ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"CONSULTORIA PARA LA DETERMINACION DE BRECHAS DE SEGURIDAD EN UNA RED INALAMBRICA"

TESIS DE GRADO

Previa a la obtención del título de:

Ingeniero en Electrónica y Telecomunicaciones

Presentado por:

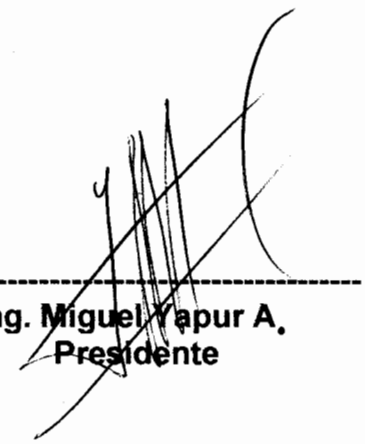
Anabel Fernanda Castillo Mora

Roberto Fernando Cabezas Cabezas

Guayaquil - Ecuador

2006

TRIBUNAL DE GRADUACION

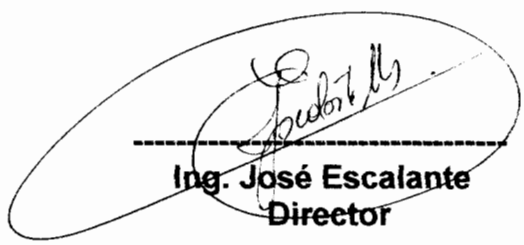


Ing. Miguel Yapur A.
Presidente

Ing. Rebeca Estrada Pico
Miembro Principal

CIB-ESPOL

Ing. Ivonne Martín Moreno
Miembro Principal



Ing. José Escalante
Director

CIB-ESPOL

DECLARACION EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"

Anabel Castillo

Anabel Fernanda Castillo Mora

Roberto F. Cabezas

Roberto Fernando Cabezas Cabezas

A DIOS por ser DIOS y hacerme entender y vivir que todo lo puedo en El que me fortalece, a mi amada Madre y amiga Marcia, a mis ángeles, a mi familia y a todos los míos.

Roberto Cabezas

Dedico esta tesis a mi papá, Raúl, mi mamá, Anabel y mis dos hermanas Sofia y Alejandra. Gracias por ser mi fuerza y mi completo apoyo

Anabel Castillo

RESUMEN

Este proyecto tiene como objetivo evaluar el problema de inseguridad de las redes inalámbricas. Por medio de una consultoría se determina cuales son las brechas de seguridad en la implementación de una WLAN y se presenta sugerencias de posibles implementaciones que refuerzan la seguridad de la red logrando erradicar sus inseguridades.

En el primer capítulo se realiza una breve explicación de lo que es la tecnología inalámbrica, se enumeran las nuevas tendencias de seguridad para la WLAN, y además trata sobre los tipos de ataques en contra de la seguridad de la red inalámbrica, mencionando algunas de las herramientas utilizadas.

El segundo capítulo es un caso de estudio realizado en el laboratorio DELTA del Instituto de Ciencias Humanísticas y Económicas (ICHE) de la ESPOL., la red fue implementada para estar en un aula, se utiliza para el dictado de clases de utilitarios de Office con acceso al Internet, en este laboratorio se procedió a revisar las características de seguridad de su ubicación física y las configuraciones de sus puntos de acceso y se determinó que cambios de seguridad se debieron realizar para aumentar el nivel de seguridad.

En el capítulo tres se explica en que consiste el proyecto de consultoría. Aquí se determinan los pasos que se deben seguir para realizar una consultoría de red en cualquier red inalámbrica, los mismos pretenden sistematizar y crear un método de consultoría que puede aplicarse para cualquier caso. Al final se determinará cual es el nivel de seguridad requerido por la red y se procede a detallar los métodos de implementación para nivel básico, intermedio y avanzado de seguridad.

El capítulo cuatro presenta recomendaciones para la administración de la seguridad de la red que permitirán mantener el nivel de seguridad implementado. Se detalla métodos para crear una política de seguridad indispensable para el manejo adecuado de la seguridad inalámbrica y se menciona técnicas para el monitoreo de la red.

En el capítulo cinco se estiman los costos de la consultoría y las implementaciones de seguridad para cada nivel de seguridad.

Por último se presentan algunas conclusiones y recomendaciones basados en nuestro estudio de seguridades de WLAN.

ÍNDICE GENERAL

ABREVIATURAS

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AP	Access Point (Punto de Acceso)
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DKE	Dynamic Key Exchange
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
GHz	GigaHertz
GRE	Generic Routing Encapsulation
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security

IV	Initialization Vector
Kbps	Kilobits per second
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
LEAP	Lightweight EAP
MAC	Media Access Controller
Mbps	Megabits per second
MD5	Message Digest 5
NAT	Network Address Translator
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
PDA	Personal Digital Assistant
PEAP	Protected EAP
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frecuencia
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
VLAN	Virtual LAN
VPN	Virtual Private Network

WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

INTRODUCCIÓN

Las redes inalámbricas de área local o WLAN (Wireless Local Area Networks) están transformando la forma de comunicarnos. No solo son más flexibles y escalables que las redes de área local cableadas, también nos permiten armar redes en lugares en donde el cableado es un limitante. Actualmente en el Ecuador la implementación de redes inalámbricas es un considerable segmento de las redes de comunicación

Sin embargo, además de sus diversas ventajas, las redes WLAN tienen un gran inconveniente, su vulnerabilidad a ataques de seguridad. Debido a que los datos se transmiten por el aire estos son fácilmente interceptados. El estándar 802.11 de la IEEE para las WLAN tiene establecido un sistema de seguridad denominado WEP (Wired Equivalent Privacy) que ha quedado obsoleto para las nuevas técnicas de ataques en contra de las WLAN.

Muchas compañías han instalado redes inalámbricas sin considerar los problemas de seguridad que tendrían que afrontar. A pesar de que en la época actual él tema pueda sonar irrelevante, con el creciente desarrollo en la era de la información pronto tendremos que confrontarlo. Debido a estos factores consideramos que es necesario hacer una evaluación de los riesgos de seguridad para las redes inalámbricas implementadas en Ecuador.

Esta evaluación consiste en un monitoreo del medio de alcance de la WLAN y de los posibles problemas de seguridad que podrían encontrarse en dicho medio. Con la ayuda de software se puede determinar cuales y cuantos son estos riesgos. Finalmente al conocer las fallas del sistema de seguridad podremos encontrar las posibles soluciones que optimizarán el uso de la red.

CAPÍTULO 1

TECNOLOGÍAS

TECNOLOGÍAS Y ESTÁNDARES DE SEGURIDAD EN UNA WLAN

1.1. ¿Qué es una WLAN?

Las redes de área local inalámbricas no requieren cables para transmitir datos, utilizan ondas de radio o infrarrojas para enviar paquetes a través del aire. Gracias a esta característica, permite la instalación de redes sin problemas, móviles y flexibles, que hasta cierto punto son rápidas, seguras y fáciles de configurar.

Las redes inalámbricas se diferencian de las LAN convencionales principalmente en la capa física (como son enviados los bits de una estación a otra) y la de enlace de datos (describe como se empaquetan y verifican los bits) del modelo OSI (Open System

Interconnect Protocol Stack). Las demás capas son esencialmente similares lo que permite una interacción entre las redes cableadas existentes y las inalámbricas. En la figura 1.1 se ve las capas del modelo OSI y de las capas fundamentales de una WLAN.

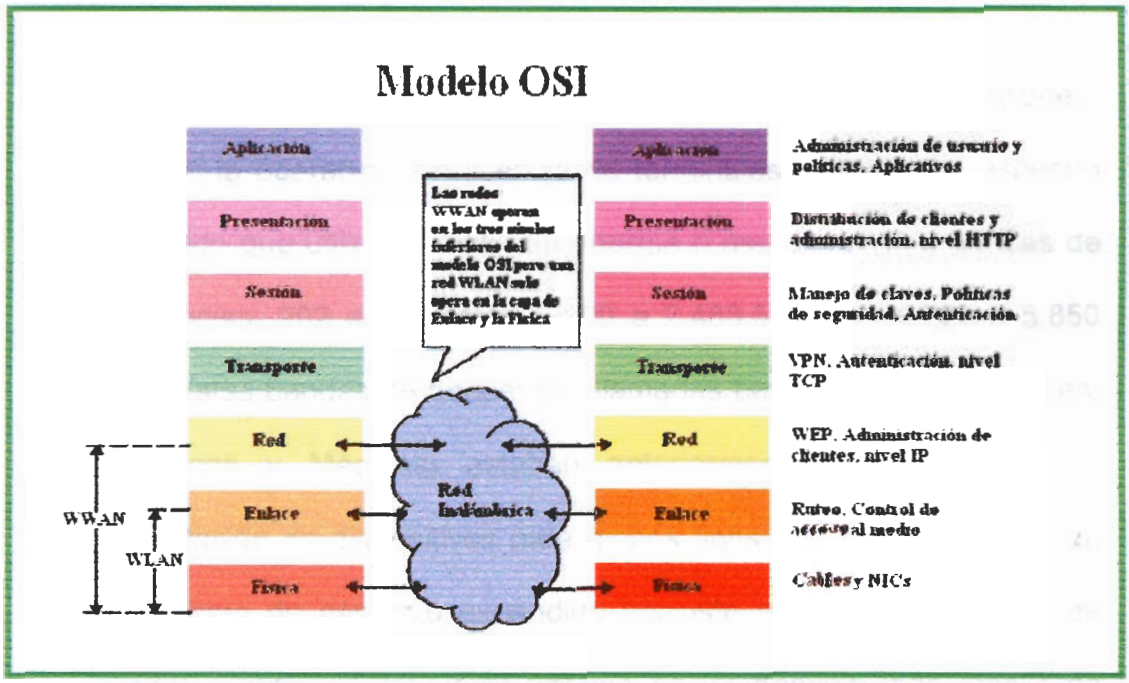


Figura 1.1. El modelo OSI y un ejemplo funcional de las capas fundamentales de una WLAN

Las redes inalámbricas que utilizan radiofrecuencia pueden clasificarse según su capa física en sistemas de banda estrecha o de frecuencia dedicada y sistemas basados en espectro extendido.

La primera opera de modo similar a la forma en que se difunden las ondas desde una estación de radio. Hay que sintonizar en una frecuencia muy precisa tanto el emisor como el receptor. La señal

puede traspasar paredes y se propaga sobre un área muy amplia, así que no es necesario orientarla. Sin embargo, estas transmisiones tienen problemas debido a las reflexiones que experimentan las ondas de radio.

A partir de 1985 la FCC (Comisión Federal de Comunicaciones) permitió la operación sin licencia de terminales basados en espectro extendido que utilicen 1 vatio de energía o menos, en tres bandas de frecuencias: 902 a 928 MHz, 2.400 a 2.483,5 MHz y 5.725 a 5.850 MHz. Estas bandas de frecuencia, llamadas bandas ICM (Industriales, Científicas y Médicas) estaban anteriormente restringidas a su implantación en dispositivos para dichos fines. El funcionamiento de un sistema de espectro expandido consiste en tomar una señal de banda normal y distribuir su energía en un dominio más amplio de frecuencias. Así, la densidad promedio de energía es menor en el espectro equivalente de la señal original.

Las redes LAN inalámbricas ofrecen diversas ventajas sobre las redes LAN convencionales debido a su movilidad. El usuario puede trasladarse de un lado a otro y permanecer conectado a la red LAN. La red puede establecerse sin caer en los gastos y los requerimientos de colocar cables e instalar conectores en paredes. Además, las redes

inalámbricas son flexibles, dado que las máquinas de escritorio pueden cambiarse de lugar sin ningún trabajo de infraestructura. Esto resulta particularmente útil al instalar sitios temporales de trabajo.

Gracias a su fácil instalación, estas redes inalámbricas reducen significativamente la complejidad y los gastos de una red dentro de una empresa. La libertad de movimiento crea oportunidades de interacción que antes no existían. Incluso estas redes se han instalado en lugares públicos como aeropuertos, hoteles y cafeterías con los llamados hotspots. Se puede ver una red inalámbrica en la figura 1.2.

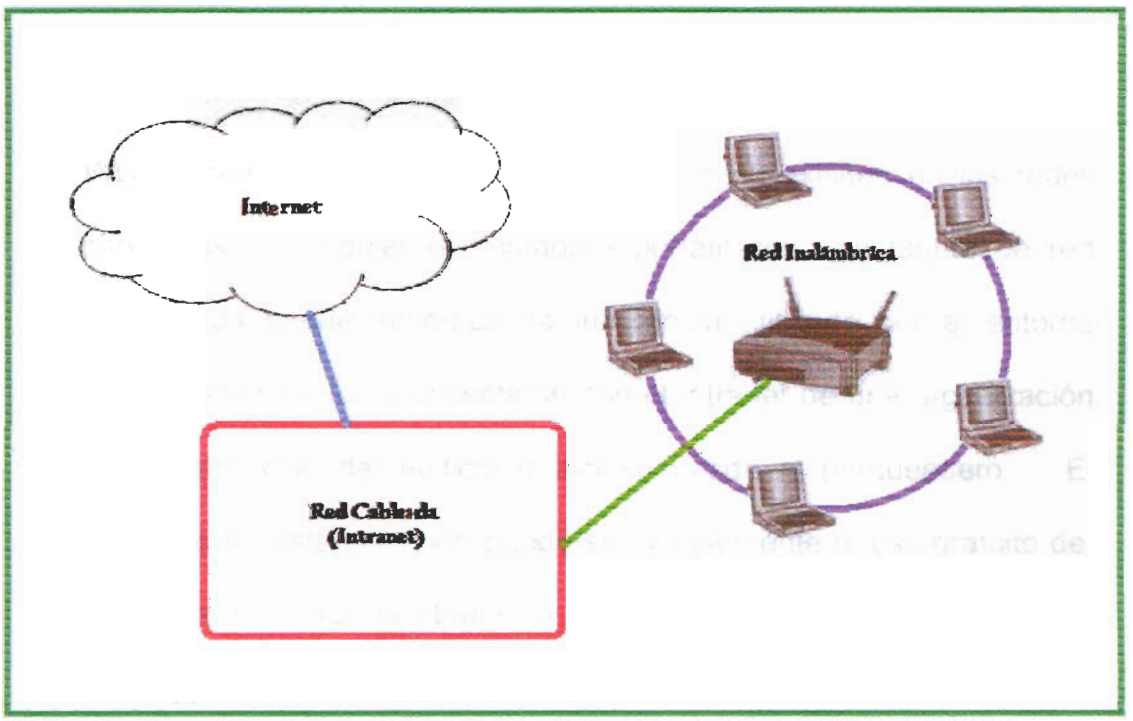


Figura 1.2. Ejemplo de una red inalámbrica simple modo infraestructura

La elección de la configuración de una red inalámbrica depende del uso que se le vaya a dar a la misma. Existe la configuración Ad Hoc o peer-to-peer (colega con colega) que es una red de área local independiente no conectada a una infraestructura cableada de manera que todas las estaciones están conectadas las unas con las otras. Otro tipo de configuración es el modo infraestructura que conecta a los clientes al intranet corporativo a través de un punto de acceso y opera de la misma manera que un cliente de la red cableada. También existen las llamadas hotspots que proveen de servicio inalámbrico en una variedad de áreas públicas, usualmente se conectan únicamente al Internet.

Sin embargo debido a que los datos se transmiten en forma aérea las WLAN crean problemas de seguridad que no existían en las redes cableadas. Cualquier computadora portátil con una tarjeta de red inalámbrica puede sintonizar la frecuencia utilizada por el entorno WLAN desprotegido y conectarse con el intranet de una organización desde otro piso del edificio o incluso desde el parqueadero. El propósito de esta conexión puede ser simplemente el uso gratuito del internet o peor aún la obtención de datos sensibles y echar abajo la red. [3],[4]

1.2. Estándar 802.11

Como respuesta a la creciente demanda de redes inalámbricas en 1997 surge la norma IEEE 802.11 que define el control de acceso al medio y las características de la capa física en una WLAN. La norma inicialmente estableció un sistema de 2 Mbps y es el estándar predominante para redes inalámbricas de área local. Las WLAN se transmiten en el espectro no licenciado de 2.4 GHz como fue acordado por la mayoría de agencias reguladoras alrededor del mundo, aunque existe una ligera variación dependiendo del país.

Este estándar incluye tres unidades de capas físicas: dos unidades de radio (ambas operan en la banda de 2400 a 2500 MHz) y una unidad infrarroja de banda base. Según esta norma las WLAN utilizan canales de radio frecuencia que no se sobreponen. Además establece una modulación de señal de espectro expandido por secuencia directa (DSSS) para la una unidad de radio. Con esta técnica de modulación, cada bit de los datos a transmitir, es sustituído por una secuencia de 11 bits correspondiente identificable por el receptor, así aunque parte de la señal de transmisión se vea afectada por interferencias, el receptor aún puede reconstruir la información.

La segunda unidad de radio utiliza la modulación de espectro

expandido por salto de frecuencia (FHSS). En esta modulación los datos son modulados en una serie de frecuencias que varían en una secuencia seudo-aleatoria. Este tipo de modulación es la menos utilizada. En la figura 1.3 podemos ver las diferencias entre los dos tipos de unidades.

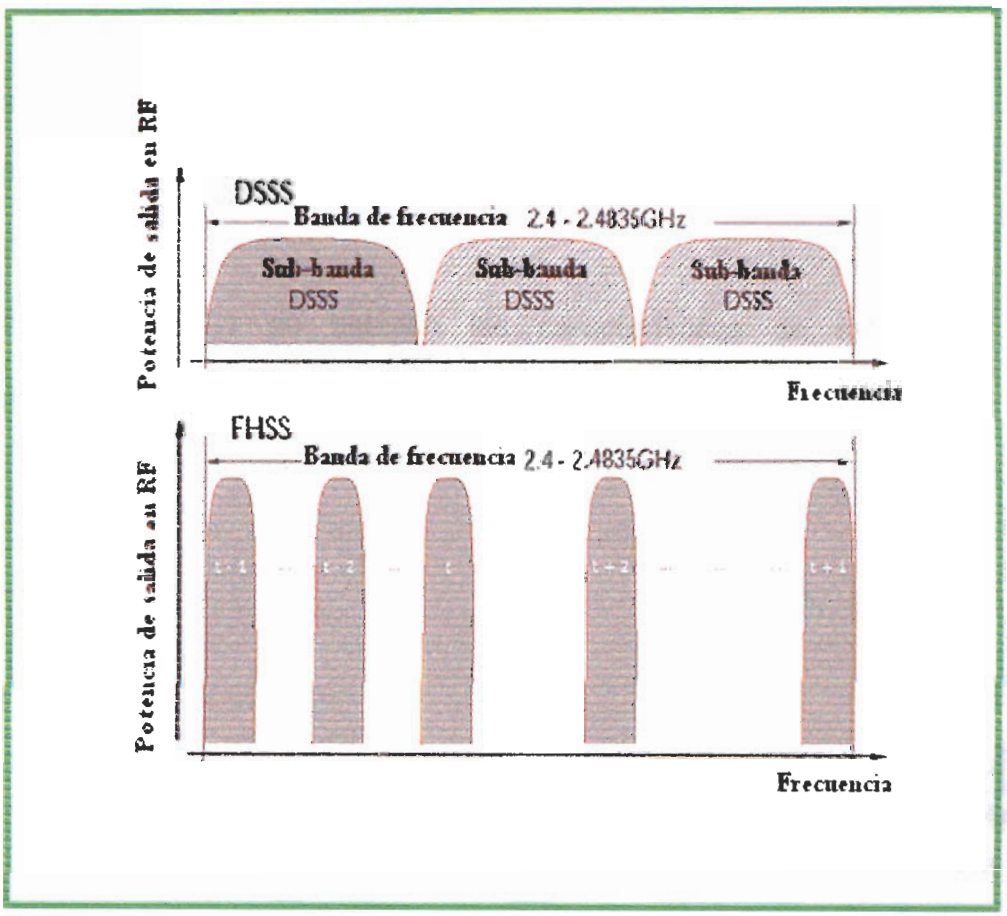


Figura 1.3. Unidades FHSS y DSSS

El estándar 802.11 soporta velocidades múltiples de transmisión de datos para adaptarse a la pérdida de fuerza en la señal y mantener la alta calidad de reestructuración de los paquetes.

Los clientes en una WLAN constantemente realizan una serie de operaciones para detectar errores y automáticamente establecer la mejor velocidad posible, subsecuentemente las velocidades pueden ser establecidas en una serie de números.

A través del tiempo este estándar ha sido mejorado. Estas extensiones son reconocidas por una letra adicional en la norma 802.11 original, incluyendo al 802.11a, 802.11b y 802.11g.

En la tabla 1.1 se detallan las características de estas tres ramificaciones.

	802.11b	802.11g	802.11a
Compatibilidad	Compatible con IEEE 802.11b. Wi-Fi CERTIFIED	Compatible con IEEE 802.11b y 802.11g. Wi-Fi CERTIFIED	Compatible con IEEE 802.11a. Wi-Fi CERTIFIED
Número de Canales	3 sin superposición	3 sin superposición	8 sin superposición (4 en algunos países)
Alcance típico en interiores	100 ft (30 m) a 11 MBps; 300 ft (91 m) a 1 Mbps	100 ft (30 m) a 54 MBps; 300 ft (91 m) a 1 Mbps	40 ft (12 m) a 54 Mbps; 300 ft (91 m) a 6 Mbps
Alcance típico en exteriores (Línea de vista)	400 ft (120 m) a 11 Mbps; 1500 ft (460 m) a 1 Mbps	400 ft (120 m) a 54 Mbps; 1500 ft (460 m) a 1 Mbps	100 ft (30m) a 54 Mbps; 1000 ft (305m) a 6 Mbps
Velocidades	11, 5.5, 2 y 1 Mbps	54, 48, 36, 24, 18, 12, 9, y 6 Mbps	54, 48, 36, 24, 18, 12, 8, y 6 Mbps
Modulación	Direct Sequence Spread (DSSS), 2.4 GHz	Orthogonal Frequency Division Multiplexing (OFDM), 2.4 GHz	Orthogonal Frequency Division Multiplexing (OFDM), 5 GHz

Tabla 1.1. Características de las normas WLAN IEEE

1.2.1. Wi-Fi

La alianza Wi-Fi es una organización sin fines de lucro formada en 1999 para certificar interoperabilidad entre productos del estándar 802.11 y promover los artículos Wi-Fi (Wireless Fidelity). Wi-Fi se conoce como el estándar global para redes LAN inalámbricas en todos los segmentos de dicho mercado. El nombre proviene de la certificación Wi-Fi que asegura que los productos inalámbricos 802.11 sean compatibles.

1.2.2. IEEE 802.11b

La especificación 802.11b fue ratificada por la IEEE en Julio de 1999 y opera en la banda de radiofrecuencia de 2.4 a 2.497 GHz. El método de modulación utilizado por el 802.11b es la modulación de espectro expandido por secuencia directa usando CCK (complementary code keying) llegando a velocidades de 11 Mbps.

1.2.3. IEEE 802.11g

La especificación 802.11g fue ratificada en Junio del 2003. Aunque el 802.11g opera en la banda de radiofrecuencia de 2.4 a 2.497 GHz al igual que el 802.11b, utiliza la modulación OFDM (múltiplexación por división de frecuencia ortogonal), método de modulación digital en el cual cada señal se separa en varios canales de banda angosta a

diferentes frecuencias, permitiendo velocidades de hasta 54 Mbps similar al 802.11a. En la figura 1.4 se muestra el espectro al modular OFDM. Esta combinación de rendimiento y banda de frecuencia permite que aquellos con infraestructura 802.11b puedan alcanzar una conexión más amplia de una forma menos costosa. Por supuesto, ciertos productos 802.11b requieren una actualización para ser compatibles con productos 802.11g.

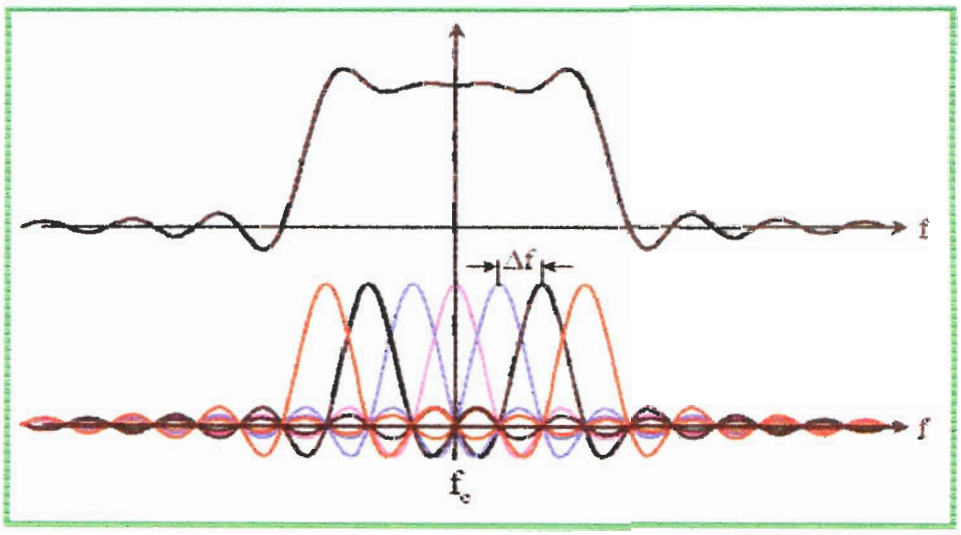


Figura 1.4. Modulación OFDM

1.2.4. IEEE 802.11a

La especificación 802.11a también fue ratificada en Julio de 1999 pero sus productos no fueron disponibles hasta el 2001 así que no ha sido tan ampliamente usado como el 802.11b. Trabaja en la banda de radiofrecuencia entre 5.15 y 5.875 GHz y utiliza el esquema de modulación OFDM lo que hace posible velocidades de hasta 54 Mbps.

Al utilizar la banda de frecuencia de 5 GHz y la modulación OFDM, el estándar IEEE 802.11a tiene dos ventajas respecto al 802.11b, incrementa la velocidad máxima de transferencia de datos por canal (de 11 Mbps a 54 Mbps) y aumenta el número de canales sin solapamiento. Hay 8 canales sin solapamiento disponibles; mientras que con la banda de 2,4 GHz sólo hay 3. El ancho de banda total disponible en la banda de 5 GHz también es mayor que en la banda de 2,4 GHz. Por ello en una WLAN basada en el 802.11a se puede admitir un mayor número de usuarios de alta velocidad simultáneos sin peligro de que surjan conflictos. Un inconveniente de utilizar la banda de 5 GHz es que las frecuencias utilizadas no están estandarizadas internacionalmente.

Otro punto es que debido a que los estándares 802.11a y 802.11b operan en bandas de frecuencia distintas, los productos no son compatibles.

La frecuencia de funcionamiento más alta del estándar 802.11a tiene como consecuencia un alcance relativamente más corto. Se necesitarán más puntos de acceso 802.11a para cubrir la misma zona. Pero incluso con estos inconvenientes, las pruebas iniciales demuestran que los productos 802.11a ofrecen un rendimiento casi

tres veces superior al de los 802.11b en cuanto a alcances en interiores.

El estándar IEEE 802.11g alcanza velocidades más altas y es compatible con los equipos 802.11b. El 802.11g opera en la misma banda de frecuencia de 2,4 GHz y modulación DSSS que el 802.11b a velocidades de hasta 11 Mbps, mientras que a velocidades superiores utiliza tipos de modulación OFDM más eficientes. Una tarjeta de interfaz de red IEEE 802.11g, por ejemplo, puede funcionar con un punto de acceso 802.11b y viceversa, a velocidades de hasta 11 Mbps. Para lograr velocidades más altas, de hasta 54 Mbps, tanto el punto de acceso como la tarjeta de red deben ser compatibles con el estándar 802.11g.

En comparación con el estándar IEEE 802.11a, el 802.11g tiene un menor ancho de banda utilizable, lo que ocasiona un menor número de usuarios WLAN de alta velocidad. Aunque las modulaciones OFDM permiten una velocidad más alta, el ancho de banda disponible total en la banda de frecuencia de 2,4 GHz no varía. El motivo es que el IEEE 802.11g todavía está restringido a tres canales en la banda de 2,4 GHz. [2]

1.3. Seguridad según el estándar 802.11

Las redes WLAN proveen una gran flexibilidad, sin embargo estas pueden convertirse en una puerta abierta al intranet corporativo. El acceso no autorizado a una red por medio de un punto de acceso inalámbrico puede ser demasiado fácil si no se emplea medidas para proteger los datos.

Cuando hablamos de la seguridad en el estándar 802.11 nos referimos a la seguridad en el nivel dos del modelo OSI, la capa de enlace. La idea es asegurar la integridad de los datos que viajan desde la computadora hasta el punto de acceso. Cualquier sistema de seguridad para una red debe poder ejecutar cuatro acciones.

1. Autenticación: Confirma si el usuario es realmente quien dice ser, por medio de una huella, tarjeta inteligente o un clave.
2. Autorización: Determina que nivel de acceso tiene el usuario.
3. Privacidad y Confidencialidad de los datos: Evita que los datos sean vistos por terceros.
4. Integridad de los datos: Previene la manipulación indebida de los datos.

Para cumplir estos propósitos en el estándar 802.11 y en las modificaciones posteriores de dicho estándar se incluyó un algoritmo llamado WEP (Wire Equivalent Privacy).

1.3.1. WEP: Wired Equivalent Privacy

El WEP (Wired Equivalent Privacy) es un algoritmo de encripción de datos basado en la codificación RC4 de RSA Data Security. Fue incluido en la primera versión del estándar IEEE 802.11 y mantenido sin cambios en las especificaciones 802.11a y 802.11b, con la finalidad de cerciorar compatibilidad entre diferentes fabricantes. El WEP es implementado en el nivel MAC y soportado por la mayoría de las soluciones inalámbricas. Este sistema de seguridad permite que dispositivos inalámbricos como PDAs (Personal Digital Assistant) y ordenadores portátiles, accedan a una red de ordenadores a través de radiofrecuencia en vez de cableado físico. Cumple tres tareas: 1) Autenticar clientes en puntos de acceso; 2) Encriptar los datos entre los clientes y el punto de acceso; y 3) Incluir en cada paquete intercambiado un código de integridad. [2]

Los sistemas WLAN pueden resistir las escuchas ilegales pasivas, sin embargo la única forma segura de prevenir que alguien pueda comprometer los datos transmitidos es utilizar mecanismos de cifrado.

El WEP pretende garantizar que los sistemas WLAN dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas mediante el cifrado de los datos que son transportados por el aire. Además el WEP aspira evitar que usuarios no autorizados puedan acceder a la red (autenticación). Este propósito secundario no está enunciado de manera explícita en el estándar 802.11, pero se considera una importante característica del algoritmo.

El cifrado es crítico para garantizar la privacidad y confiabilidad de los datos en los sistemas basados en el estándar 802.11. A la par lo es proporcionar control de acceso mediante mecanismos de autenticación. Por lo tanto, la mayor parte de los productos WLAN compatibles con 802.11 soportan WEP como característica estándar opcional.

En una red con el WEP activado todos los usuarios emplean una llave secreta compartida entre el usuario móvil y el punto de acceso. Todos los paquetes son encriptados con esta llave secreta. Un adversario que quiere acceder a la red no debería ser capaz de desencriptar los paquetes sin saber la llave. Existe una tabla que asocia una llave exclusiva con cada estación.

Este sistema usa llaves simétricas de varios tamaños. En el estándar hay dos métodos básicos el WEP64 y el WEP128 que aseguran compatibilidad con todos los adaptadores que hay en el mercado. Existen ciertos proveedores que utilizan llaves más largas como el WEP152 que incrementan el nivel de seguridad al incrementar el tamaño de la llave. La misma llave se utiliza en el punto de acceso y en las estaciones y se determina manualmente pues el estándar no contempla ningún sistema de distribución de llaves.

En la figura 1.5 se muestra el proceso de encriptación WEP, el texto cifrado se genera por un método determinado utilizando el algoritmo de encriptación RC4. Por ejemplo la clave del WEP64 se forma por 24 bits correspondientes al vector de iniciación o initialization vector (IV, que es generado dinámicamente y debería ser diferente para cada trama) más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de iniciación es lo que impide que un atacante pueda adquirir suficiente tráfico con la misma llave. El IV se genera en un extremo y se envía en la propia trama al otro extremo.

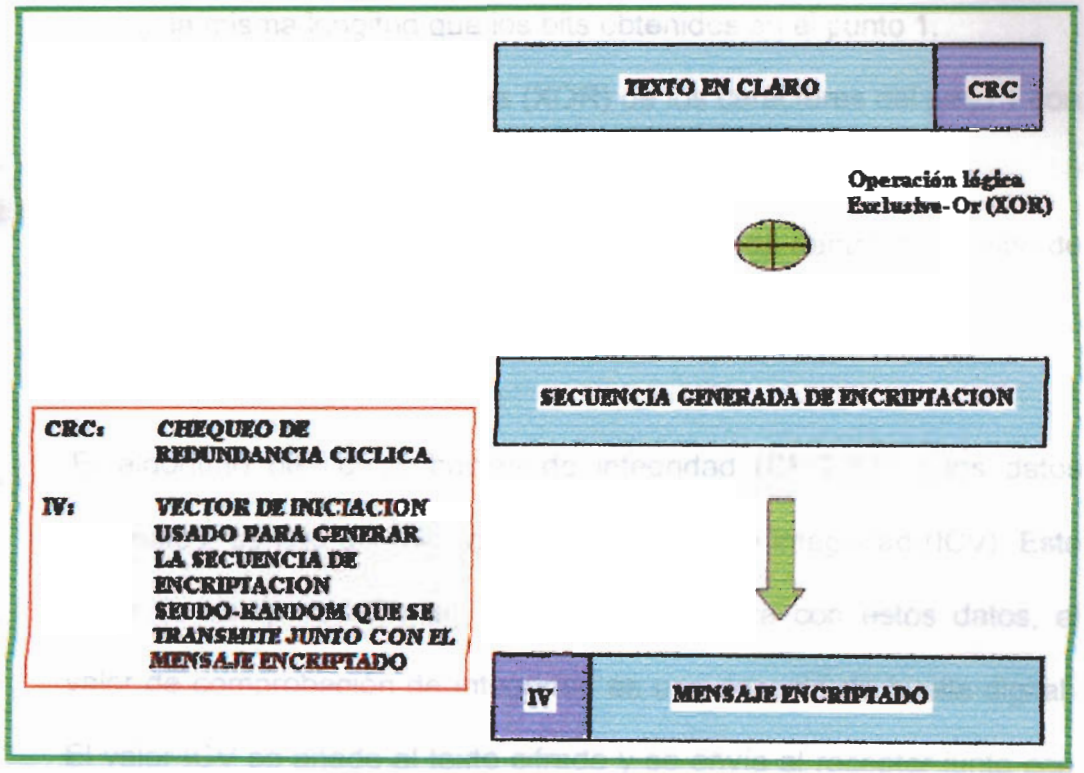


Figura 1.5 Proceso de encriptación WEP

Los pasos de cifrado que aplica el WEP son:

1. Determina un CRC (Cyclic Redundancy Check) de 32 bits de los datos. El CRC-32 permite al WEP garantizar la integridad de los mensajes.
2. Enlaza la clave secreta a continuación del IV (Vector de Iniciación).
3. El PRNG (Pseudo-Random Number Generator) de RC4 genera una secuencia de caracteres pseudoaleatorios (keystream) de

la misma longitud que los bits obtenidos en el punto 1.

4. Calcula la OR exclusiva (XOR) de los caracteres del paso 1 con los del paso 3. El resultado es el mensaje cifrado.
5. Envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos de la trama IEEE 802.11.

El algoritmo de comprobación de integridad (CRC-32) a los datos originales, genera un valor de comprobación de integridad (ICV). Este valor de comprobación de integridad se enlaza con estos datos, el valor de comprobación de integridad es una especie de huella digital. El valor ICV se añade al texto cifrado y se envía al receptor junto con el vector de iniciación, el receptor combina el texto cifrado con el flujo de clave para recuperar el texto en claro; al aplicar el algoritmo de integridad a los datos originales y comparar la salida con el vector ICV recibido, se puede verificar que el proceso de descifrado ha sido correcto ó que los datos han sido corrompidos. Si los dos valores de ICV son idénticos, el mensaje será autenticado; en otras palabras, las huellas digitales coinciden.

WEP proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN; y una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red, este es el modo

seguro.

Desafortunadamente el mecanismo del algoritmo WEP tiene fallas de seguridad bastante significativas, quizás la primordial es que muchos puntos de acceso son enviados con el sistema WEP desactivado de fábrica. Aun cuando el sistema si está activado generalmente las llaves se dejan como viene predeterminado por el proveedor, esto permite un fácil acceso a cualquier persona que sabe estos valores. En el año 2000 investigadores de la Universidad de Berkley en California publicaron un reporte detallando las vulnerabilidades del WEP, estas vulnerabilidades incluyen la corta llave de encripción (no más de 40 bits), llaves estáticas y la falta de un método de distribución de llaves. [2]

La implementación del vector de iniciación (IV) en el algoritmo WEP tiene varios problemas de seguridad. Los fabricantes determinan cómo variar el IV en sus productos y por ello en buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada trama; esto ocasiona que las primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente. Aun con un sistema más efectivo de variación, el número de bits (24) del IV es muy

pequeño, convirtiéndose en un serio problema de seguridad.

