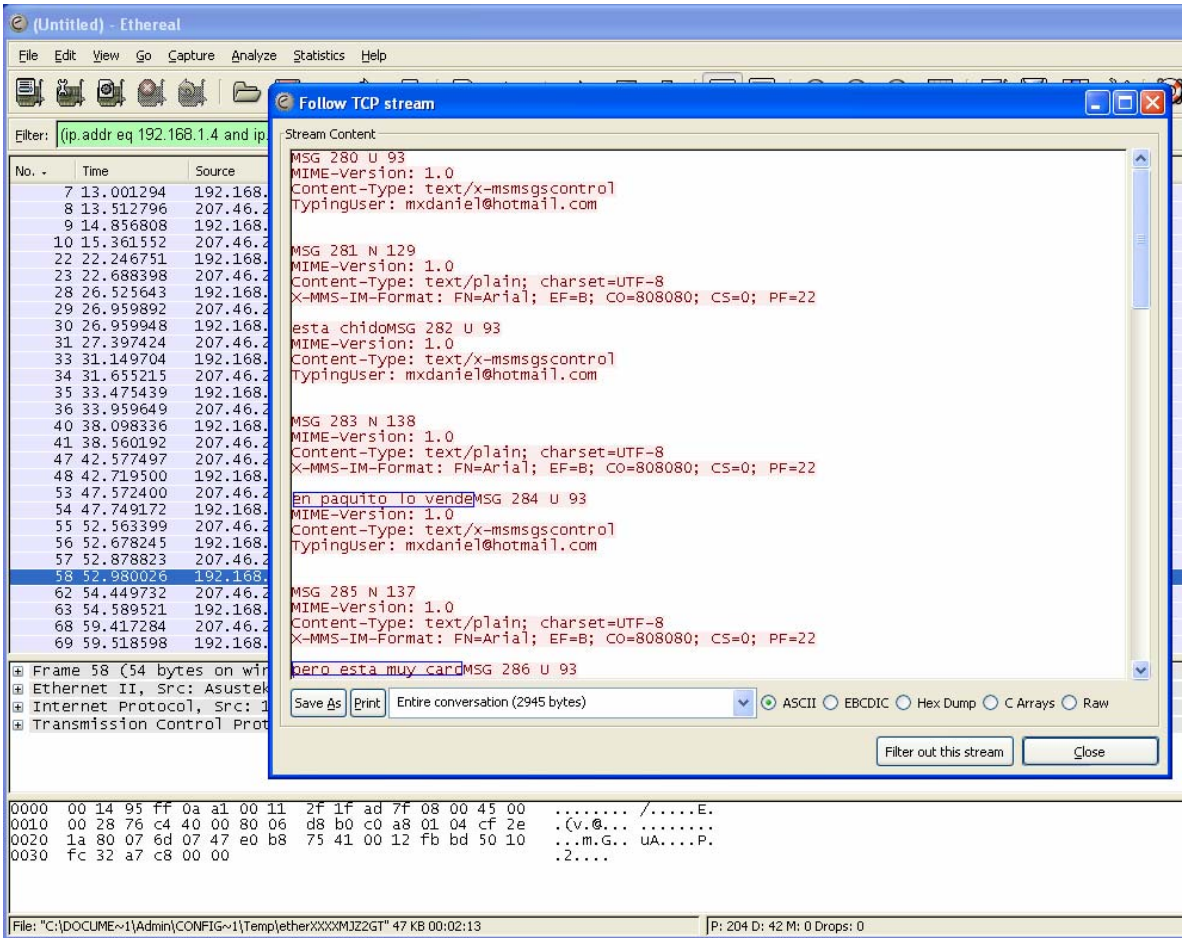


Figura 5.15 Seguimiento De Flujo TCP En Ethereal.

Como se puede ver Ethereal tiene un uso infinito es por eso que se considera una herramienta indispensable tanto como para los administradores de redes como para los hackers. Es importante codificar los datos para evitar que este tipo de programas puedan capturar nuestra información e invadir nuestra privacidad.

5.3.2 NetStumbler

NetStumbler es una de las mejores herramientas para detectar redes inalámbricas en Windows. Incluye varias características como detección fuerza de la señal, SSID, Canal de transmisión, Soporte para GPS, entre otros. Este programa ha afectado el mundo de las redes inalámbricas significantemente debido a que es una herramienta estupenda para configurar redes inalámbricas, pero también puede ser utilizada para fines de Wardriving.

Usos comunes de NetStumbler.

- Detectar Access Points.
- Verificar la configuración de la red inalámbrica.
- Medir la cobertura de la señal, así como la fuerza.
- Sirve para orientar antenas direccionales para enlaces de larga distancia.

5.3.2.1 Usando Netstumbler

Al abrir el programa nos se vera una pantalla parecida a la mostrada en la figura 5.16. En la columna principal se muestra un icono el circular el cual nos indica si el Access Point cuenta con encriptación así como el color nos indica la intensidad de la señal. Los distintos colores son los siguientes:

- Gris: No Hay Señal.
- Rojo: Señal Pobre O Con Ruido.
- Naranja: Señal Regular.
- Amarillo: Señal Buena.
- Verde Claro: Señal Muy Buena Y Fuerte.
- Verde Oscuro: Señal Excelente y Óptima.