Basándose en estas debilidades existen varios programas exploradores que permiten a cualquier persona con una computadora portátil y una tarjeta 802.11b buscar puntos de acceso con el WEP deshabilitado o con las llaves predeterminadas.

1.4. Nuevas tecnologías de seguridad en WLAN

A medida que el uso de las redes inalámbricas de área local empezó a cobrar vigencia, los problemas de seguridad del WEP empezaron a ser más notorios, no era permisible el bajo nivel de seguridad cuando la WLAN se implementaba a nivel corporativo y datos confidenciales resultaban comprometidos.

Inmediatamente después de que estos riesgos fueron expuestos, se empezaron a desarrollar estándares de seguridad que reemplazaran al WEP en las redes inalámbricas. La Wi-Fi empezó a desarrollar el WPA (Wi-Fi Protected Access) que se convirtió en el siguiente escalón en la estandarización de la seguridad, a esta le siguieron varios estándares propietarios y no propietarios que buscaban resolver el eminente problema de seguridad en una WLAN. La figura 1.6 muestra la evolución de los estándares no propietarios.

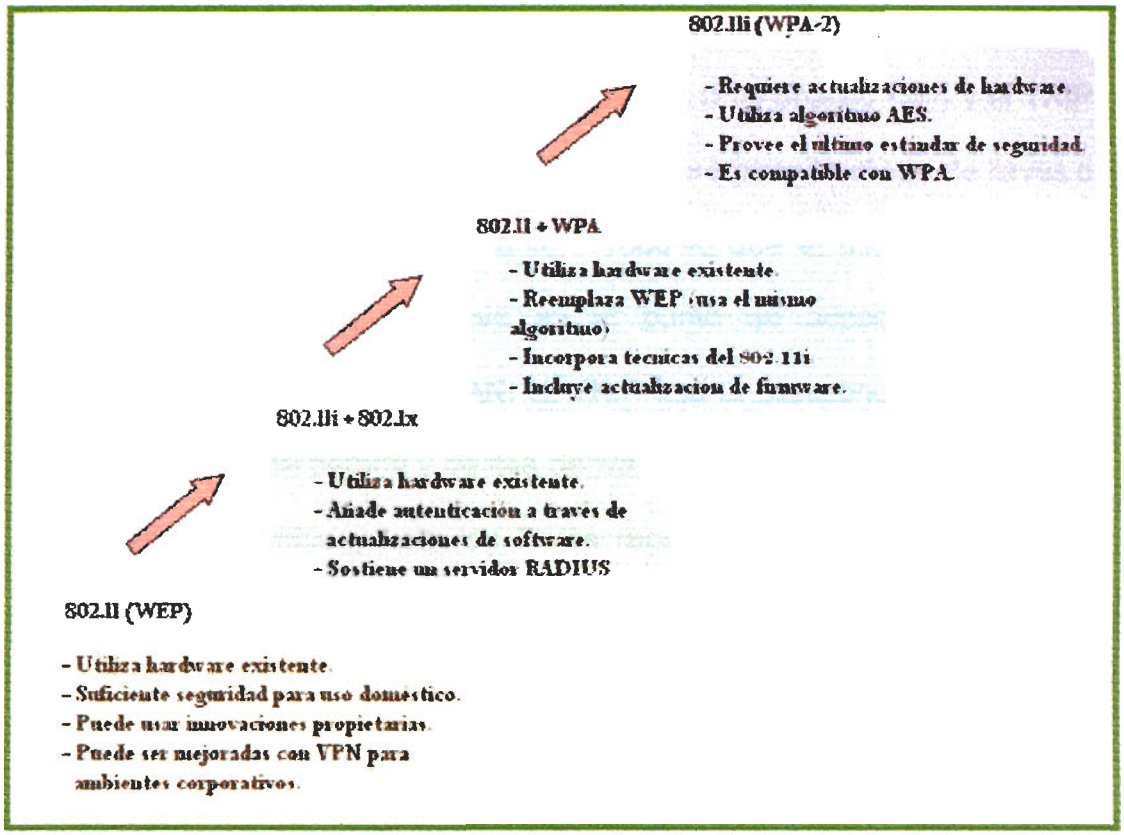


Figura 1.6. Evolución de los estándares de seguridad WLAN no propietarios

1.4.1. WPA: Wi-Fi Protected Access

El WPA (Wi-Fi Protected Access) es un estándar de seguridad que resuelve los problemas de cifrado del WEP. Está diseñado como una actualización de software para hardware certificado Wi-Fi existente. Este protocolo se envuelve alrededor del WEP y resuelve sus brechas de seguridad. El WPA también incluye los beneficios de autenticación del 802.1X y es compatible con el estándar 802.11i.

Aunque ningún método puede considerarse 100% seguro, el WPA

logra una gran mejora a los niveles de seguridad del WEP mediante un modo de funcionamiento llamado PSK (Pre-Shared Key) y el TKIP (Temporal key integrity protocol). El primero permite el uso de llaves o claves ingresadas manualmente. Todo lo que el usuario tiene que hacer es ingresar la clave en el punto de acceso y en cada computador de la red WLAN. El TKIP usa la llave original WEP solo como punto de partida y de ella deriva matemáticamente sus llaves de cifrado. Cambia y rota las llaves regularmente de manera que la misma llave de cifrado no se usa dos veces. Genera una llave de cifrado cada 10,000 paquetes y usa una función de mezclado para intercalar el vector de inicialización con la llave compartida. Esto sucede automáticamente y es invisible para el usuario.

Las especificaciones 802.1X fueron desarrolladas por el EAP (Extensible Authentication Protocol) y definen técnicas de autenticación para equipos anexos a un puerto LAN permitiendo control de acceso a la red basado en puertos.

Se decidió incluir estas especificaciones en el estándar 802.11i además del WPA y WPA2 debido a su alta funcionalidad. [6]

1.4.2. WPA2

El Wi-Fi Protected Access 2 o WPA2 es la certificación Wi-Fi del

estándar 802.11i, probado para interoperabilidad. Sus características son las del estándar 802.11i que mencionaremos posteriormente.

1.4.3. 802.1x

El estándar 802.1x es utilizado para empaquetar el EAP en tramas ethernet que no utilizan PPP (Point to Point Protocol). Se encarga de la autenticación y de nada más. Esto es deseable en situaciones en las que las funciones adicionales del PPP no son necesarias o adicionan una carga no deseada.

El protocolo utilizado en este estándar es conocido como encapsulación EAP sobre LAN, EAPOL por sus siglas en inglés.

En el caso de las WLANs, este estándar de seguridad se caracteriza por tener una estructura de autenticación basada en puerto que permite autenticar los usuarios del sistema en cada puerto a través de un servidor externo y una distribución dinámica de llaves de sesión para encriptación WEP, se requiere un servidor RADIUS (Remote Authentication Dial-In User Service).

1.4.4. EAP: Extensible Authentication Protocol

El EAP (Extensible Authentication Protocol) generalmente funciona

directamente sobre las capas de enlace de datos como un protocolo punto a punto, como el PPP o el IEEE 802, sin requerir IP. Este protocolo puede ser utilizado en circuitos conmutados, enlaces dedicados y enlaces cableados o no cableados; fue desarrollado para mitigar la proliferación de soluciones de autenticación propietarias que podían causar problemas en la inter-operabilidad entre equipos de diferentes proveedores.

Lleva el nombre de "extensible" porque soporta múltiples mecanismos de autenticación, el dialogo entre el usuario y el servidor de autenticación se lleva a cabo en tramas EAP. La forma encapsulada del EAP, conocida como EAP sobre LAN o EAPOL, es usada para todo tipo de comunicación entre el usuario y el autenticador.

En una red WLAN el punto de acceso actúa como un Proxy EAP entre el terminal y el servidor de autenticación (SA), aceptando paquetes EAPOL del terminal y diseccionándolos al SA con un protocolo como por ejemplo RADIUS. A su vez, el punto de acceso direcciona todos los paquetes EAP del SA sobre EAPOL al terminal inalámbrico.

RADIUS es un esquema de nombre de usuario y clave que permite que solo usuarios aprobados ingresen a la red; no afecta a los datos

cifrados. La primera vez que un usuario trata de ingresar a la red, archivos secretos o ubicaciones de red, este debe ingresar su nombre y clave y ponerlo a consideración del servidor RADIUS; el servidor entonces verifica que el individuo tiene una cuenta y, si esto se cumple, asegura que la persona use la clave correcta antes de que pueda ingresa a la red.

Debido a que el EAP fue originalmente diseñado para redes cableadas este asume que la capa física es segura. En el caso de una WLAN esta premisa no es cierta porque un adversario puede fácilmente escuchar el aire para obtener tráfico EAP. Por lo tanto, debe haber algún método de proteger criptográficamente al EAP de cualquier ataque adversario. Para ello se han diseñado varios métodos de protección que veremos en la sección 1.4.5.

Incorpora un sistema dinámico para asignar claves WEP, generando una nueva para cada sesión. Básicamente su uso dentro de una WLAN es la autenticación por lo que generalmente se combina con el estándar 802.1x para el control de acceso.

El 802.1x no es únicamente un estándar inalámbrico, este provee un esquema de autenticación que puede ser aplicado a la mayoría de

tecnologías IEEE 802, en vez de utilizar identificadores de hardware como direcciones MAC. El 802.1x utiliza credenciales de usuario individuales además de control de acceso basado en puertos, esto significa que las credenciales de usuario tienen que ser verificados antes de que el switch o punto de acceso establezca un enlace de capa de enlace.

A partir del EAP se desarrollaron varios tipos de protocolos de seguridad. En la tabla 1.2 se pueden ver las características de dichos protocolos y en la siguiente sección se explicarán con mayor detalle.

	Características	Propietario	Vulnerabilidades
EAP	• Protocolo punto a punto. • Soporta múltiples tipos de autenticación.	NO	• Capa física no segura. • Requerimientos de identidad y respuesta son enviadas sin cifrado.
LEAP	• Soporta redes con varios sistemas operativos	CISCO	• Su capacidad depende del tamaño de su clave. • Usa MV-Chap conocido por su vulnerabilidad en la auntenticación.
FAST	• Empezó como TEAP • Minimiza los requerimientos de hardware.	CISCO	• No utiliza certificados.
AKA	• Convergencia entre WLAN y UMTS. • Permite conexión GSM.	NOKIA	• Solo para GSM.
SIM	• Enlaza WLAN con redes celulares de segunda generación. • Utiliza tarjeta SIM.	IETF	• Necesita tarjeta SIM.
MD5	• Apretón de manos simple. • Requiere poca memoria y es fácil de implementar.	RSA Security	• Susceptible a ataques man-in-the-middle. • No provee métodos de autenticación de AP.
PEAP	• Combina la autenticación especificada por el administrador y EAP.	CISCO, Microsoft, RSA	• No se encuentra.
TLS	• Autenticación en doble sentido. • Descendiente directo de SSL.	Microsoft	• Requiere PKI.
TTLS	• Utiliza un túnel. • Autentica en un solo sentido.	Funk Software, Certicom	• Certificados menos seguros que los utilizados en TLS.

Tabla 1.2. Protocolos EAP

1.4.5. LEAP, FAST, AKA

El LEAP (Lightweight Extensible Authentication Protocol) es la solución de Cisco para proveer un sistema fuerte de autenticación implementado en su infraestructura inalámbrica Airones, utiliza los principios del EAP como su fundamento. En este protocolo las credenciales del usuario están basadas en un nombre de usuario y una clave. En un sistema con WEP activado, el LEAP reduce significativamente el riesgo de que un adversario intercepte y descifre la llave, esto lo logra a través de la generación dinámica de una llave WEP por usuario, por sesión.

Un componente importante de este sistema Cisco son los ACS (Cisco Secure Access Control Server) o AR (Cisco Access Register), estos servidores RADIUS determinan el largo de la sesión; cuando la sesión expira o el terminal se aleja del punto de acceso y se acerca a otro, un nuevo proceso de re-autenticación comienza y se genera una nueva llave de sesión, todo esto es totalmente transparente para el usuario.

Este sistema se ha convertido en la forma más popular de EAP debido a su aplicación relativamente fácil y a la popularidad de la línea de productos Cisco Aironet.

El EAP/AKA (Extensible Authentication Protocol - Authentication and Key Agreement) utiliza un método de convergencia entre las WLAN y UMTS, la modificación AKA del protocolo EAP fue desarrollado por Nokia y es una versión avanzada que permite conexión con sistemas se tecnología GSM, el AKA soporta autenticación mutua y extiende el código de autenticación a 128 bits para protegerse en contra de ataques de fuerza bruta.

La versión EAP/FAST empezó como TEAP (Tunneled EAP) pero evolución convirtiéndose en uno de los mecanismos más comprensibles y seguros del protocolo EAP, se ha probado incorruptible por ataques de diccionario y Man-in-the-middle; además provee autenticación segura basada en una infraestructura ya implementada, minimiza los requerimientos de hardware y no requiere certificados o infraestructura de llave pública (PKI).

1.4.6. SIM, MD5, PEAP

El EAP/SIM (Extensible Authentication Protocol - Subscriber Identity Module) es la extensión de EAP que enlaza a las redes WLAN con las redes celulares de segunda generación como GSM y GPRS (General Packet Radio Service), provee autenticación mutua del equipo del usuario a la red y de la red al usuario, esto asegura que solo usuarios

validos accedan a la red móvil; utiliza la llamada tarjeta SIM, un tipo de tarjeta inteligente que contiene información de usuario que puede ser usado para procesos de contabilidad, además de datos que son utilizados en el cifrado de la voz y datos transmitidos. Las tarjetas SIM son mayormente utilizadas en teléfonos móviles aunque hay versiones para computadores portátiles, PDA y otros equipos para integrar en una WLAN la capacidad de las redes GSM inteligentes.

Otra variación del EAP es el MD5, el Message Digest 5 (MD5) es un simple apretón de manos en una dirección en el cual el SA autentica al terminal, las credenciales están basadas en el conocimiento mutuo del nombre de usuario y de la clave. El MD5 requiere muy poca memoria y es fácil de implementar y manejar, por lo tanto es ideal para terminales inalámbricos con memoria y poder de procesamiento limitado.

Cuando se autoriza con este protocolo, una secuencia de mensajes de pedido/respuesta EAP son intercambiados entre el usuarios y el servidor de autenticación, si las credenciales del usuario en la respuesta concuerdan con la llave secreta en la base de datos del servidor, un paquete de autenticación es enviado al punto de acceso permitiendo que uno de los puertos de datos sea asignado al usuario.

Sin embargo el MD5 no utiliza una llave WEP por sesión y esto puede tornarse en un riesgo de seguridad.

Protected EAP (PEAP) se refiere a formas de combinar la autenticación especificada por el administrador y el protocolo de confiabilidad EAP, establece un túnel seguro entre el terminal y el SA, esto permite que los administradores de la red utilicen protocolos que no fueron desarrollados para trabajar con EAP propiamente; existen dos tipos de PEAP, el primero utiliza el Microsoft Challenge Response Access Protocol (MS-CHAP) mientras que el segundo utiliza características del TLS (Transport Layer Security).

Este estándar surgió por la necesidad de contrarrestar los puntos débiles del EAP, fue desarrollado como una solución propietaria de Cisco, Microsoft y RSA.

1.4.7. TLS, TTLS

La modificación EAP/TLS (Transport Level Security) es una autenticación en doble sentido en la cual el SA autentica el terminal y a su vez el terminal autentica al servidor, es el descendiente directo del protocolo SSL (Secure Sockets Layer) usado por servidores de WEB para proteger información. Esta autenticación mutua asegura

protección en contra de ataques "Man in the middle"; el TLS utiliza certificados digitales en el SA y en el usuario para prevenir ataques de inyección.

El principal problema del EAP/TLS es que requiere que los usuarios de la red tengan certificados digitales, lo que significa un arduo trabajo de administración para emitir estos certificados; para ello fue propuesto el EAP/TTLS (EAP over Tunneled TLS), en este protocolo solo el servidor necesita el certificado mientras que los clientes simplemente generan una llave para cada sesión, la autenticación de los usuarios se realiza por otro método, por ejemplo una llave compartida con un servidor RADIUS.

La diferencia entre este método y el TLS radica en su método de "tunneling", un túnel es establecido entre el cliente y el servidor TTLS basado en el nombre de usuario y la llave. El servidor TTLS puede trabajar tanto como una autoridad de autenticación o pasar un mensaje de TLS a otro servidor en la red LAN, como un directorio activo RADIUS, cuando la autenticación es exitosa, el túnel es levantado y las compuertas se abren para el tráfico.

1.4.8. Seguridad 802.11i

El estándar 802.11i fue ratificado oficialmente en Junio del 2004 como parte de la familiar 802.11, utiliza el AES (Advance Encryption Standard) con una llave de 128 bits para protección de cifrado y otras mejoras de seguridad al WEP, fue probado y certificado por la Wi-Fi Alliance y su versión certificada lleva el nombre de WPA2; además de un método de cifrado mejorado, este estándar utiliza el 802.1X, optimizando el manejo de llaves y autenticación de usuario.

El estándar de seguridad 802.11i incorpora fuertes métodos de autenticación y de cifrado de datos convirtiéndose en un importante representante de lo que sería la solución a los problemas de seguridad en redes basadas en el 802.11, es la versión de segunda generación de seguridad de dicha norma.

Incorpora el TKIP (Temporal Key Integrity Protocol) y el CCMP (Counter Mode with CBC-MAC Protocol), el primero implementa medidas que reducen la velocidad a la cual el adversario puede intentar realizar intentos fraudulentos de enviar mensajes falsos, con el método de cambiar las llaves de cifrado este número de intentos se reduce a 2 cada 60 segundos, esto disminuye la probabilidad de un fraude exitoso con datos falsificados y la cantidad de información que

un adversario puede obtener sobre la llave.

El CCMP requiere hardware con poder de procesamiento mucho mayor y más memoria que los métodos antes mencionados, esta basado en el AES (Advanced Encryption Standard). El Counter Mode es utilizado para privacidad de datos mientras que el CBC-MAC (Cipher Block Chaining - Message Authentication Code) es utilizado para integridad de datos y autenticación.

1.5. Métodos de encriptación

Los algoritmos de encriptación son algoritmos matemáticos complejos, los fundamentos y procedimientos de la operación de encriptación se llaman sistema de cifrado o encriptación, para descifrar los algoritmos es necesaria una llave, esto es, una secuencia de caracteres utilizado en el algoritmo de encriptación.

Un algoritmo de encriptación debe cumplir ciertas características:

1. Debe ser fácil de utilizar para los usuarios, pero difícil de descifrar para los interceptores.
2. Debe pretender ser lo más eficiente y práctico además de ser seguro, tomando en consideración el tiempo que tomará cifrar un sistema y cuanta memoria ocupa.

3. Se asume que el enemigo conoce la naturaleza del sistema de cifrado y que lo único que le falta es la llave.

A medida de que la capacidad de los procesadores aumenta, la complejidad de estos algoritmos de encriptación aumenta también. Hace algunos años los complicados procesos matemáticos que se requerían para descifrar un texto encriptado tomarían meses e incluso años. Hoy, computadoras con alta capacidad de procesamiento pueden hacerlo en minutos, a través de los años se ha buscado crear algoritmos que ofrezcan total confiabilidad e integridad de los datos ofreciendo así un alto nivel de seguridad.

1.5.1. RC4

El RC4 es un algoritmo de flujo (no de bloques), creado en 1987 por Ronald Rivest (la R de RSA - Secreto Comercial de RSA Data Security), fue publicado el 13 de Septiembre de 1994 usando en sci.crypt, es usado por diversos programas comerciales como Netscape y Lotus Notes.

Trabaja a partir de una clave de 1 a 256 bytes (8 a1024 bits), inicializando una tabla de estados, esta tabla se usa para generar una lista de bytes pseudo-aleatorios, los cuales se combinan mediante la

función XOR con el texto en claro; el resultado es el texto cifrado.

En agosto del 2001 se descubrió una debilidad del RC4, esta radica en el uso del vector de iniciación, se determinó un método que utiliza únicamente el primer byte generado por la secuencia pseudoaleatoria con el objetivo de obtener la clave de encriptación. También en agosto del 2001, un sistema práctico y barato para conseguir la clave fue implementado aprovechando la vulnerabilidad del RC4, los programas freeware Airsnort y WEPCrack utilizan esta técnica.

1.5.2. RSA

El algoritmo de llave pública RSA fue creado en 1978 por Rivest, Shamir y Adlman, y es el sistema criptográfico asimétrico más conocido y usado. El sistema RSA se basa en el hecho matemático de la dificultad de factorizar números muy grandes, para factorizar un número empezamos a dividir sucesivamente éste entre 2, entre 3, entre 4,..., y así sucesivamente, buscando que el resultado de la división sea exacto, con lo que tendremos un divisor del número, si el número considerado es un número primo (el que sólo es divisible por 1 y por él mismo), tendremos que para factorizarlo habría que empezar por 1, 2, 3,..... hasta llegar a él mismo, por ser primo ninguno de los números anteriores es divisor suyo. Y si el número primo es lo

suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo, de esta premisa de factorización de los números primos y con métodos matemáticos el RSA crea sus claves.

El sistema RSA permite longitudes variables en sus claves, siendo aconsejable el uso de claves de no menos de 1024 bits (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 ordenadores trabajando juntos para hacerlo), presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos, por ser más rápidos. Se suele usar también en los sistemas mixtos para cifrar y enviar la clave simétrica que se usará posteriormente en la comunicación cifrada.

1.5.3. DES

El DES (Data Encryption Standard) es el sistema de encriptación más conocido y ampliamente utilizado en el mundo, fue propuesto en 1975 y aprobado en 1977 como un estándar de la Federal Information Processing Standard (FIPS), a pesar de varios ataques, el algoritmo del DES se mantuvo seguro hasta casi finales de los años 90, cuando fue infiltrado por la poderosa computadora del EFF, Eletronic Frontier Foundation, después de 56 horas, este fue el primer sistema de

encriptación estandarizado

La llave DES consiste de 64 bits binarios, de los cuales 56 son generados aleatoriamente y usados directamente por el algoritmo, los otros 8 bits, que no son utilizados por el algoritmo, pueden ser usados para detección de errores, los 8 bits detectores de error son establecidos para hacer la paridad de cada trama de 8 bits de la llave impar. Los usuarios autorizados receptores deben tener la llave para poder descifrar la información, sin embargo los pasos que sigue el algoritmo son de conocimiento público.

Lo primero que se realiza es una permutación de los 64 bits del bloque de entrada, realmente, esta permutación no añade seguridad alguna y su principal función es la de facilitar la carga de los bits de información en bloques de 8 bits a un chip especializado en DES.

Después de esta permutación inicial, los 64 bits resultantes se dividen en dos partes de 32 bits cada una, la mitad de la derecha (Ri) se introduce en una función donde es combinada con la clave, se realiza una XOR con el resultado de la función y con la mitad de la izquierda (Li), adicionalmente se genera una subclave Ki distinta de los 64 bits de la clave, se descartan los 8 bits de paridad quedando una clave de 56 bits en la cual se realiza una permutación.

Los 48 bits resultantes de la XOR entre la parte derecha Ri expandida y la subclave Ki se introducen de seis en seis en ocho bloques que son conocidos como S-Box, de tal manera que el primer bloque de 6 bits se introduce en la S-Box 1, el segundo en la S-Box 2, y así sucesivamente, el funcionamiento del DES se ve en la figura1.7.

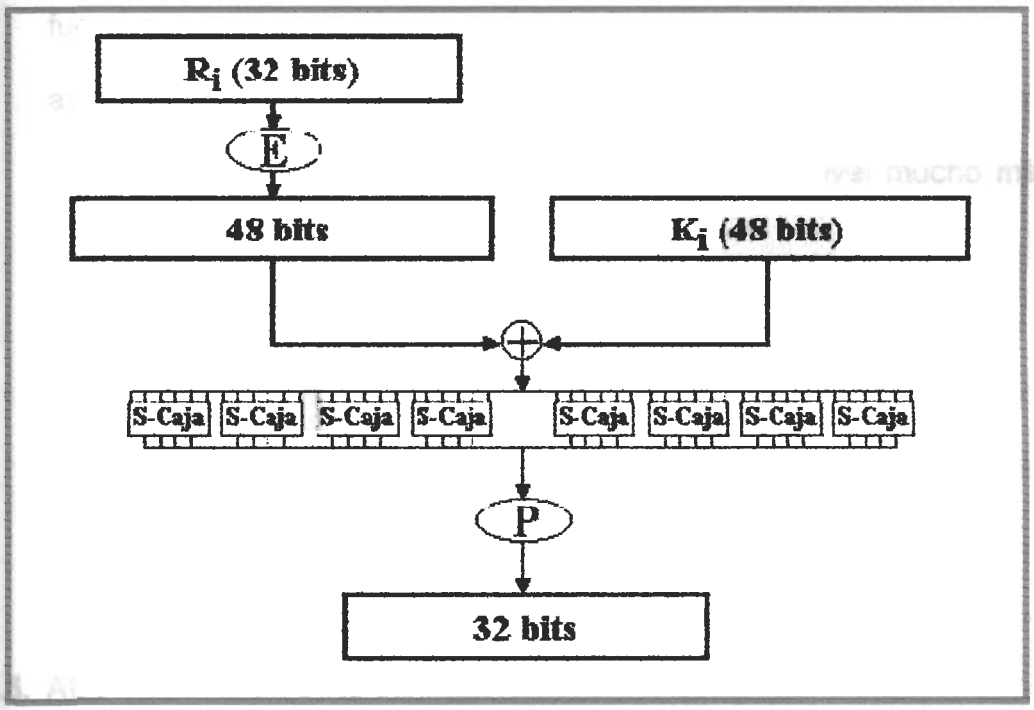


Figura 1.7 Funcionamiento del DES

El algoritmo esta diseñado para cifrar y descifrar bloques de datos de 64 bits bajo el control de la llave de 64 bits; el descifrado se lleva a cabo utilizando la misma llave que la encriptación, pero el algoritmo se aplica de manera inversa.

1.5.4. 3DES

Al encontrar cierta fragilidad en el sistema de codificación DES, los desarrolladores de este sistema aumentaron su complejidad mediante la aplicación de 3 llaves tipo DES y un procedimiento de cifrado y descifrado DES. El triple DES o 3DES fue propuesto por IBM cuando fue claro que la seguridad del DES había sido comprometida por lo avances de la tecnología computacional, comparado con el algoritmo del DES, el algoritmo del triple DES provee de un nivel mucho más alto de seguridad.

Cada proceso de cifrado/descifrado del 3DES (como está especificado en la norma ANSI X9.52) es una operación compuesta de operaciones de cifrado y descifrado DES.

1.5.5. AES

El algoritmo DES fue aceptado hasta finales del siglo XX en USA (y por extensión en el resto del mundo) como estándar de cifrado en bloque especialmente para aplicaciones bancarias pero dejó de serlo después de 20 años debido a su baja longitud de clave (56 bits) y los avances de la informática que lo han convertido en un algoritmo muy vulnerable.

En mayo del año 2002 el NIST National Institute of Standards and Technology elige el algoritmo belga RIJNDAEL como nuevo estándar para algoritmo de cifrado de bloque y se convierte en una norma con el nombre de AES (Advanced Encryption Standard).

Utiliza tamaño de clave variable (128, 192 y 256 bits que es el estándar o bien múltiplo de 4 bytes) y no es un algoritmo de Feistel, es decir, no divide al bloque de texto en claro en dos partes. Aunque utiliza un método de cajas similar al DES, el estándar AES presenta altos niveles de seguridad y todavía no ha sido comprometido.

1.6. Tipos de ataques

En la actualidad existen varios riesgos de seguridad en las redes WLAN, la figura 1.8. muestra pautas de ataques. Todas las redes LAN, cableadas o no, son vulnerables a dos tipos de ataques:

1. Ataques activos en donde los intrusos ganan acceso de la LAN para destruir o alterar los datos.
    - Estos ataques incluyen aquellos en los que se intenta evitar o romper herramientas de protección, introducir código malicioso, robar o modificar información.

- Generalmente este tipo de ataques toman una de estas cuatro formas (o una combinación de ellas): enmascaramiento en el cual el intruso usa exitosamente la identidad de un usuario autorizado en la red, repetición en el cual el intruso monitorea la transmisión pasivamente y luego retransmite los mensajes como si fuera un usuario válido, modificación de mensajes que ocurre cuando un intruso altera los mensajes originales y finalmente DoS (Denial of Service) en el cual el intruso no permite el tráfico normal de la red.

2. Ataques pasivos en donde los intrusos ganan acceso a la LAN pero solo pueden escuchar los datos transmitidos.

- Estos ataques incluyen análisis de tráfico, monitoreo de comunicaciones no protegidas, descifrado de mensajes con pobre encriptación, y captura de información de autenticación.

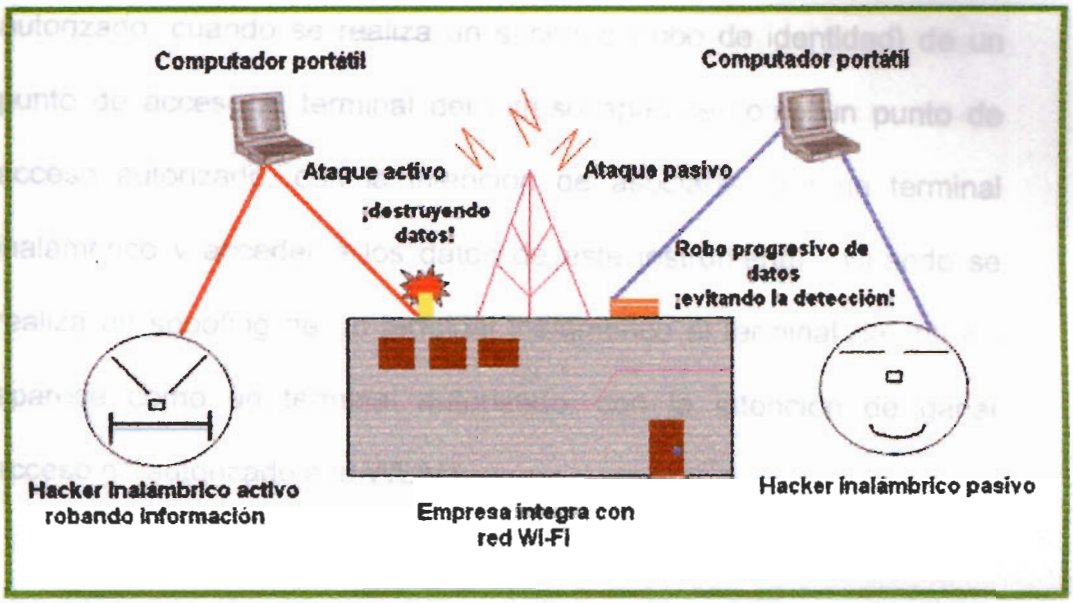


Figura 1.8. Pautas de ataques pasivos y activos

1.6.1. Asociaciones Maliciosas

Este es el más común de los ataques pasivos, la señal de RF de una red 802.11 puede extenderse más allá de los confines de un edificio. Con una laptop o terminal inalámbrico un intruso simplemente transita a través de los distritos de negocios, pacientemente escuchando por una señal RF fuerte; sin buena seguridad, se necesita poco esfuerzo para penetrar en la red.

1.6.2. MAC Spoofing

Uno de los tipos de ataques activos más básico es el de spoofing donde el adversario configura su terminal inalámbrico para parecer que tiene la misma dirección MAC de un punto de acceso o terminal

autorizado, cuando se realiza un spoofing (robo de identidad) de un punto de acceso el terminal del intruso aparece como un punto de acceso autorizado, con la intención de asociarse con un terminal inalámbrico y acceder a los datos de este instrumento. Cuando se realiza un spoofing de un terminal inalámbrico el terminal del intruso aparece como un terminal autorizado, con la intención de ganar acceso no autorizado a la WLAN.

El adversario captura una serie de paquetes de trama inalámbrica obtenidos durante las horas normales de tráfico en la ubicación de la red inalámbrica, las tramas capturadas contienen información necesaria para engañar a los filtros de las direcciones MAC, utilizando estos datos el intruso es capaz de conseguir información muy valiosa del Log localizador de paquetes.

1.6.3. Man in the Middle

El tipo de ataque conocido como Man-in-the-Middle u Hombre en el medio es aquel en el que el adversario evita el proceso de autorización o provee credenciales falsas mediante un hurto de identidad.

El adversario puede utilizar instrumentos inalámbricos para aparecer

como un cliente específico y de esa manera obtener una conexión a la red, este entonces, interrumpe la sesión de datos de un cliente específico y re-dirige el flujo de datos a su máquina; esto le permite al adversario no solo escuchar los datos sino también cambiarlos.

Otra forma de atacar es valiéndose del ARP (Address resolution protocol), el adversario re-dirige a una sesión de un cliente específico mediante un cambio en la tabla de correspondencia MAC/IP, para esto es necesario un acceso a la red de área local.

Este ataque requiere de software sofisticado y puede causar daño significativo y pérdida de datos, el adversario se inserta entre el punto de acceso y el terminal inalámbrico para capturar paquetes en transmisión, el terminal inalámbrico ve al intruso como un punto de acceso autorizado, mientras que el punto de acceso ve al intruso como un terminal autorizado, los dos elementos no detectan al intruso y continúan enviando información, el intruso captura información y es capaz de inyectar falsos datos en la red.

1.6.4. Ataque DoS

El ataque DoS (Denial of Service) interrumpe a la red mediante una inundación del ancho de banda con datos sin sentido con la intención

de causar que la red se paralice. Para iniciar un ataque DoS, el intruso descubre un punto de acceso en la WLAN y luego envía un flujo continuo de información sin sentido. El flujo puede saturar el punto de acceso, causando que este quede fuera de servicio.

Los ataques DoS pueden ser tan sofisticados como enviar tramas de disasociación de administración o tan simples como utilizar un generador de RF en la banda de 2.4 GHz para saturar el canal.

1.6.5. Ataques de inyección

El ataque de inyección supone que el intruso conoce el texto original para un mensaje cifrado y puede utilizar esta información para construir un paquete correctamente cifrado, este proceso incluye construir un nuevo mensaje, calcular el CRC-32 y realizar una serie de cambios para que el texto original del mensaje sea reemplazado por este nuevo mensaje; esto puede efectuarse por la siguiente propiedad: RC4(X) xor X xor Y = RC4(Y), este nuevo paquete puede ser ahora enviado a un punto de acceso o estación móvil y será aceptado como válido.

De esta manera se puede solicitar información de autenticación, incluso sin el conocimiento completo del paquete es posible con

ciertos cambios en los bits del mensaje ajustar el CRC cifrado para obtener una versión correcta del paquete modificado.

1.7. Software para pruebas y monitoreo de seguridad WLAN

En la actualidad existen muchas herramientas para el monitoreo de redes inalámbricas, estas herramientas incluyen software que permite medir parámetros físicos de la red lo que nos ayuda ha mantener un control estricto en niveles de potencia y posibles intrusos, sin embargo también se ha desarrollado software que se aprovecha de las muy conocidas vulnerabilidades del WEP y mediante un simple procesamiento de paquetes capturados puede encontrar las llaves de una red; este tipo de software se puede encontrar incluso de forma gratuita y ha dado paso a una serie de intrusos que hacen uso de estos programas para entrar ilegalmente a redes WLAN.

1.7.1. NetStumbler

NetStumbler es una herramienta para Windows que permite a un usuario detectar WLANs con los estándares 802.11b, 802.11a y 802.11g.

Tiene muchos usos:

1. Verifica que una red esté instalada de la forma predeterminada.

2. Encontrar puntos con mala cobertura en una WLAN.
3. Detectar otras redes que pueden estar causando interferencia.
4. Detectar puntos de acceso no autorizados.
5. Ayudar a apuntar antenas direccionales para enlaces WLAN.
6. Encontrar redes inalámbricas abiertas.

Utiliza el método de escaneo activo enviando una trama cada segundo pidiendo respuesta.

Se ha convertido en una de las herramientas más populares para revelación de redes inalámbricas, parte de su popularidad se debe a que soporta una gran variedad de NICs (Network Interface Cards), además su interfase tipo windows permite ver de manera fácil los puntos de acceso encontrados con su dirección MAC, el SSID, el nombre, el canal, el proveedor, si el WEP está activado o no, la potencia de la señal, y las coordenadas GPS si este punto de acceso tiene un equipo de este tipo.

1.7.2. WEPCrack

WEPCrack es una herramienta de uso abierto para romper las llaves secretas WEP del estándar 802.11. Esta herramienta es una implementación de la forma de ataque descrita por Fluhrer, Mantin,

and Shamir. Su lanzamiento fue en Agosto del 2001 antes que Airsnort, aunque este tuvo una mayor acogida debido a su implementación más completa.

Tiene componentes que le permiten realizar los diferentes pasos del ataque. El WeakIVGen.pl es un programa auto ejecutable (script) que le permite la emulación de una salida IV/cifrado que se podría observar en un punto de acceso. El script prism-getIV.pl busca IVs que se ajusten a la secuencia de las llamadas llaves secretas débiles. Este captura el primer byte del mensaje cifrado y lo reemplaza, poniendo al IV de la llave débil en un log. Finalmente el script WEPCrack.pl utiliza los datos colectados para tratar de encontrar la llave secreta.

1.7.3. Airsnort

La herramienta AirSnort en una WLAN es utilizada para recuperar llaves de cifrado. Es software opera pasivamente monitoreando transmisiones, computando la llave de cifrado cuando una cantidad suficiente de paquetes ha sido obtenida.

Como hemos establecido, el WEP tiene muchas fallas de seguridad. De la misma manera que el WEPCrack, este programa utiliza la debilidad descrita por Fluhrer, Mantin, and Shamir.

AirSnort requiere de aproximadamente 5 a 10 millones de paquetes cifrados para encontrar la llave de cifrado en menos de un segundo.

1.7.4. BTScanner

El BTScanner es una herramienta específicamente diseñada para extraer la mayor cantidad de información posible de un equipo bluetooth sin el equipo requerido. Extrae información HCI y SDP y mantiene la conexión abierta para monitorear el RSSI y la calidad del enlace. Esta basado en el modelo BlueZ Bluetooth snack, que incluye recientes avances Linux.

Además, el BTScanner también contiene una lista completa de los números OUI de la IEEE y las tablas de clase, utilizando esta información es posible encontrar con un pequeño margen de error el tipo de equipo host.

1.7.5. Kismet

Kismet es un detector, sniffer y detector de intrusos para redes inalámbricas 802.11 de nivel dos, trabaja con cualquier tarjeta de red inalámbrica que soporta modo de monitoreo y puede identificar tráfico 802.11b, 802.11a y 802.11g.

Este programa identifica redes mediante un método pasivo de colección de datos y detección de redes que se ajustan al estándar revelando redes escondidas, separa e identifica las diferentes redes inalámbricas en el área, corre en el sistema operativo Linux y su funcionalidad es similar a la de NetStumbler pero con un par de características adicionales como mapeo gráfico y decodificación de paquetes WEP.

1.7.6. SSID Sniff

El SSID sniff puede ser utilizado cuando se busca encontrar puntos de acceso y guardar tráfico capturado, viene con un script configurado y soporta tarjetas Cisco Aironet y aquellas basadas en random prism2.

1.7.7. WIDS

WIDS es un IDS inalámbrico, detecta el atoramiento de tramas de administración y puede ser usado para atraer tráfico inalámbrico, adicionalmente tramas de datos también pueden ser descifradas y vueltas a inyectar en otro equipo.

CAPÌTULO 2

CASO DE ESTUDIO: LABORATORIO DELTA

2.1 Análisis de la Red Actual

Como se mencionó anteriormente la ventaja de las redes de área local inalámbricas es su facilidad de instalación y expansión, aprovechando dichas ventajas el Instituto de Ciencias Humanísticas y Económicas de la Escuela Superior Politécnica del Litoral (ESPOL) decidió implementar una red inalámbrica en uno de sus nuevos laboratorios de computación. Como parte de la optimización del uso de esta red se nos permitió hacer un estudio de seguridad en dicha red, el cual será detallado en este capítulo.

Para comenzar el estudio, lo primero es entender en detalle el funcionamiento de la red, partiremos conociendo los elementos que conforman la red y sus especificaciones, concentrándonos en las

propiedades de seguridad que dichos elementos nos otorgan. Luego analizaremos las vulnerabilidades que la capa física de la red nos presenta, esto se realizará con la ayuda del programa NetStumbler, el cual nos permite medir no solo el nivel de interferencia de otras redes y la potencia de la señal de la red, sino también nos da una idea de que tan vulnerable es la red inalámbrica para intrusiones de agentes externos.

Al finalizar el análisis de la red procederemos a recomendar e implementar posibles soluciones para los problemas de seguridad de la red, finalmente evaluaremos la efectividad de las seguridades implementadas.

2.1.1 Esquema de la red

En la implementación de redes inalámbricas se requieren de ciertos componentes y de la definición de determinados parámetros, cada uno de estos es fundamental para el funcionamiento exitoso de la red.

Primero está el hardware que está compuesto por dos bloques funcionales, los puntos de acceso que conectan a la red y el adaptador inalámbrico instalado en cada computador o terminal.

Los puntos de acceso físicamente son pequeñas cajas, usualmente con una o dos antenas, este receptor/transmisor está conectado a la red alámbrica (LAN) o a un enlace de banda ancha mediante cables Ethernet.

Las antenas o bridges (puentes) mejoran la cobertura de la señal de radio frecuencia, extendiendo el alcance de una WLAN 802.11, los puentes proveen una conexión punto a punto entre dos LANs.

El adaptador inalámbrico funciona como un NIC (network interface card) que permite al cliente del terminal o computador acceder a la red.

Otra parte importante en la implementación de redes inalámbricas es la interoperabilidad, los componentes antes mencionados deben poder interactuar efectivamente y deben ser certificados por la alianza Wi-Fi, en la actualidad la mayoría de los productos en el mercado soportan dicha regulación.

La frecuencia utilizada debe ser otro punto cuidadosamente verificado, se debe procurar que la frecuencia adecuada sea utilizada en los puntos de acceso, seleccionando el canal apropiado; se debe tomar

en cuenta que los productos 802.11a son intrínsicamente incompatibles con los productos 802.11b porque estos trabajan en frecuencias diferentes. Además, aunque los productos 802.11b y 802.11g trabajan en la misma frecuencia, estos deben ser diseñados para trabajar en modo dual o actualizados debido a las diferencias de modulación.

El número de usuarios simultáneos que un punto de acceso puede soportar depende principalmente en la cantidad de tráfico en un determinado momento del día, el ancho de banda es compartido entre los usuarios en una WLAN como en una red cableada; el funcionamiento de una red es dependiente del número de usuarios y la actividad de cada uno de ellos, en el caso de una red 802.11b, cada punto de acceso tiene un throughput de 11 Mbps, esta capacidad es adecuada para:

- 50 usuarios nominales que la mayor parte del tiempo están en descanso y ocasionalmente revisan texto en correo electrónico.
- 25 usuarios que usan mucho el correo electrónico y cargan o descargan archivos de tamaño moderado.
- 10 a 20 usuarios que usan la red constantemente y trabajan

con archivos pesados.

Para incrementar la capacidad, más puntos de acceso deben ser adicionados, lo que permite a más usuarios entrar en la red; en teoría tres puntos de acceso darían un ancho de banda de 33 Mbps para ser compartido entre los usuarios, sin embargo en la realidad cada cliente es asociado con un solo punto de acceso, del cual tiene la señal de mayor potencia, lo que nos indica que estos 33 Mbps pueden no ser equitativamente distribuídos.

Finalmente es muy importante ubicar los puntos de acceso en lugares estratégicos para evitar cobertura para usuarios inapropiados o no autorizados, muchos administradores de red olvidan evitar la ubicación de puntos de acceso en paredes externas, creando riesgos de seguridad en parqueaderos. Mantener un cierto nivel de montado en la señal permite una conexión permanente alrededor del edificio, pero estos deben ser puestos en diferentes canales para evitar interferencia o choque de señales.

La distancia de transmisión y el throughput (rendimiento) de una WLAN tiene una relación inversamente proporcional, en donde el throughput decrece cuando la distancia del punto de acceso se

incrementa, la mayoría de puntos de acceso tienen un rango de alcance de 300 pies (aproximadamente 100 metros).

Las WLAN pueden ser una puerta abierta a la red corporativa. El acceso no autorizado a la red mediante la WLAN puede ser demasiado fácil si no se implementa medidas mínimas de seguridad. Los parámetros que se deben tomar en cuenta para la seguridad en las redes son:

- El SSID (Service Set Identifier) un nombre común que identifica a la red inalámbrica. Este debe ser compartido solo entre aquellos que tienen acceso legítimo a la red y debe ser cambiado periódicamente.

- La dirección MAC (Media Access Control) es la dirección única de cada componente de red que lo identifica. Un filtrado de las direcciones en la red se crea con la ayuda de una lista que se crea para cada punto en cada WLAN.

- El WEP (Wired Equivalent Privacy) mencionado en el capítulo anterior, debe ser activado pues provee la seguridad mínima establecida por el estándar 802.11.

Estos son los parámetros fundamentales de una red WLAN, pero

adicionalmente siempre es útil hacer un censo más profundo del edificio en donde se va ha implementar la red mediante:

- Revisión de los planos y documentos de cableado eléctrico, paredes, puertas y ventanas.

- Identificar los lugares en donde la cobertura será atenuada mediante pruebas preliminares.

- Identificar la interferencia de canales, para una ubicación optima de los puntos de acceso.

- Revisar las conexiones eléctricas para evitar que el rendimiento del punto de acceso se vea afectado por problemas eléctricos aleatorios.

La implementación de la red depende mucho del uso que se le vaya a dar a la misma. De la misma forma el nivel de seguridad y las técnicas utilizadas son específicos para cada red.

Nuestro caso de estudio es la red inalámbrica del laboratorio DELTA del Instituto de Ciencias Humanísticas y Económicas (ICHE) de la ESPOL, esta red fue implementada para estar dentro de un aula, y se utiliza para el dictado de clases donde se requiere principalmente el

uso de los programas utilitarios de Microsoft Office con un acceso al Internet. La red consta de 40 ordenadores dotados con adaptadores de red distribuidos como se indica en la figura 2.1., un router inalámbrico y dos puntos de acceso que funcionan como repetidores.

El hardware utilizado en esta red es marca D-Link:

- Router inalámbrico DI-614+
- Puntos de Acceso DWL-2100AP
- Tarjetas o adaptadores de red DWL-520+

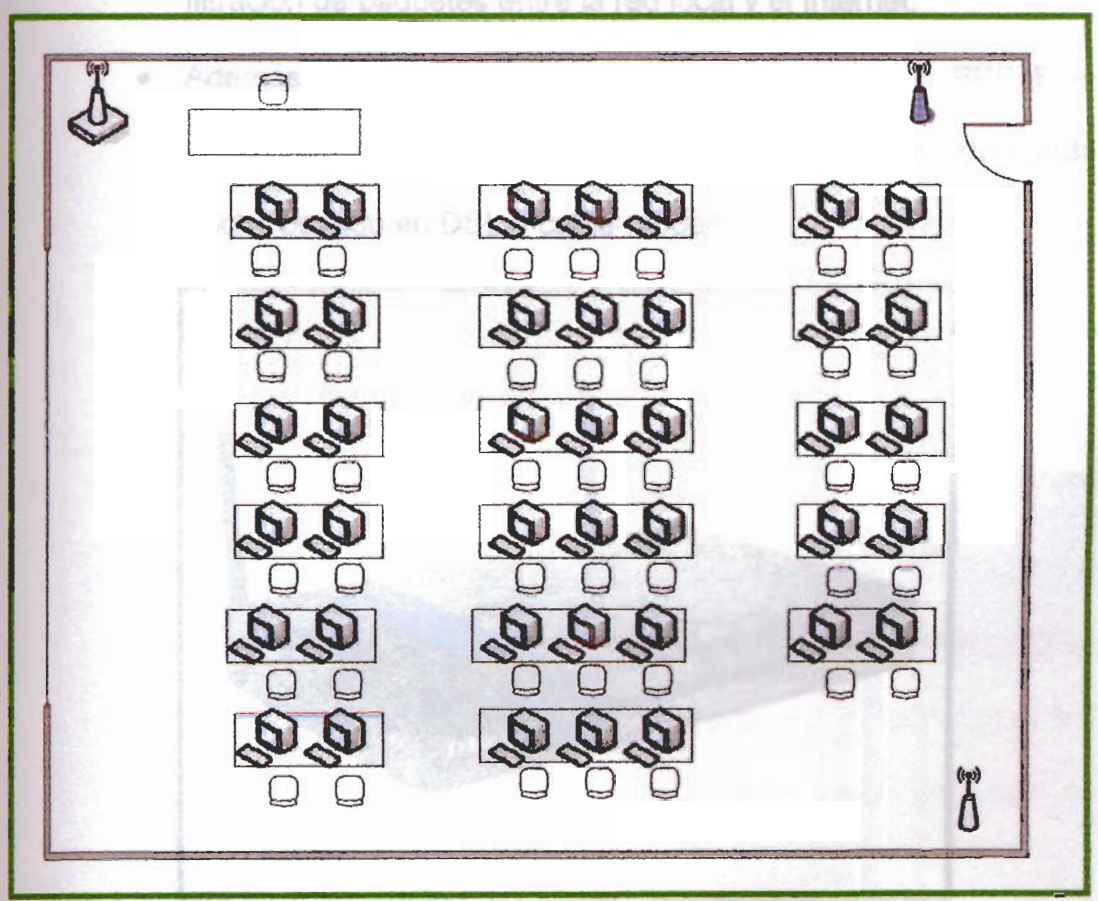


Figura 2.1. Esquema de la Red

Las características del router D-Link DI-614+, el cual se ve en la figura2.2 son:

- Permite una velocidad de 22 Mbps.
- Posee un switch integrado de 4 puertos permite conexión directa hasta con 4 computadores.
- Permite WEP con claves de 64, 128, o 256 bits.
- Permite la implementación de IPSec y redes privadas virtuales (VPN).
- Posee un Firewall integrado, servicio DHCP y servicios de filtración de paquetes entre la red local y el Internet.
- Además soporta direcciones estáticas y posee un PPPoE el cual le permite la conexión con cualquier proveedor de banda ancha basado en DSL o *cable-modem*.

Figura 2.2. Router inalámbrico DI-614+

Las características del punto de acceso DWL-2100AP, el cual se ve en la figura2.3 son:

- Trabaja con los estándares 802.11b (11 Mbps) y 802.11g (54 Mbps).
- Mediante un método propietario de D-Link llamado 108G alcanza velocidades de 108 Mbps.
- Puede trabajar como punto de acceso, puente y repetidor.
- Funciona en la banda de frecuencia de los 2.4GHz a 2.4835GHz.
- Su alcance es de 100 metros en ambientes cerrados y 400 metros en ambientes abiertos.
- Utiliza el método de modulación OFDM.
- Con respecto a la seguridad, este punto de acceso tiene capacidad para claves de 64, 128 y 152 bits en el WEP.
- Puede ser configurado para trabajar con el WPA, el estándar 802.1x, EAP-MD5, EAP-TLS, EAP-TTLS y EAP-PEAP.

Figura 2.3. Punto de Acceso DWL-2100AP

Las tarjetas o adaptadores de red (dispositivo D-Link AirPlus DWL-520+), que se muestra en la figura 2.4. representa un innovador adaptador PCI conforme al estándar IEEE 802.11b dotado de un innovador chip que utiliza la tecnología patentada Digital Signal Processing.

El adaptador DWL-520+ es totalmente conforme con el estándar IEEE 802.11b que hace que sea operativo con todos los dispositivos IEEE 802.11b, conectado a dispositivos conformes con el estándar antes mencionado, el adaptador soporta un aumento de la velocidad de transmisión del 20%.

En caso de conexiones con otros productos D-Link AirPlus, las prestaciones son todavía más elevadas y la velocidad alcanza los 22Mbps; el adaptador DWL-520+ ofrece además un cifrado WEP a 256 bits, lo que garantiza un alto nivel de seguridad para los datos en las comunicaciones.

Figura 2.4. Tarjeta de red D-Link AirPlus DWL-520+

El adaptador D-Link AirPlus DWL-520+ incluye una utilidad de configuración que permite identificar las redes inalámbricas disponibles y soporta la creación y la memorización de perfiles de conexión detallados para las redes utilizadas con más frecuencia; el dispositivo DWL-520+ es una potente tarjeta PCI a 32 bits que puede instalarse rápida y fácilmente en un PC, utilizando el adaptador con otros productos D-Link AirPlus es posible disponer de una conexión

inmediata a la red. Estos adaptadores inalámbricos pueden utilizarse en modalidad ad-hoc para conectarlos directamente a otras tarjetas o en modalidad infraestructura para conectarlos a un punto de acceso inalámbrico, garantizando el acceso a Internet desde casa o desde la oficina. Para conocer información técnica del router y los ap, se puede observar el anexo 3.

La ubicación física del laboratorio es en el bloque de aulas 32-B, al lado izquierdo se encuentra un pequeño jardín y a continuación un comedor, en la derecha están oficinas separadas por un corredor, en la parte frontal se ubica un aula y en la posterior es un paso de acceso libre entre los dos bloques de aulas y unas escaleras que dan acceso a los pisos superiores, esto se puede observar en la figura 2.8.

Después de la instalación de la red no se realizaron cambios mayores a las configuraciones por lo que la mayoría de los parámetros de la red están con los valores predeterminados de fábrica y sin ninguna especificación con respecto a la seguridad.

2.1.2 Pruebas de Campo de alcance de la señal

El mejor método para revisar las necesidades de seguridad de una red es utilizando las herramientas disponibles para los posibles intrusos de la red, para el monitoreo de la red utilizamos el programa NetStumbler,

este programa gratuito nos fue muy útil para tener una mejor idea del funcionamiento de la red y las vulnerabilidades de esta.

El primer paso del monitoreo fue determinar que información de la red estaba accesible a cualquier usuario externo con una computadora portátil.

La figura 2.5. muestra la interfaz presentada por el programa NetStumbler, lo que proporciona la siguiente información sobre la red:

- El SSID es DELTA.
- La dirección MAC del router es 004005B5FE13.
- La dirección MAC del primer punto de acceso es 000F3DA25D6C.
- La dirección MAC del segundo punto de acceso es 000F3DA25D62.
- Ambos están trabajando en el canal 1. El programa divide a las señales según el canal en el que trabajan por lo que pudimos ver que los únicos puntos de acceso trabajando en Δ^{1} son los del laboratorio DELTA.

- Los niveles de señal, relación señal a ruido y potencia en cada instante.

- No está activado ningún tipo de seguridad. Esto lo podemos determinar mediante los símbolos al lado izquierdo de la dirección MAC:

  Sin seguridad

  WEP activado

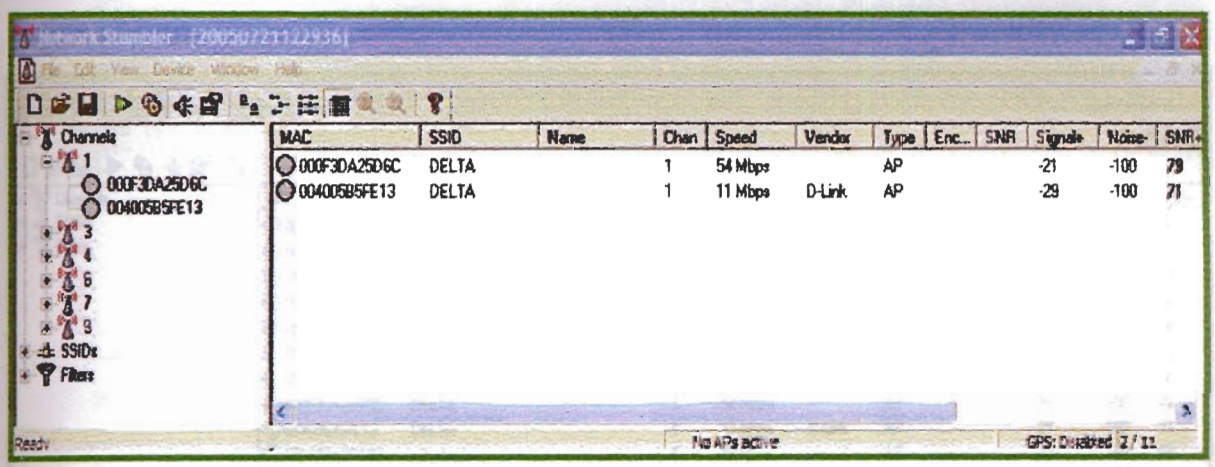


Figura 2.5. Datos mostrados por NetStumbler de la red

Todos los datos mencionados están disponibles para cualquier usuario que posea este u otro programa de monitoreo de seguridad. Además, cualquier usuario externo puede recibir una dirección temporal gracias al servidor DHCP y acceder sin ningún problema a la red.

Debido a que poca información sensible se va a transmitir en esta red,

el problema de seguridad se centra en el uso del limitado ancho de banda de la red inalámbrica, lo que podría causar posteriores problemas de conexión.

En la vecindad del laboratorio DELTA encontramos nueve redes en un área de aproximadamente 50 metros alrededor del laboratorio, las cuales podrían causar interferencia, la figura 2.6 muestra la información obtenida en la vecindad de la red.

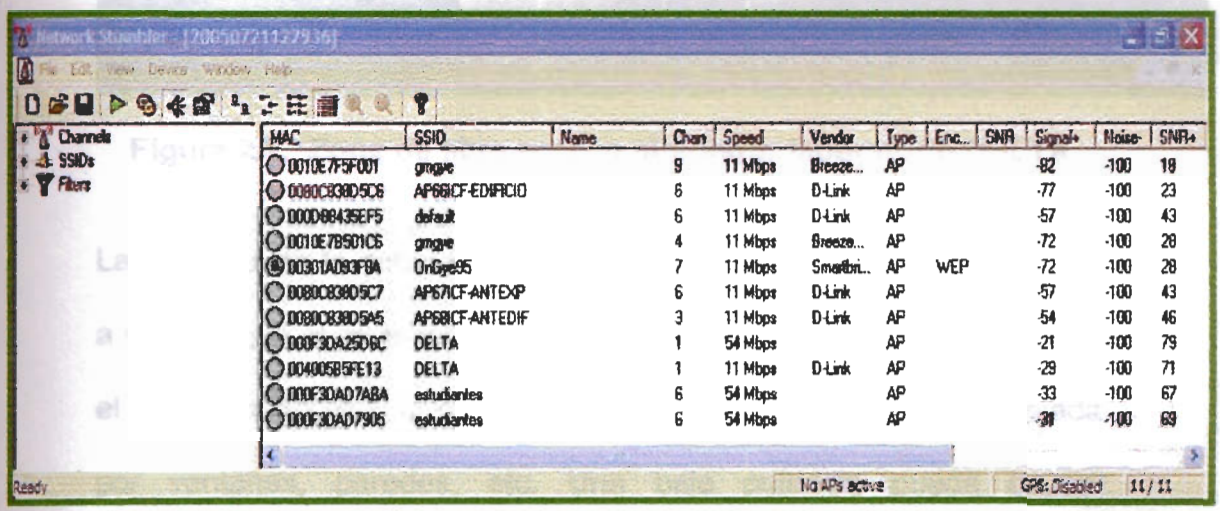


Figura 2.6. Información obtenida en la vecindad de la red con NetStumbler

El programa permite ver la potencia de la señal en diferentes ubicaciones, para este propósito requerimos medir la potencia de la señal fuera del laboratorio DELTA en donde una señal permitiría a intrusos ingresar a la red.

Figura 2.7. Zona de libre acceso alrededor laboratorio DELTA

La potencia de la señal es atenuada por interferencia de varios tipos, a medida que el receptor se aleja del emisor, en el caso de las WLAN el punto de acceso, la potencia de la señal es refractada y reflejada por ventanas, paredes, etc. Una baja potencia puede causar problemas de recepción y uso de la red, por otro lado, una señal en lugares no regulados permite que intrusos no permitidos puedan formar parte de la red, la figura 2.7. muestra una zona de libre acceso alrededor del laboratorio.

La potencia del emisor, la pérdida y la sensitividad del receptor

contribuyen a la potencia de la señal en el lado del receptor. Esta se mide como SNR (signal-to-noise ratio) o relación señal a ruido. El SNR compara la potencia pico de la señal a la potencia del ruido. El ruido se refiere a la radiación de radio frecuencia presente en el ambiente. Tanto el SNR como el ruido se miden en decibeles.

Se considera que los niveles promedio de relación señal a ruido permisibles en una WLAN son:

- 40dB SNR = Señal excelente.
- 25dB a 40dB SNR = Señal muy buena.
- 15dB a 25dB SNR = Señal baja.
- 10dB a 15dB SNR = Señal muy baja.
- 5dB a 10dB SNR = No hay señal.

La medida de la relación señala ruido en el receptor se hizo en seis zonas que podían presentar un peligro para la seguridad debido a que son zonas de libre circulación y sin ningún tipo de supervisión; las primeras tres zonas son las escaleras que se ubican en la parte posterior del laboratorio, la zona 4 y 5 son dos puntos en el comedor en la parte izquierda, finalmente las últimas dos zonas se refieren a las escaleras del bloque de aulas adyacente al del laboratorio DELTA y al paradero de buses. Observamos la relación señal a ruido desde las

figuras 2.9. hasta la figura 2.20.

Los colores con que están representadas las mediciones tomadas en las diferentes zonas no son los colores originales del programa NetStumbler, se han modificado para facilitar la comprensión de los mismos. En la tabla 2.1. vemos el registro de la relación señal a ruido en las seis zonas analizadas.