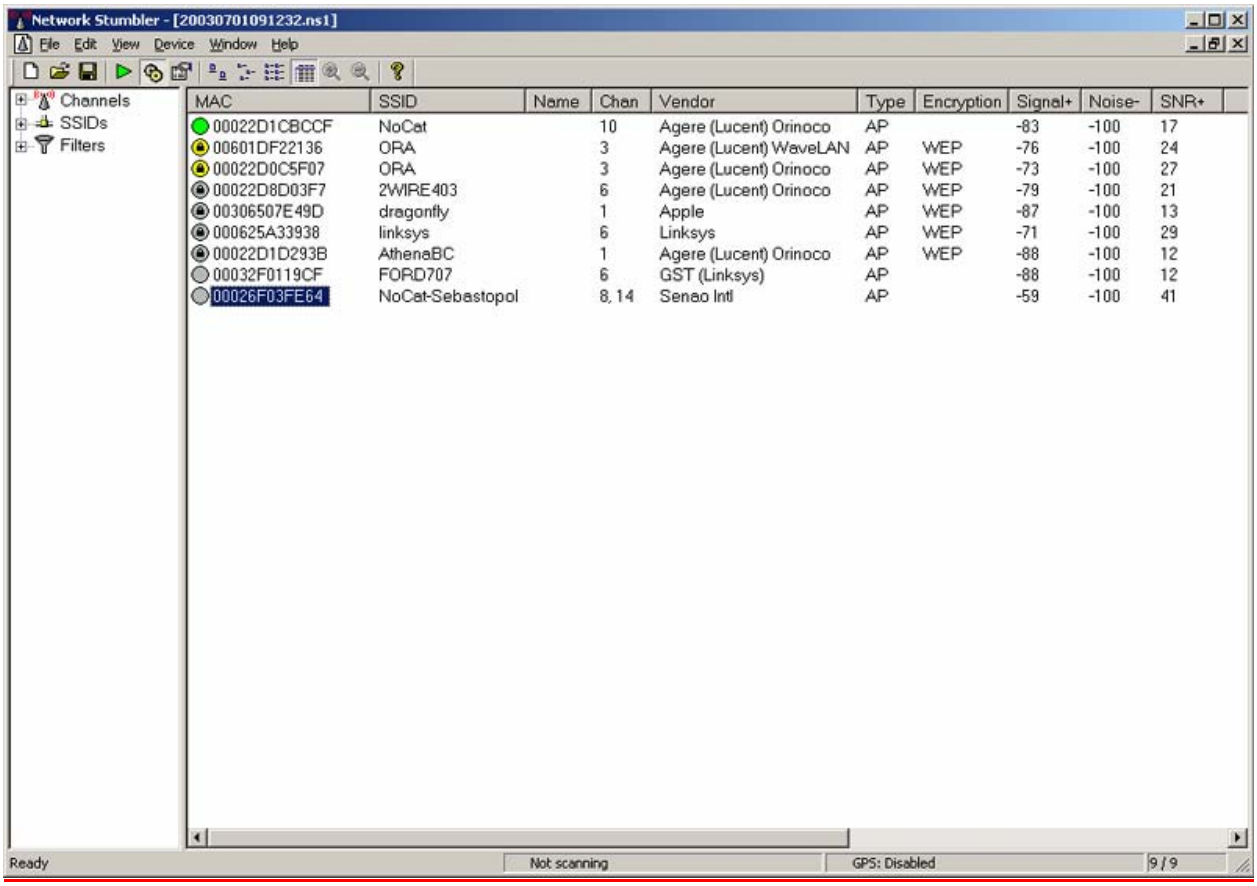


Figura 5.16 Pantalla Principal De Netstumbler.

Las otras columnas nos muestran los datos de la red como dirección MAC del Access Point, SSID, Nombre del AP, Canal de transmisión, velocidad de transmisión, vendedor, Codificación WEP entre otras.

Al seleccionar la red tenemos la opción para ver una grafica de señal de ruido en la cual nos indica la calidad y cantidad de la señal (figura 5.17). La parte verde indica el nivel de la señal, la parte roja indica el nivel de ruido, la parte entre la parte roja y la parte verde es el ratio de la señal-ruido (SNR).

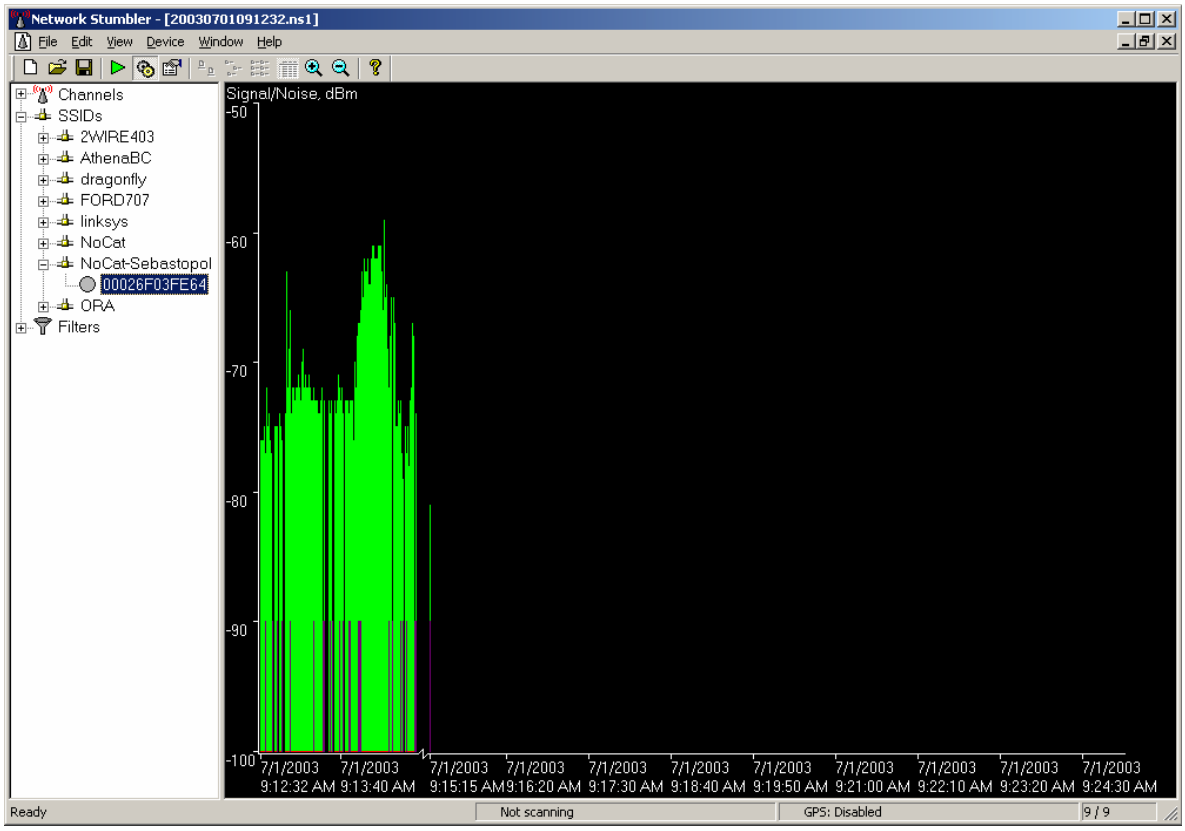


Figura 5.17 Grafica De La Comparación Señal-Ruido.

Como se puede notar Netstumbler es una excelente herramienta tanto como para configurar, implementar y buscar redes inalámbricas. Su uso en el wardriving es principalmente para buscar redes y recabar datos de estas brindando datos muy importantes.

5.3.3 Kismet

Kismet es un capturador de paquetes gratuito que incluye varias herramientas. Soporta los chipsets Prims2 de tarjetas inalámbricas. Kismet es capas de capturar datos de múltiples fuentes y puede guardar los datos capturados en un formato compatible con Ethereal. Su uso principalmente es para analizar redes inalámbricas y para encontrar llaves WEP. El funcionamiento de kismet es completamente diferente al Netstumbler. La tarjeta de red trabaja en modo monitor esto significa que nuestra tarjeta de red inalámbrica no emite ninguna señal solo recibe las señales inalámbricas. Si la tarjeta no soporta el modo monitor en Linux Kismet no funcionara.