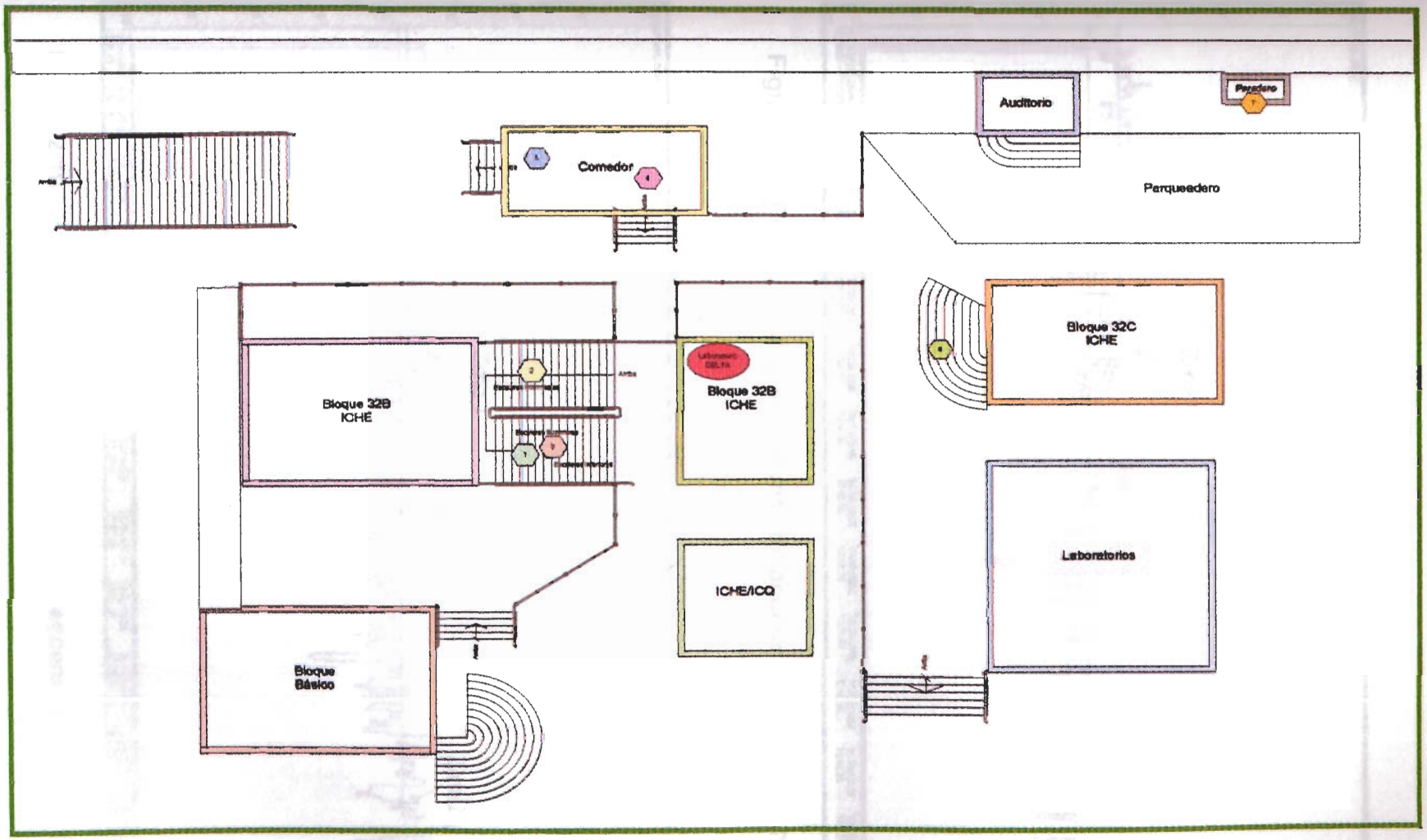


Figura 2.8. Mapa de las zonas de prueba

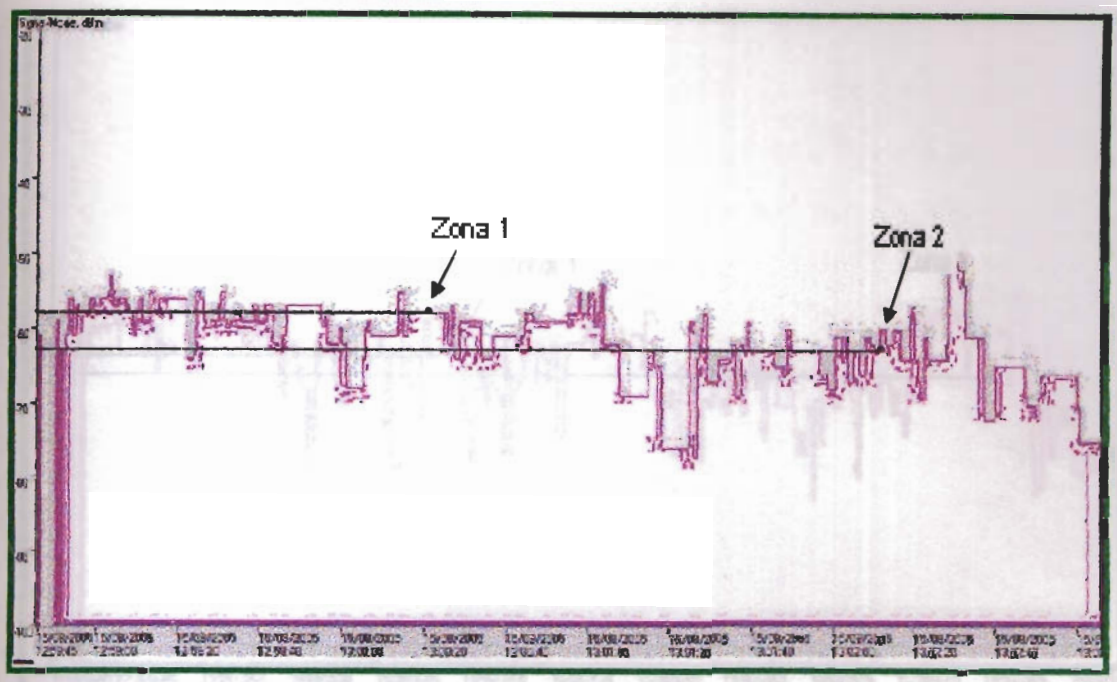


Figura 2.9. Potencia del primer punto de acceso en zonas 1 y 2

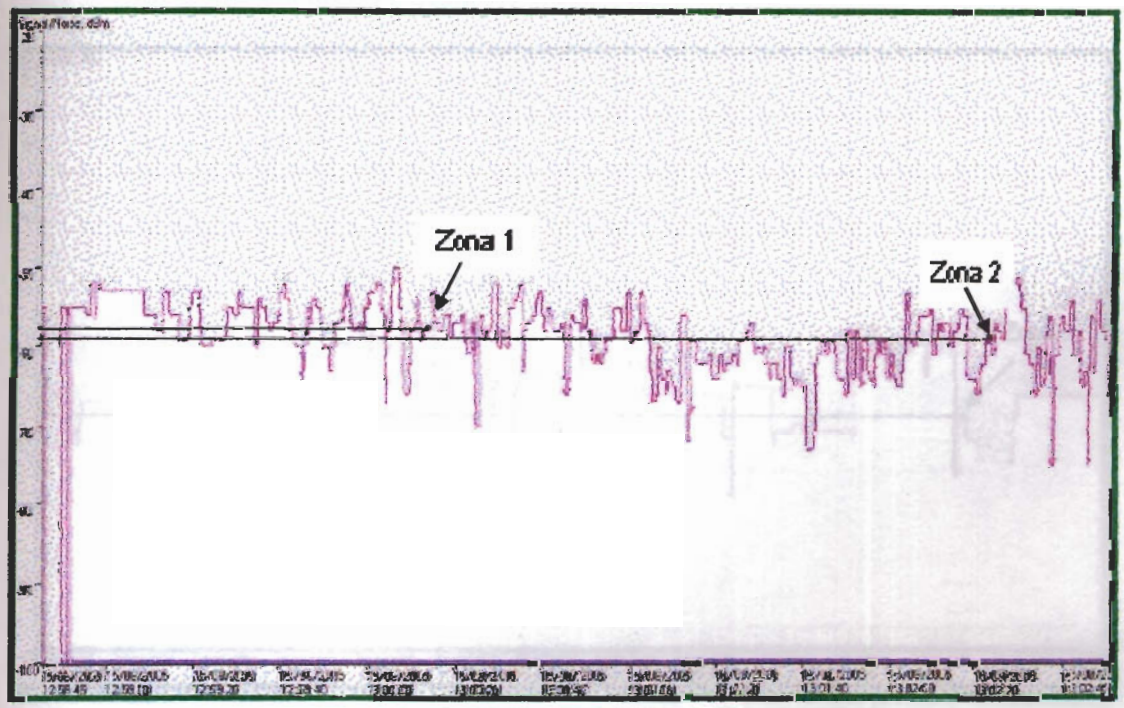


Figura 2.10. Potencia del segundo punto de acceso en zonas 1 y 2

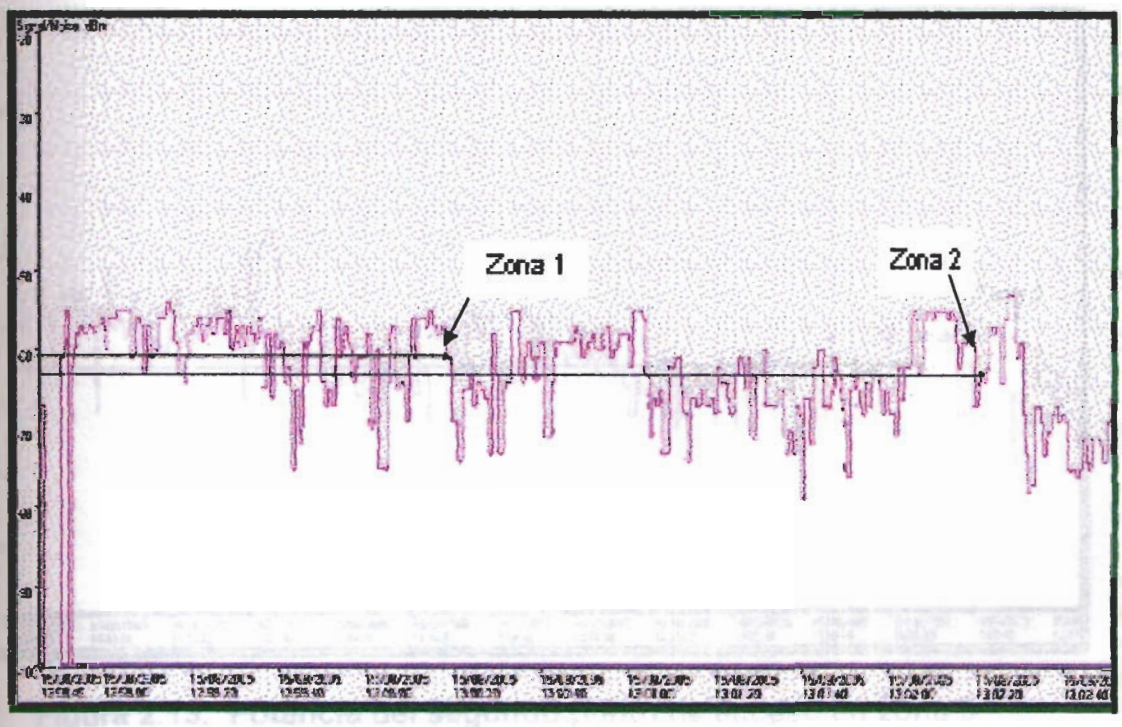


Figura 2.11. Potencia del router en zonas 1 y 2

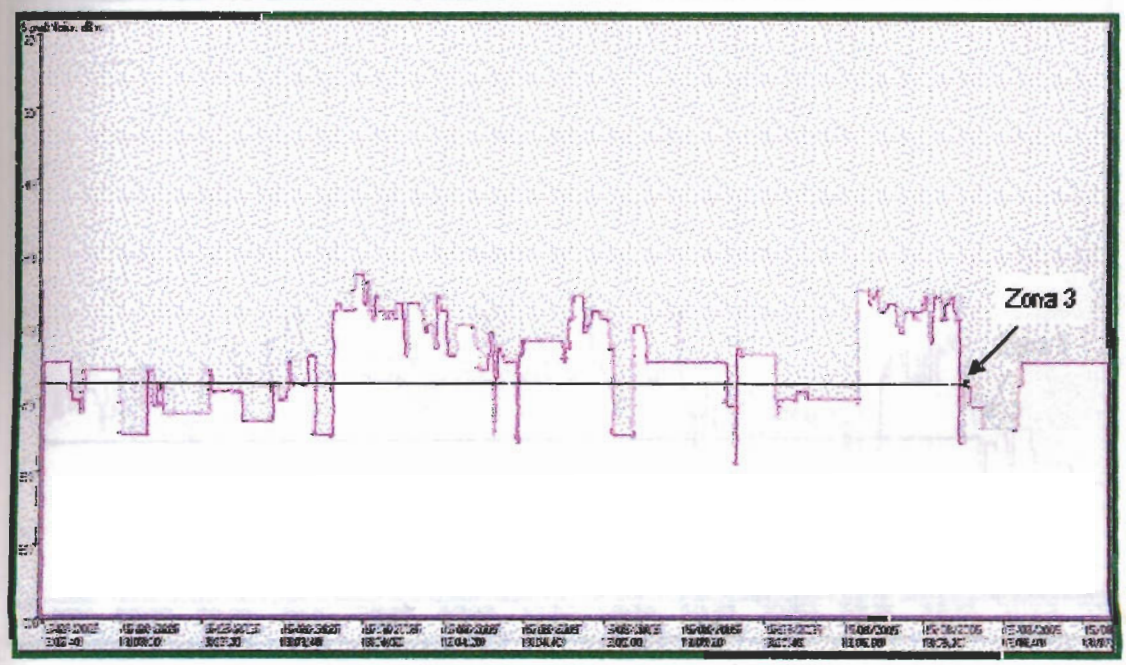


Figura 2.12. Potencia del primer punto de acceso en la zona 3

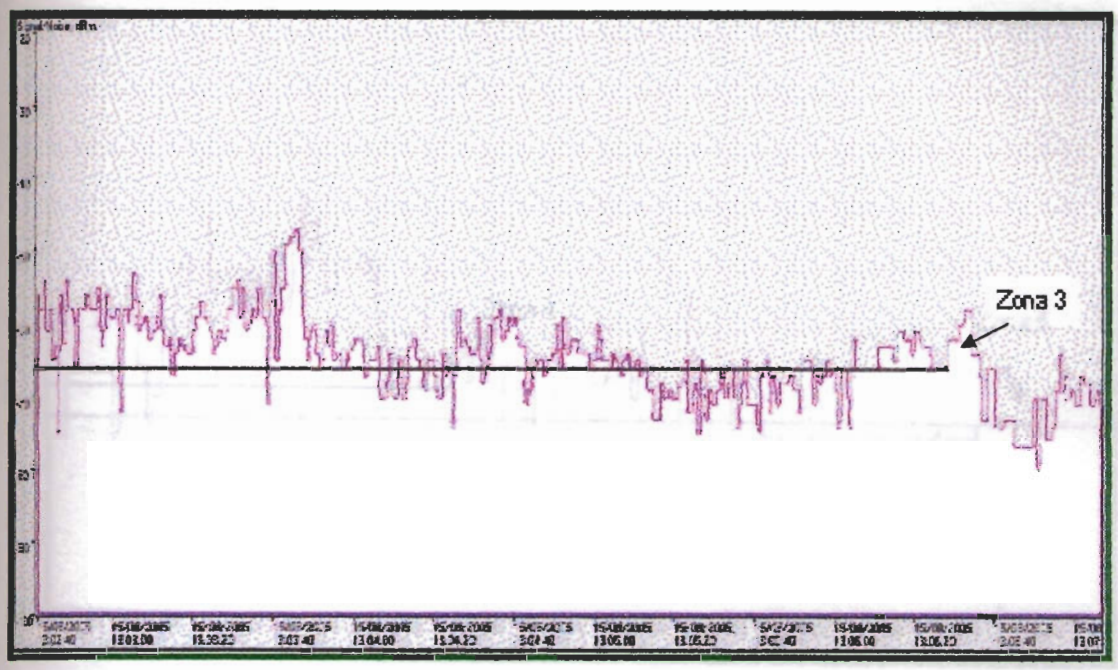


Figura 2.13. Potencia del segundo punto de acceso en zona 3

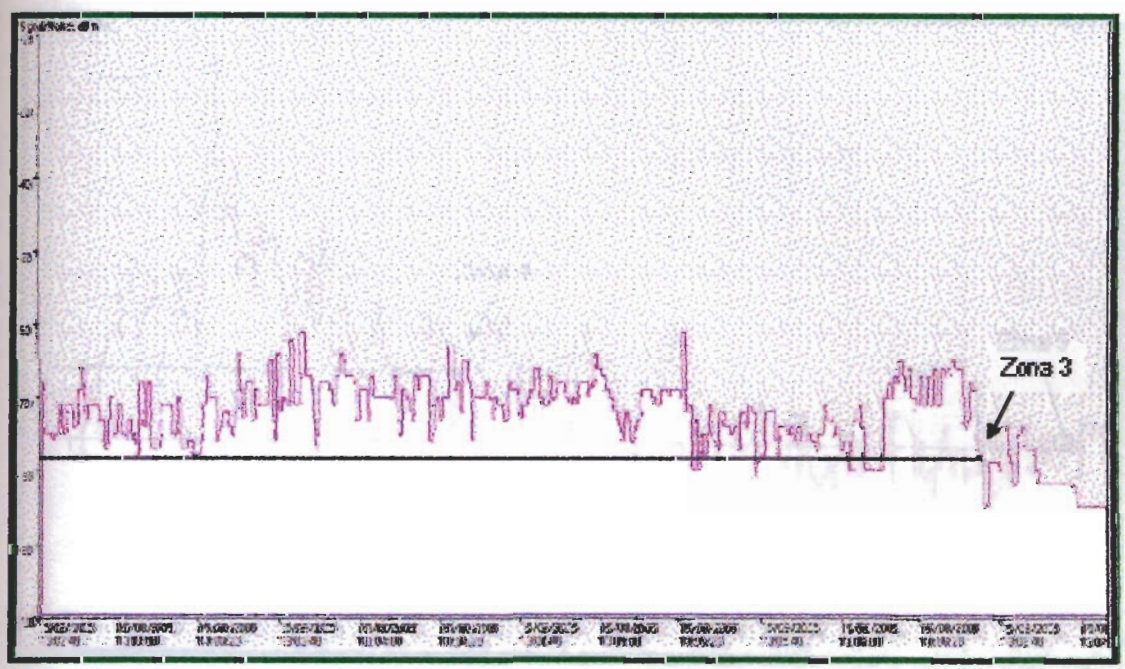


Figura 2.14. Potencia del router en zona 3

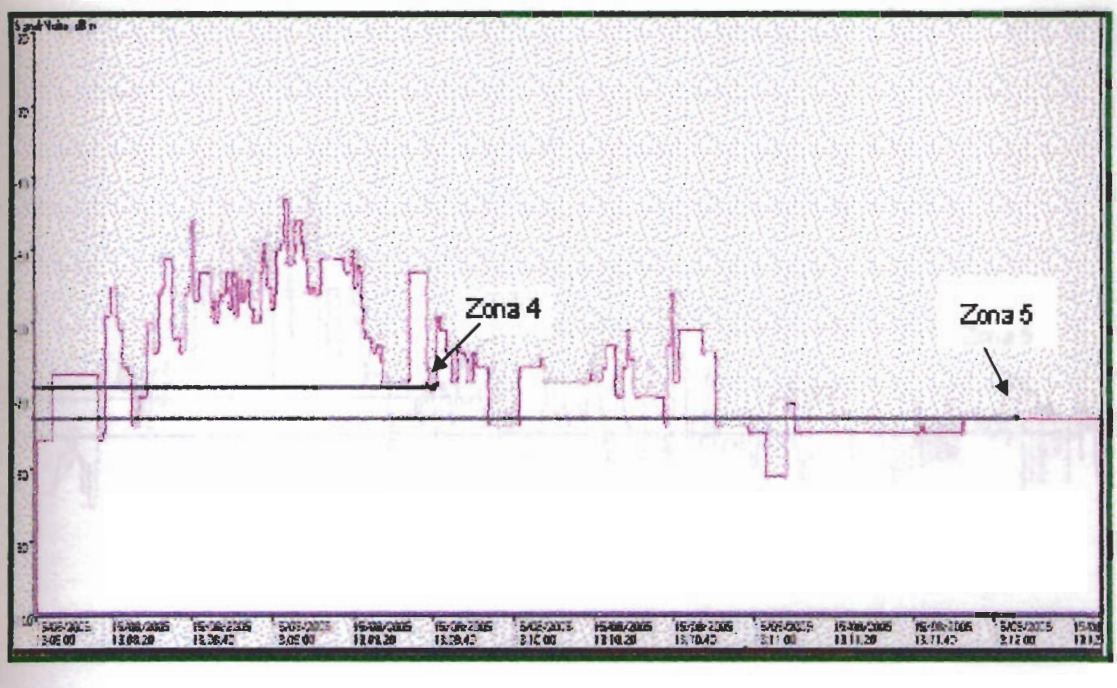


Figura 2.15. Potencia del primer punto de acceso en zonas 4 y 5

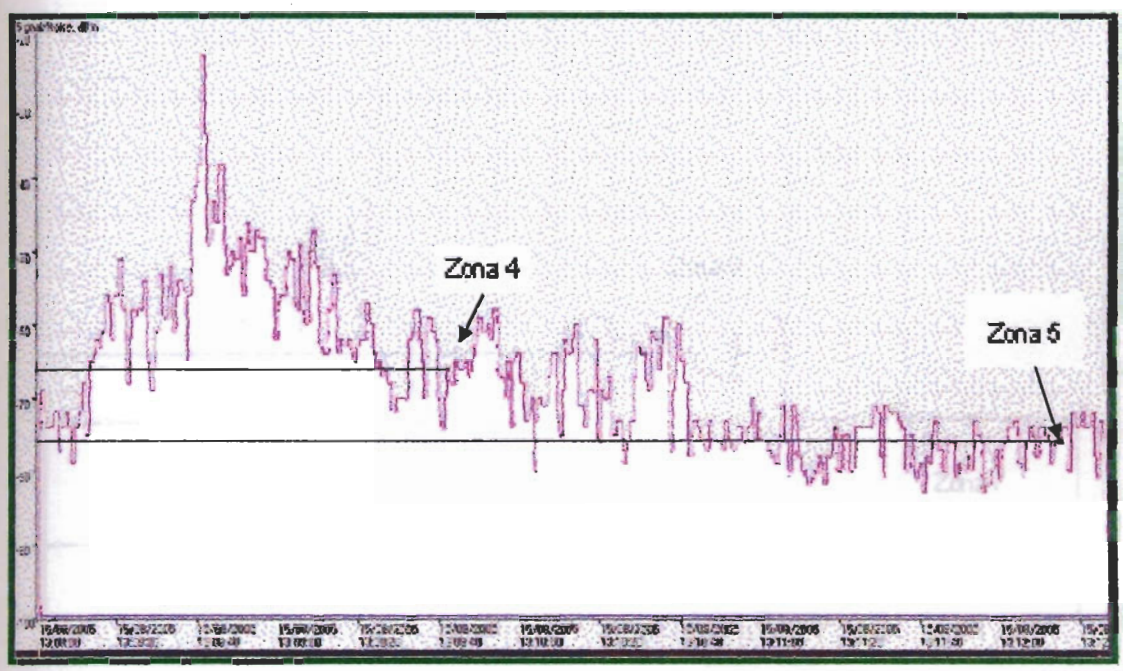


Figura 2.16. Potencia del segundo punto de acceso en zonas 4 y 5

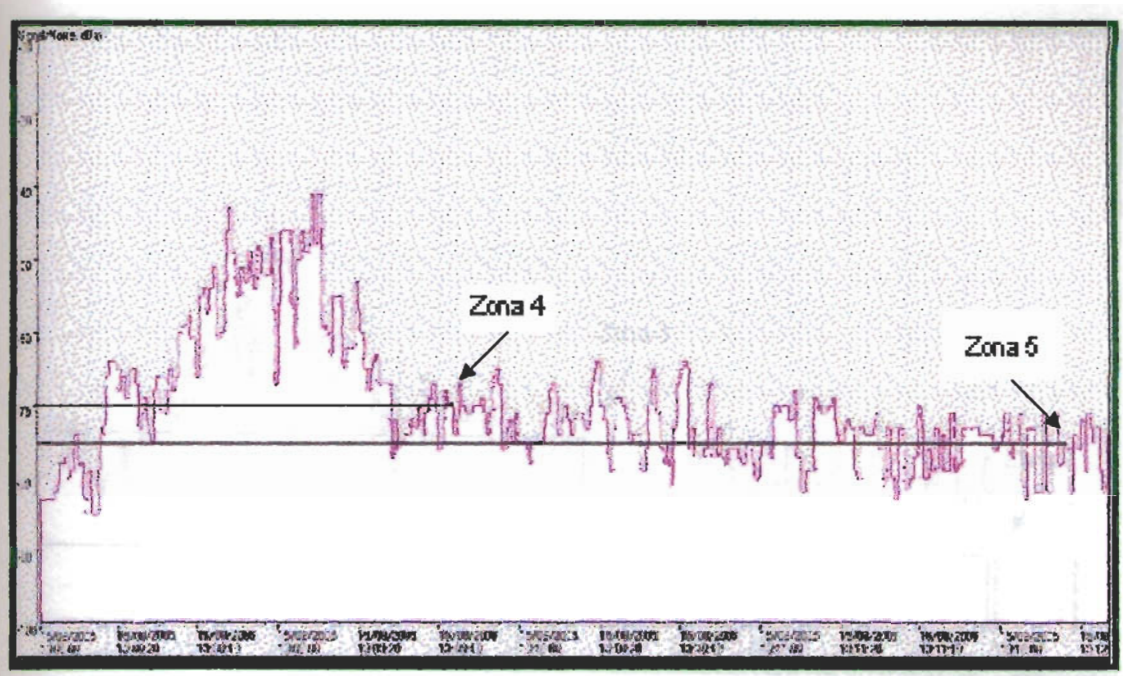


Figura 2.17. Potencia del router en zonas 4 y 5

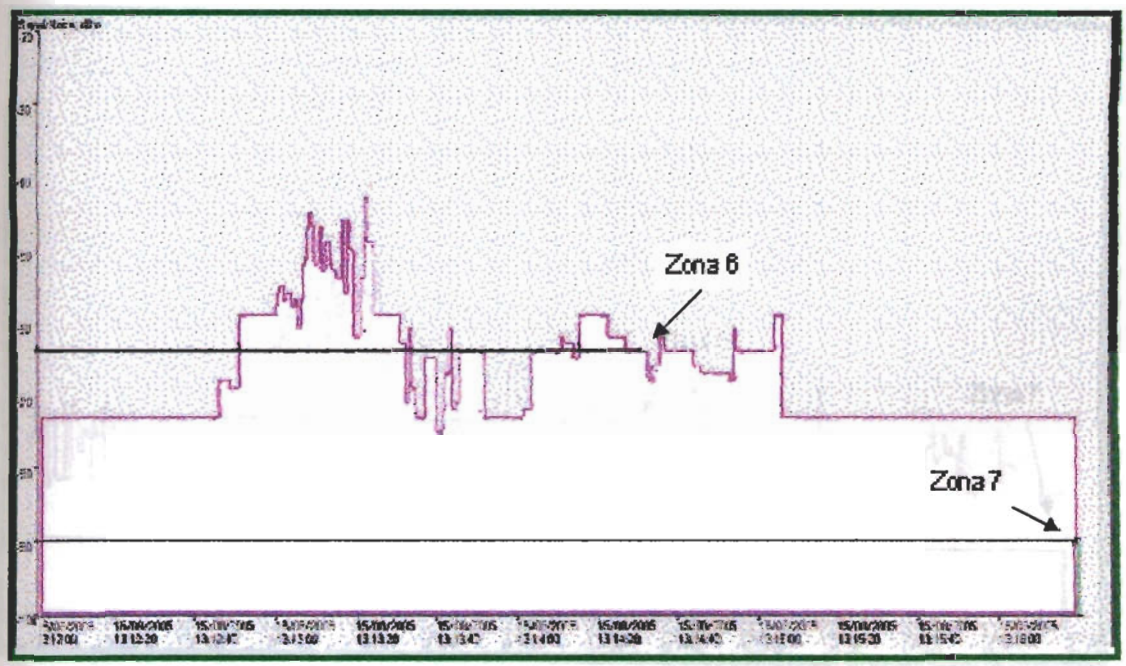


Figura 2.18. Potencia del primer punto de acceso en la zona 6 y 7

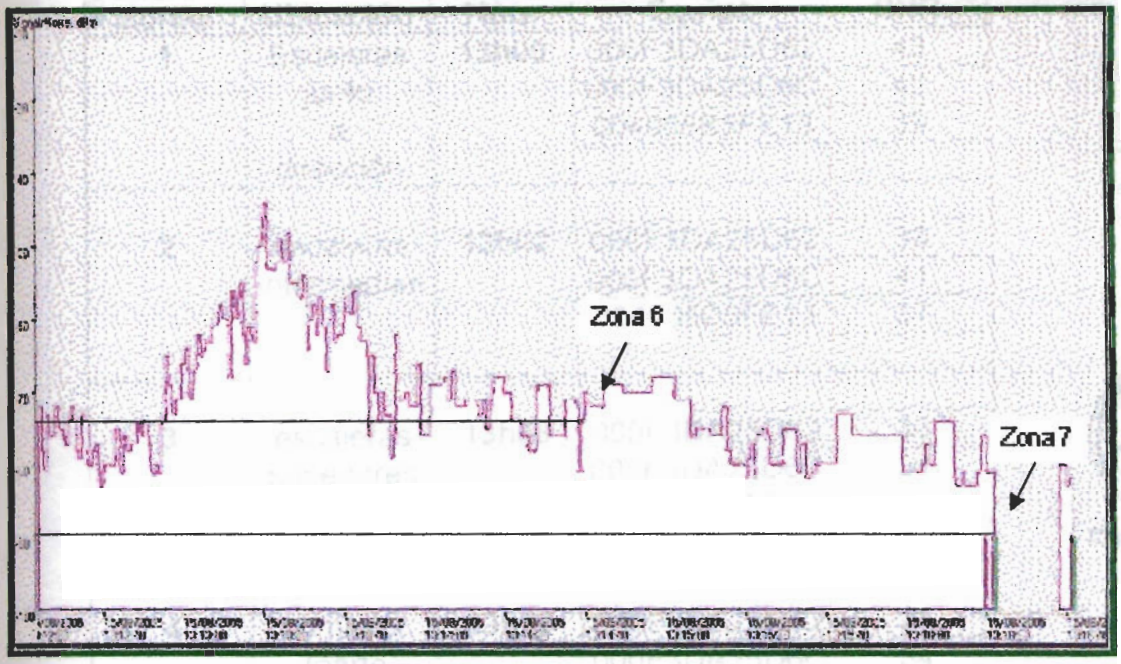


Figura 2.19. Potencia del segundo punto de acceso en zonas 6 y 7

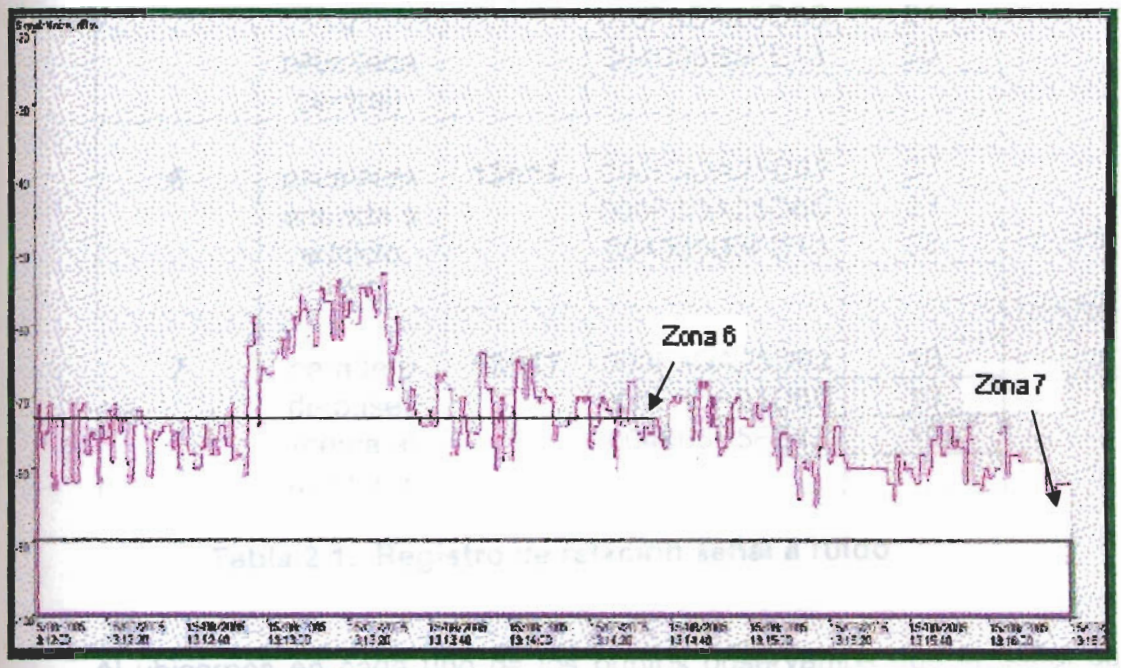


Figura 2.20. Potencia del router en zonas 6 y 7

Zonas	Ubicación	Hora	Equipo	SNR
1	Escaleras junto a dirección	13h00	000F3DA25D62	43
			000F3DA25D6C	42
			004005B5FE13	39
2	escaleras intermedias	13h02		
			000F3DA25D62	38
			000F3DA25D6C	41
			004005B5FE13	37
3	escaleras superiores	13h06		
			000F3DA25D62	38
			000F3DA25D6C	34
			004005B5FE13	22
4	comedor (parte central)	13h09		
			000F3DA25D62	31
			000F3DA25D6C	34
			004005B5FE13	30
5	comedor (escaleras a bilbioteca central)	13h12		
			000F3DA25D62	27
			000F3DA25D6C	24
			004005B5FE13	25
6	escaleras entrada a edificio 32 C	13h14		
			000F3DA25D62	37
			000F3DA25D6C	27
			004005B5FE13	28
7	paradero de buses (cerca al auditorio)	13h17		
			000F3DA25D62	10
			000F3DA25D6C	10
			004005B5FE13	10

Tabla 2.1. Registro de relación señal a ruido

Al ubicarnos en cada uno de los puntos observamos que la señal es fuerte en la zona 1, 2, 3, 4 mientras que en las otras zonas la señal era

más atenuada, en la zona 5 y 6 seguía siendo viable la captura de paquetes pero en la zona 7, el paradero, la señal era casi nula.

2.1.3 Determinación de Riegos de seguridad

Finalmente después de revisar todos los datos obtenidos se procede a determinar cuales son los riesgos de seguridad que presenta la red inalámbrica del laboratorio DELTA, esto requiere un análisis de tres puntos:

1. Los riesgos que implica la ubicación física de la red.
2. El tipo de intrusos que pretendieran entrar a la red.
3. La clase de información que circula en la red.

Ubicación física: Determinamos que la red del laboratorio DELTA esta en una posición bastante vulnerable pues alrededor existe un gran espacio abierto sin supervisión, cualquier usuario con una computadora portátil puede ubicarse en esta área sin ningún problema y sin llamar mayormente la atención, como lo pudimos comprobar personalmente.

Alrededor del laboratorio existen también una serie de redes inalámbricas que pueden causar cierto nivel de interferencia. Esto ocasiona problemas funcionales y es necesario establecer un canal

libre para que pueda trabajar la red.

Con la ayuda del software vimos exactamente en que zonas la señal permite que cualquier usuario pueda ingresar a la red; en las escaleras entre los bloques claramente pudimos notar que la señal permitía el acceso sin ningún problema, en el comedor la señal era menor, pero igual permitía la intrusión, la señal era mínima en el paradero y en el bloque 32C, aunque en este último si sería permisible la captura de paquetes.

La ubicación de los puntos de acceso, cada uno en una esquina, evita que la señal sea limitada solo al laboratorio, por esta razón existe una fuerte señal en el exterior.

Intrusos: El laboratorio DELTA se encuentra en el campus Prosperina de la ESPOL., debido a la distancia a la que este campus se encuentra de la ciudad de Guayaquil la población que se encuentra en está área es principalmente estudiantes universitarios y profesores.

Con pocas excepciones, este tipo de personas simplemente requeriría acceso a la red para el uso de Internet; el nivel tecnológico de nuestro país es un limitante, aunque existe una gran acogida de la tecnología

portátil e inalámbrica a nivel corporativo, no muchas personas en el Ecuador tienen los recursos económicos para adquirir este tipo de implementos, esto disminuye el número de posibles intrusos.

Además, no muchas personas conocen las técnicas utilizadas para la intromisión y observación de redes, aunque esta información está disponible libremente en el Internet.

Clase de información: Por la naturaleza de la red la información que circula es muy poco sensible, como se mencionó la utilidad de la red se limita al uso del Internet, no es una red corporativa por lo que ninguna información financiera o administrativa importante es enviada.

El problema principal de seguridad sería el uso de los recursos de la red, es decir, el ancho de banda para el acceso a Internet, un gran número de usuarios externos podría saturar a la red, además, un usuario pernicioso podría utilizar la red como fuente de un ataque externo.

Sin descartar por supuesto a intrusos maliciosos que simplemente pretendan manipular la red creando congestión con ataques de DoS, existirán usuarios cuya única intención es causar problemas o medir

sus capacidades.

A todos estos posibles riesgos se suma el hecho de que en un futuro la tecnología del Internet nos permitirá hacer todas las transacciones financieras en línea, en la actualidad muchos usan el Internet para hacer compras enviando números de tarjetas de crédito o datos personales confidenciales, si bien es cierto esta información está protegida por sus propios medios de seguridad, muchas veces esta información es confirmada en nuestras cuentas de correo electrónico y en la red inalámbrica todos estos datos están disponibles para cualquier intruso con el suficiente conocimiento y un software capturador de paquetes.

2.2 Implementación de seguridades

Cuando hablamos de implementar seguridades en general estamos tocando una de las partes más importantes de la administración de una red, cada sistema de seguridad se ajusta a las necesidades y recursos de la WLAN.

El sistema de seguridad que se tenía en el laboratorio Delta era nulo en el momento del análisis. Se procedió a realizar una implementación de seguridad muy básica en función de la importancia

de los datos que transitan por esta red y al limitante económico.

2.2.1 Implementación del WEP como sistema de seguridad

Aun conociendo las vulnerabilidades del WEP como sistema de seguridad cabe resaltar que éste resulta mejor que no tener ninguno, es más, el nivel de tecnología que existe en nuestro país lo convierte en un sistema bastante sólido, como mencionamos, no existe mucha gente en la capacidad para convertirse en intruso de una red inalámbrica.

También se toma en cuenta que los datos que desea proteger la red del laboratorio DELTA no justifican una gran inversión en seguridad, el implementar en WEP reducirá significativamente el ingreso de personas ajenas a la red que simplemente quiera utilizar el ancho de banda de Internet; además este también impedirá una captura de paquetes rudimentaria.

Como mencionamos todos los equipos inalámbricos que son certificados por la alianza WI-Fi permiten la implementación de una clave WEP para cifrar los datos, los equipos D-Link no son la excepción.

Para activar el WEP entramos a la página de configuración del router, abrimos el browser del Internet Explorer y tipeamos la dirección IP del router, allí se requiere ingresar la clave de administrador, que siempre debe ser cambiada del valor predeterminado de fábrica, aquí encontramos toda la información de la configuración del DI-614+. La figura 2.21. muestra la información del router DI-614+.

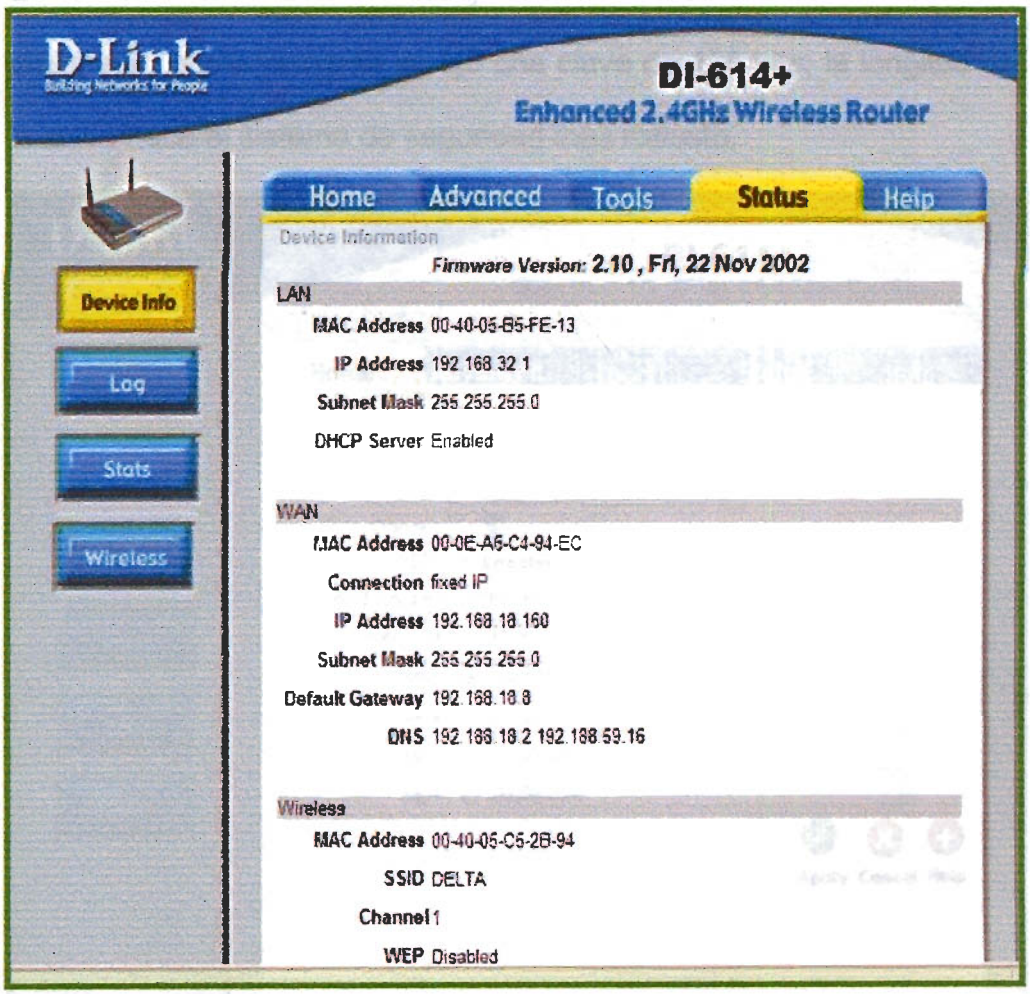


Figura 2.21. Pantalla de información del router DI-614+ laboratorio DELTA

Para poder configurar el WEP fuimos a la ventana *Home* y en la viñeta *Wireles* encontramos los valores determinados para el SSID, el canal y el WEP, activamos el WEP (Seleccionando Enabled) e ingresamos la clave; se debe seleccionar la longitud de la clave y el formato, que puede ser hexadecimal o ASCII. La figura 2.2.. muestra la pantalla de configuración del WEP.

En el laboratorio DELTA se fijo una clave de 64 bits de manera preliminar, posteriormente se fijó una clave de 128 bits; la longitud de la clave hace el sistema de seguridad más robusto.

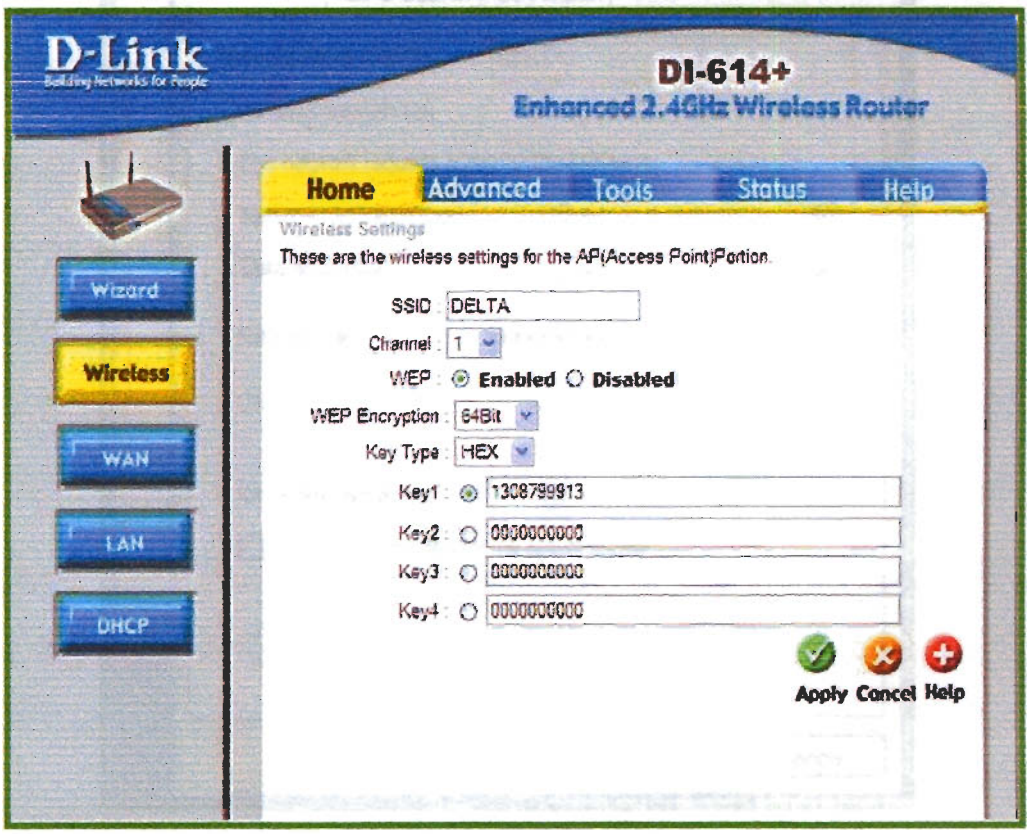


Figura 2.22. Pantalla de configuración del WEP laboratorio DELTA

Adicionalmente se requiere configurar el WEP con la misma clave en cada una de las PC dentro de la red, este cambio se realiza en la parte de propiedades de la conexión inalámbrica, en la ventana de *wireless networks,* aquí entramos la ventana de propiedades de la red DELTA. La figura 2.23. muestra la ventana de configuración del WEP.

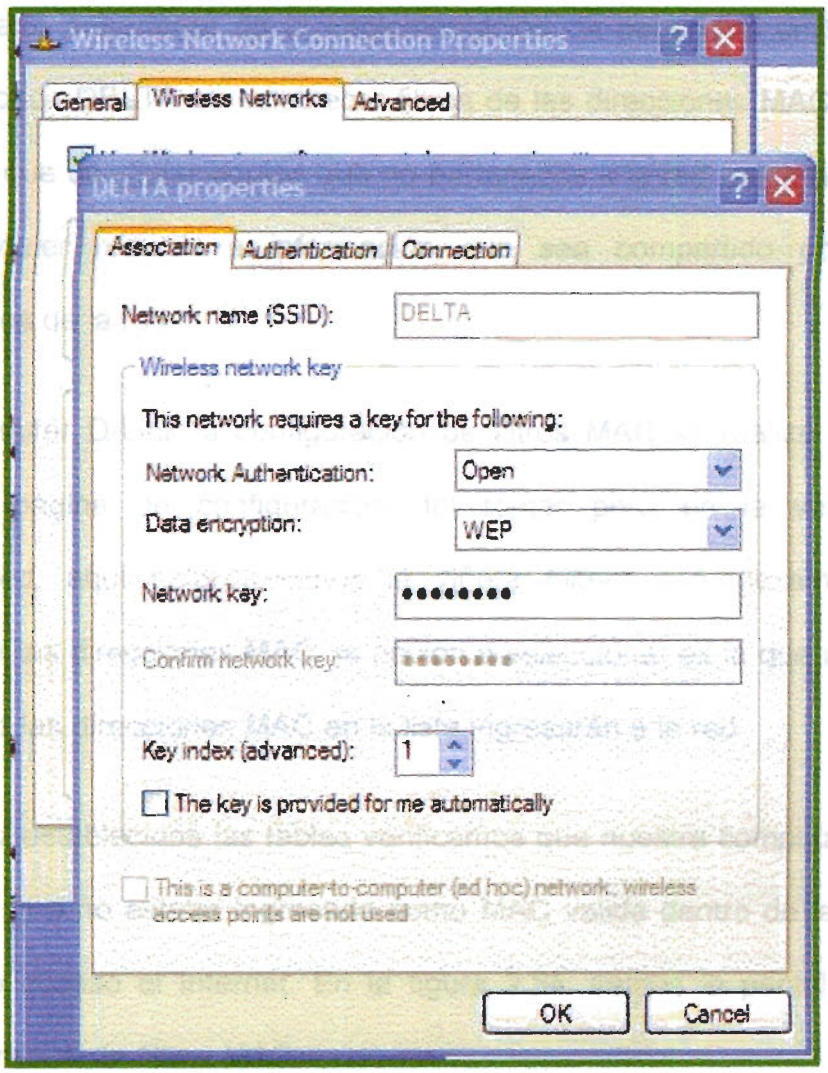


Figura 2.23. Ventana de configuración del WEP en cada terminal

Cabe resaltar que el momento que se activa el WEP en el router las computadores se desconectan de la red hasta que se reinicie, finalmente pudimos comprobar que si el WEP no estaba activado en los terminales estos no ingresan a la red.