Usos comunes de Kismet:

- Detectar Access Points.
- Verificar la configuración de la red inalámbrica.
- Detectar redes cercanas que puedan causar interferencia..
- Detectar problemas de conectividad.

Diferencia entre Kismet y Netstumbler:

- Kismet Trabaja En Modo Monitor (Promiscuo).
- Kismet Muestra Información De Clientes Conectados A La Red.
- Kismet Permite Guardar La Información Capturada A Un Archivo.

5.3.3.1 Usando Kismet

Kismet puede ser usado en modo cliente/servidor en el cual el programa admite conexiones remotas al programa. Se puede instalar en algún lado y dejar trabajando y acceder a el vía remota para monitorear las actividades de una red inalámbrica. Kismet cuenta con una interfaz grafica llamada ncurses. Ncurses es una especie de GUI en la cual se muestra la información de la red inalámbrica así como los comandos que se pueden ejecutar. En la figura 5.18 se muestra la pantalla de ncurses.

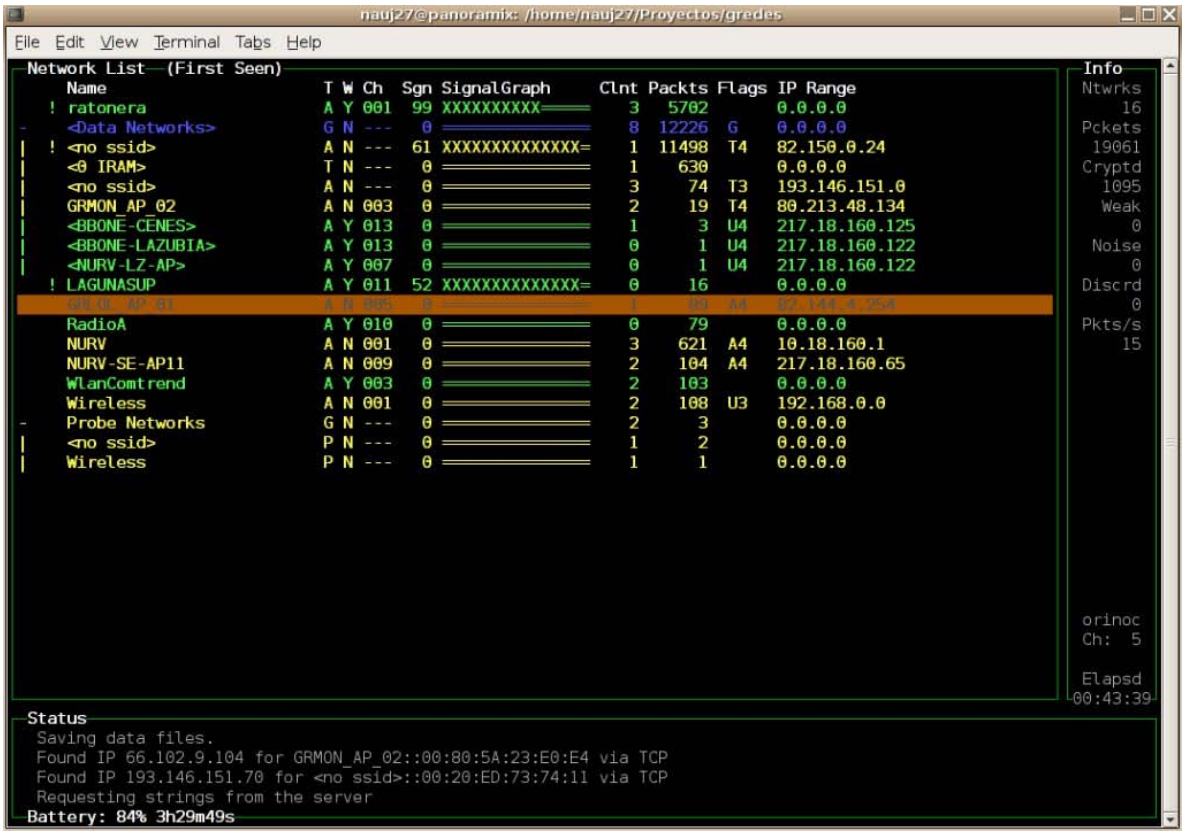


Figura 5.18 Pantalla Grafica De Kismet.

Para ejecutar kismet necesitamos primero habilitar la tarjeta de red y ponerla en modo monitor, todo esto vía línea de comandos en la shell de Linux.

 # ifconfig <interface> up

En el campo de l <interface> ponemos el nombre de nuestra tarjeta de red por ejemplo ath0 o eth0. Una vez que la tarjeta esta habilitada la tendremos que poner en modo monitor para hacer esto ejecutamos el siguiente comando:

 # iwconfig <interface> mode monitor

Ahora que nuestra tarjeta de red inalámbrica esta en modo monitor podemos iniciar kismet.

 # Kismet

En la ventana principal (figura 353533) nos muestra la grafica los datos mas importantes de nuestra red como son: nombre de la red, estado de la señal, grafica de la señal, numero de clientes, paquetes recibidos, y dirección IP. Para salir de Kismet solo hay que presionar la tecla Q. Como se ha visto kismet tiene muchas opciones así como usos el programa puede guardar todos los datos que captura en archivos. Kismet en definitiva es un programa que se debe tener para auditar redes inalámbricas. Para conocer mas el uso de kismet se recomienda visitar su página donde se puede ver la documentación necesaria así como solventar dudas, la página es la siguiente:
http://www.kismetwireless.net/documentation.shtml.

5.3.4 BackTrack

Backtrac es la evolución de Auditor, que fue su primera versión. Backtrack es una colección de herramientas de seguridad basado en un live-cd de Linux. El sistema arranca directamente del CD-Rom si necesidad de instalarlo en el disco duro. Este incluye herramientas de todo tipo para auditorias en seguridad informática, sus principales herramientas están divididas en los menús: Foot-printing, analysis, scanning, wireless, brute-forcing, cracking.

Las herramientas principales para el Wardriving que se incluyen en esta distribución son las necesarias para hacer una auditoria a una red inalámbrica. Su pantalla principal se muestra en la figura 5.19.

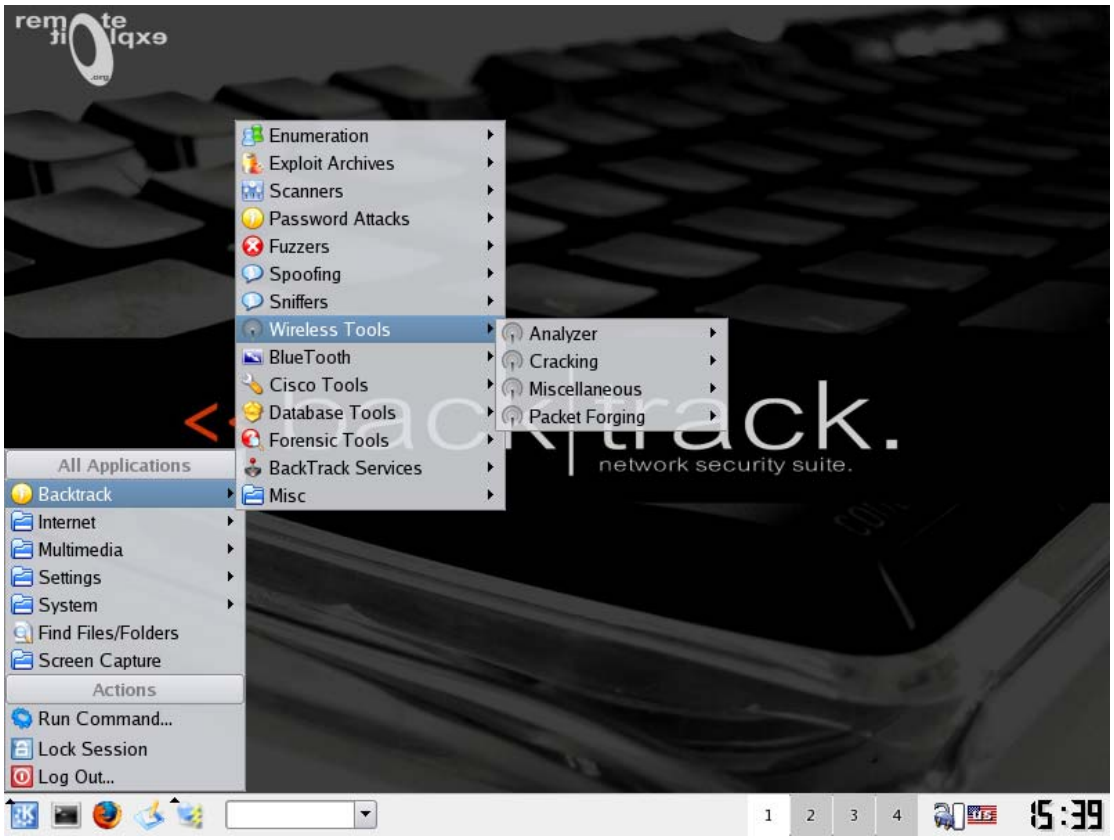


Figura 5.19 Pantalla Principal De Las Utilerías De Backtrack.

Muchas de las herramientas están configuradas para que al arrancar el cd detecte el hardware automáticamente y lo configure, como es el caso de Kismet, esto ayudando a evitar instalar la tarjeta inalámbrica.

5.3.4.1 Requerimientos De Backtrack

Al ser Backtrack una distribución Linux no necesita muchos recursos de hardware por lo cual en casi computadora puede funcionar, los requerimientos mínimos para un funcionamiento con interfaz grafica son los siguientes:

- CD-ROM.
- 144 MB en memoria Ram.
- Pentium o superior.
- Mouse y Teclado.
- No se requiere disco duro ya que todo se carga en la memoria ram.

Este programa es de los mejores complementos para seguridad informática y es totalmente gratuito se puede descargar una imagen del disco de la página principal del proyecto en la dirección:

http://www.remote-exploit.org/

5.3.4.2 Programas Para Auditoria Inalámbrica

Entre los programas mas importantes que se incluyen en backtrack son los siguientes:

- Scripts Con Drivers Para Diferentes Tarjetas Inalámbricas.
- Air Crack. (WEP Cracker)
- Kismet. (Buscador De Redes Inalámbricas)
- File2air (Inyector De Paquetes)
- GPSMAP (Mapeo De Redes Inalámbricas)
- Wellenreiter (Buscador Grafico De Redes Inalámbricas)
- Airodump (Capturador De Trafico)
- Aireplay (Inyector De Paquetes)
- Wep_Crack (Wep Cracker)

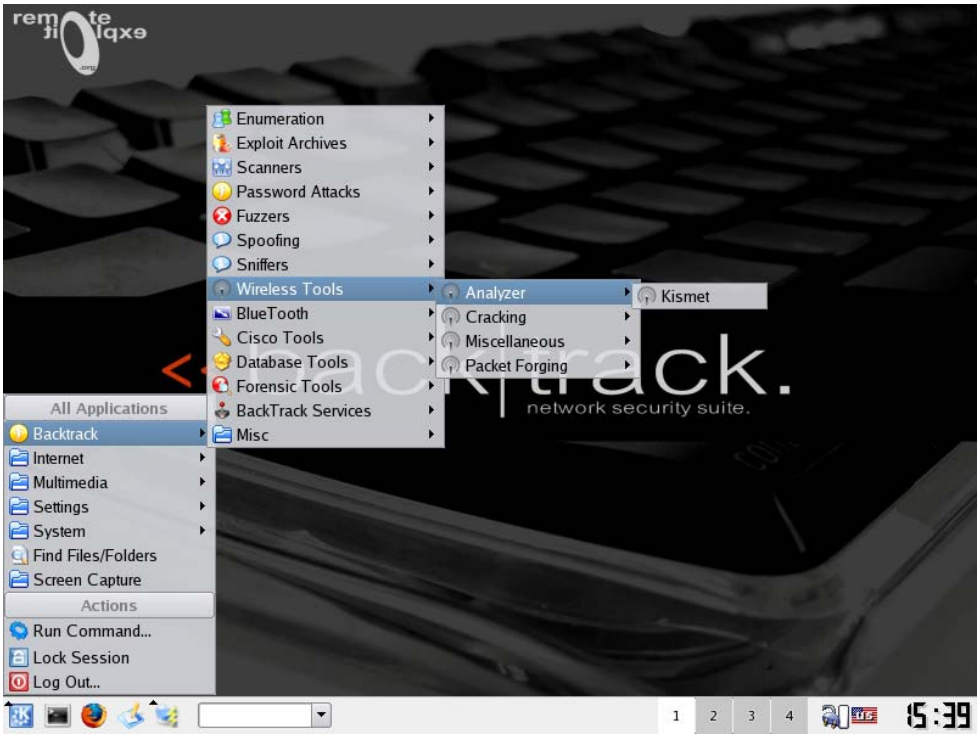


Figura 5.20 Pantalla De Las Utilerías Para Redes Inalámbricas De Backtrack.