2.2.2 Creación de filtros MAC

Otra parte importante de la implementación de seguridad en la red inalámbrica DELTA es establecer filtros de las direcciones MAC, esto impide que cualquier equipo que no pertenezca a la red tenga acceso a cualquier recurso e información que sea compartido por los miembros de la red.

En el router D-Link la configuración de filtros MAC se realiza en la misma página de configuración del router pero en la ventana *Advanced,* aquí seleccionamos la viñeta *Filters* y empezamos a ingresar las direcciones MAC, la opción a seleccionar es la que indica que solo las direcciones MAC en la lista ingresarán a la red.

Una vez establecidas las tablas verificamos que nuestra computadora portátil, que no estaba ingresada como MAC valida dentro de la red, no tuvo acceso al Internet. En la figura 2.24. vemos la pantalla de configuración de filtros MAC.

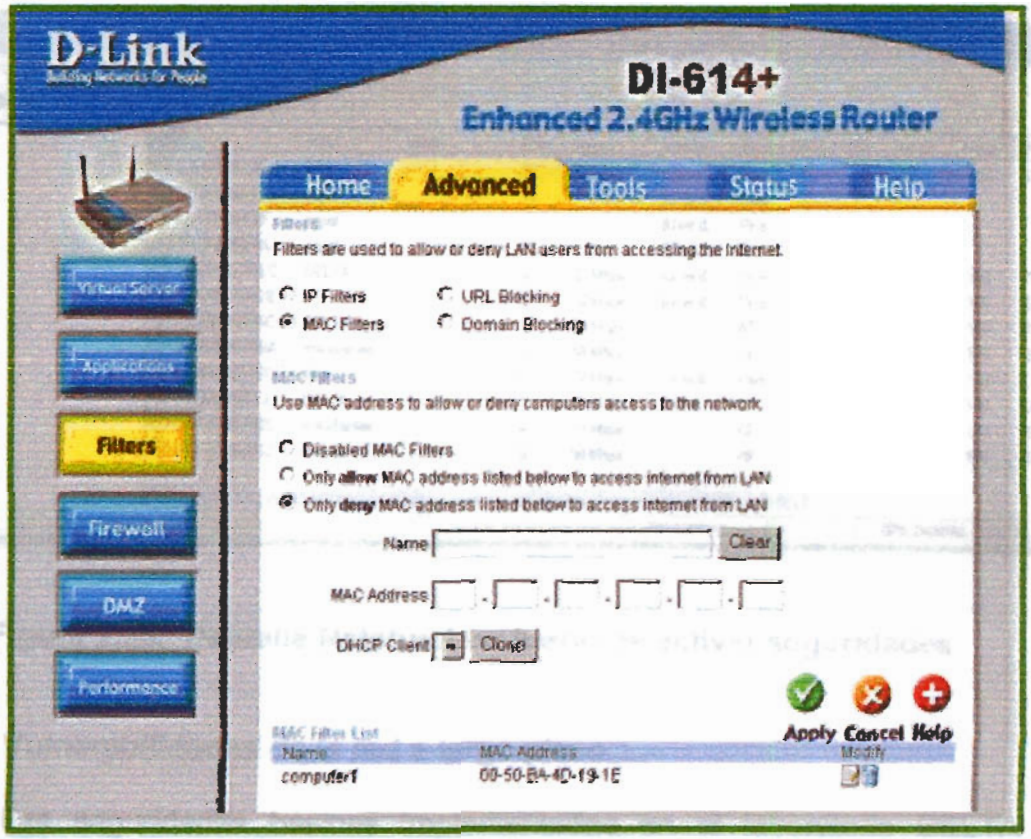


Figura 2.24. Pantalla de configuración filtros MAC laboratorio DELTA

2.2.3 Pruebas

Inicialmente comprobamos que los sistemas estaban funcionando tratando de ingresar a la red con nuestra computadora portátil, pudimos verificar que efectivamente la red no permitía el ingreso a computadoras fuera de las configuradas con las implementaciones de seguridad; además utilizando el programa Netstumbler comprobamos que la red se presenta con el icono de protegida por el WEP. La figura 2.25. nos muestra la pantalla del NetStumbler luego de activar seguridades.

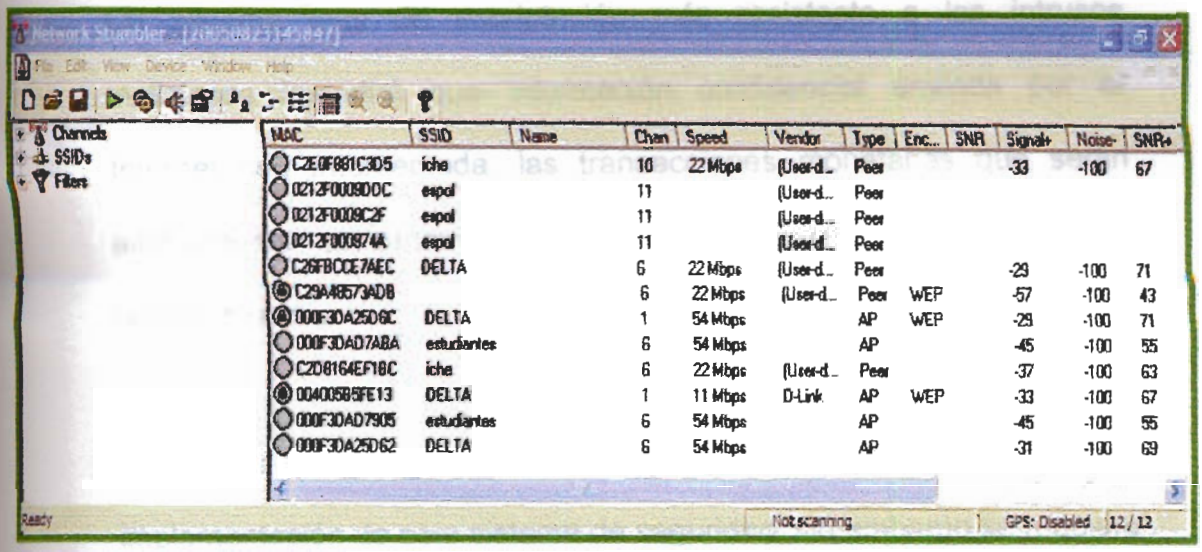


Figura 2.25. Pantalla Netstumbler luego de activar seguridades

2.3 Vulnerabilidades de la red a largo plazo

Las seguridades básicas implementadas en el laboratorio DELTA abordan los problemas actuales de la red, previenen que un usuario pasajero ingrese a la red y utilice los recursos ilegalmente, además desalienta intrusos maliciosos que encuentran una red protegida.

Sin embargo consideramos que nuestro análisis no estaría completo sin presentar los posibles problemas que pueden surgir en un futuro cercano, mencionamos las razones por las que una inversión monetaria significativa en seguridad no sería justificada en este momento pero, con los avances de la tecnología y con los diferentes usos que se podría dar a la red en un futuro, una seguridad más robusta puede ser necesaria.

Un sistema más de encriptación más resistente a los intrusos maliciosos impedirá que información confidencial enviada por el Internet sea interceptada, las transacciones monetarias que serán ampliamente utilizadas en el futuro no correrán riesgo de ser comprometidas.

Sugerimos la implementación del WPA; el router DI-614+ si permite la implementación de este sistema de seguridad, sin embargo se requiere de actualizaciones de software para las tarjetas de cada terminal, esta inversión se puede hacer en el largo plazo, cuando se considere que el costo sea justificado por la validez de los datos.

CAPÍTULO 3

PROYECTO

ANÁLISIS DE SEGURIDAD DE LA WLAN

3.1 Procedimiento para realizar una consultoría de seguridad de red

El objetivo de este proyecto es establecer un modelo para una consultoría de seguridad para redes inalámbricas. Esto implica un procedimiento que el consultor debe seguir para poder encontrar las brechas de seguridad, determinar que recursos debe proteger de intrusos y establecer cual es la implementación más adecuada para resguardar la WLAN.

El estudio práctico realizado en el laboratorio DELTA nos dio las pautas para generalizar los pasos requeridos para la evaluación de la seguridad en una WLAN. El proceso requiere de tres etapas principales:

1. Un estudio de la situación del sistema y sus componentes de

hardware.

2. Un estudio físico del exterior de la red para comprender las vulnerabilidades a las que está expuesta.
3. Un estudio para determinar el tipo de datos que se manejan en la red.

Posteriormente se debe determinar cual implementación de seguridad es la más adecuada tomando en cuenta los resultados de la evaluación. Presentaremos tres implementaciones según el nivel de riesgo en el que se encuentra la red.

3.1.1 Ventajas de una consultoría externa

Las redes inalámbricas introducen nuevos retos de seguridad. Las mismas tecnologías inalámbricas que operan sin las barreras físicas de sus equivalentes cableados, incrementan flexibilidad, aumentan productividad y reducen costos pueden exponer los recursos de la red a riesgos considerables. En el mercado existe una gran variedad de equipos y productos que ofrecen soluciones para dichos problemas de seguridad, sin embargo la tarea de determinar cual es la mejor solución para cada tipo de red no es un procedimiento sencillo.

Los conceptos y metodologías de seguridad de las redes inalámbricas

son únicos y hechos a la medida de los requerimientos y vulnerabilidades de estas. El equipo que implementa la seguridad inicialmente debe evaluar un grupo, posiblemente confuso, de mecanismos de cifrado y autenticación que serán usados en la WLAN.

Dentro de una corporación o empresa todos tienen un diferente punto de vista sobre los niveles de seguridad que la WLAN necesita. Los usuarios requieren una red sin muchas trabas que les permita hacer su trabajo sin mucho control. Los encargados de administrar la red están preocupados sobre la facilidad de manejo de los sistemas y al mismo tiempo tener un estricto control. A la gerencia le interesa la relación costo beneficio de la protección. Hacer que todos lleguen a un acuerdo es casi imposible.

Un consultor externo tiene el nivel de conocimiento necesario para implementar la solución más adecuada además de que provee un punto de vista externo e imparcial sobre todos los aspectos que conciernen la seguridad de la red inalámbrica.

3.1.2 Personal y equipos necesarios

Los requerimientos de personal para la consultoría inicialmente serían dos consultores con completo conocimiento de implementación de

redes y tecnología inalámbrica.

El equipo necesario es una computadora portátil con el programa NetStumbler.

Para la implementación de seguridad se puede requerir de hardware y software adicional según cada caso.

El tiempo necesario para la consultoría e implementación de la seguridad es variable. Este será determinado por el tipo de implementación de seguridad y por el tamaño de la red.

Para la consultoría se requiere de la completa colaboración del equipo administrador de la red y del área gerencial.

3.1.3 Acuerdos

Es importante que antes de iniciar la consultoría se establezca cuales son los permisos y las limitaciones del consultor dentro de la empresa. Se debe firmar un acuerdo en el que ambos lados establecen las normas de trabajo. En este documento debe constar la autorización de los dueños de la red para monitorear sus recursos. Por el lado del consultor este debe asegurarse de tener completa colaboración y

acceso a ciertos pormenores de la empresa sin los cuales la consultoría no se podría llevar a cabo. El anexo 1 presenta un ejemplo de esta certificación.

3.1.4 Evaluación de seguridad

Al momento de tomar una decisión sobre una implementación de seguridad de cualquier tipo el primer paso es realizar una evaluación de los riegos y vulnerabilidades de seguridad para comparar el costo de una posible brecha versus el costo de la implementación de posibles soluciones.

Una evaluación de seguridad permite tomar una decisión adecuada de cuantos riesgos pueden ser tomados en la seguridad WLAN y cuando estos riesgos son demasiado altos.

Este es un proceso sistemático en el cual se identifica, analiza y cuantifica los riesgos de seguridad en una red inalámbrica. Consta de tres etapas: evaluación de las condiciones actuales de la red, evaluación de las vulnerabilidades de la red y evaluación de los riesgos de la red.

3.1.4.1 Evaluación de las condiciones actuales de la red

Esta primera parte de la evaluación de seguridad requiere de la

colaboración del administrador de la red inalámbrica. El consultor, con la ayuda del administrador, debe llenar la primera parte del formulario de estudio de condición actual de la red que se encuentra en el anexo 2.1.

Para empezar se requiere las características de los equipos inalámbricos utilizados. Equipos inalámbricos son cualquier router inalámbrico, punto de acceso y tarjeta de red inalámbrica que sea utilizada en la red. Es importante detallar la marca y tipo de equipo utilizado puesto que el consultor debe realizar una investigación de las especificaciones técnicas de los equipos. Es importante que esta información sea anexada al formulario.

Conocer los equipos con los que la red inalámbrica trabaja es indispensable para la correcta determinación de la solución que será implementada. Algunos equipos soportarán las implementaciones mientras que otros pueden requerir actualizaciones de software o firmware. Esta información puede ser encontrada en la página Web del fabricante o en los manuales que vienen con el equipo.

A continuación se llenará la parte del formulario que requiere las

características principales de la red: el SSID o nombre de la red, el número de estaciones de trabajo y puntos de acceso, el canal en el que los puntos de acceso están trabajando y si las direcciones IP se asignan dinámicamente con un DHCP o son estáticas. Es muy probable que el administrador conozca toda esta información sin embargo para verificarla se recomienda revisar la página de configuraciones del punto de acceso o router. El siguiente punto trata de seguridad y examina que precauciones de seguridad se han tomado previa la auditoria. Dichas precauciones pueden ser la activación del WEP, deshabilitar el broadcast del SSID, cambiar la clave de administrador del AP o router y crear tablas de acceso MAC. Si existiere otro tipo de seguridad debe ser mencionada para conocimiento del consultor.

Todos estos datos son primordiales para determinar las características de la red. Una vez definida la red podremos proceder a determinar cuales son sus vulnerabilidades y riesgos.

3.1.4.2 Estudio de vulnerabilidades

El objetivo de esta fase es examinar el sistema, para encontrar debilidades que pueden ser explotadas y determinar las probabilidades de que alguien se aproveche de estas

vulnerabilidades.

Las redes WLAN son inherentemente inseguras por el medio en el que trabajan. Por lo tanto su vulnerabilidad radica en el nivel en el que un intruso tiene acceso al medio en el que se está transmitiendo los datos. El espacio aéreo es un medio no controlado y compartido; carece de la protección física de su contraparte cableada. Una vez que un usuario conecta un punto de acceso inalámbrico su señal viaja a través de las paredes, techos y ventanas del edificio. Esto convierte a toda la red en una entidad accesible desde otro piso del edificio, de un edificio contiguo, del parqueadero o desde el otro lado de la calle. Señales de radio de un solo punto de acceso pueden viajar cientos de metros fuera del edificio. Adicionalmente los puntos de acceso comparten el medio aéreo. Cualquier implemento inalámbrico puede ver el tráfico de todos los otros componentes inalámbricos en la red. La única frontera de las redes inalámbricas es la potencia de su propia señal.

El estudio de vulnerabilidades determina en que puntos o locaciones la red de la empresa está abierta para intrusos. Este procedimiento requiere completar la segunda parte del formulario

en el anexo 2.2 con la ayuda del programa NetStumbler.

El programa NetStumbler es un programa de descubrimiento y monitoreo de una WLAN. Utiliza un escaneo activo que envía señales de prueba esperando una respuesta de puntos de acceso que le envían su SSID. El uso de este freeware (programa gratuito) es relativamente simple. La figura 3.1 presenta una pantalla del programa NetStumbler.

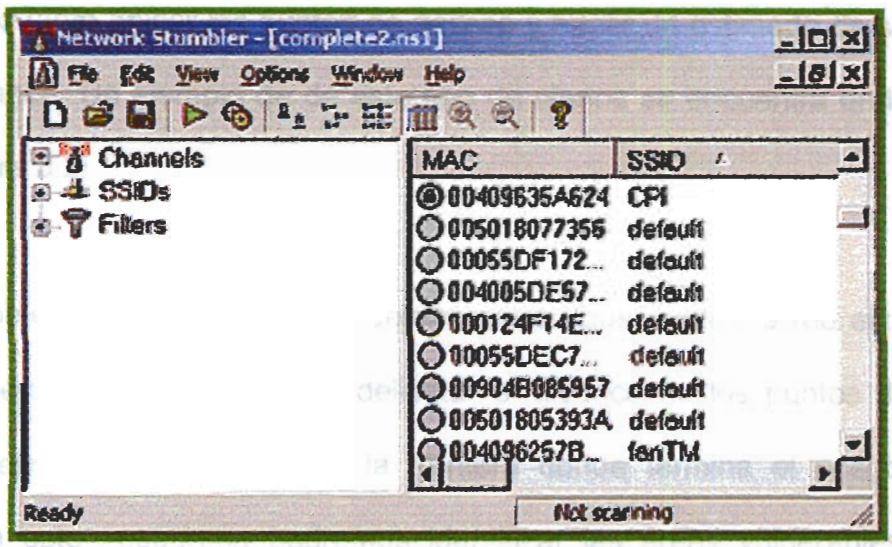


Figura 3.1. Pantalla NetStumbler

El NetStumbler inmediatamente empieza a escanear por señales cuando se ejecuta. Cuando comienza, el NetStumbler crea un nuevo archivo con el año, mes, día y hora en formato de 24 horas. Por ejemplo, si es 4 de Abril del 2005 a las 4:20 P.M. el archivo

creado será 200504041620. Mediante fácil acceso podemos ver el listado de todos los puntos de acceso que el programa encontró.

Es recomendado que el consultor se familiarice con todas las opciones que ofrece este programa antes de iniciar el trabajo de consultoría.

Empezamos por dibujar un plano del edificio en donde se encuentra la red y sus alrededores. En este gráfico es muy importante ubicar los puntos de acceso y hacer un estimado de su alcance. Un ejemplo de de este tipo de planos se encuentra en la figura 3.2.

El objetivo de este plano es determinar en que puntos la red esta "abierta" para intrusos. Al delimitar el alcance de los puntos de acceso estamos dibujando la frontera donde termina el riesgo. Con este esquema podremos identificar las áreas vulnerables. Todos estos datos deben ser comprobados por un monitoreo en las zonas con el programa NetStumbler.

El monitoreo con el programa NetStumbler requiere de que el consultor físicamente se ubique en las zonas que en el plano

aparecen como vulnerables y analice las relación señal a ruido determinando si esta es suficiente para que un intruso logre entrar a la red. Todos los resultados del NetStumbler, presentando el gráfico señal a ruido versus tiempo y observaciones sobre el nivel de supervisión del área, deben ser incluidos con el formulario.

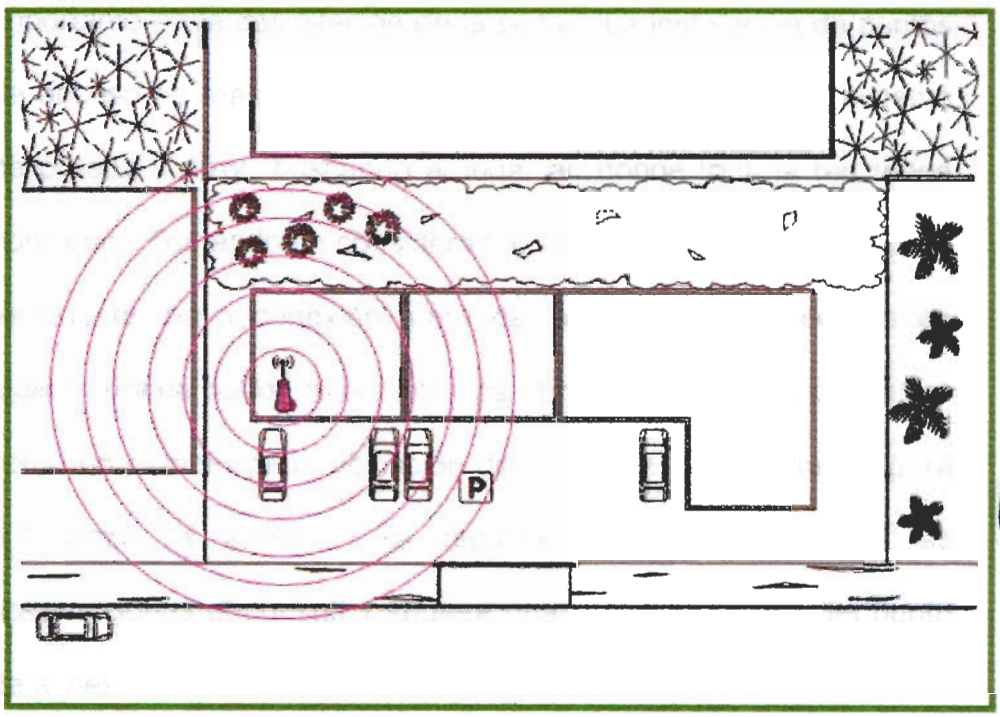


Figura 3.2. Ejemplo de plano con ubicación de punto de acceso

El programa NetStumbler adicionalmente presenta información de otros puntos de acceso en el área. El siguiente tema del formulario pide detallar otros puntos de acceso encontrados en el área. Estos puntos de acceso pueden pertenecer a otras redes inalámbricas en

la vecindad o pueden ser puntos de acceso infiltrados en la red. Es importante que el consultor verifique el origen y la ubicación de cada punto de acceso con el fin de conocer si son un peligro para la WLAN de la empresa.

La ubicación del punto de acceso puede ser un punto muy importante en la delimitación de la señal. La instalación de puntos de acceso se realiza la mayoría de veces a través de un sistema de prueba y error, buscando el lugar en donde toda la red tenga conexión. Tomando en consideración la seguridad lo que se busca es que no haya conexión fuera de los confines del edificio en lugares donde puede haber intrusos. En la figura 3.3 su puede ver como un cambio de la ubicación del punto de acceso de la figura 3.2 limita la señal. Se recomienda que dentro de las observaciones el consultor sugiera una nueva ubicación del punto de acceso si esta es necesaria.

Otras observaciones pueden incluir comentarios sobre las condiciones espaciales del edificio y exteriores, advertencias sobre puntos de acceso detectados por NetStumbler o cualquier otra indicación que el consultor considere pertinente para la consultoría.

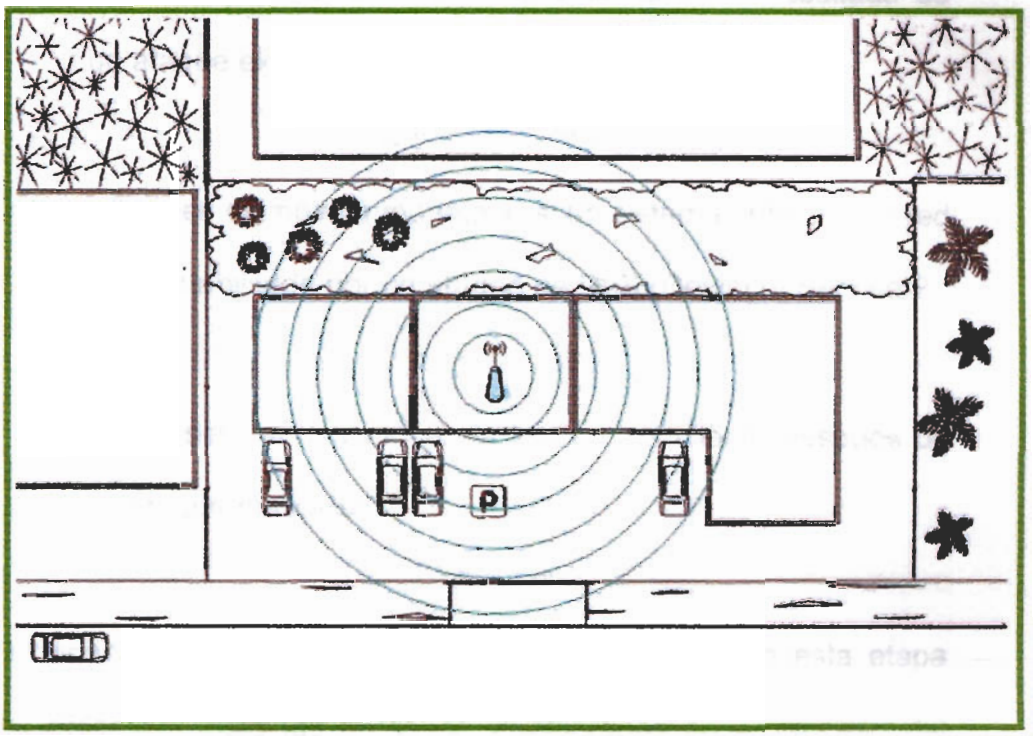


Figura 3.3 Ejemplo de ventaja de cambio de ubicación del punto de acceso

3.1.4.3 Estudio de riesgos

Para medir de una manera adecuada el impacto de un riesgo se debe determinar los valores que se está tratando de proteger. Los bienes deben ser reconocidos y valorados. En el caso del estudio en una red WLAN, los valores que se desea proteger son los datos que se envían. A cada "dato" se le debe asignar un valor. Las preguntas claves son:

- ¿Cuál es el impacto monetario si la integridad de mis datos

o su confidencialidad es comprometida como resultado de un ataque externo?

- ¿Cuál es el impacto monetario si un sistema crítico de la red es deshabilitado por un ataque de DoS (Denial of Service)?

- ¿Cuál será el impacto en la lealtad del cliente después de un ataque malicioso?

El departamento gerencial debe estar involucrado en esta etapa del proceso. Solo las personas involucradas en el proceso del negocio pueden responder estas preguntas adecuadamente.

Esta etapa es muy importante para asegurarse que el alcance de las medidas de seguridad implementadas son las adecuadas para los riesgos asociados con la sensitividad de los datos en la WLAN.

El consultor debe guiar al dueño o gerente para llenar la tercera parte del formulario que encontramos en el anexo 2.3. Este debe explicar cuidadosamente cada una de las categorías y especificar como los datos mencionados pueden ser comprometidos en la WLAN. Solo el delegado de la empresa puede estimar el valor del

riesgo en cada caso.

Fue necesario dividir el tipo de datos en categorías para facilitar la identificación y valorización de los recursos:

- **Categoría 1: Información de Negocios**

  Esta categoría abarca toda la información referente a las relaciones de comercio o lucro con otras empresas. El evaluador debe determinar que sucedería si datos sobre negociaciones futuras o pasadas es comprometido ¿Cuál sería el costo de que la competencia conozca mis acuerdos con otras compañías? ¿Qué sucede si mi red esta fuera de servicio por un tiempo e información de negociaciones es perdida?

- **Categoría 2: Información Corporativa**

  Cuando nos referimos a la información corporativa estamos definiendo todo lo que se relaciona a la asociación empresarial: las leyes, los estatutos y los pormenores de la sociedad ¿Qué efecto tendría si las particularidades legales de mi compañía son conocidos? ¿Puede esto implicar pérdida monetaria?

- **Categoría 3: Información técnica y de desarrollo**

  A veces la propiedad intelectual es mucho más valiosa que la financiera. Varias veces información de desarrollo circula entre colaboradores de un mismo proyecto. Un nuevo producto en progreso no esta listo para ser presentado al público ¿Puedo ser víctima de un robo intelectual? ¿Qué pérdidas implicaría que a competencia utilice mi idea?

- **Categoría 4: Información de mercadeo**

  Información sobre posicionamiento en el mercado de un producto y las diferentes estrategias de mercadeo puede ser muy importante ¿Este tipo de información es accesible a través de mi red inalámbrica? ¿Existirá pérdida en el caso de que la competencia conozca mis estrategias de venta?

- **Categoría 5: Información operacional y secretos de oficio**

  Cada empresa tiene su forma de proceder y sus técnicas de funcionamiento. A veces estos procedimientos son únicos y vitales para el producto final ¿Cuánto le interesa a la competencia mi forma de operar? ¿Cuál será el impacto monetario si esta información se conoce públicamente?

- **Categoría 6: Información de recursos humanos**

  Las fichas y hojas de vida del personal de una compañía usualmente están en una base de datos. Esta información no solo es confidencial sino que puede ser una vulnerabilidad para la seguridad empresarial. Si estos datos pueden ser accedidos a través de la red, están a riesgo en una WLAN ¿Cómo me afectaría si esta información es expuesta?

- **Categoría 7: Información financiera**

  Ciertas veces en la red circula información bancaria, movimientos de bolsa y transacciones financieras en general. Este tipo de información es más fácil de valorar ¿En promedio, cuanta pérdida me ocasionaría si mis datos financieros son interceptados?

- **Categoría 8: Código Fuente**

  Compañías desarrolladoras de software guardan recelosamente el código fuente. Con la importancia de la computación y el auge de la automatización muchas compañías manejan complejos programas de software ¿Puede ser el código fuente objeto de un robo?

- **Categoría 9: Información confidencial del cliente**

  El manejo de datos confidenciales de un cliente puede ser un asunto de mucho cuidado. Aunque esos datos no tengan valor monetario, la pérdida de la confianza puede causar muchas pérdidas monetarias al largo plazo ¿Cuánto me costaría la pérdida de clientela debido a la pérdida de confidencialidad?

- **Categoría 10: Acceso a través de la red a otras empresas**

  En ocasiones el objetivo de los intrusos no es nuestra propia red. Si nuestra red tiene acceso a otras redes de compañías amigas esta puede convertirse en una puerta trasera ¿Cómo afectaría mis negocios con mi compañía aliada si se crea una brecha de seguridad a través de mi red?

- **Categoría 11: Datos confidenciales enviados en aplicaciones de Internet**

  El acceso a Internet puede ser una vulnerabilidad adicional si no hay seguridad en una red inalámbrica. Paquetes interceptados pueden contener información confidencial

como cuentas de usuarios o números de tarjetas de crédito. El valor en este caso puede ser estimado solo si hablamos de transacciones empresariales, cualquier trámite personal no será tomado en cuenta ¿Cómo afectaría monetariamente si los datos enviados a través de Internet son interceptados?

- **Categoría 12: Otros**

  En esta categoría entra toda la información que el gerente o administración considera importante y no fue incluída en las categorías anteriores.

Al terminar este formulario tendremos una idea del valor monetario de la información manejada en la empresa. Esto podría ser muy útil para que el dueño de la empresa entienda la necesidad de una implementación de seguridad para la red inalámbrica. Sin embargo el objetivo principal de esta etapa es estimar cual sería el riesgo si los datos son comprometidos y si este riesgo amerita una implementación de seguridad más robusta e inevitablemente más cara.

3.1.4.4 Conclusiones del estudio

Al finalizar todas las etapas del estudio el consultor poseerá toda la

información necesaria para sacar conclusiones sobre el estado de seguridad de la red inalámbrica de la empresa. En este punto el trabajo del consultor consiste en determinar que tipo de seguridad requiere de acuerdo a la exigencia de la red, se deberá determinar si la WLAN requiere de una implementación de seguridad mínima, media o avanzada. Cada una de estas será explicada a continuación.

3.2 Consideraciones de seguridad según el tamaño y uso de la red

En todas las redes inalámbricas las vulnerabilidades se presentan de la misma manera, en cada caso el envío de los datos por el aire hace que los datos estén disponibles para cualquiera que desee escuchar. Por ello esta claro que toda red WLAN debe implementar un sistema de seguridad. Sin embargo muchas compañías pequeñas manejan una red inalámbrica para unos pocos usuarios no pueden incurrir en altos costos para la implementación de un esquema de seguridad. Al mismo tiempo, grandes empresas que piensan implementar redes inalámbricas de amplio uso no pueden arriesgar sus recursos con medidas de seguridad elementales.

El nivel de seguridad requerido por la red inalámbrica depende de diferentes características como el tamaño de la red, que tan vulnerables

son sus datos y el tipo de información que maneja. El consultor debe tomar en cuenta cada uno de estos puntos para decidir que sistema recomendar. Aunque esta decisión es particular en cada caso podemos definir de manera general que implicaría cada tipo de red:

- Redes que requieren seguridad mínima: Generalmente son redes pequeñas o medianas. Pueden considerarse en esta categoría las redes cuyo valor de riesgo no sea mayor a los $1000 o que no se encuentren en zonas vulnerables. Empresas cuya señal inalámbrica está contenida dentro del perímetro de sus instalaciones también requieren una implementación de seguridad mínima.

- Redes que requieren seguridad media: Empresas medianas o grandes cuya información se considere más confidencial. Su valor riesgo es mayor a los $1000 y/o esta en zonas de alto tráfico externo y con un alto nivel de vulnerabilidad.

- Redes que requieren seguridad avanzada: Una empresa grande cuya red tiene un valor riesgo muy alto. Es vulnerable a ataques intrusos y sus datos son altamente

sensibles.

Al finalizar el estudio se debe presentar un informe que detalle los resultados de las etapas y especifique cual es el nivel de seguridad que la red requiere y presentarlo al dueño o gerente de la compañía. En definitiva será este quien determine que seguridad desea implementar de acuerdo a los resultados y costos de la solución. El anexo 3 presenta el resultado de la consultoría en la red inalámbrica del laboratorio DELTA. El anexo 4 presenta un análisis de la validez de las soluciones.

En la figura 3.4 podemos entender un poco mejor el proceso de seleccionar la implementación adecuada. Los datos recolectados en el estudio nos presentarán la respuesta de las preguntas planteadas.

3.2.1 Seguridad mínima

El principal atractivo de esta implementación es su sencillez. La seguridad 802.11 básica (WEP estática) emplea una clave compartida para controlar el acceso a la red y usa la misma clave para cifrar el tráfico inalámbrico.

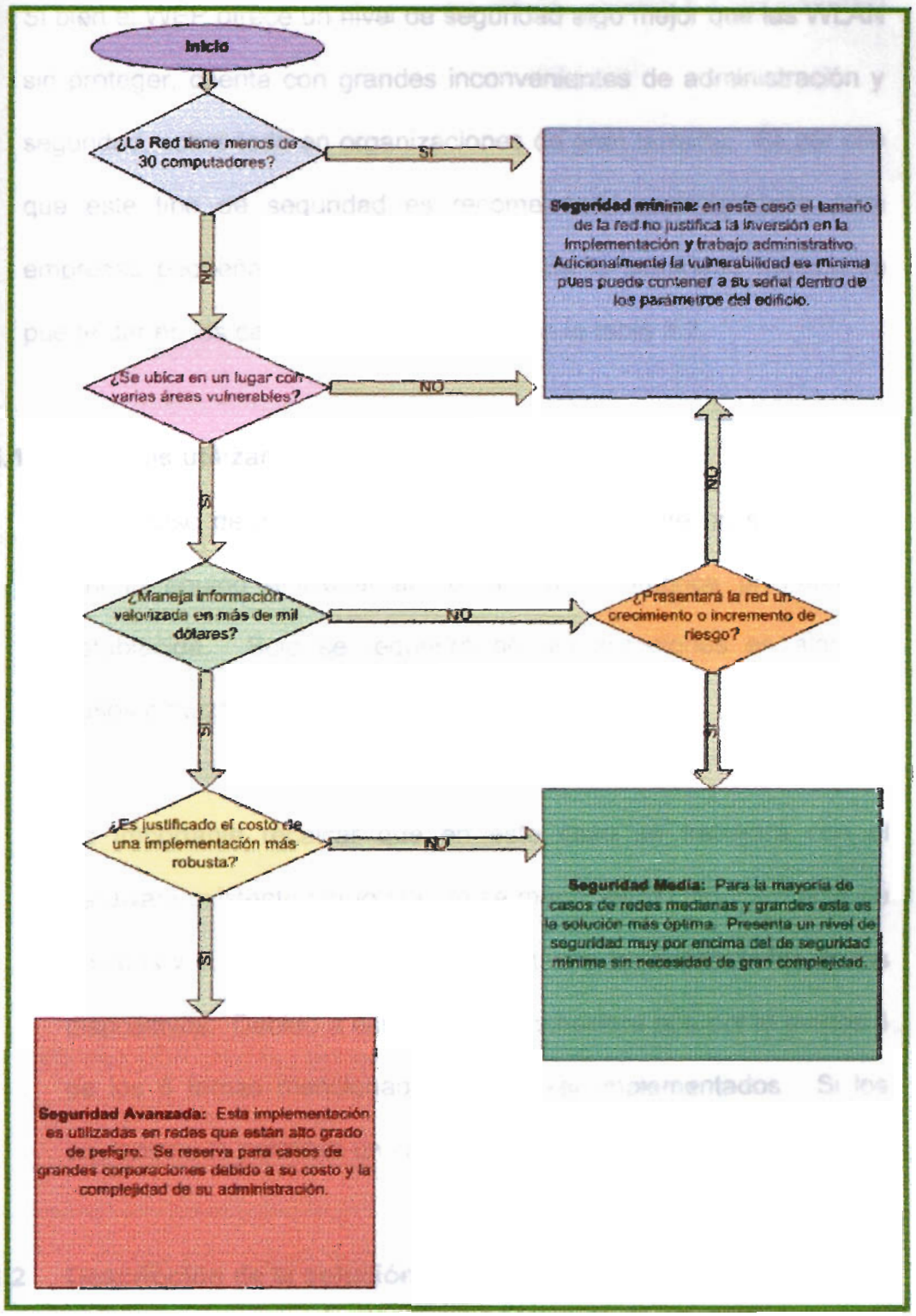


Figura 3.4. Diagrama de flujo para selección de la implementación de seguridad

Si bien el WEP ofrece un nivel de seguridad algo mejor que las WLAN sin proteger, cuenta con grandes inconvenientes de administración y seguridad, sobre todo en organizaciones de gran tamaño. Es por ello que este tipo de seguridad es recomendado esencialmente para empresas pequeñas. La implementación de la seguridad mínima se puede dar en los casos que se muestran en la tabla 3.2.