5.4 Ejemplo De Decodificación De Llave WEP

Paso 1 Primero se inicializa la tarjeta de red (eth0) desde la línea de comando (shell) y se pone en modo monitor con los siguientes comandos:

```
# ifconfig eth0 up
# iwconfig eth0 mode monitor
```

Paso 2 Una vez que ya tenemos la tarjeta de red inalámbrica en modo monitor tenemos que montar la unidad USB (son1) donde vamos a guardar los datos capturados para poder crackear la llave WEP:

```
# cd \
# cd mnt
# mount /dev/son1 /mnt/son1
# cd son1
```

Paso 3 Una vez que tenemos la unidad montada donde se van a guardar los paquetes capturados iniciamos airodump para capturar los paquetes con el siguiente comando:

```
# airodump eth0  captura.cap
```

Hecho esto nos saldrá una ventana parecida a la de la figura 5.21.

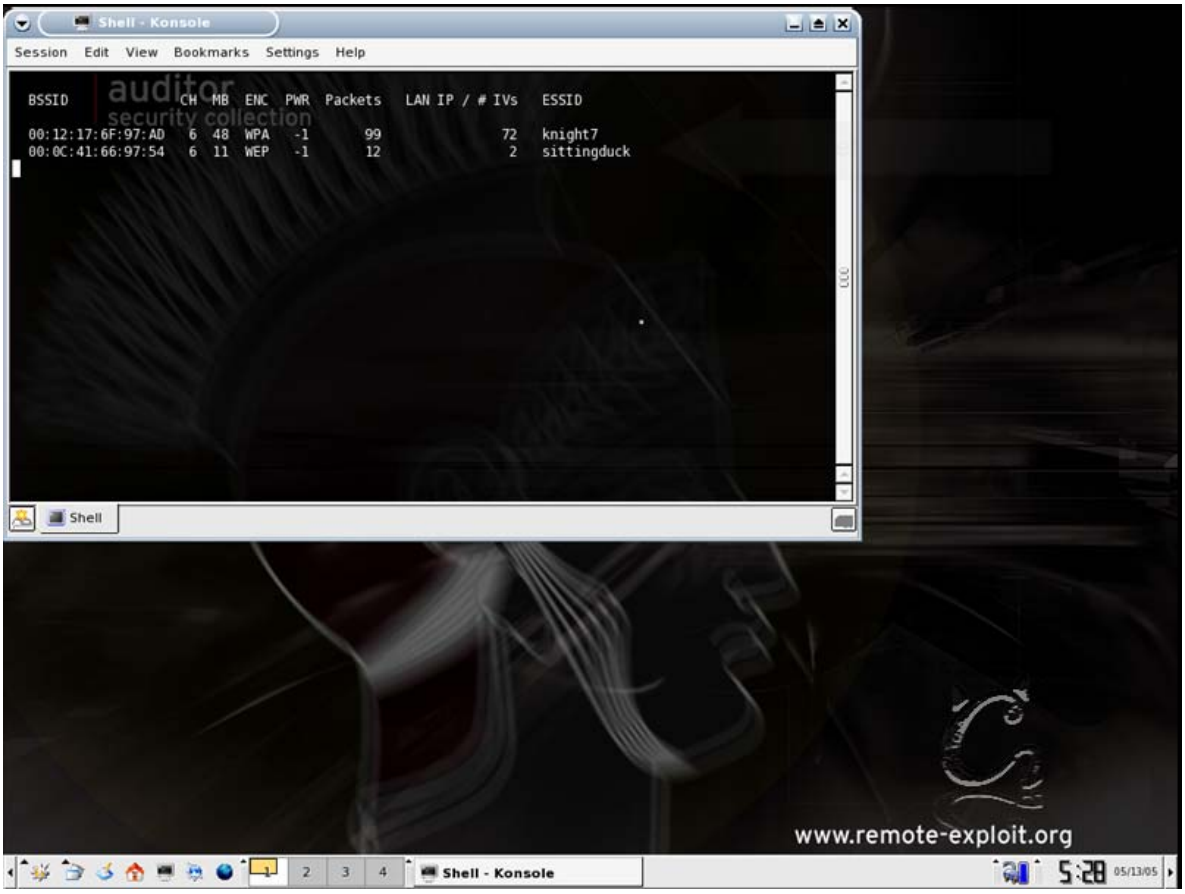


Figura 5.21 Pantalla De Ejecución De Aerodump.

Paso 4 Al paso del tiempo se podrá observar el flujo de paquetes en la red así como los IVs que son los que utilizamos para crackear la clave WEP. Dado que el flujo de datos es muy lento tendremos que inyectar paquetes en la red para que el flujo se incremente con el programa Aireplay como se muestra en la figura 5.22. Tendremos que seleccionar la red a la que se van a inyectar los paquetes basados en su BSSID para asegurarnos que solo a esa red se inyecten los paquetes.

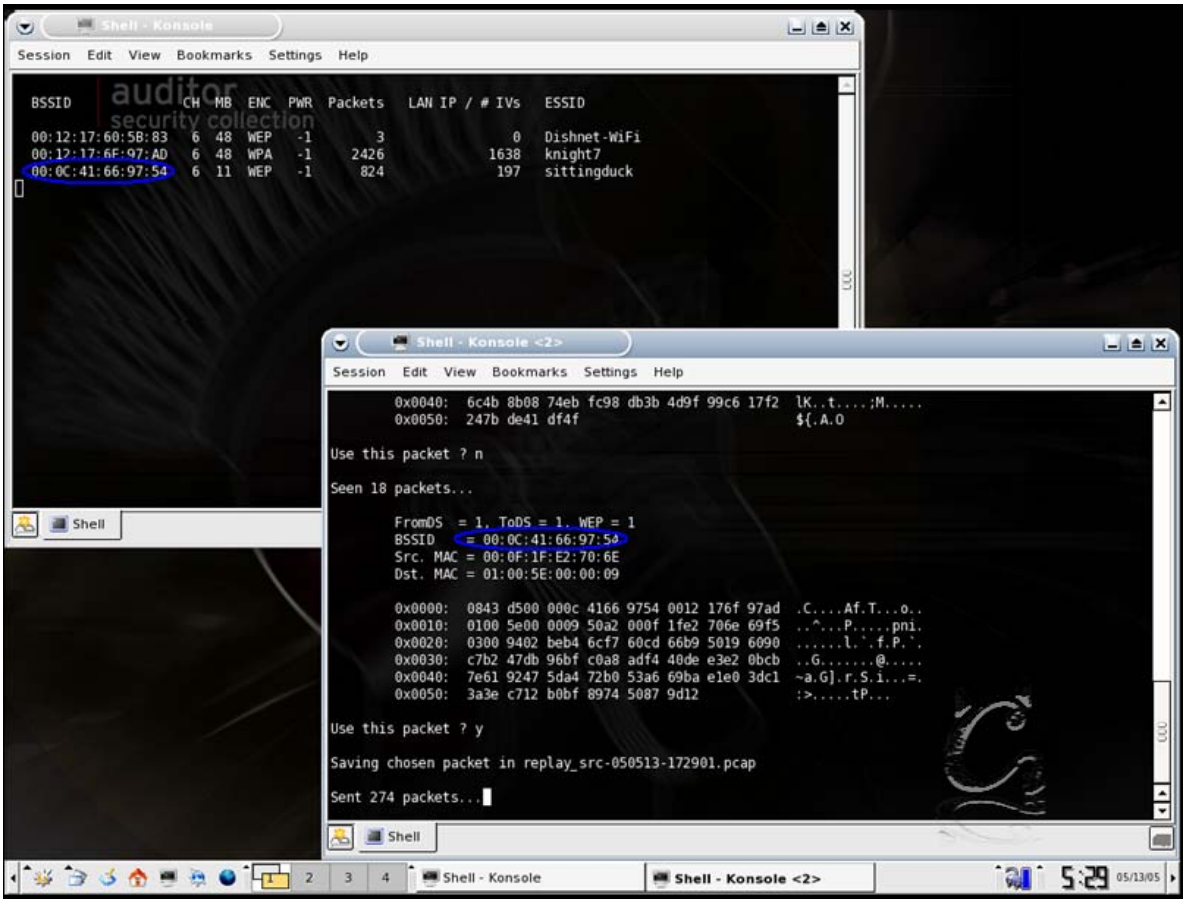


Figura 5.22 Pantalla De Ejecución De Aireplay.

Se necesitan inyectar los suficientes paquetes para que aumente el IV y así sea mas fácil encontrar la llave WEP, se recomiendo por lo menos inyectar paquetes hasta que los IV capturados lleguen mínimo a 500 000, se puede ver un ejemplo en la figura 5.23 donde se ven los IVs.

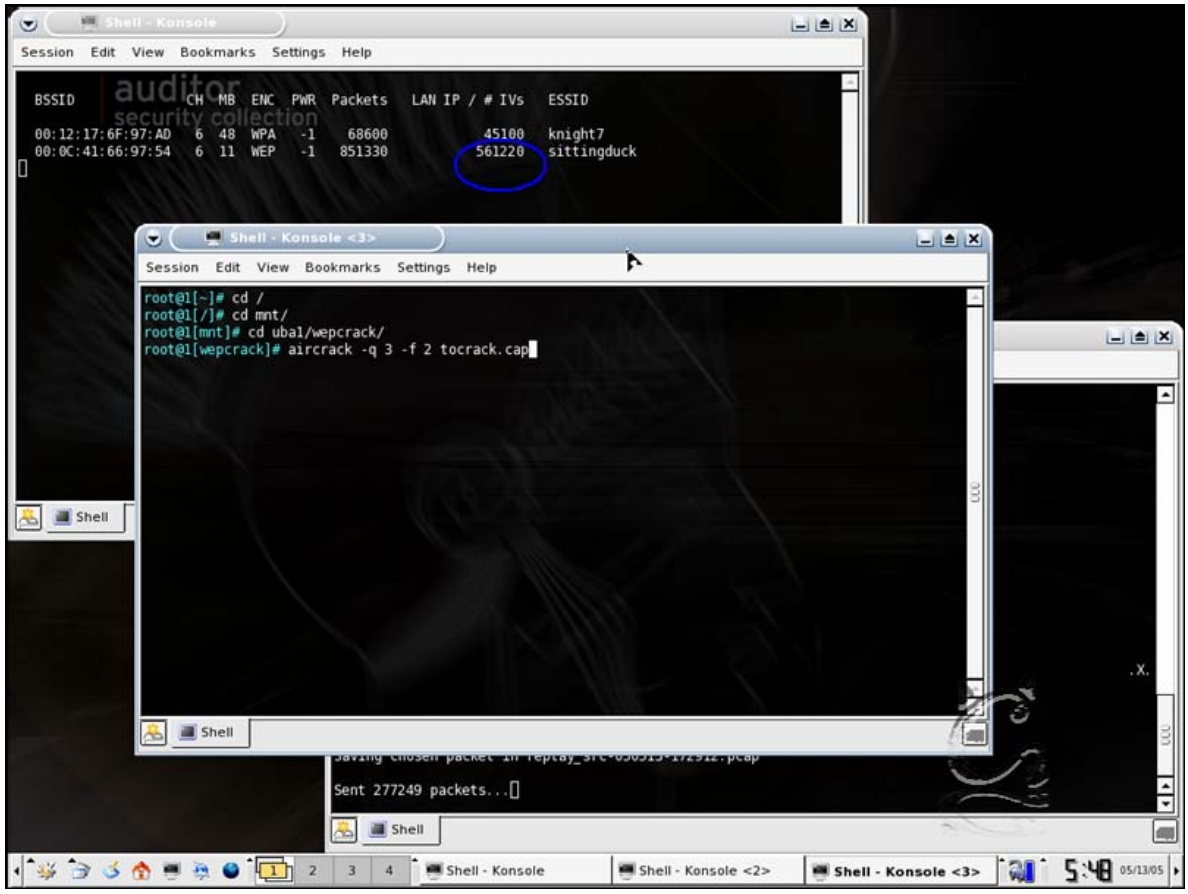


Figura 5.23 Pantalla De Ejecución De airodump.

Paso 5 Una ves que se tienen lo suficientes IVs se procede a crackear la llave WEP con el programa aircrack y el archivo donde se capturaron los paquetes en este caso captura.cap con los siguientes comandos:

aircrack –q 3 –f 2 captura.cap

El proceso no tomara mucho tiempo para encontrar la llave WEP al terminar se mostrara una pantalla con la llave descifrada como se puede ver en la figura 5.24.