3.2.1.1 Equipos utilizados

En el caso de la seguridad mínima generalmente no se necesita ningún equipo adicional al de la red inalámbrica previamente establecida. Solo se requerirá de actualizaciones en algunos casos o quizá pequeños reajustes de hardware.

Es importante recalcar que en este caso se trabajará con el hardware existente por lo que no se mencionará ninguna marca de equipos y la implementación es subjetiva a las capacidades de los dispositivos. Debido a este punto se considera que por lo menos 5 de los 6 temas mencionados deben ser implementados. Si los equipos no lo permiten un cambio de hardware es requerido.

3.2.1.2 Descripción de la solución

La solución consta de seis puntos que mejorarán de manera

significativa la seguridad de una WLAN hogareña o de pequeña empresa que no tiene ningún tipo de seguridad:

CASO 1

Premisa	Respuesta
¿La red tiene menos de 30 computadores?	SI

CASO 2

Premisa	Respuesta
¿La red tiene menos de 30 computadores?	NO
¿Se ubica en un lugar con áreas vulnerables?	NO

CASO 3

Premisa	Respuesta
¿La red tiene menos de 30 computadores?	NO
¿Se ubica en un lugar con áreas vulnerables?	SI
¿Maneja información valorizada en más de 1000 dólares?	NO
¿Presentará la red un crecimiento o incremento de riesgo?	NO

Tabla 3.1. Casos para la aplicación de seguridad mínima

1. Mantener control del área de cobertura de la señal y proteger con clave segura los puntos de acceso. Muchos puntos de acceso permiten que se ajuste la potencia de la señal. Se debe ubicar al punto de acceso lo más lejos posible de las paredes y ventanas. Se requiere probar la señal en estas ubicaciones para comprobar que la conexión es pobre. Adicionalmente es necesario probar que la clave del punto de acceso no sea la original y usar una clave fuerte para proteger cada punto de acceso.

2. Es importante utilizar el SSID (Service Set Identifier) de manera inteligente. Se debe deshabilitar la opción de "broadcast" del SSID. Esto previene que el punto de acceso comunique el nombre de la red asociándose con clientes que no están configurados con el SSID de la red. También es importante no dejar como SSID el de fábrica.

3. Se requiere la implementación de autenticación MAC (Media Access Control). Con un número de usuarios manejable se puede restringir el acceso en cada punto de acceso. Esto se logra creando una tabla de direcciones MAC. El punto de acceso solo permitirá el acceso a la red de los equipos cuyas

direcciones están en la tabla.

4. Debido al limitante del hardware es necesario implementar el nivel de seguridad más alto que el equipo soporta. Incluso una clave WEP de 128 bits en conjunto con los puntos antes mencionados presenta una mejora. En lo posible se debe implementar autenticación de usuario implementando WPA en los puntos de acceso y las tarjetas de red.

5. Muchos puntos de acceso pueden ser reiniciados con sus valores iniciales mediante un simple mecanismo. Es importante que estos no estén a libre acceso de cualquier intruso.

6. Deshabilitar las funciones SNMP (Simple Network Management protocol) ya que permiten que un intruso ingrese al punto de acceso con privilegios de lectura y escritura.

3.2.1.3 Implementación de la seguridad mínima

Al momento de implementar el consultor debe tener a la mano la documentación de los equipos de la red inalámbrica. Estas especificaciones fueron solicitadas como parte del estudio. Aunque muchos pasos serán similares para toda marca de

dispositivos es importante que se revisen estos documentos.

Primero nos basaremos en el estudio de vulnerabilidades para determinar la ubicación adecuada del punto de acceso. Probablemente se requerirá de varias pruebas de conectividad con el programa NetStumbler para determinar el mejor lugar. Adicionalmente nos podemos asegurar de que cumpla el punto cinco, alejándolo del alcance de personal que no este autorizado.

A continuación se procederá a ingresar en la página de configuraciones del punto de acceso. El consultor verificará que las claves de administrador fueron cambiadas. Si este no es el caso se encargará de escoger junto con el administrador la clave más adecuada.

En la página de configuraciones se debe deshabilitar la opción "broadcast SSID". Inmediatamente el consultor podrá verificar que la red no es identificada por el programa NetStumbler. En este paso se requiere configurar a cada máquina que pertenece a la red para que se conecte aunque no reciba el SSID en forma de broadcast.

Procedemos a crear la tabla de direcciones MAC en el punto de acceso. Aunque algunos puntos de acceso permiten crear la tabla con las direcciones MAC que en ese momento estén conectadas a la red, puede ser necesario que el consultor tenga un listado de las direcciones MAC de los equipos que pertenecen a ella. Se ingresará la dirección y se procederá a verificar que el equipo con dicha MAC pueda ingresar a la red.

Siguiendo en la página de configuraciones habilitaremos la opción de cifrado en WEP. Necesitaremos ingresar una clave de 128 bits con caracteres alfa numéricos. Se debe recalcar al administrador la importancia de una clave difícil de descifrar. Puede que en el momento que se activa el WEP el punto de acceso se reinicie y los equipos pierdan conexión. Cada equipo debe ser configurado con la misma clave WEP para que puedan ingresar a la red. Esto se lo hace manualmente de manera muy simple, especialmente si el equipo utiliza un sistema operativo Windows actualizado. Si tanto el punto de acceso como los adaptadores de red pueden trabajar con WPA es recomendado que este se active en vez del WEP. Este sistema de claves dinámicas es más robusto y presenta un nivel aun mayor de protección.

La opción SNMP también se encontrará en la página de configuración de algunos puntos de acceso. Es importante verificar inicialmente si esta herramienta no es utilizada para tareas de administración antes de desactivar el tráfico SNMP.

3.2.2 Seguridad media

La implementación de seguridad media de una WLAN proporciona un método más consistente de autenticación y autorización con el protocolo 802.1X. 802.1X es un estándar del IEEE para realizar la autenticación del acceso a una red y administrar las claves utilizadas para proteger el tráfico. Su uso no se limita a las redes inalámbricas, también se implementan en muchos conmutadores de LAN.

El protocolo 802.1X implica al usuario de la red, un dispositivo de acceso a la red (como un punto de acceso inalámbrico) y un servicio de autenticación y autorización en forma de servidor RADIUS. El servidor RADIUS desempeña la labor de autenticar las credenciales de los usuarios y de autorizar el acceso de éstos a la WLAN.

Esta solución también se basa en el protocolo EAP para llevar a cabo la comunicación de autenticación entre el cliente y el servidor RADIUS (transmitida por el punto de acceso). En este caso utilizaremos el

protocolo PEAP (Protected EAP) que es un método de autenticación en dos fases.

En la primera fase se establece una sesión de TLS (Transport Layer Security) para el servidor y se permite que el cliente autentique al servidor mediante el certificado digital del servidor. La segunda fase necesita un segundo método de EAP con túnel dentro de la sesión de PEAP para autenticar al cliente en el servidor RADIUS.

Este tipo de seguridad se aplica en para los casos especificados en la tabla 3.2 y su diseño se puede ver en la figura 3.5.

3.2.2.1 Equipos utilizados

La implementación de la seguridad media requiere de otros equipos adicionales. El principal es un servidor RADIUS que permita la implementación del PEAP para el funcionamiento del 802.1X. Aunque existen varias implementaciones de distintas marcas, algunas incluso diseñadas especialmente para redes WLAN, decidimos recomendar una implementación con Windows Server 2000 o Windows Server 2003 con componentes IAS. La ventaja de este servidor es que como producto Windows es utilizado ampliamente y conocido por la mayoría de

administradores de red.

CASO 1

Premisa	Respuesta
¿La red tiene menos de 30 computadores?	NO
¿Se ubica en un lugar con áreas vulnerables?	SI
¿Maneja información valorizada en más de 1000 dólares?	NO
¿Presentará la red un crecimiento o incremento de riesgo?	SI

CASO 2

Premisa	Respuesta
¿La red tiene menos de 30 computadores?	NO
¿Se ubica en un lugar con áreas vulnerables?	SI
¿Maneja información valorizada en más de 1000 dólares?	SI
¿Es justificado la inversión en una implementación más robusta?	NO

Tabla 3.2. Casos para la aplicación de seguridad intermedia

Los equipos necesarios para esta implementación son:

- Inicialmente debe existir una infraestructura WLAN bien diseñada y completamente funcional. El hardware de red debe ser compatible con 802.1X y WEP de 128 bits para el

cifrado.

- Los equipos de la red deben tener Windows XP con SP1 pues este proporciona algunas funcionalidades de características de 802.1X y WLAN. (Microsoft proporciona clientes 802.1X para Windows 2000 y Windows 9x (disponible como descarga gratuita)).

- Servidores RADIUS con los componentes de Servicios de Certificate Server e IAS de Windows Server 2003. Servicios de Certificate Server e IAS tienen características que han sido diseñadas explícitamente para redes WLAN basadas en 802.1X. Se debe trabajar en un entorno de Active Directory con Windows Server 2003 y Windows 2000.

El consultor debe familiarizarse con los conceptos de implementación y manejo de Windows Server. Parte de los conceptos de la implementación de un servidor RADIUS serán explicados en la parte de implementación.

3.2.2.2 Descripción de la solución

El sistema de seguridad basado en RADIUS reduce

significativamente las vulnerabilidades del WEP aumentando el nivel de integridad de los datos y su confidencialidad. Permite una administración directa de las direcciones MAC con una base de datos central.

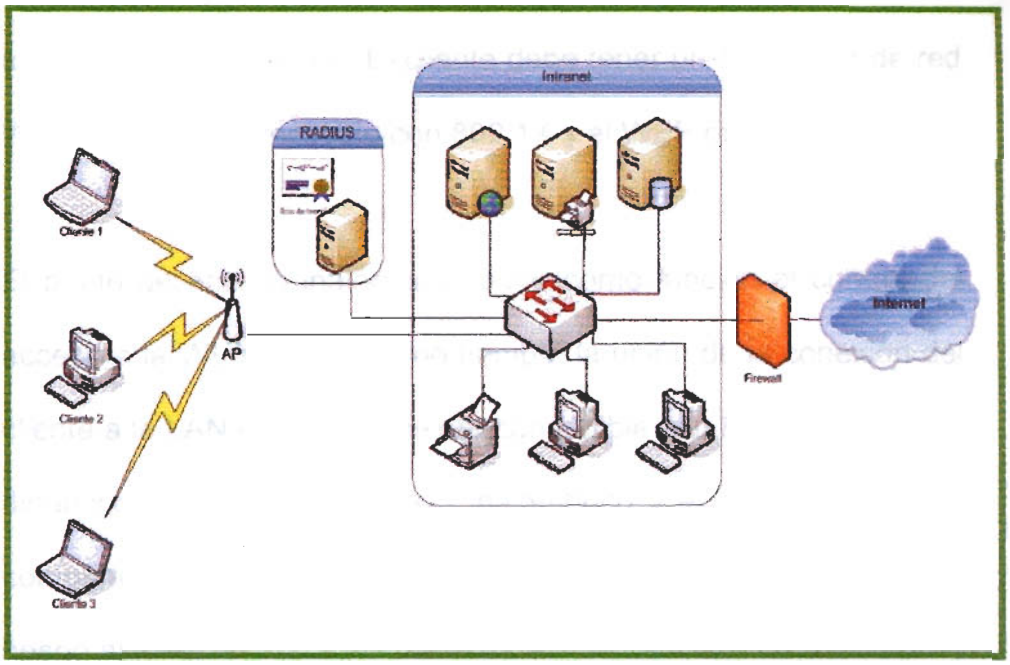


Figura 3.5. Diseño de una red con seguridad intermedia

El servidor RADIUS es utilizado para la autenticación mediante un directorio, en el caso de una red inalámbrica, esto posibilita la creación de llaves dinámicas específicas a cada usuario y sesión. Cada uno de los componentes de este sistema juega un papel muy importante. El estándar 802.1X requiere que el usuario le provea sus credenciales antes de acceder a la red. Las credenciales

pueden ser en la forma del nombre y clave de usuario, un certificado o un token. En el caso inalámbrico el usuario se refiere a un equipo o dispositivo que ejecuta una aplicación que requiere acceso a los recursos de red. El propietario de las credenciales que se usan para autenticar al cliente en la red puede ser tanto un usuario como un equipo. El cliente debe tener un adaptador de red WLAN que sea compatible con 802.1X y el WEP dinámico.

El punto de acceso inalámbrico tiene como función el control del acceso a la WLAN y, al mismo tiempo, la unión de la conexión del cliente a la LAN interna. Debe ser compatible con 802.1X y el WEP dinámico. El punto de acceso inalámbrico y el servidor RADIUS comparten un secreto que les permite identificarse mutuamente sin riesgo alguno.

El servidor de autenticación (RADIUS) verifica que las credenciales son del usuario que dice ser y solo después de esto el usuario es autorizado a utilizar la red. Esencialmente toma decisiones relativas a la autorización en función de una directiva de acceso a red.

Adicionalmente el servidor verifica que el punto de acceso es un

componente válido de la red. Esto es importante para proteger al usuario de conectarse a un punto de acceso no autorizado que puede ser usado para capturar información de manera fraudulenta.

Si el usuario es tanto autenticado como autorizado para ingresar a la red y el punto de acceso es verificado como parte de la red, entonces el servidor se comunica directamente con el punto de acceso para autorizar el acceso del usuario a la red. El servidor crea un par único de llaves de encripción para este usuario y para cada sesión, las que son mandadas tanto al punto de acceso como al cliente para de manera única y segura encriptar la información entre los dos.

La seguridad de este tipo anula dos limitaciones significativas de la seguridad WEP o de nivel físico. Provee llaves de encriptación únicas para cada usuario cada vez que entran a la red y elimina todo el trabajo de administración de llaves asociado con mantener una llave única tanto en los equipos como en el punto de acceso. Un esquema del funcionamiento de la solución intermedia se puede encontrar en la figura 3.6.

Paso a paso la autenticación del usuario a la red por el método

801.1X se hace de la siguiente manera:

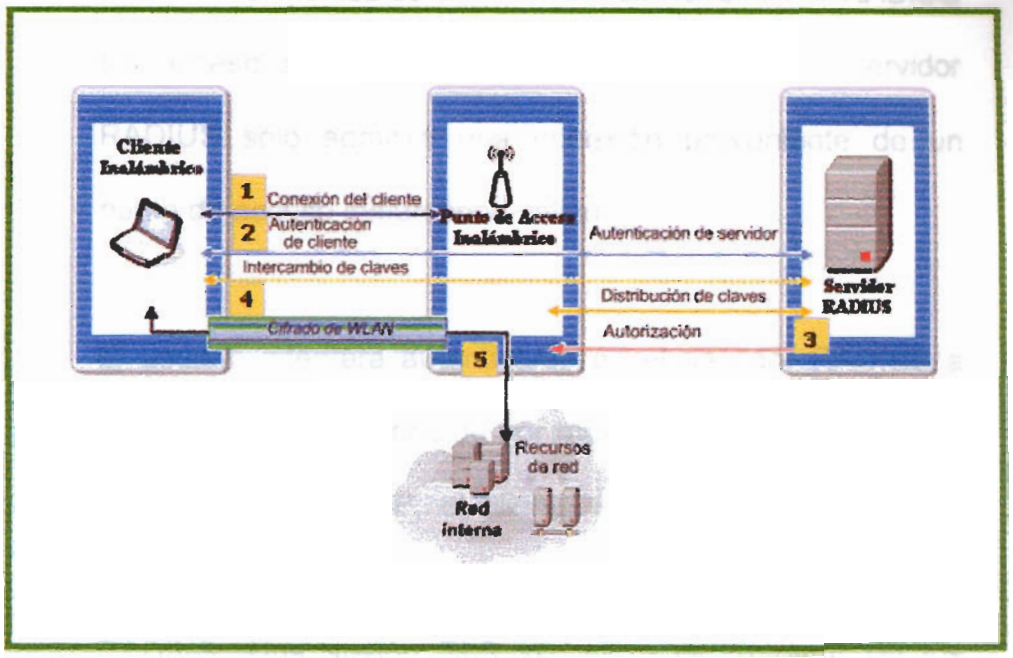


Figura 3.6. Esquema de la autenticación con RADIUS

1. **Conexión del Cliente:** Cuando el usuario inalámbrico se encuentra dentro del alcance del punto de acceso inalámbrico, intenta conectarse a la red inalámbrica que se encuentre activa en este punto y que el Identificador del conjunto de servicios (SSID) haya identificado.

2. **Autenticación del cliente:** Según el estándar 802.1X el punto de acceso inalámbrico se configura para permitir sólo conexiones seguras. Así, cuando el cliente intente conectarse al punto, éste lo delatará. A continuación, el

punto de acceso establece un canal restringido que permite al cliente comunicarse únicamente con el servidor RADIUS sin acceso al resto de la red. Por su parte, el servidor RADIUS sólo admitirá una conexión proveniente de un punto de acceso inalámbrico válido.

El usuario intentará autenticarse en el servidor RADIUS a través del canal restringido por medio de 802.1X. Dentro de la negociación PEAP, el cliente establece una sesión de seguridad de la capa de transporte (TLS) con el servidor RADIUS. Una sesión TLS se utiliza como parte de los servidores PEAP por las siguientes razones:

- Permite que el usuario autentique el servidor RADIUS. El usuario sólo establecerá la sesión con un servidor que cuente con un certificado en el que el confíe.

- Protege el protocolo de autenticación MS-CHAP v2 evitando la captura de paquetes.

- La negociación de la sesión TLS genera una clave

que el cliente y el servidor RADIUS pueden utilizar a fin de establecer claves maestras comunes. Posteriormente estas serán utilizadas para generar aquellas claves que van a emplearse para cifrar el tráfico de WLAN.

El usuario se autentica en el servidor RADIUS utilizando el protocolo EAP MS-CHAP v2 mediante el protocolo PEAP. El tráfico dentro del túnel de TLS nunca se expone al punto de acceso inalámbrico: sólo el cliente y el servidor RADIUS pueden verlo.

3. **Comunicación Servidor a Punto de Acceso:** El servidor RADIUS comprueba las credenciales del usuario en relación con el directorio. Si el usuario se autentica correctamente, el servidor RADIUS obtendrá información para decidir si autoriza al cliente a usar la WLAN. De esta forma, concede o deniega el acceso al cliente de acuerdo con la información del directorio y también con las restricciones que se definen en la directiva de acceso correspondiente. El servidor RADIUS transfiere la responsabilidad de decidir sobre el acceso al punto de acceso después de esta verificación.

Si el usuario obtiene acceso, el servidor RADIUS transmitirá la clave maestra del usuario al punto de acceso inalámbrico. En este punto el cliente y el punto de acceso comparten material de claves comunes que pueden utilizar para cifrar y descifrar el tráfico de WLAN.

Con el WEP dinámico las claves maestras se utilizan directamente como clave de cifrado, sin embargo estas claves deben cambiarse cada cierto tiempo para impedir ataques de recuperación de claves WEP. El servidor RADIUS lleva esto a cabo obligando al usuario de forma constante a volver a autenticarse y generar un conjunto de claves nuevo.

4. **Cifrado del tráfico:** En este paso el punto de acceso une la conexión de la WLAN del cliente a la LAN interna, lo que posibilita que el cliente se comunique con total libertad con los sistemas de la red interna. Así, ahora el tráfico que fluye entre el cliente y el punto de acceso está cifrado.

5. **Solicitud dirección IP:** Si el usuario necesita una dirección IP, podría solicitarla del servidor de protocolo de

configuración dinámica de host (DHCP) de la red cableada. Una vez se haya asignado la dirección IP, el usuario podrá empezar a comunicarse con normalidad con los recursos de la red de la empresa.

3.2.2.3 Implementación de la seguridad media

Para empezar debemos tener un equipo con el sistema operativo Windows Server 2003 instalado. Este dispositivo será utilizado como servidor RADIUS. Para ello debe ser adecuado con IAS (Internet Authentication Service) que puede considerarse la versión de Microsoft de un servidor RADIUS.

Existen una serie de secuencias de comandos y herramientas para ayudar a simplificar la configuración y el funcionamiento de esta solución en la página de soporte técnico de Microsoft. Es importante que el consultor tenga a la mano esta herramienta que facilitará la implementación. El nombre del archivo es PEAPWLAN.msi y debe ser instalado en el servidor.

Al instalar este archivo se creará un shell de comandos con el directorio de trabajo actual establecido en la carpeta de instalación de herramientas. Desde ahí se pueden ejecutar la serie de

comandos que son necesarios para implementar la solución. Dichos comandos se los puede encontrar en el anexo 5.

Adicionalmente se debe instalar CAPICOM que es la biblioteca del sistema que permite ejecutar secuencias de comandos de operaciones de certificado y seguridad, la consola de administración de directiva de grupo (GPMC) se utiliza para instalar y configurar los objetos de directiva de grupo utilizados y Microsoft baseline security analyzer (MBSA) una herramienta necesaria para comprobar que las actualizaciones de seguridad del sistema operativo son actuales y detectar posibles problemas con la configuración de seguridad de los servidores. Todos estos archivos pueden ser descargados de la página de Microsoft.

Es importante en este punto también preparar el dominio del servicio de directorio Microsoft Active Directory creando grupos de seguridad necesarios. Estos grupos son:

- Usuarios de LAN inalámbrica: especifica que usuarios pueden autenticarse en la WLAN.

- Equipos de LAN inalámbrica: especifica que equipos

pueden autenticarse en la WLAN.

- Acceso a LAN inalámbrica: este grupo se utiliza en la directiva de acceso de RADIUS para controlar el acceso a la WLAN.

- Configuración del equipo de LAN inalámbrica: especifica que equipos reciben configuración de WLAN de la directiva de grupo.

El siguiente paso es implementar una entidad emisora de certificados específica muy sencilla. A diferencia de la mayoría de las entidades emisoras, se utilizará para emitir sólo un tipo de certificado: certificados de servidor para los servidores IAS. El comando *MSSsetup InstallCA* logrará este propósito. Se deben configurar los siguientes parámetros de la entidad emisora (lo que se logra con el comando *MSSsetup ConfigureCA*):

- Direcciones URL de punto de distribución de la lista de revocación de certificados (CDP): especifica las ubicaciones desde las que se puede obtener una lista de revocación de certificados actual. Contiene la ruta de

acceso LDAP de la lista de revocación de certificados publicada en Active Directory.

- Direcciones URL de Acceso a la información de entidad emisora (AIA): indica la ubicación desde la que se puede obtener un certificado de la entidad emisora.

- Período de validez: Indica el período de validez máximo de los certificados emitidos.

- Período de la lista de revocación de certificados: indica la frecuencia de publicación de la lista de revocación de certificados.

- Período de coincidencia de la lista de revocación de certificados: indica el período de coincidencia entre la emisión de una nueva lista de revocación de certificados y la caducidad de la lista de revocación de certificados anterior.

- Período de diferencia entre listas de revocación de certificados: indica la frecuencia de publicación de diferencias entre listas de revocación de certificados.

- Auditoria de la entidad emisora: indica la configuración de auditoria de la entidad emisora de certificados.

La configuración de estos parámetros depende de la necesidad del administrador, sin embargo se recomienda que la duración de la entidad emisora sea de 25 años y el certificado tenga una validez de 2 años.

Ya creado el emisor de certificados, el siguiente paso en la implementación es la instalación del IAS. Esto se logra mediante el comando *MSSSetup InstallIAS*. También debe registrarse en el Active Directory, esto significa la adición de la cuenta de equipo del servidor IAS para el grupo de seguridad Servidores RAS e IAS, lo que garantiza que los servidores IAS tengan permiso para leer las propiedades de acceso remoto de las cuentas de usuario y equipo en Active Directory.

Se debe importar el objeto de directiva de grupo de la directiva de inscripción automática de certificados IAS preconfigurado para permitir la emisión automática de certificados en los servidores IAS. Esto permitirá el uso de los certificados para la autenticación del IAS.

Se deben configurar los siguientes tipos de valor de configuración en el servidor IAS:

- Registro de solicitudes
- Directiva de acceso remoto
- Configuración de solicitudes de conexión

IAS puede registrar información de autenticación y de cuentas en registros RADIUS. Sin embargo no crea registros RADIUS de forma predeterminada y no se ha habilitado el registro RADIUS en esta solución con el fin de reducir la carga de administración.

Se debe crear una nueva directiva de acceso remoto en el menú de Herramientas administrativas en servicio de autenticación de Internet. Se debe seleccionar medio inalámbrico y EAP protegido (PEAP) en la lista de tipos de EAP. En Configurar se debe mostrar el certificado de servidor IAS emitido anteriormente en el campo certificado emitido. La contraseña segura (EAP MSCHAPv2) debe aparecer en la lista Tipos de EAP.

Las solicitudes de conexión se deben configurar en el perfil de la directiva de acceso inalámbrico estableciendo en la ficha

restricciones de marcado en la opción minutos que el cliente puede estar conectado (tiempo de espera de sesión) el valor de 60 (minutos) en una WLAN 802.11b (de 11 Mbps) o 15 (minutos) en una WLAN 802.11a de velocidad superior o en una 802.11g (de 54 Mbps).

Con el comando *MSSTools AddRADIUSClient* adicionamos puntos de acceso clientes. Aquí este comando nos pedirá ingresar el nombre y la dirección IP del punto de acceso. Aquí se crea automáticamente una clave que comparten el servidor y el punto de acceso para autenticarse. En el punto de acceso se debe habilitar la autenticación 802.1x y configurar la dirección IP del servidor RADIUS en el punto con conexión a través del puerto predeterminado.

En el Active Directory a través de la directiva de red inalámbrica en el servidor IAS permite establecer configuraciones de cliente específicos de la WLAN. Se selecciona el objeto directivas de red inalámbrica (IEEE 802.11) en el panel de exploración y se crea una directiva de red inalámbrica en el menú acción. Es recomendado llamar a la directiva configuración de cliente WLAN de Windows XP (PEAP-WEP). En la fecha de redes preferidas se agrega la red

con su SSID, se selecciona la ficha 802.1x y se determina el PEAP y se selecciona la entidad emisora de certificados.

Los equipos cliente deben estar unidos al dominio y es necesario que se conecten a una LAN con cable para recibir la configuración de cliente WLAN. [8]

3.2.3 Seguridad avanzada

El último nivel de seguridad se recomienda para empresas grandes con datos altamente sensibles. Se basa en tecnologías de VPN probadas y de confianza para proteger la confidencialidad de los datos enviados a través de Internet. Aunque la solución de seguridad intermedia puede ser suficiente para la mayoría de escenarios, se ha decidido poner a disposición esta implementación como una medida más definitiva que separa de manera más concisa la red inalámbrica de la red cableada. Los casos en los que la seguridad avanzada es la recomendada se presentan en la tabla 3.3.

La tecnología de redes privadas virtuales o virtual private networks (VPN) ha sido ampliamente usada desde hace algún tiempo para accesos remotos. Probablemente son la manera más conocida y usada de cifrado de red. Estas protegen la confidencialidad de los

datos enviados a través de Internet creando un túnel seguro. Al ser evidentes las vulnerabilidades de seguridad en las redes inalámbricas inmediatamente se pensó en el uso de VPN para cifrar los datos que viajan a través de una WLAN.

CASO SEGURIDAD AVANZADA

Premisa	Respuesta
¿La red tiene menos de 30 computadores?	NO
¿Se ubica en un lugar con áreas vulnerables?	SI
¿Maneja información valorizada en más de 1000 dólares?	SI
¿Es justificado la inversión en una implementación más robusta?	SI

Tabla 3.3. Caso para la aplicación de seguridad avanzada

La implementación de VPN para eficazmente eliminar el riesgo de seguridad en una red WLAN se realiza con la ayuda del protocolo IPSec (Internet Protocol Security). Se escogió este recurso debido a que el IPSec es mucho más resistente en ambientes de redes "temperamentales" como es el caso inalámbrico comparado con otros protocolos de entunelamiento como el PPTP. Adicionalmente autentica y encripta los datos de manera adecuada sin necesidad de

una gran cabecera.

El costo y el nivel de administración que requiere esta implementación son limitantes para empresas pequeñas y medianas. Se requiere de equipos adicionales como switches o gateways VPN que incrementan la inversión. Es por ello que esta solución solo se implementará para casos extremos. Este caso está detallado en la tabla.

3.2.3.1 Equipos utilizados

La implementación de seguridad avanzada requiere de equipos VPN o de software especial. Sin embargo la solución por medio de software no es tan eficiente como se requiere en el caso de las redes inalámbricas. En el caso de una implementación con hardware se requiere de una gateway VPN. La función de este equipo es fundamental para la encriptación de los datos y creación del túnel.

Aunque las gateways VPN convencionales se pueden adaptar para ser usadas en la red WLAN, en el mercado existen equipos especiales para este tipo de implementaciones. Para la solución utilizamos una gateway WLAN que provee funciones adicionales que permiten una mejor administración y monitoreo de la red

inalámbrica. En la figura 3.7 vemos el diseño de la red con seguridad intermedia y la ubicación de la WLAN/VPN gateway.

Para implementar la solución avanzada de seguridad se requieren los siguientes equipos:

- La infraestructura WLAN debe estar implementada y trabajando de manera apropiada. Los puntos de acceso deben permitir el paso de tráfico IPSec (la gran mayoría de proveedores lo hace) y permitir la autenticación por medio de 802.1X.

- Los equipos de la red deben tener Windows XP o Windows 2000, en lo posible, pues este sistema operativo tiene funcionalidades para la creación de un cliente IPSec.

- Servidor RADIUS del tipo IAS de Windows Server 2003. Este será utilizado para la autenticación de los usuarios de la red inalámbrica y será consultado por el gateway.

- Gateway inalámbrica BlueSocket WG-2100. Este equipo permite la conexión de 1 a 50 puntos de acceso y 40 a 500

usuarios inalámbricos conectados al mismo tiempo.

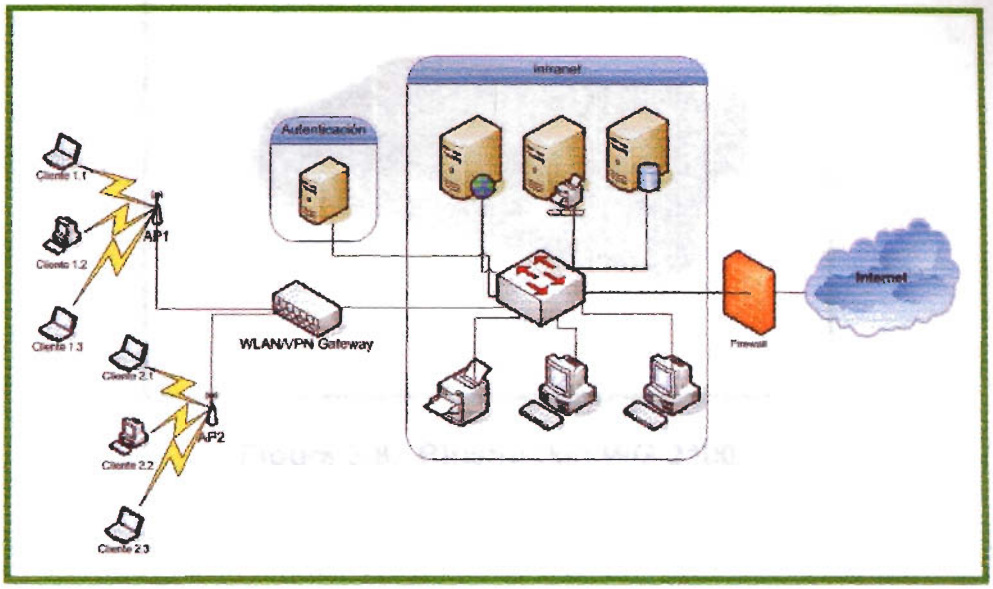


Figura 3.7. Diseño de una red con seguridad avanzada

El gateway inalámbrico de marca BlueSocket, presentado en la figura 3.8, fue seleccionado debido a varias razones. El equipo es compatible con cualquier punto de acceso y adaptador inalámbrico lo que elimina la necesidad de actualizaciones adicionales de hardware. Este equipo fue diseñado específicamente para proveer seguridad para la WLAN. Se sitúa entre el punto de acceso y la red cableada y no requiere ningún cambio adicional a la red WLAN existente en el área de hardware o software de cliente. Es un firewall efectivo entre la red WLAN no confiable y la red corporativa cableada confiable.

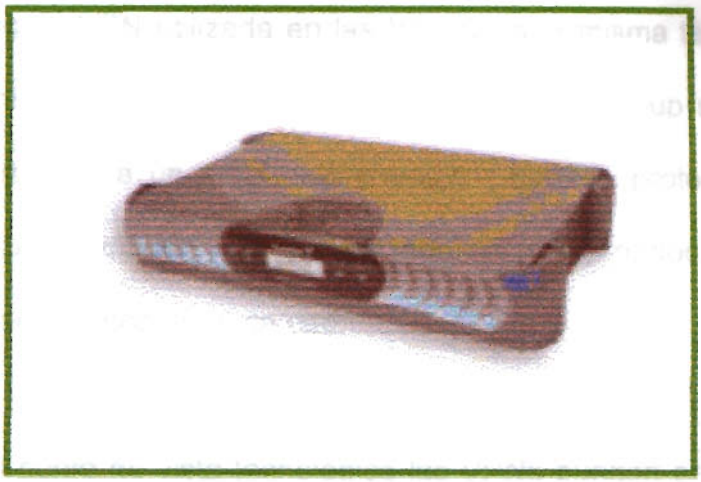


Figura 3.8. BlueSocket WG-2100

La simplicidad de su administración e instalación también fue considerada. Utiliza un sistema llamado RBAC (role-based access control) o control de acceso basado en roles. Todos los usuarios asociados a cada rol tienen el mismo grupo de permisos. Así el administrador no tiene que tener un control individual para cada usuario.

Provee control de acceso mediante un servidor RADIUS o LDAP (Local Directory Access protocol) y soporta IPSec que es el mejor tipo de seguridad disponible para comunicaciones de tipo IP. Adicionalmente permite la asignación personalizada de ancho de banda o que garantiza un buen enlace para todos los usuarios.

3.2.3.2 Descripción de la solución

La tecnología VPN utilizada en las WLAN es la misma tecnología que permite a una empresa proveer un acceso dial-up seguro a una red remota a un empleado o socio. Emplea protocolos de autenticación y cifrado muy fuertes que se han probado seguros después de muchos años de uso.

Desde un punto de vista tecnológico las VPNs pueden ser divididas en dos grupos basados en la capa del modelo OSI en la cual operan (capa 2 o capa 3). Las VPN de capa 2 son diseñadas en el nivel de enlace del modelo OSI. Este tipo de VPNs incluyen PPTP (Point-to-Point Tunneling Protocol) y L2TP (Layer 2 Tunneling Protocol). Ambos son utilizados principalmente para acceso remotos de tipo dial-in, aunque el segundo se considera más escalable.

Entre los protocolos de capa de red se encuentran MPLS (Multiprotocol Label Switching) e IPSec. Este tipo de protocolos presentan ventajas de escalabilidad y facilidad de manejo propias de una red de dicha capa.

Como núcleo de la tecnología VPN se encuentra el protocolo

IPSec y el protocolo de autenticación IKE (Internet Key Exchange). El IKE usa cualquier tipo de llave o certificado digital para autenticar a los usuarios del sistema. Una vez autenticado la VPN utiliza túneles (una conexión punto a punto segura) para transmitir y recibir los paquetes de datos en los que tanto los datos como las cabeceras están cifradas.

El protocolo IPSec es un conjunto de estándares abiertos para asegurar una comunicación privada y segura. En las VPNs que utilizan IPSec se usa los servicios definidos por IPSec para asegurar la confidencialidad, integridad y autenticidad de la información enviada a través de redes públicas. En el caso de las redes inalámbricas IPSec asegura la información sobreponiéndose encima del tráfico 802.11 enviado en claro.

Cuando este protocolo es usado en una red inalámbrica, un cliente IPSec es configurado en cada terminal cliente (usuario autorizado) de la red y se requiere que el usuario establezca un túnel IPSec para enviar el tráfico a la red cableada. Filtros son establecidos para evitar que cualquier tráfico inalámbrico llegue otro destino de que no sea la gateway inalámbrica.