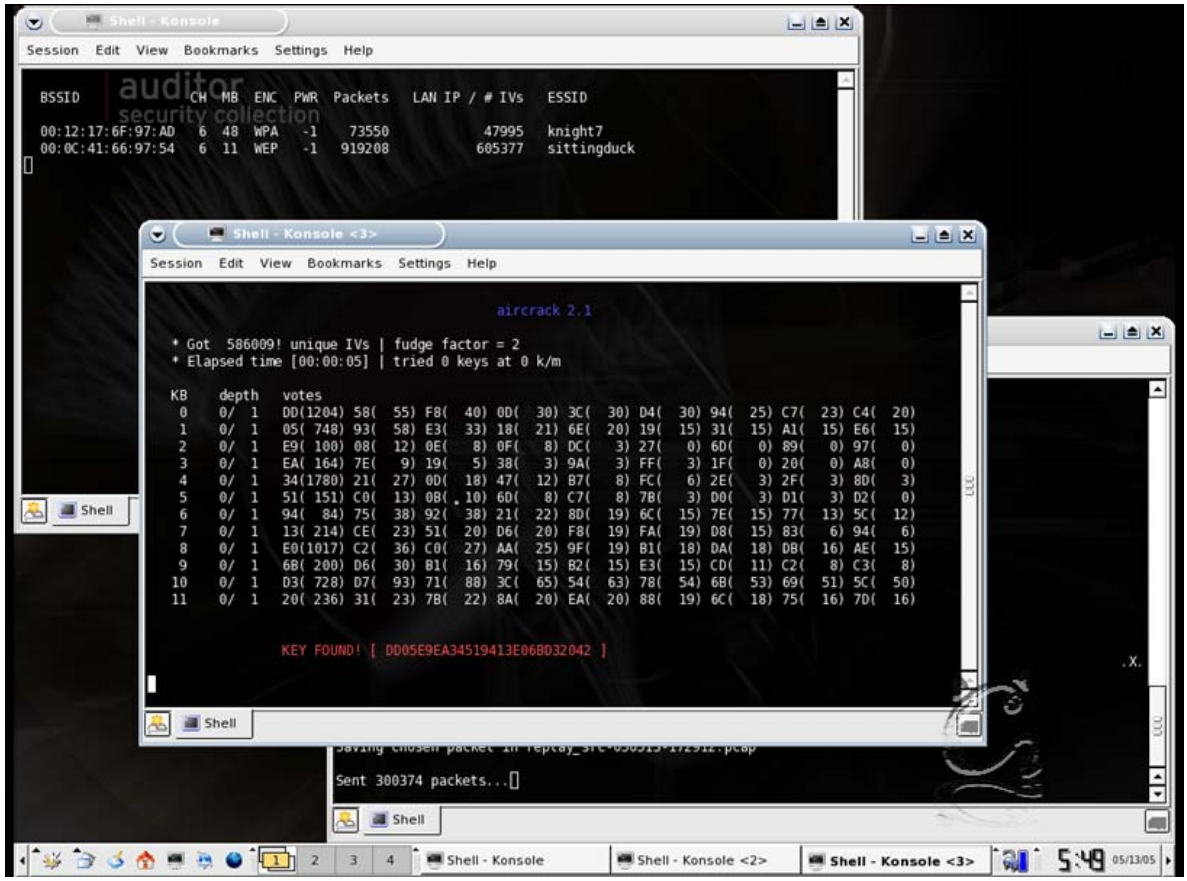


Figura 5.24 Llave WEP encontrada.

Paso 6 Una ves que se encontró la llave la podemos utilizar para conectarnos a la red con el siguiente comando:

iwconfig ath0 mode managed key 1A:43:DC:4C:9D:8B:47:CC:55:CD

Para obtener una dirección IP vía DHCP.:

dhcpcd eth0

Finalmente ya estamos dentro de la red.

CONCLUSIONES

Con la evolución de las telecomunicaciones, la forma mas viable de comunicación es la inalámbrica debido a que nos provee movilidad y capacidad de hacer otras cosas al mismo tiempo. Las redes inalámbricas han evolucionado mucho en estos últimos años, las velocidad de trasmisión crecen así como los fabricantes de hardware. Estos basan sus diseños en funcionalidad dejando descuidados los factores de seguridad.

Al utilizar las redes inalámbricas el medio de transmisión de las ondas de radio frecuencia es el aire. Al no poder limitar este, existe la posibilidad de que otras personas puedan recibir las señales, por eso es importante establecer los mecanismos de seguridad necesarios. Como se vio en este trabajo casi ningún medio de transmisión es totalmente seguro pero se puede hacer más difícil de vulnerar aplicando técnicas de codificación y autentificación. Es de suponerse que depende el tipo de ambiente en donde se despliegue la rede inalámbrica van a ser las medidas de seguridad, no es lo mismo asegurar una red empresarial que una red domestica o una peque empresa.

En las redes domesticas se puede optar por habilitación del protocolo WEP de 128 bits de codificación o con un sistema de llaves preestablecidas como PSK. Esto es más que suficiente para que se evite que un usuario normal acceda a nuestra red.

En el sector empresarial se corre con diferentes tipos de riesgos desde los empleados resentidos o curiosos, hasta los competidores. En este tipo de ambiente se necesita establecer un nivel de seguridad que tiene que ver con el diseño e implementación de la red, hasta las políticas de usuarios.

Al configurar la red inalámbrica en estos ambientes se deben de establecer los medios más fuertes de seguridad sin restar la facilidad y funcionalidad de uso. Lo más recomendable es un sistema de autentificación tipo Kerberos o RADIUS para los Access Points. Si la red inalámbrica es usada solo para clientes de negocios así como visitantes en general, se puede separar la red para que a esta no pueda entrar a la red local.

La tecnología crece así como los conocimientos de los usuarios, es importante asegurarnos de que cuando salga una nueva tecnología no comprar la primera generación de dispositivos, hay que esperar un cierto tiempo para ver si esa tecnología tiene futuro y es segura. Al comprar dispositivos electrónicos hay que informarnos así como leer los manuales de usuario para evitar problemas. No es recomendable usar los dispositivos con configuraciones de fábrica dado que estas pueden no tener habilitadas las opciones de seguridad.

Este trabajo trato demostrar las herramientas y métodos usados para encontrar una llave WEP y entrar en una red inalámbrica. Actualmente esto lo puede hacer cualquier persona con conocimientos básicos en redes, pero es importante el saber las causas de por que pasan las cosas para encontrar soluciones eficaces.

Creo que el propósito se cumplió, las cosas que aprendí fue acerca de las redes inalámbricas así como del sistema operativo Linux entre otras Este trabajo represento un reto personal para obtener unas de las cosas necesarias para alcanzar mis metas.

REFERENCIAS

[1] Gatrner-1 — **Christy Pettey**, Articulo Titulado “Gartner Says Wireless LANs are the Major Wireless Security Problem Facing Businesses Through 2008, Analysts Discuss How to Secure a Wireless Network at Gartner IT Security Summit 2004 “ , Gartner, 2004. http://www.gartner.com/press_releases/asset_88267_11.html

[2,6] CWNA-1 — **Planet3 Wireless**, Certified Wireless Network Administrator Official Study Guide, Planet3 Wireless, 2002 USA, ISBN: 0-9716057-2-6

[3,4,5] BSWN-1 — **Jahanzeb Khan, Anis Khwaja**, Building Secure Wireless Networks with 802.11, Wiley Publishing, 2003 USA, ISBN 0−471−23715−9

[7] HSIYN-1 — **Lee Barken**, How Secure Is Your Wireless Network? Prentice Hall, 2003 USA, ISBN : 0-13-140206-4

[8] MWS-1 — **Cyrus Peikari, Seth Fogie**, Maximum Wireless Security, Sams Publishing, 2002 USA, ISBN : 0-672-32488-1

[9] IMDB-1 — Writing credits **Lawrence Lasker & Walter F. Parkes ,** Directed by John Badham, WarGames , Metro Goldwyn Mayer 1983 USA, http://www.imdb.com/title/tt0086567/

[10] WDDD-1 — **Chris Hurley, Michael Puchol, Russ Rogers**, WarDriving: Drive, Detect, Defend: A Guide to Wireless Security, Syngress Publishing 2004 USA, ISBN:1931836035

[11] EBAY-1 — http://stores.ebay.com/War-Driving-World

[12] EBAY-2 — http://stores.ebay.com/War-Driving-World_Wardriving-Kits

[13]EUG-1 **Ulf Lamping, Richard Sharpe,** Ethereal User's Guide 18189 for Ethereal 0.10.14, 2004-2005. http://www.ethereal.com/docs/

PAGINAS WEB

802.11 Planet.com
hwagm.elhacker.net
stores.ebay.com/War-Driving-World
Wlana.org
www.cwnp.com/cwna
www.ethereal.com
www.kismetwireless.net
www.netstrumbler.com
www.remote-exploit.org
www.wardriving.com

GLOSARIO

Access Point (AP): Dispositivo centralizado inalámbrico que controla el tráfico en una red inalámbrica. Todo el tráfico entre las computadoras que se comunican debe pasar a través del Access Point.

ACK (Confirmación): Notificación enviada desde un dispositivo de red a otro para confirmar que ocurrió cierto evento (por ejemplo, la recepción de un mensaje).

Asynchronous Transfer Mode (ATM): Modo de operación de la banda ancha. Toda la información que viaja en red vía ATM, primero es divida en pequeños fragmentos de un mismo tamaño llamadas celdas. Entonces son enviadas en la red.

Autentificación: Mecanismo para asegurarse de que un usuario es el que dice ser. La autentificación más común es cuando se accede a la red o a una cuenta de correo.

ASCII (American Standard Code for Information Interchange): Código estándar americano para intercambio de información. Sistema de codificación de 7 bits que asigna un número del 0 al 127 a cada letra, número, caracteres especiales.

Caballo de Troya: Programa el cual contiene código adicional escondido, desarrollado para obtener algún tipo de información o causar algún daño, principalmente para espiar.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA): Un método similar a CSMA/CD y es usado para reducir las colisiones entre paquetes en una red que comparte el medio de transmisión.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD): Es un metodo que es usado para controlar el acceso a un medio de transmisión compartido como cable para evitar colisiones y errores de transmisión.

Challenge Handshake Authentication Protocol (CHAP): Protocolo de autentificación en el cual cliente y servidor usan claves que han sido pre-configuradas en cada sistema. En CHAP toda la información incluyendo nombres de usuario y contraseñas se transmiten codificadas en la red.

Computer Memory Card International Association (PCMCIA): es una tarjeta utilizada en computadoras portátiles para expandir las capacidades de esta. Se usan para ampliar capacidades en cuanto a: memoria, disco duro, tarjeta de red, capturadora de radio y tv, puerto paralelo, puerto serial, puerto USB, etc. Las tarjetas PCMCIA de 16 bits pueden recibir el nombre de PC Card y las de 32 bits el de CARD BUS.

Cyclic−Redundancy−Check (CRC): Método usado en para detectar errores en la transmisión de datos. CRC es un valor numérico calculado en base a los datos a enviar, el destinatario tiene que realizar el mismo proceso para asegurarse que los datos han llegado con éxito sin modificaciones u errores.

Denial of Service (DoS): Tipo de ataque en el cual un adversario hace múltiples peticiones a un host manteniéndolo ocupado para evitar que conteste peticiones de usuarios genuinos.

Conexión Dial-Up: Tipo de conexión de red que se establece comunicando dos hosts usando módems conectados a la línea telefónica.

Digital Subscriber Line (DSL): Tipo de conexión de banda ancha en la que se provee una conexión de alta velocidad usando el mismo par de cables de la línea telefónica.

Direct Sequence Spread Spectrum (DSSS): Método de transmisión en redes inalámbricas en la cual la señal ocupa toda la banda disponible resultando en una transmisión más susceptible a interferencias.

Distribution System Service (DSS): Servicios que se proveen e redes inalámbricas LAN. DSS provee 5 servicios básicos: Asociación, reasociación, disasociación, distribución e integración.

Dynamic Host Configuration Protocol (DHCP): Protocolo de asignación de direcciones IPs dinámicas. Con un sistema de direcciones dinámicas un dispositivo puede tener diferentes direcciones IP cada vez que se conecte a la red.
Firewall : Sistema diseñado para prevenir el acceso no autorizado a una red privada. Los firewalls pueden ser implementados via software o hardware, o en combinación.

Frequency Hopping Spread Spectrum (FHSS): Método de transmisión de redes inalámbricas en el cual la onda portadora de datos oscila en la banda.

Hacker: Una persona que disfruta explorando los detalles de las computadoras y de cómo extender sus capacidades, muchas veces es asociado a alguien con intenciones malévolas.

Handshake (Saludo): Secuencia de mensajes intercambiados entre dos o más dispositivos de red para garantizar la sincronización de la transmisión.

Host: Dispositivo que permite a los usuarios comunicarse con otros sistemas de una red.

Local Area Network (LAN): Red de área local.

Network Interface Card (NIC): Dispositivo hardware que es usado para conectar un dispositivo a la red.

Peripheral Component Interconnect (PCI): Es un tipo de bus para agregar periféricos a la tarjeta madre de la computadora.

Promiscuo (Modo): Interfaz Ethernet que permite leer toda la información sin importar su destino, aplicable a un segmento de Red.

Service Station Identifier (SSID): El SSID es un identificador de hasta 32 caracteres. Este sirve para identificar principalmente redes inalámbricas existentes, se puede configurar en los Access Points.

Shell: Intérprete de comandos de un sistema operativo. Es el que se encarga de tomar las órdenes del usuario y hacer que el resto del Sistema Operativo las ejecute.

TCP/IP (Tranfer Control Protocol/Internet Protocol): Arquitectura de red con un conjunto de protocolos que permiten compartir recursos a través de una red.

Texto Plano: Datos digitales que son transmitidos sin un medio de codificación y que pueden ser descubiertos si se capturan los paquetes en el transcurso de la red.

Wired Equivalent Privacy (WEP): Protocolo de seguridad para redes LAN inalámbricas definido por el estándar 802.11.

Wireless Roaming: Capacidad de las redes inalámbricas que permite a un usuario moverse entre diferentes Access Point sin perder la conexión.