La confidencialidad de los datos se obtiene mediante la encriptación por el estándar DES (Data Encryption Standard), 3DES o AES (Advanced Encryption Standard).

El IPSec tiene muchas características de seguridad. Se puede configurar el método de cifrado, la autenticación por equipos y asignación de credenciales, integridad de los datos, ocultar direcciones, asociaciones de seguridad y duración de las claves. El estándar IPSec requiere del uso sea de integridad de los datos o cifrado de los datos, las dos son opcionales.

Los servicios de seguridad dentro de IPSec se proveen por uno de dos protocolos, el AH (Authentication Header) y el ESP (Encapsulating Security Payload). Cada protocolo provee de ciertos servicios y pueden ser usados por separado o juntos, aunque no es realmente necesario usar ambos.

El AH provee integridad de los datos sin conexión y autenticación del origen de los datos para paquetes IP. Integridad sin conexión quiere decir que el paquete IP original no fue modificado en el camino del origen al destino. La autenticación del origen de los datos verifica la fuente de los datos. Juntos estos dos servicios

son la autenticación de los datos.

El AH contiene información criptográfica para la verificación de errores del contenido del paquete, incluyendo las partes de la cabecera IP que son invariables en transito. El algoritmo criptográfico utilizado para la verificación de errores o "checksum" es el HMAC (Hashed-bases message autentication code) en conjunto con el MD5 (Message Digest 5) o el SHA-1 (Secure Hash Algorithm 1). Estos son llamados algoritmos hash y su función es tomar un mensaje de tamaño variable y producir un valor de tamaño único. En el destino el mensaje se verifica comparando el valor recibido con el cálculo del checksum.

El AH también provee de servicios anti-repetición que pueden ser usados para prevenir ataques DoS. Sin embargo este no provee servicios de confidencialidad por lo que no se usa tan ampliamente.

El ESP provee confidencialidad del tráfico IP además de la autenticación y servicios anti-repetición. La confidencialidad es lograda mediante cifrado. El proceso de cifrado toma un mensaje, el texto en claro, y lo pasa a través de un algoritmo matemático

para producir el texto cifrado. En el destino se realiza un proceso inverso llamado descifrado. El ESP soporta una serie de algoritmos simétricos de cifrado para el cifrado de los datos. El más utilizado es el DES, aunque debido a sus susceptibilidades a dado paso a otros como el 3DES y AES. Debido a su alto nivel de confidencialidad, el ESP es el protocolo más utilizado del conjunto IPSec y es el que se aplica para la VPN como estrategia de seguridad inalámbrica.

Dos modos IPSec, túnel y transporte, son utilizados para proveer una comunicación segura entre dos puntos, usualmente el usuario y la gateway de seguridad. El gateway de seguridad en este caso es el equipo BlueSocket WG-2100 que provee los servicios IPSec (funciona como terminación de la conexión IPSec) y pasa tráfico a través del túnel al otro lado. El modo túnel encapsula y protege el paquete IP por completo mientras que en el modo transporte solo la cabecera es insertada dentro del paquete.

El protocolo IKE para el manejo de llaves es parte importante de esta instalación. Mejora al IPSec adicionando herramientas, flexibilidad y facilidad de configuración. Permite la negociación automática de las asociaciones de seguridad y facilita el

intercambio seguro de llaves.

El IKE permite que dos puntos intercambien llaves de encripción de manera segura. El intercambio de llaves Diffie-Hellman es usado de manera que no se envían señales de sesión directamente sobre la red.

La negociación se refiere a establecer políticas de seguridad o asociaciones de seguridad (SA) entre equipos. Un SA es una regla que se crea para un usuario específico, con cada regla identificada por un index único. Cuando un datagrama IPSec llega a un punto el equipo terminal utiliza este índice para encontrar en la Base de Datos (Security Association Database (SADB)) la política utilizada para ese datagrama.

Para que dos equipos intercambien información segura necesitan estar de acuerdo en que algoritmos criptográficos usar. Este acuerdo son las asociaciones de seguridad que especifican información de que algoritmos da autenticación y cifrado se van a usar, las llaves compartidas por sesión, la duración de las llaves, el tiempo de duración de la asociación misma, además de otra información.

Existen dos tipos de asociaciones: las IKE SA son bi-direccionales y proveen un canal seguro de comunicación entre dos puntos que puede ser usado para negociar la comunicación y las IPSec SA que son unidireccionales y son usadas para la comunicación en si entre dos equipos. Para la comunicación en dos sentidos entre dos equipos debe haber por lo menos dos IPSec SAs, una en cada dirección.

La conexión IPSec se realiza en dos fases para el intercambio de SAs. En la primera fase se inicia el canal seguro, estableciendo el IKE SA. En la fase dos se negocian las IPSec SAs. En la fase uno se realiza un intercambio llamado modo principal y en la fase dos el intercambio es de modo rápido.

En el modo principal de la fase uno se negocia el método de autenticación, que en este caso es por medio de llave compartida. La llave es negociada en intervalos regulares de manera que nunca será comprometida.

El proceso de establecimiento del túnel consta de 4 pasos presentados en la figura 3.9:

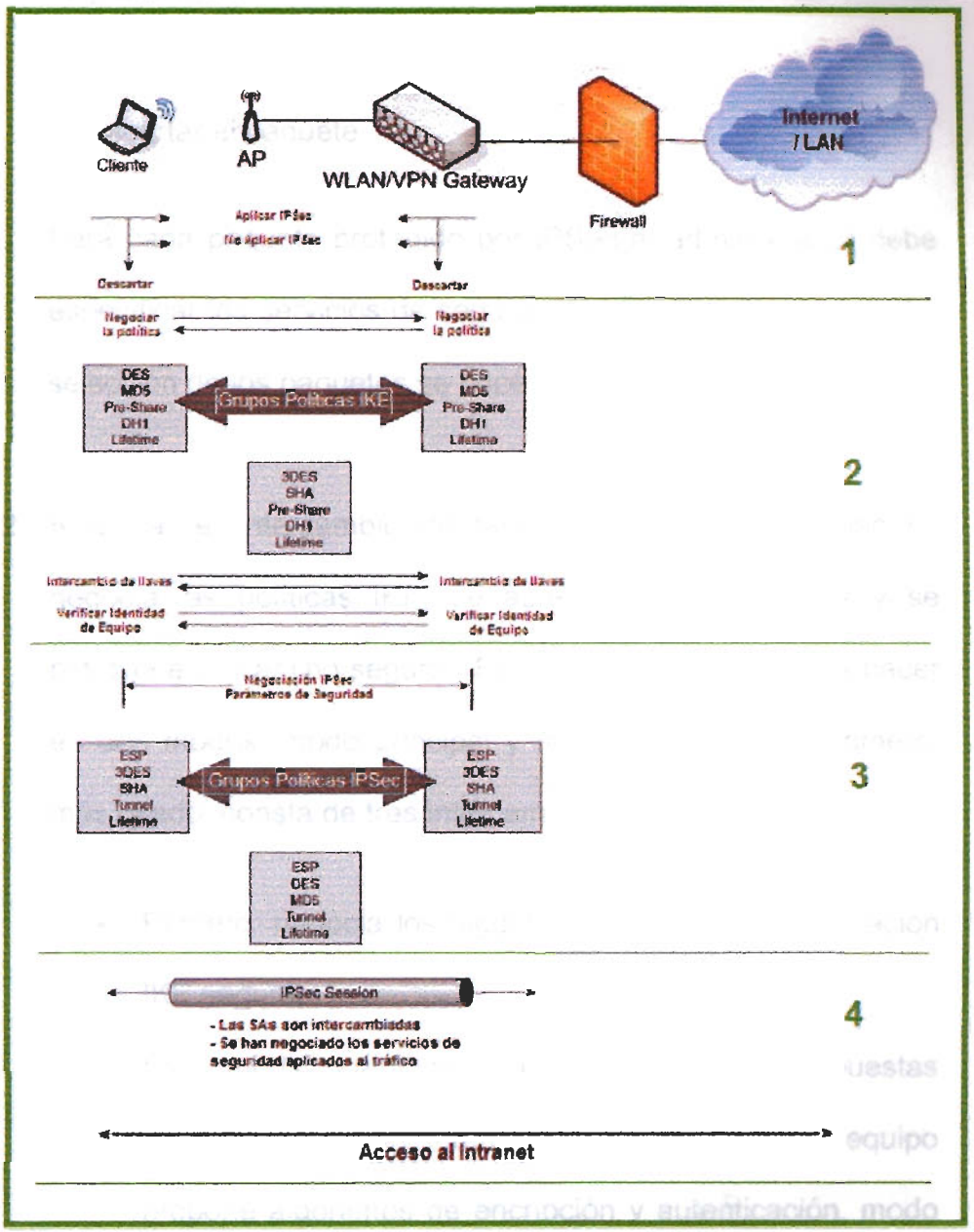


Figura 3.9. Pasos para la creación del túnel IPSec

1. Determinar que tráfico requiere ser protegido y cual puede ser enviado como texto en claro. Para cada paquete se tiene la opción de:

- Aplicar IPSec
- No aplicar IPSec
- Descartar el paquete

Para cada paquete protegido por IPSec el administrador debe especificar los servicios de seguridad aplicados al paquete. La selección de los paquetes se hace por medio del cliente VPN.

2. Negociar el intercambio de fase 1 IKE. En este paso se negocia las políticas IKE, se autentica a los equipos y se establece un camino seguro. Esta negociación se puede hacer en dos modos, modo principal y modo agresivo. El primero, más usado, consta de tres intercambios:

   - Primero: negocia los algoritmos para una comunicación IKE segura.

     El momento que inicia una conexión segura propuestas de seguridad son intercambiadas. El primer equipo propone algoritmos de encripción y autenticación, modo y largo de la llave. El otro equipo debe responder con un grupo de propuestas igual para que la comunicación sea viable.

- Segundo: Se realiza un intercambio de llaves compartidas que serán utilizadas posteriormente para el cifrado.
- Tercero: Verifica la identidad del otro lado.

En el modo agresivo se realiza procedimientos similares pero en menos pasos o intercambios.

3. En este paso o la llamada fase dos se negocian los parámetros de seguridad IPSec. Aquí se define los parámetros de seguridad que se aplicarán al tráfico pertinente que pasará por el túnel que se negoció en la fase anterior.

   Se definen:

   - Parámetros de Seguridad IPSec y grupos de propuestas IPSec.
   - Se establecen las Asociaciones de Seguridad.
   - Periódicamente se renegocian las SA cuando el tiempo de vida expira por seguridad.

   Todo esto se realiza en un solo paso.

   La información de intercambio es agrupada en un conjunto de

propuestas similar a la del IKE con propuestas de modo IPSec, algoritmos de encripción y autenticación, dirección IP de destino, modo transporte y duración de la llave.

4. Cuando finalmente se ponen de acuerdo en los servicios de seguridad esta información es guardada en la base de datos de SADB con su correspondiente índice. Así el tráfico podrá ser intercambiado formándose el túnel iPSec.

Mediante esta serie de estándares el IPSec establece el túnel de comunicación segura que impide que usuarios extraños a la red ingresen a ella, mediante la autenticación, y que los datos sean interceptados, a través de los métodos de cifrado. Cumple así el objetivo de asegurar la red inalámbrica.

Para la seguridad avanzada la gateway inalámbrica se encuentra entre los puntos de acceso y el intranet o internet. Inicialmente esta verifica la identidad de un usuario mediante la autenticación. El usuario presenta el nombre de usuario, la clave y la WG (wireless gateway) verifica esta credencial con una base de datos interna y posteriormente con una base de datos externa de tipo RADIUS. Después de eso la WG define

mediante reglas de autorización cuales equipos de la red están disponibles para el usuario y que ancho de banda se le debe asignar. Finalmente define el protocolo de entunelamiento, que en el caso de esta solución es una VPN de tipo IPSec. Así la WG funciona como VPN gateway además de proveer servicios adicionales de administración de la red inalámbrica. [12]

3.2.3.3 Implementación de la seguridad avanzada

El equipo WG-2100 idealmente debe ser ubicado en el cuarto de servidores. Se debe conectar el equipo con las interfases de red al lado protegido y al lado inalámbrico de la red. En la parte posterior existen dos puertos eth0 y eth1 denominados protegido y administrado respectivamente. La interfaz denominada *protected* (protegida) debe conectarse al lado cableado de la red. La interfaz llamada *managed* (administrada). La conexión debe hacerse con un cable cruzado si se conecta directamente al punto de acceso. El siguiente paso es prender el equipo.

Ahora si podemos empezar a configurar el equipo. Ingresamos a la consola de administración a través de un browser escribiendo http://direccion_IP/admin.pl. La dirección IP será presentada en la pantalla LCD de la WG. La clave de fábrica para el administrador

es blue, y debe ser cambiada la primera vez que se ingresa. Es importante recalcar que ha esta consola se puede acceder bajo dos usuarios, admin y monitor, y solo la primera tiene permisos para modificar las configuraciones.

El siguiente paso es establecer direcciones IP y otros parámetros de la interfaz protegida. Esto se logra mediante la selección del icono *protected* en el menú de interfaces. Aquí tendremos acceso a la configuración del puerto eth0.

Para establecer la red administrada (red inalámbrica) primero hay que habilitar la opción de DHCP de la WG (Run DHCP Server) y establecer el rango de direcciones y la máscara de subred. También se puede activar el NAT (Network Address Translation) para proteger las direcciones de la red cableada del lado inalámbrico.

Luego necesitamos determinar que destinos en la red están abiertos o cerrados para ciertos usuarios. El destino puede ser un solo equipo dentro de la red o todos los equipos disponibles. Esto se puede configurar en la parte *destinations* del menú. Podemos crear un host o una red, definiendo las direcciones IP y

poniéndoles un nombre. Adicionalmente en la opción *services* del menú se puede establecer que servicios serán limitados o están disponibles para los usuarios (ejemplos de servicios son HTTP, FTP, LDAP, etc.).

A continuación seleccionamos el protocolo de entunelamiento. En la opción *VPN* del menú se selecciona IPSec, dando paso a la pantalla de las configuraciones IPSec. Creamos una configuración escogiendo el tipo de cifrado, el cifrado para el IKE y el tipo de compresión. En el menú de cifrado, encryption, tendremos la opción de escoger entre DES, 3DES y AES con checksum MD5 o SHA1. Se recomienda la opción 3DES con SHA1. Debemos habilitar la opción de llaves compartidas, pre-shared keys, para asegurar la conexión. Establecemos un nombre para esta configuración IPSec.

Las últimas versiones de Windows vienen con clientes IPSec implementados que permiten asegurar datos transmitidos desde la máquina hasta el servidor IPSec. Aunque este cliente evita el gasto adicional en software para cada usuario no es tan sencillo de configurar por lo que la WG-2100 tiene una herramienta que facilita la implementación nativa del IPSec, la BlueSocket MS IPSec

Configuration Tool. Esta tiene que ser instalada en cada equipo. El programa instalado es un ejecutable que presentará una ventana para la configuración.

En la opción *setup* establecemos que el adaptador es el cliente Windows IPSec, determinamos que política vamos a utilizar y definimos la dirección IP de la WG como VPN Gateway. Con respecto a la política utilizada, existe un default que viene con la herramienta llamada Policy.bin que puede ser utilizada como punto de partida. En opciones avanzadas podemos habilitar la propiedad de *Enhanced Mobility* que permite moverse entre subredes inalámbricas, eso en el caso de que exista más de un punto de acceso.

Después de reiniciar el equipo desde *Start/Settings/Control Panel/Administrative Tools/Local Security Policy* de Windows podemos seleccionar las propiedades locales de seguridad, entrando a la carpeta *IP Security Policies on Local Machine*. Aquí podemos definir la política de seguridad que se desea utilizar para la VPN on el WG-2100. En las reglas de salida se selecciona autenticación por llave compartida y se establece la misma llave ya definida en la WG. Se implanta como final del túnel la dirección IP

de la interfaz inalámbrica de la WG. En las reglas de entrada se establece la llave compartida pero como fin del túnel se ingresa la dirección IP del equipo.

Es importante definir los roles que permitirán o negarán acceso inalámbrico al usuario a los servicios de la red. También por medio de los roles se define el ancho de banda disponible para cada usuario y el tipo de protocolo de entunelamiento que es usado.

En la opción *role* definimos todas estas características nombrando a cada rol según el tipo de usuarios que utilizarán esos servicios. En cada servicio se puede seleccionar se el acceso es permitido o negado y si este es unidireccional (de entrada o de salida) o si es bi-direccional.

Finalmente es necesario crear usuarios y asignarles el rol que utilizarán. Del menú seleccionamos la opción *users* y creamos uno nuevo para cada usuario, determinando el nombre, el rol y la clave. Si se desea trabajar con un servidor de autenticación RADIUS en vez de crear un nuevo usuario se selecciona el servidor y se define los roles. [13]

CAPÍTULO 4

ADMINISTRACIÓN DE LA SEGURIDAD

4.1 Políticas de Seguridad en la empresa

Al finalizar la implementación de seguridad en la red inalámbrica, la administración y el uso eficaz de la solución queda en manos del equipo de administración de la red y de los usuarios. Aun cuando el nivel de seguridad se incrementa valiosamente al aplicar uno de los tres métodos de seguridad mencionados en el capítulo anterior, un mal uso y una mala administración de la red pueden crear grandes problemas de seguridad que deben ser tomados en cuenta.

Para educar y restringir a los empleados del uso inadecuado de la WLAN se recomienda crear una política de seguridad de redes inalámbricas. Esta política puede cambiar de empresa a empresa pero debe estar sujeta a ciertos parámetros invariables.

4.1.1. Definición de Política de Seguridad

Una política de seguridad es un tratado formal de las reglas que las personas que tienen acceso a la tecnología y recursos de la organización deben seguir.

Para iniciar la creación de una política de seguridad se debe definir los objetivos principales:

- Definir los recursos que deben ser protegidos, los riesgos y los objetivos de seguridad.
- Identificar las prácticas y medidas de seguridad que se manejan en la red.
- Dictar el comportamiento adecuado y la forma de hacer cumplir las reglas.
- Debe ser un consenso entre los diferentes grupos de interesados incluyendo gerentes, administradores de red y usuarios finales.

La política de seguridad debe tener un equilibrio entre ser específica y fácil de implementar. Debe ser concisa y al mismo tiempo fácil de entender.

4.1.2. Características de una política de seguridad inalámbrica

Las partes más importantes que se deben incluir dentro de la política WLAN son:

1. Objetivo: ¿Qué es lo que la política pretende lograr?
2. Propiedad y autoridad: ¿Quién creo, aprobó y hará cumplir la política?
3. Rango: ¿Quién debe cumplir esta política y dónde?
4. Contabilidad de riesgos: ¿Qué recursos están en peligro? ¿Cuáles son las amenazas y su impacto?
5. Medidas de seguridad: ¿Cuáles prácticas y medidas de seguridad se utilizarán?
6. Uso aceptable: ¿Qué deben hacer los usuarios para cumplir con la política?
7. Métodos de implementación: ¿Cómo la política será implementada, probada y ejercida?
8. Auditoria y cumplimiento de la política: ¿Cómo se monitoreará y asegurará el cumplimiento de la política?

Una política más completa adicionalmente puede incluir:

- Delegación de la autoridad y responsabilidad: La política debe delegar autoridad a una figura que tiene la responsabilidad y autoridad sobre la red inalámbrica. El "administrador de seguridad" estará a cargo de todas las funciones de seguridad y de asignar a otros individuos o equipos a diferentes funciones si es necesario. Se recomienda que este sea un administrador de red.

- Definición de amenazas: Se debe determinar cuales amenazas y vulnerabilidades tiene la organización en lo que se refiere a la operación WLAN. Entender cuales son los riesgos previene en contra de ataques y costos posteriores. Todos estos datos ya se tienen como resultado de la consultoría realizada en la red.

- Segregación de la Red: La política necesita crear una frontera que divide la red inalámbrica "no segura" de la red cableada más "segura". El objetivo es que cualquier brecha de seguridad de la red inalámbrica no afecte el medio cableado.

- Autenticación: La autenticación es esencial para la operación segura de una red inalámbrica y el modo de autenticación debe

ser incluido en la política. Todos los usuarios deben autenticarse y la implementación y mantenimiento de el método de autenticación debe definirse.

- Seguridad de puntos de acceso: La política debe explicar la necesidad de asegurar los AP inalámbricos tanto lógica como físicamente. Puede ser necesario definir quién está autorizado para cambiar la configuración.

- Comunicaciones Ad-Hoc: Es recomendable que la política no permita que los clientes se conecten en comunicaciones ad-hoc. El peligro es que muchos usuarios maliciosos utilizan este tipo de comunicaciones para realizar ataques en contra de la WLAN.

- Educación y alertas: La política debe incluir provisiones para incrementar y mantener la alerta de seguridad entre los usuarios. Si los usuarios, administradores de red y gerentes tienen conocimiento de las técnicas de seguridad mejoran la postura de seguridad de toda la red. Si los gerentes y usuarios están al tanto de los riesgos que implican la violación de ciertas partes de la política, estos probablemente estarán más dispuestos a cumplirlas.

La política de seguridad establece un modelo para la red existente. Una buena política crea un conjunto de reglas y estándares que tanto los usuarios como los administradores y gerentes deben seguir. Esta manejará las implementaciones inalámbricas futuras, asegurando una expansión uniforme y compatible con el equipo existente. La política facilita la administración de la red y determina autoridad.

4.1.3. Creación de una política de seguridad inalámbrica

Al finalizar la consultoría e implementación de seguridad para la red inalámbrica el consultor debe requerir la creación de una política de seguridad inalámbrica. Como se mencionó, esta política debe crearse como trabajo conjunto entre las tres unidades involucradas: el usuario final, el administrador de la red y el área de gerencia.

El consultor debe actuar como un guía en este proceso. Es importante que este recalque los siguientes puntos al iniciar la creación de las políticas:

- Las políticas de seguridad inicialmente deben identificar quien es el usuario final de la tecnología WLAN. Se debe determinar quien puede instalar equipo inalámbrico, no solo puntos de acceso.

- Es una buena idea establecer de manera definitiva que la única fuente autorizada para proveer servicios inalámbricos es la empresa. Esto puede prevenir que usuarios o grupos crean que debido a que existe una WLAN aprobada ellos pueden proveer su propio acceso si no está disponible en donde ellos quisieran. Se puede determinar que cualquier punto de acceso no autorizado será confiscado y el usuario sancionado.

- Es importante proveer limitaciones en la ubicación física del equipo.

- Probablemente se requerirá definir la clasificación de la información que puede ser enviada a través de la WLAN junto con las tecnologías de encripción requeridas.

- Se debe definir los recursos, servicios, equipos y aplicaciones a los que se puede acceder desde la WLAN junto con las medidas utilizadas para limitar el uso del ancho de banda.

- Vale la pena describir la configuración del hardware y software de los equipos inalámbricos permitidos, incluyendo las definiciones de seguridad para puntos de acceso y clientes.

- Puede también describir cualquier tipo extra de seguridad como

IDS (sistemas detectores de intrusos) o firewalls. Se debe asegurar que los usuarios están al tanto de los riesgos, las partes relevantes de la política y las medidas de seguridad instaladas.

- Detallar los usos apropiados y no apropiados de la WLAN y las posibles consecuencias si no se siguen esas normas. El usuario final debe conocer y entender las políticas para el uso de la red inalámbrica.

Todos estos puntos deben ser tratados en conjunto por los gerentes, administradores y usuarios. Además los datos de la seguridad implementada deben ser revisados. Al tener esta información a la mano el siguiente paso es empezar a escribir la política de seguridad. Esta debe cumplir con las características principales mencionadas anteriormente pero debe ajustarse a las necesidades de la empresa.

Un tipo de política de seguridad se encuentra en el anexo 6. En ella se define como sistema de seguridad la implementación VPN como es el caso de la solución de seguridad avanzada. Se debe permitir que la política sea evaluada por una o dos semanas para receptar sugerencias y preguntas. Finalmente al ser aprobada debe ser remitida a todos los usuarios finales de la red.

4.2 Sistemas de detección de intrusos

Aun con las implementaciones de seguridad correctamente ejecutadas y una política de seguridad que educa a los empleados en el uso correcto de la red inalámbrica, el administrador deberá realizar monitoreos periódicos de la red.

Ninguna solución es infalible. El avance de la tecnología da paso a herramientas cada vez más sofisticadas para el ingreso ilegal a la red. Es importante estar atento y no permitir que pequeñas fallas de seguridad comprometan la red que estamos tratando de proteger.

Aun cuando el nivel de autenticación y encripción es muy alto todavía existe el problema de los puntos de acceso intrusos. Este problema se acentúa en la implementación de seguridad básica, por lo cual es importante definir que es un punto de acceso intruso y que problemas de seguridad puede causar.

4.2.1. Puntos de acceso intrusos

Cualquier punto de acceso no autorizado por el equipo administrador de red se considera un punto de acceso intruso. Este puede ser un equipo instalado por un empleado que desea moverse de su escritorio, probablemente sin ningún tipo de seguridad, dejando una puerta

abierta a la red corporativa. También pueden ser equipos intencionalmente instalados por un intruso para obtener información.

En el caso del empleado, la necesidad de movilidad, junto con los bajos costos de equipos de redes inalámbricas, provocan que se evite las rígidas medidas de seguridad inalámbrica conectando un punto de acceso en un jack ethernet. Estos puntos de acceso intrusos son fáciles de instalar y proveen movilidad a los empleados que la buscan. Sin embargo el resultado es un punto de entrada ampliamente abierto a la red corporativa, como se muestra en la figura 4.1. Un punto de acceso intruso extiende de manera efectiva la conexión ethernet a cualquiera dentro y fuera del edificio.

Como quedó establecido en capítulos anteriores, cualquier equipo con una tarjeta de red puede conectarse a estos AP intrusos o simplemente escuchar el tráfico que se transmite a través de la red.

Usuarios maliciosos que instalan puntos de acceso intrusos pueden aprovecharse de errores de configuración en el equipo de usuario para provocar que equipos de la red corporativa se conecten a ellos. Muchas veces los usuarios usan los computadores portátiles para conectarse a redes abiertas durante el fin de semana, bajando las

protecciones de seguridad y permitiendo errores de asociaciones como este, mostrado en la figura 4.2.

Figura 4.1. Punto de acceso intruso caso 1

Por estas razones los puntos de acceso intrusos representan problema para la seguridad de la empresa incluso cuando esta ha invertido en una solución de seguridad. Es importante por lo tanto realizar un monitoreo constante de la red para encontrar estos equipos y de esta manera poder eliminarlos.

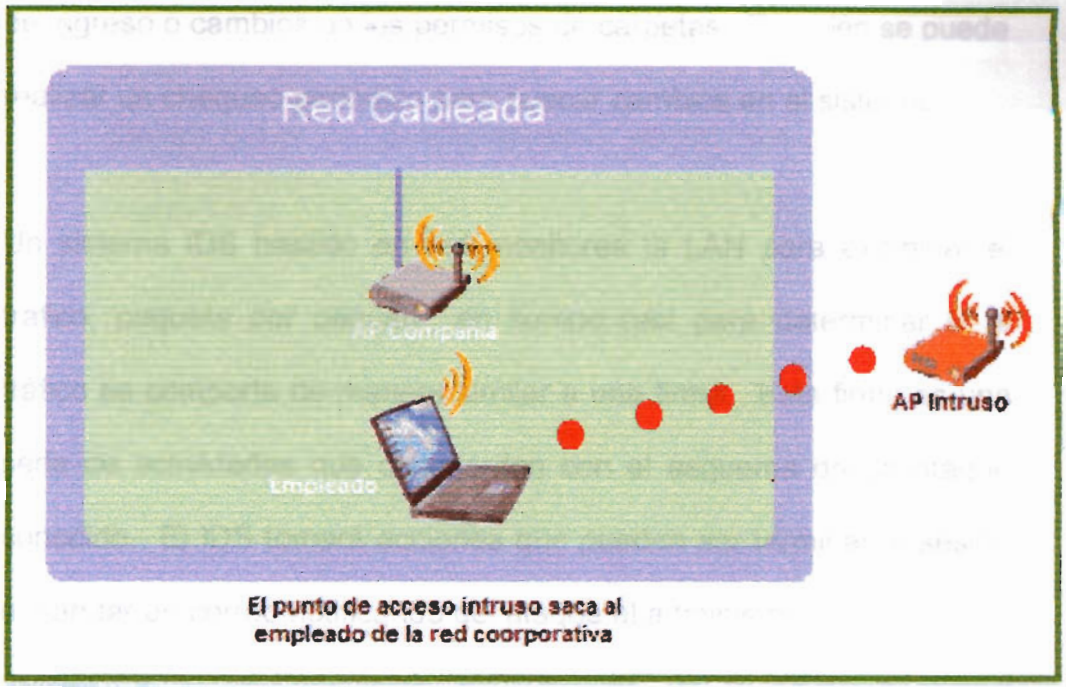


Figura 4.2. Punto de acceso intruso caso 2

4.2.2. Monitoreo y Detección de Intrusos

Un sistema de detección de intrusos (IDS por sus siglas en inglés) es una herramienta efectiva para determinar si usuarios no autorizados están tratando de acceder, han ingresado o han comprometido la red. Los IDS para las WLAN pueden ser de tipo usuario, de tipo red o híbrido. Un IDS basado en usuario aumenta un nivel de seguridad para un equipo particularmente vulnerable o esencial. Este consta de un agente instalado en un sistema individual, por ejemplo una base de datos y monitorea el tráfico de dicho servidor.

Crea registros de comportamiento sospechoso, como muchos intentos

de ingreso o cambios en los permisos de carpetas. También se puede realizar un chequeo periódico para buscar cambios en el sistema.

Un sistema IDS basado en red monitorea la LAN para examinar el tráfico, paquete por paquete, en tiempo real para determinar si el tráfico se comporta de manera similar a una firma. Esta firma es una serie de actividades que concuerdan con el esquema de un ataque conocido. El IDS tomará acciones que pueden ser terminar la sesión o mandar un correo notificando del ataque al administrador.

En el caso de las redes inalámbricas los IDS deben tener las siguientes características:

- Ser capaz de identificar la ubicación física de los equipos inalámbricos dentro del edificio y en sus alrededores. Esto se hace por medio de técnicas de triangulación.

- Detección de comunicaciones de tipo punto a punto no autorizadas que pueden permitir que una portátil externa se asocie a un portátil de la compañía.

- Análisis de la comunicación inalámbrica y monitoreo de el tráfico 802.11 en radio frecuencia.

- La generación de una alarma cuando un punto de acceso intruso entra en funcionamiento dentro del perímetro de seguridad.

- Detección de intentos de inundación de paquete antes de que comprometan seriamente la red inalámbrica.

En el mercado existen una serie de productos adecuados para el monitoreo inalámbrico que cumplen con estas características y adicionalmente proporcionan herramientas de administración muy útiles. Sin embargo estas soluciones vienen con un costo. El administrador de red debe determinar si el costo de la implementación de estos equipos es justificado.

Ejemplos de estos sistemas IDS es AirMagnet, AirDefense y AirWave:

- AirMagnet le da la posibilidad al administrador de detectar una serie de vulnerabilidades y ataques de red. Todo comienza con una política en donde el sistema permite definir cual es la seguridad utilizada por la WLAN (WEP, 802.1x, VPN, etc.). Automáticamente cada cliente y punto de acceso será analizada y se crearan alertas en el momento que cualquier violación de la política de seguridad.

- AirDefense es un sistema basado en sensores que son un IDS basado en red. Constantemente monitorea toda la actividad en la red inalámbrica permitiendo el control del espacio aire de la localidad manteniendo un estricto control del cumplimiento de las políticas de seguridad.

- AirWave provee soluciones de software con facilidad de configuración, monitoreo basado en usuario, detección de puntos de acceso y monitoreo de la radio frecuencia.

Sin embargo, en el caso de que se decida no invertir en una de estas soluciones de monitoreo, existen varios recursos accesibles sin costo. Estos son programas que aunque no proveen las características administrativas pueden ser muy buenas herramientas de monitoreo. Programas como el NetStumbler, Kismet y SSID Sniff son relativamente fáciles de utilizar. El administrador puede encargarse de realizar evaluaciones periódicas para determinar la presencia de puntos de acceso intrusos.

Adicionalmente, para la solución avanzada, la WG-2100 provee funciones de monitoreo que crean registros de las actividades de la red. Está en manos del administrador revisar estos registros.

CAPÌTULO 5

COSTOS

Una de las partes que algunos clientes consideran muy importante es la que se refiere al costo de los servicios que se le prestan a sus empresas, decimos que algunos clientes porque existe una parte que sabe que para poder ser una empresa de calidad y ser líderes en el sector que prestan servicios no se deben escatimar esfuerzos económicos por tener los mejores servicios a ofrecer.

En esta parte del proyecto tenemos dos puntos a tratar que son los costos por realizar la consultaría y los costos por implementación de la seguridad sea mínima, media o avanzada.

5.1. Costos de la consultoría

Nuestro servicio de consultoría basa sus costos en base a un presupuesto que contiene los siguientes puntos:

- Suministros de oficina: Aquí está lo que es hojas para impresión, tinta y todo lo concerniente a este ítem, cabe recalcar que cada uno de estos puntos no serán escritos en la hoja del presupuesto pues allí va el valor total de los servicios a prestar, el cual lleva el nombre de valor de la consultoría (anexo 7) .

- Movilización: Son los gastos que se van a generar para llegar hasta el sitio en donde se va a realizar la consultoria, debido a que puede ser tanto dentro de la ciudad como en cualquier parte del país y estos valores cubrirían desde gasolina hasta incluso pasajes de avión.

- Prestación de servicios: Este es el valor que tiene destinado la consultora por realizar el análisis de la red y entregar el informe respectivo a la empresa que ha solicitado los servicios, luego de haber finalizado la consultoría.

Como se lo mencionó anteriormente, todos estos puntos son enmarcados dentro de valor de la consultoría, pues en un presupuesto no debe estar minuciosamente detallado cada punto tomado en cuenta para el valor a proponer.

5.2. Costos de la implementación

La implementación de la seguridad en la empresa tendrá su costo como se lo mencionó anteriormente basado en la necesidad de un nivel de seguridad mínimo, medio o avanzado.

5.2.1 Costo de implementación mínima

Siendo la implementación más sencilla es lógico pensar que, su implementación no tendrá mayores costos, solo si no se llegaran a poder implementar 5 de los 6 temas mencionados en el capítulo 3 se procedería un cambio de hardware donde esos valores no entrarían en nuestros servicios pues no los damos.

En caso contrario los valores que tendría esta implementación solo serían los referentes a:

- Mantener control del área de cobertura de la señal y proteger con clave segura los puntos de acceso.
- Deshabilitar la opción de "broadcast" del SSID (Service Set

Identifier).

- Implementación de autenticación MAC (Media Access Control).
- Designar una clave WEP de 128 bits.
- Reiniciar los puntos de acceso.
- Deshabilitar las funciones SNMP (Simple Network Management protocol).

Que estarían dentro de los servicios que presta un profesional en seguridades, teniendo un costo de $ 200. La tabla 5.1 muestra los costos.

5.2.2 Costo de implementación media

En este tipo de implementación los costos dependen de los equipos que se requieren (sin poner en este caso una actualización de hardware de ser necesaria para este tipo de seguridad, pues no ofrecemos dicho servicio), su instalación y puesta en funcionamiento, además de la capacitación en el manejo de los mismos.

Esto lo detallaremos de la siguiente manera:

- Servidores RADIUS con los componentes de Servicios de Certificate Server e IAS de Windows Server 2003, cuyo costo es $ 835.

COSTO DE IMPLEMENTACION MINIMA	
Descripción de lo que se va a realizar	**Valor**
Mantener control del área de cobertura de la señal y proteger con clave segura los puntos de acceso. Deshabilitar la opción de "broadcast" del SSID (Service Set Identifier). Implementación de autenticación MAC (Media Access Control). Designar una clave WEP de 128 bits. Reiniciar los puntos de acceso. Deshabilitar las funciones SNMP (Simple Network Management protocol).	$ 200

Tabla 5.1. Costo de implementación mínima

- Capacitación en Windows Server 2000 o Windows Server 2003, para la administración correcta de la seguridad, con un costo de $ 300.
- Instalación y puesta en funcionamiento de la implementación: $ 600.

Lo que daría un valor final de $ 1735 detallado en la tabla 5.2.

COSTO DE IMPLEMENTACION MEDIA		
Equipos / software	**Cantidad**	**Valor**
Servidor RADIUS con los componentes de Servicios de Certificate Server e IAS de Windows Server 2003	1	$ 835
Capacitación en Windows Server 2000 o Windows Server 2003 (curso)	1	$ 300
Instalación y puesta en funcionamiento de la implementación	1	$ 600
Total		$ 1735

Tabla 5.2. Costo de implementación media

5.2.3. Costo de implementación avanzada

Al hablar de este tipo de implementación debe tener en claro la empresa a ponerla en marcha que no se escatimará en gastos pues los costos serán altos debido a los requerimientos necesarios, esto está de más mencionarlo pues si se llega a necesitar esta instalación es porque quien la solicita maneja información totalmente sensible.

Partiendo de una infraestructura WLAN bien implementada y en funcionamiento apropiado, con puntos de acceso permitiendo tráfico IPsec, lo cual es a nivel de hardware, basaríamos nuestro trabajo en los siguientes puntos:

- Gateway inalámbrica BlueSocket WG-2100, con este equipo podemos tener la conexión de 1 a 50 puntos de acceso y de 40 a 500 usuarios inalámbricos al mismo tiempo, con un costo de $ 13000.

- Servidores RADIUS con los componentes de Servicios de Certificate Server e IAS de Windows Server 2003, cuyo costo es $ 835.

- Capacitación en Windows Server 2000 o Windows Server 2003, para la administración correcta de la seguridad, con un costo de $ 300.

- Instalación y puesta en funcionamiento de la implementación $ 800.

Con lo que se tendría un costo total de $ 14935 detallado en la tabla 5.3.

COSTO DE IMPLEMENTACION AVANZADA		
Equipos / software	**Cantidad**	**Valor**
Gateway inalámbrica BlueSocket WG-2100	1	$ 13000
Servidor RADIUS con los componentes de Servicios de Certificate Server e IAS de Windows Server 2003	1	$ 835
Capacitación en Windows Server 2000 o Windows Server 2003 (curso)	1	$ 300
Instalación y puesta en funcionamiento de la implementación	1	$ 800
Total		$ 14935

Tabla 5.3. Costo de implementación avanzada

CONCLUSIONES Y RECOMENDACIONES

Las facilidades de movilidad y escalabilidad que ofrece la tecnología inalámbrica la convierten en una opción insuperable para la implementación de redes LAN. Al evaluar sus virtudes no hay duda de que las redes inalámbricas son la mejor opción. Debido a que permiten la movilidad aumentan la productividad de los trabajadores significativamente. Convierten a una computadora portátil en una oficina móvil. Los costos de su implementación son menores a los de cableado y la extensión de la red con nuevos equipos anualmente tiene un costo mínimo.

Sin embargo, el mayor problema de la implementación WLAN es la inseguridad. El medio en el cual se transmiten los datos es muy vulnerable y el rango de transmisión no se puede contener dentro de un área predeterminada. La seguridad WEP definitivamente no es suficiente para resolver el problema. Es necesaria una implementación de seguridad más

fuerte.

En el Ecuador la implementación de redes inalámbricas todavía es en pequeña escala. En la medida de que el uso de estas redes aumente, los problemas de seguridad aumentarán a la par. No podemos dejar que dichos problemas nos impidan aprovechar las facilidades de las WLAN. Es necesario empezar con una evaluación de seguridad.

La consultoría logra determinar cual es el nivel de inseguridad de la red. Permite que un consultor externo, imparcial, evalúe la red en los tres puntos que, basados en la experiencia del caso de estudio, consideramos los más relevantes.

El caso de estudio nos demostró que muchas veces una implementación muy compleja de seguridad no siempre es viable o necesaria. Como resultado de la consultoría se determina la magnitud de la necesidad de seguridad y se recomienda el tipo de implementación para cada caso. El gerente tiene la última palabra sobre la viabilidad de la implementación.

Pudimos darnos cuenta que en el mercado existen muchos tipos de soluciones de seguridad para las WLANs. Evaluamos cuidadosamente cada uno de los métodos. Para cada implementación seleccionamos los equipos

debido a sus características de seguridad y facilidad de administración. Debido a los costos consideramos que la implementación más viable es la intermedia, dejando la implementación más robusta para corporaciones grandes con redes extensas.

Es importante que el administrador de la red se mantenga siempre al pendiente de la seguridad WLAN. Aun después de que el método de seguridad sea implementado, un monitoreo permanente es siempre recomendado.

Al finalizar este proyecto pudimos determinar cuan importante es la seguridad en una red inalámbrica. Hace mucho tiempo dejó de ser opcional para convertirse en necesaria. La formación de una empresa de este tipo puede resultar un proyecto rentable pues la tecnología WLAN es un mercado en crecimiento. Aun con los costos adicionales para seguridad las redes inalámbricas siguen siendo una opción excelente para una empresa grande o en constante expansión.

ANEXOS

ANEXO 1

ANEXO 1
Acuerdo

Consultoría de Red

La compañía (Nombre de la compañía) ha llegado a un acuerdo con (Nombre de la consultora) para la realización de una **Evaluación de Seguridad** en su red inalámbrica. Para llevar a cabo esta evaluación se le permite a (Nombre de la consultora) monitorear la red con el programa NetStumbler y examinar los equipos de la red inalámbrica con la supervisión del administrador de la red.

Por su parte la compañía (Nombre de la compañía) se compromete a proveer a (Nombre de la consultora) con la información necesaria para la ejecución de la consultoría. Esta información esta sujeta a completa confidencialidad por parte de (Nombre de la consultora) y no será utilizada para ningún otro propósito.

Las dos partes están de acuerdo con estos términos.

Firma Autorizada (Nombre de la compañía)
Nombre:
Cargo:
C.I.:

Firma Autorizada (Nombre de la consultora)
Nombre:
Cargo:
C.I.:

ANEXO 2

ANEXO 2.1
Formulario de Estudio de Condición Actual de la Red

ESTADO ACTUAL DE LA RED

C&C

Equipos Inalámbricos Utilizados

Equipo	Marca	Tipo	Cantidad

Carácteristicas

SSID	
Número de estaciones de trabajo	
Número de puntos de acceso	
Canal en el que trabaja	
Utiliza DHCP	

Seguridad

	Si	No
WEP		
SSID broadcast		
Clave de AP de fabrica		
Tablas MAC		

Otro tipo de seguridad _____

Empresa	
Administrador de Red	
Consultor	
Fecha	

ANEXO 2.2
Formulario de Estudio de Vulnerabilidades

EXTERIORES

C&C

PLANO

Puntos de Acceso intrusos detectados por NetStumbler

SSID	Canal	SNR

Observaciones:

ANEXO 2.3
Formulario de Estudio de Riesgos

TIPO DE DATOS

INTRANET

1 Información de Negocios
Valor estimado de pérdida ☐

2 Información Coorporativa
Valor estimado de pérdida ☐

3 Información técnica y de desarrollo
Valor estimado de pérdida ☐

4 Información de mercadeo
Valor estimado de pérdida ☐

5 Información operacional y secretos de oficio
Valor estimado de pérdida ☐

6 Información de recursos humanos
Valor estimado de pérdida ☐

7 Información financiera
Valor estimado de pérdida ☐

8 Código fuente
Valor estimado de pérdida ☐

9 Información confidencial del cliente
Valor estimado de pérdida ☐

10 Acceso a través de la red a otras empresas
Valor estimado de pérdida ☐

INTERNET

11	Datos confidenciales enviados en aplicaciones de internet	Valor estimado de pérdida
12	Otros ----------	Valor estimado de pérdida

Valor estimado de pérdida total

ANEXO 3

ANEXO 3
Resultado de Estudio: Laboratorio DELTA

ESTADO ACTUAL DE LA RED

C&C

Equipos Inalámbricos Utilizados

Equipo	Marca	Tipo	Cantidad
Router Inalámbrico	D-Link	DI-614+	1
Punto de Acceso	D-Link	DWL-2100AP	2
Adaptador de Rede	D-Link	DWL-520+	40

Carácteristicas

SSID	DELTA
Número de estaciones de trabajo	40
Número de puntos de acceso	3
Canal en el que trabaja	1
Utiliza DHCP	si

Seguridad

	Si	No
WEP		X
SSID broadcast	X	
Clave de AP de fabrica		X
Tablas MAC		X

Otro tipo de seguridad Ninguno

Empresa	ICHE-ESPOL
Administrador de Red	Ing. Nelson Laayedra
Consultor	R. Cabezas y A. Castillo
Fecha	26 de Septiembre, 2005

ESPECIFICACIONES TÉCNICAS ROUTER Y PUNTO DE ACCESO

DI-614+

D-Link AirPlus 2.4GHz Internet Server Wireless and Access Point with 4-port 10/100 switch port. (4 x)

Características Técnicas

CPU	ARM-7
Memoria	512 Kbytes Flash Memory 2 Mbytes SDRAM
Estándares	IEEE 802.3 10BaseT ETHERNET IEEE 802.3u 100BaseTX FAST ETHERNET IEEE 802.11b Wireless LAN (22 Mbps), Wi-Fi Compatible ANSI/IEEE 802.3 NWAY auto-negociacion
Protocolos Soportados	TCP/IP, NAT, DHCP, RIP1/RIP2, Ruteo Estático, Ruteo dinámico, soporta PPPoE para xDSL o cable modem, Virtual Server.
Soporta VPN (en modo Pass-Through)	IPSec
Firewall	NAT Incorporado, utilizado para la Inspección Completa del Paquete
Administración	Web-Based; SNMP agent (con MIB-II)
Upgrade Firmware	TFTP
Puertas	4 x Nway 10BASE-T/100BASE-TX Fast Ethernet LAN 1 x 10Base-t WAN
LED's	Power, WAN, LAN, WLAN, Status, Link/Act. ,10/100
Banda Frecuencia Wireless	2.4 ~ 2.4835 GHz (sujeto a regulación local)
Técnicas de modulación	DSSS (Direct Sequence Spread Spectrum) PBCC (Packet Binary Convolutional Coding)
Números de Canales Wireless	USA & Canada: 11
Wireless Transmit Power	Nominal Temp. Range: 14dBm TYP
Wireless Data Rate	22 Mbps, 11 Mbps, 5.5 Mbps, 2 Mbps & 1 Mbps Auto Fall-Back
Wireless Security	64-bit, 128-bit, 256-bit WEP Encription

Wireless Media Access Control	CSMA/CA con ACK
Wireless Operating Range	Espacio Abierto: 100 – 300m Indoor: 25 – 100m
Wireless Antenna	Antenna diversity System (2dB gain) Dual detachable reversed SMA dipole antenna (RX/TX)

Características Físicas

Poder	5 VDC 2.5A
Temperatura Operación	0°C ~ 55° C
Temperatura Almacenada	0° C ~ 55° C
Humedad	Max 95% No Condensado
Certificación EMI	FCC Class B

DWL-2100AP

D-Link AirPlus XtremeG 2.4GHz Wireless Access Point, 54Mbps/108Mbps (802.11g). (15 x)

Características Técnicas

Estándar	IEEE 802.11g IEEE 802.11b IEEE 802.3 Ethernet/ IEEE 802.3u FastEthernet
Puerta	1 x RJ-45, 100Base-TX
Seguridad	Encriptación 64/128/152 bits WEP 802.1x WPA
Tasa de Transferencia y Técnicas de Modulación	802.11g : D-Link 108Mbps 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, Auto Fallback 802.11b : 11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps, Auto Fallback
Rango de Cobertura. Valores nominales	Hasta 100 mts. In-door Hasta 400 mts. Out-door Factores del entorno pueden afectar adversamente los rangos de cobertura.
Antena	Externa desmontable con conector RSMA Sistema de Antena Giratoria; dipolo con ganancia de 2 dBi
Rango de Frecuencia	2.400 – 2.4835 GHz
Técnicas de Modulación	- 802.11g: BPSK, QPSK, 16QAM, 64QAM, OFDM - 802.11b: DQPSK, DBPSK y CCK
Arquitectura de Red	Soporta Modo Estructurado (Comunicaciones de redes alambradas via Access Point con Roaming)
Modos de Operación	Access Point Wireles Bridge • Point-to-Point • Point-to-Multipoint Client Access Point Repeater
Leds de Diagnóstico (Verde)	- WAN - LAN (10/100Mbps) - WLAN
Método de acceso	CSMA/CA con Ack

Administración	Web Based DHCP Cliente/Servidor

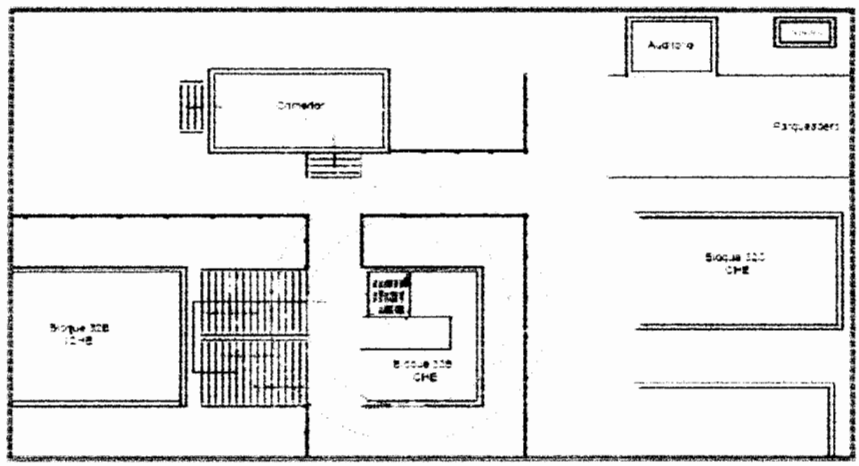
Características Físicas

Alimentación	Externa, 5VDC, 2.0A
Consumo	10 Watt
Dimensiones	142 x 109 x 31 mm
Peso	200grs.
Temperatura de Operación	0ºC a 55ºC
Temperatura de Almacenaje	-20ºC a 75ºC
Humedad	5% - 95% no condensada
Emisión	FCC Class B, CE Class B

EXTERIORES

C&C

PLANO



Puntos de Acceso intrusos detectados por NetStumbler

SSID	Canal	SNR
estudiantes	6	-33
gmgye	4	-67
espol	11	-76
iche	6	-46
glolu-redi	4	-75
expigo	10	-77
OnGye95	7	-70
AP67ICF-ANTEXP	6	-55
FIMCP	11	-80
default	6	-74

Observaciones:

- Gran número de APs ext.
- No es posible mover APs.
- Monitorear paradero y escaleras por ser zonas abiertas.

TIPO DE DATOS

C&C

INTRANET

1 Información de Negocios

Valor estimado de pérdida $ 0

2 Información Coorporativa

Valor estimado de pérdida $ 0

3 Información técnica y de desarrollo

Valor estimado de pérdida $ 0

4 Información de mercadeo

Valor estimado de pérdida $ 0

5 Información operacional y secretos de oficio

Valor estimado de pérdida $ 0

6 Información de recursos humanos

Valor estimado de pérdida $ 0

7 Información financiera

Valor estimado de pérdida $ 0

8 Código fuente

Valor estimado de pérdida $ 0

9 Información confidencial del cliente

Valor estimado de pérdida $ 0

10 Acceso a través de la red a otras empresas

Valor estimado de pérdida $ 0

INTERNET

11 Datos confidenciales enviados en aplicaciones de internet

Valor estimado de pérdida | $ 100 |

12 Otros Perdida de productividad por robo de ancho de banda

Valor estimado de pérdida | $ 50 |

Valor estimado de pérdida total | $ 150 |

Conclusiones de la consultoría:

Al aplicar la consultoría al laboratorio DELTA del Instituto de Ciencias Humanísticas y Economía pudimos determinar que el laboratorio tiene un riesgo muy bajo de pérdidas en caso de una intrusión en su red. El valor de $100 estimado de pérdida en caso de que algún estudiante este realizando transacciones financieras por Internet se suma a los $50 que se perderían en caso de falta de productividad por robo de ancho de banda. El valor estimado de pérdida por disminución de productividad se atribuye a horas de clase perdidas por la "lentitud" del servicio de Internet.

Aun cuando la red se encuentra en un área vulnerable y tiene un número de equipos mayor a 30 la información que maneja presenta un costo menor a los mil dólares, con poca probabilidad de crecimiento, por lo que la implementación sugerida es la de seguridad mínima.

ANEXO 4

ANEXO 4
Análisis de la validez de las soluciones

El resultado de la consultoría presenta tres soluciones que difieren en su nivel de seguridad, complejidad y costo. La tabla A.1 presenta cuales son las características de cada nivel de seguridad.

	Seguridad mínima	Seguridad media	Seguridad avanzada
Longitud de la llave	128	128	Varios
Autenticación segura	No	Sí	Sí
Cifrado de datos de alta seguridad	No	Sí	Sí
Autenticación de equipo	Sí	Sí	Sí
Autenticación de usuario	No	Sí	Sí
Llaves rotativas	No	Sí	Sí (IPSec)
Seguridad en conjunto	Débil	Fuerte	Muy Fuerte
Software de cliente	No	Windows XP	Cliente VPN (Windows)
Sistema operativo	Todos	Windows XP	Todos

Tabla A.1. Características de las implementaciones

En la figura A.1 podemos ver cuales son los ataques más comunes en contra de las redes inalámbricas. Como podemos advertir los más frecuentes son los ataques de puntos de acceso intrusos mientras que los ataques más malignos, como exposición de datos sensibles o ataques DoS, son menos habituales. Sin embargo estos últimos pueden crear un daño económico

mucho mayor a la empresa por lo que se deben tomar precauciones para evitarlos también.

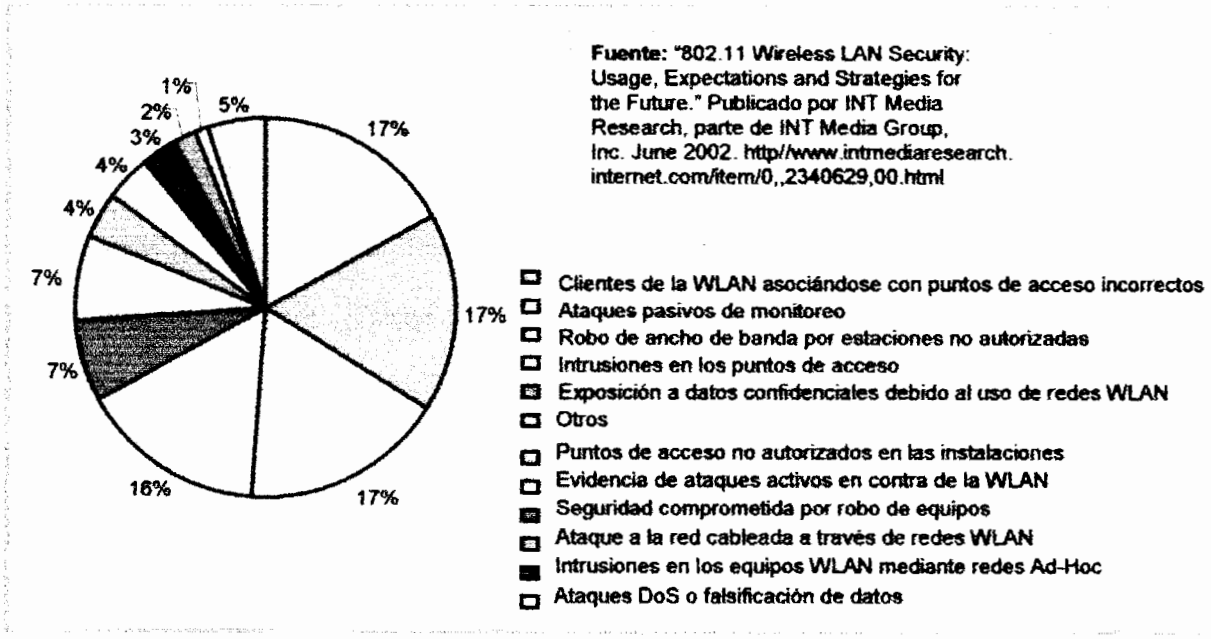


Figura A.1. Porcentaje de ataques reportados contra redes WLAN

Mitigación de riesgos por la seguridad mínima

Por sus características el nivel de seguridad mínima no combate el problema de los puntos de acceso intrusos, los ataques más comunes, pero presenta resistencia a los ataques activos mediante las tablas de direcciones MAC y deshabilitando el SNMP. Al deshabilitar el SSID evita ser identificado por ataques pasivos de monitoreo. Además las tablas MAC y la clave aumentan significativamente el nivel de dificultad de robo de ancho de banda. La ubicación adecuada de los puntos de acceso elimina el riesgo de intrusión física en ellos. Sin embargo la exposición de datos, los ataques DoS y la

falsificación de información se pueden lograr por intrusos con conocimientos avanzados.

Mitigación de riesgos por la seguridad media

El requisito de autenticación segura de la seguridad media impide la utilización no autorizada de la red. Si bien la solución no se ocupa directamente de los puntos de acceso inalámbrico no autorizados, la implementación de una solución inalámbrica segura como ésta elimina, casi por completo, los motivos para establecer una WLAN no oficial. La asignación y modificación dinámicas de las claves de cifrado con regularidad y el hecho de que las claves sean exclusivas para cada sesión de usuario implica que siempre y cuando la actualización de la clave se realice con suficiente frecuencia, no se podrán descubrir las claves ni disponer de acceso a los datos de ninguna forma conocida. La autenticación mutua entre el cliente, el servidor RADIUS y el punto de acceso inalámbrico hace que sea muy difícil que un atacante pueda suplantar a alguno de ellos. La autenticación segura en la red impide que usuarios no autorizados se conecten a la red e introduzcan datos imitados desde el interior. Los ataques de exceso de datos y otros ataques de DoS en la red se pueden evitar si se controla el acceso a la WLAN mediante 802.1X.

Mitigación de riesgos por la seguridad avanzada

La solución de seguridad avanzada previene los ataques de manera similar a la seguridad media, con métodos de autenticación tipo IPSec. Presenta niveles de encripción avanzados que previenen cualquier tipo de ataque de monitoreo pasivo. Por este medio también previene cualquier ataque DoS o de falsificación de datos. Adicionalmente no permite el paso de información no autorizada (otra que no sea paquetes IPSec) eliminando por completo la posibilidad de un ataque a la red cableada por medio de la WLAN. El alto nivel de encripción y de autenticación de la solución IPSec además de las ventajas administrativas de la gateway inalámbrica utilizada en esta solución hacen que la seguridad de nivel avanzada cumpla con los estándares más altos de regulaciones legales de confidencialidad.

Justificación de la inversión

Mientras el nivel de seguridad aumenta en proporción el costo de la solución se incrementa. Como podemos ver una solución de tipo avanzada previene los ataques más comunes casi en su totalidad, convirtiéndose en necesaria para una empresa que requiere mantener estándares altos de confidencialidad de datos. Lo que debemos evaluar es si el costo de la solución implementada se justifica en el aspecto económico.

Si una empresa decide implementar una red inalámbrica y al mismo tiempo maneja información sensible que no desea exponer debe incurrir en gastos de seguridad mayores a los invertidos en una red cableada. No obstante el ahorro anual que produce una red inalámbrica justifica esta inversión. La implementación de una red inalámbrica presenta ahorros estimados del 32% en el primer año, como se presenta en la figura A.2. Cada año la flexibilidad y escalabilidad de la WLAN permiten ahorros aún mayores debido a que no se necesita gastar en cableado estructurado y mano de obra.

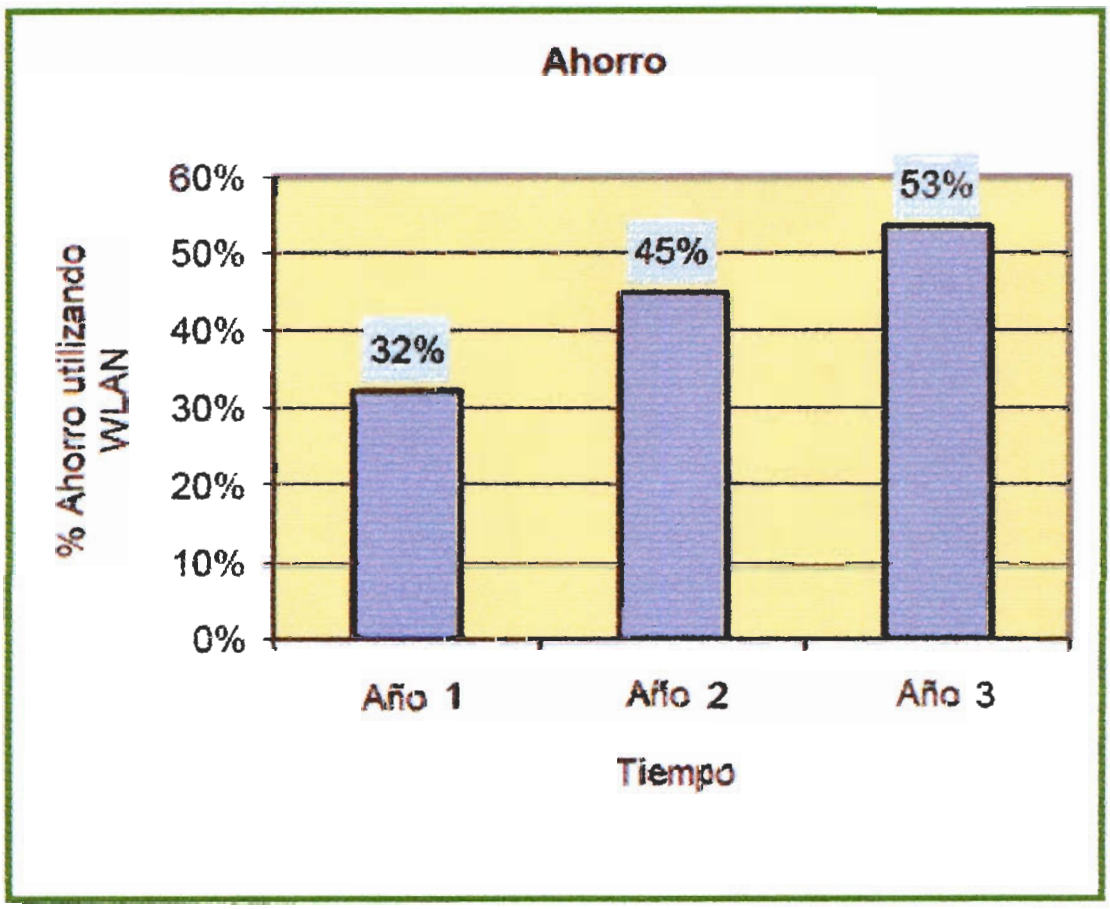


Figura A.2. Ahorro anual por la implementación de redes inalámbricas

Tomando en cuenta la productividad adicional que resulta del uso de una WLAN además del ahorro en implementación anual está es una excelente opción para la creación de nuevas redes en el entorno empresarial.

ANEXO 5

ANEXO 5
Herramientas de la Solución Intermedia

Tabla 1. Lista de archivos utilizados para la implementación de Seguridad Intermedia

Nombre de archivo	Descripción
Archivos CMD principales	
MSSSetup.cmd MSSTools.cmd	Éstos son los archivos por lotes que proporcionan la interfaz con los archivos de Microsoft Windows Scripting Host (WSH) y simplifican la sintaxis. Permiten ejecutar distintos trabajos especificando el nombre del trabajo como un solo parámetro en la línea de comandos. La sintaxis es la siguiente: **msssetup** *NombreTrabajo* [/param:*valor*] **msstools** *NombreTrabajo* [/param:*valor*] Donde *NombreTrabajo* es el nombre de la operación. Si ejecuta esta secuencia de comandos sin un NombreTrabajo, todos los trabajos disponibles aparecerán con una descripción sencilla de la función de cada trabajo.
Archivos WSH XML	
msssetup.wsf msstools.wsf	Éstos son archivos WSH XML, que especifican los trabajos individuales disponibles. Los trabajos definidos en los archivos WSF llaman a los procedimientos definidos en los archivos VBS. La sintaxis es la siguiente: **Cscript //job:** *NombreTrabajo* msstools.wsf [/param:*valor*] Si ejecuta esta secuencia de comandos sin un NombreTrabajo, todos los trabajos disponibles en el

	archivo WSF aparecerán con una descripción sencilla de la función de cada trabajo.
Archivos VBScript	
ias_setup.vbs	Rutinas utilizadas durante la configuración del Servicio de autenticación de Internet (IAS).
ias_tools.vbs	Rutinas utilizadas durante la operación y la supervisión del IAS.
Gen_setup.vbs	Rutinas que no son específicas de IAS o los Servicios de Certificate Server y que se han utilizado durante la implementación.
ca_setup.vbs	Rutinas utilizadas durante la configuración de la entidad emisora de certificados.
ca_monitor.vbs	Rutinas utilizadas por las funciones de supervisión de la entidad emisora.
constants.vbs	Constantes utilizadas por los otros archivos VBS.
helper.vbs	Rutinas genéricas utilizadas por los otros archivos VBS.
pkiparams.vbs	Constantes utilizadas para definir muchos de los parámetros de configuración de la entidad emisora.
Archivos varios	
InstCAPICOM.cmd	Archivo CMD para simplificar la instalación de CAPICOM.
CreateShortCut.cmd	Archivo CMD que llama a una rutina desde el archivo VBS para crear un acceso directo en el escritorio del usuario. El acceso directo inicia CMD.EXE con el directorio actual en la carpeta de instalación de la secuencia de comandos.
ComputerCerts.msc	Consola de administración predefinida para ver los certificados en el almacén de equipos.
AddRADIUSClient.exe	Utilidad para agregar clientes de RADIUS a IAS desde la línea de comandos. (**Nota:** esta

	herramienta requiere la instalación de .NET Framework.)
Interop.SDOIASLib.dll	Biblioteca de compatibilidad que necesita AddRADIUSClient.exe.
Fuente	Carpeta que contiene el código fuente de la herramienta AddRADIUSClient.
Archivos de directiva de grupo	
MSSWLANGPOs	Esta carpeta contiene el archivo de definición XML y los archivos de datos de los dos objetos de directiva de grupo predefinidos que se proporcionan con esta solución.
Documentos	
Securing Wireless LANs.rtf	Archivo Léame que contiene el mismo texto que este capítulo.

Tabla 2. Lista de trabajos en MSSSetup.wsf

Nombre del trabajo	Descripción
ListJobs	Enumera todos los trabajos del archivo WSF.
ConfigureCA	Configura los parámetros del Registro de la entidad emisora.
ConfigureTemplates	Configura las plantillas de certificado de entidad emisora.
CheckCAEnvironment	Comprueba el entorno antes de instalar la entidad emisora.
InstallCA	Instala los Servicios de Certificate Server.
CreateShortcut	Crea un acceso directo a **MSS WLAN Tools** en el escritorio.
ImportSecurityGPO	Importa al dominio un objeto de directiva de

	grupo con la configuración de seguridad del servidor.
ImportAutoEnrollGPO	Importa al dominio un objeto de directiva de grupo con la configuración de inscripción automática de certificados.
CheckDomainNativeMode	Comprueba si el dominio está en modo nativo.
VerifyCAInstall	Comprueba que la instalación de la entidad emisora ha sido satisfactoria.
VerifyCAConfig	Comprueba que la configuración de la entidad emisora ha sido satisfactoria.
CheckIASEnvironment	Comprueba el entorno antes de instalar IAS.
InstallIAS	Instala los Servicios de autenticación de Internet en el servidor.
CreateWLANGroups	Crea grupos de seguridad en Active Directory®.
AddWLANGroupMembers	Rellena los grupos de seguridad con los miembros correctos.

Tabla 3. Lista de trabajos en MSSTools.wsf

Nombre del trabajo	**Descripción**
ListJobs	Enumera todos los trabajos del archivo WSF.
AddRADIUSClient	Procedimiento interactivo para agregar un cliente de RADIUS a IAS (parámetros: [/path:*NombreArchivoSalida*]).
AddSecRADIUSClients	Procedimiento interactivo para agregar un cliente de RADIUS a IAS (parámetros: [/path:*NombreArchivoEntrada*]).
GenRADIUSPwd	Genera una entrada y un secreto de cliente de RADIUS (parámetros: /client:*NombreCliente*

	/ip:*DirecciónIPCliente* [/path:*ArchivoSalida*]).
ExportIASSettings	Exporta una configuración de servidor IAS a los archivos (parámetros: [/path:*CarpetaParaGuardarArchivosConfiguración*]).
ImportIASSettings	Importa una configuración de servidor IAS de los archivos (parámetros: [/path:*CarpetaConArchivosParaImportar*]).
ExportIASClients	Exporta clientes de RADIUS de IAS al archivo (parámetros: [/path:*CarpetaParaGuardarArchivoClientes*]).
ImportIASClients	Importa clientes de RADIUS de IAS del archivo (parámetros: [/path:*CarpetaConArchivoClientesParaImportar*]).
BackupIAS	Hace una copia de seguridad de la configuración de IAS en el archivo (parámetros: [/path:*CarpetaParaGuardarArchivoCopiaSeguridad*]).
RestoreIAS	Restaura la configuración de IAS del archivo (parámetros: [/path:*ArchivoCarpetaParaRestaurar*]).
CheckIAS	Comprueba que el servidor IAS está respondiendo (parámetros: [/verbose]).
CheckCA	Comprueba que el servicio de entidad emisora está respondiendo y que la lista de revocación de certificados (CRL) es válida (parámetros: [/verbose]).

ANEXO 6

ANEXO 6
Política de Red Inalámbrica

<Nombre de la compañía>

1.0 Propósito

Esta política prohíbe el acceso a la red de <Nombre de la compañía> a través de una conexión inalámbrica no segura. Solo sistemas inalámbricos que cumplen los parámetros especificados por esta política o han sido acreditados por un permiso particular de la entidad supervisora de seguridad pueden conectarse a las redes de <Nombre de la compañía>.

2.0 Rango

Esta política cubre todos los equipos de comunicación inalámbrica (computadores personales, teléfonos celulares, asistentes personales, etc.) conectados a cualquiera de las redes internas de <Nombre de la compañía>. Esto incluye cualquier forma de equipo inalámbrico capaz de transmitir información por paquetes. Equipos inalámbricos o redes sin conexión a la red de <Nombre de la compañía> no son sujetos a esta política.

3.0 Política

3.1 Registrar todos los puntos de acceso y adaptadores inalámbricos

Todos los equipo inalámbricos y estaciones base o puntos de acceso conectados a la red corporativos deben ser registrados y aprobados. Estos puntos de acceso son sujetos a pruebas periódicas y auditorias. Todos los adaptadores de red utilizados en computadores portátiles o fijos corporativos deben ser registrados.

3.2 Tecnología aprobada

Toda la tecnología WLAN debe utilizar productos de marcas aprobadas por la compañía con las respectivas configuraciones de seguridad.

3.3 Encripción y Autenticación VPN

Todos los equipos con que utilizan tecnología WLAN deben utilizar el método de acceso por medio de Redes Virtuales Privadas (VPN)

configuradas para descartar cualquier tipo de información no autenticada o no cifrada. Para cumplir con esta política, las implementaciones inalámbricas deben mantener una encripción de por lo menos 56 bits. Todos deben tener una dirección de hardware, MAC, registrada. Todas las implementaciones deben soportar y emplear autenticación robusta por medio de una base de datos externa como RADIUS o algo similar.

3.4 Determinación del SSID

El SSID debe ser configurado de manera que no contiene ninguna información que identifica a a compañía como el nombre de la compañía, nombre de algún empleado o identificador del producto.

4.0 Cumplimiento de la política

Cualquier empleado que hay violado esta política puede ser sujeto a una acción disciplinaria que puede llegar hasta el despido del cargo.

5.0 Definiciones

Autenticación de Usuario: Método mediante el cual el usuario de un sistema inalámbrico puede ser verificado como legítimo.

ANEXO 7

ANEXO 7
Proforma de Consultoría

PROFORMA

Consultores C & C

Empresa que solicita la consultoria:
Fecha:
Tiempo de validez:

Valor de la consultoria	$ 300
Total	$ 300

_____

Gerente

[10] ALIANZA WI-FI, *Wi-Fi Protected Access*, http://www.wi-fialliance.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf.

[11] MICROSOFT, *Wireless Networking Web site*, http://www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.msp.

[12] MASON, Andrew, *CCSP Self-Study text*: *Network Security and Virtual Private Network Technologies*, Cisco Press, Octubre 1, 2004.

[13] BLUESOCKET INC., *Brochure WG-2100*, http://www.wizard security.net/blue_socket/brochure.pdf

BIBLIOGRAFÍA

[1] DELAET Gert y SCHAUWERS Gert, *Network Security Fundamental*, Cisco Press, Septiembre 8, 2004.

[2] RITTINGHOUSE John y RANSOME James, *Wireless Operational Security*, Digital Press, 2004.

[3] HAYES Ian, *Just Enough Wireless Computing*, Prentice Hall, Agosto 12, 2002.

[4] PAHLAVAN Kaveh y KRISHNAMURTHY Prashant, Principles of *Wireless Networks: A Unified Approach*, Prentice HALL, Diciembre 11, 2001.

[5] PEIKARI Cyrus y FOGIE Seth, *Maximum Wireless Security*, Sams, Diciembre 18, 2002.

[6] THOMAS Tom, *Network Security First-Step*, Cisco Press, Mayo 21, 2004.

[7] VLADIMIROV Andrew, GAVRILENKO Konstantin y MIKHAILOVSKY Andrei, *Wi-Foo: The Secrets of Wireless Hacking*, Addison Wesley Professional, Junio 28, 2004.

[8] MICROSOFT, *Elección de una estrategia para la seguridad en LAN inalámbricas*, http://go.microsoft.com/fwlink/?LinkId=23459.

[9] INTEL, *Security Best Practices*, http://www.intel.com/business/bss/infrastructure/wireless/security/best_practices.htm.